www.takbook.com

استراتژی امنیت اطلاعات در سازمان‌های مالی

دکتر سید سامان کریمی

استراتژی امنیت اطلاعات در سازمان‌های مالی

دکتر سید سامان کریمی

Survey Information Security Strategy in Financial Organization

ارشدان

ISBN: 978-600-995-819-1

Dr.Seyedsaman Karimi

www.takbook.com

سرشناسه	:	کریمی، سیدسامان، ۱۳۶۳- Karimi, Seyedsaman
عنوان و نام پدیدآور	:	استراتژی امنیت اطلاعات در سازمان‌های مالی/ تالیف و گردآوری سیدسامان کریمی.
مشخصات نشر	:	تهران: موسسه آموزشی تالیفی ارشدان، ۱۳۹۸.
مشخصات ظاهری	:	۱۵۱ص.: جدول، نمودار.
شابک	:	۹۷۸-۶۰۰-۹۹۵-۸۱۹-۱
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	کتابنامه.
موضوع	:	سازمان‌های مالی -- تدابیر ایمنی Financial institutions -- Security measures
موضوع	:	خدمات مالی -- تدابیر ایمنی Financial services industry -- Security measures
موضوع	:	صورت‌های مالی Financial statements
موضوع	:	تکنولوژی اطلاعات -- تدابیر ایمنی Information technology -- Security measures
موضوع	:	ماموران اطلاعاتی Intelligence officers
رده بندی کنگره	:	HG۱۷۳
رده بندی دیویی	:	۳۳۲
شماره کتابشناسی ملی	:	۵۷۷۵۷۳۱

ارشدان

مؤسسه آموزشی تألیفی ارشدان

■ نام کتاب:	استراتژی امنیت اطلاعات در سازمان‌های مالی
■ تألیف و گردآوری:	سید سامان کریمی
■ ناشر:	آموزشی تألیفی ارشدان
■ ویرایش:	اول
■ نوبت چاپ:	اول ۱۳۹۸
■ حروفچینی و صفحه آرایی:	www.irantypist.com
■ شابک:	۹۷۸-۶۰۰-۹۹۵-۸۱۹-۱
■ شمارگان:	۱۰۰۰
■ مرکز خرید آنلاین:	www.arshadan.com www.arshadan.net
■ مرکز پخش و توزیع:	۰۲۱۴۷۶۲۵۵
■ ایمیل نویسنده:	saman_karimi@ut.ac.ir
■ قیمت:	۴۲۰۰۰ تومان

www.takbook.com

فهرست مطالب

عنوان **صفحه**

پیشگفتار ۶

فصل اول: مقدمه ۷

۱-۱ مقدمه ۸

۱-۲ مساله تحقیق ۹

۱-۳ تعاریف ۱۲

۱-۳-۱ استراتژی ۱۲

۱-۳-۲ استراتژی در کسب و کار ۱۳

۱-۳-۳ استراتژی سیستمهای اطلاعاتی ۱۴

۱-۳-۴ امنیت سیستمهای اطلاعاتی ۱۴

۱-۳-۵ استراتژی امنیت اطلاعات ۱۵

فصل دوم: مروری بر ادبیات تحقیق ۱۷

۲-۱ مقدمه ۱۸

۲-۲ مروری بر متون ۱۸

۲-۳ تنظیمات جاری برای استراتژی امنیت اطلاعات ۲۸

۲-۳-۱ تنظیم کردن با استراتژی تجاری ۳۲

۲-۳-۲ تنظیم کردن با استراتژی سیستمهای اطلاعاتی ۳۲

۲-۳-۳ تنظیم کردن با سیستمهای اطلاعاتی و استراتژیهای تجاری ۳۳

۲-۳-۴ استراتژی امنیت اطلاعات به خودی خود کار میکند ۳۳

۲-۳-۵ استراتژی امنیت اطلاعات موجود نیست ۳۴

۲-۳-۶ خلاصهای از تنظیمات ۳۴

۲-۴ ارائه تشخیص نقش برای استراتژی امنیت اطلاعات ۳۵

۲-۴-۱ بالا به پایین ۳۷

۲-۴-۲ تصویر عمومی ۴۱

www.takbook.com

۲-۴-۳ رقبا ۴۱
۲-۴-۴ تغییر پیوسته ۴۲
۲-۴-۵ بهترین عملکرد ۴۳
۲-۴-۶ سازماندهی مجدد ۴۴
۲-۴-۷ ارتباطات قدرت ۴۵
۲-۴-۸ پیروی از قانون ۴۵
۲-۴-۹ خلاصه نقشها ۴۶
فصل سوم: روش تحقیق ۴۷
۳-۱ مقدمه ۴۸
۳-۲ روش تحقیق ۴۹
۳-۳ جمع آوری داده ارائه شده ۵۰
۳-۴ تحلیل داده ارائه شده ۶۱
فصل چهارم: جمع آوری داده، تحلیل و یافته‌ها ۶۵
۴-۱ مقدمه ۶۶
۴-۲ جمع آوری داده ۶۶
۴-۳ تحلیل داده ۶۹
۴-۳-۱ کد گذاری باز ۷۲
۴-۳-۲ نتایج کد گذاری باز ۸۱
۴-۳-۳ کد گذاری محوری ۸۴
۴-۳-۴ نتایج کد گذاری محوری ۸۸
۴-۳-۵ کد گذاری انتخابی ۸۹
۴-۳-۶ نتایج کد گذاری انتخابی ۱۰۰
۴-۴ نتیجه ۱۱۰
فصل پنجم: نتیجه گیری، دلالت، محدودیتها و توصیه ها ۱۱۷
۵-۱ مقدمه ۱۱۸
۵-۲ جمع بندی ۱۱۸
۵-۳ دلالت ۱۲۱

www.takbook.com

۵-۴ محدودیتها ۱۲۱
۵-۵ توصیه‌ها ۱۲۲
۵-۶ خلاصه ۱۲۶
پیوست ها ۱۲۷
ضمیمه A: سوالات مصاحبه ۱۲۸
ضمیمه B: تحلیلهای کلی اولیه ۱۲۹
References ۱۳۱

www.takbook.com

پیشگفتار

خدای را بسی شاکرم که از روی بخشندگی، پدر و مادری فداکار نصیبم ساخته تا در سایه درخت پربار وجودشان بیاسایم و از ریشه آنها شاخ و برگ گیرم و از سایه وجودشان در راه کسب علم و دانش تلاش نمایم. والدینی که بودنشان تاج افتخاری است بر سرم و نامشان دلیلی است بر بودنم، چرا که این دو وجود، پس از پروردگار، مایه هستی ام بوده اند دستم را گرفتند و راه رفتن را در این وادی زندگی پر از فراز و نشیب آموختند. آموزگارانی که برایم زندگی، بودن و انسان بودن را معنا کردند.

این کتاب را ضمن تشکر و سپاس بیکران و در کمال افتخار تقدیم می‌نمایم به:

- محضر ارزشمند پدر و مادر عزیزم به خاطر همه‌ی تلاشهای محبت آمیزی که در دوران مختلف زندگی ام انجام داده اند و بامهربانی چگونه زیستن را به من آموخته اند.
- به خواهر مهربانم که در تمام طول تحصیل همراه و همگام من بوده است.
- به استادان فرزانه و فرهیخته ای که در راه کسب علم و معرفت مرا یاری نمودند.
- به آنان که در راه کسب دانش راهنمایم بودند.
- به آنان که نفس خیرشان و دعای روح پرورشان بدرقه‌ی راهم بود.
- پروردگارا به من کمک کن تا بتوانم ادای دین کنم و به خواسته‌ی آنان جامه‌ی عمل بپوشانم.
- پروردگارا توفیق خدمتی سرشار از شور و نشاط و همراه و همسو با علم و دانش و پژوهش جهت رشد و شکوفایی ایران کهنسال عنایت بفرما.

لازم می‌دانم از مجموعه بانک سامان و اساتید محترم سرکار خانم ف. ضرابیه، جناب آقای مصطفی محمدی و سر کار خانم م. عبداللهی صمیمانه قدردانی کنم که بی تردید حضور و همراهی شان سبب شد در این مجال کوتاه تحقیق و پژوهش اینجانب میسر شود.

سید سامان کریمی

تیرماه ۱۳۹۸

www.takbook.com

فصل اول

مقدمه

www.takbook.com

۱-۱ مقدمه

معمولا کسب و کار از طریق دیدگاهی که در استراتژی تجاریش ترویج می‌دهد، جهت کلی استراتژیک یک سازمان را شکل می‌دهد (Miller, 1981; Wommack,1979 Cohen & Cyert, 1973;). با پدیدار شدن اتوماسیون، اداره یا حوزه فناوری اطلاعات استراتژی سیستم-های اطلاعاتی را برای خودکارسازی به وجود آورده و آن را با دیدگاه استراتژی تجاری اداره تنظیم کردند (Doherty & Fulford, 2006). سرعت و وسعت بخش‌هایی که سیستم‌های اطلاعاتی در آنها نفوذ کرده است، موجب شده که سیستم‌های اطلاعاتی به دو دلیل به امنیت اطلاعات نیازمند باشند. اول، محافظت از اطلاعاتی که در سازمان مورد اعتماد هستند در سیستم اطلاعاتی‌شان استقرار یابند؛ دوم، حفظ دارایی‌های حفاظت شده فناوری اطلاعاتی از آسیب دیدن به خاطر در معرض خطر قرار گرفتن؛ و آگاه ساختن صاحبان اطلاعات از اینکه اگر نقض عهدی در مورد داده‌هایشان رخ داده یا سیستم‌های اطلاعاتی خودکارشان در معرض خطر قرار گرفته‌اند (Gilbert, 2008; McFadzean, Ezingeard, & Birchall, 2011; Smedinghoff, 2005). اینها در فناوری اطلاعات و کسب و کار امنیت اطلاعات در نظر گرفته می‌شود تا مفید بودن سیستم اطلاعاتی را برای کاربرانش را تضمین کند (Eloff & von Solms, 2000).

یکی از اهداف مدیران ارشد اطمینان بخشیدن در مورد جلوگیری از دست دادن داده و اجتناب از رسیدن آسیب محتمل به شهرت سازمان‌شان است. هدف دیگر، تمرکز بر ساخت سیستم دفاعی برای حفاظت از دارایی‌های اتوماسیون برای جلوگیری از به خطر افتادن اطلاعات است (Anderson, 2003; Dlamini, Eloff, &Eloff, 2009; Dutta & McCrohan, 2002; Knapp & Boulton, 2006). شهرت سازمان و احتمالا بقای اقتصادی آنها به داشتن محیطی امن به عنوان یکی از عوامل مهم برای عملکرد امن در برابر تهدیدهای بدخواهانه است، به طور مثال یک فرد سعی در گرفتن نام کاربری و رمز از پرسنل نا آگاه شبکه کرده، که بعدا بتواند در شبکه نفوذ کرده و اطلاعات را از شبکه بیرون بکشد (Bhalla, 2003;Hinde, 2003; Knapp & Boulton, 2006; Oreku & Mtenzi, 2009). هزینه‌های مربوط به درمان نشت اطلاعات، مثل اطلاع رسانی به قربانیان از گم شدن داده‌هایشان و ترمیم اطمینان عمومی می‌تواند بسیار زیاد باشد (Baskerville, 1993; Doherty & Fulford, 2006; Dutta & McCrohan, 2002; Garg, Curtis,& Halper, 2003; Rowe & Gallaher, 2006).

www.takbook.com

اغلب مفهوم استراتژی امنیت اطلاعات به درستی درک نمی‌شود. مدیریت سازمانی آن را به عنوان پیاده سازی ضروری کنترل‌ها و ابزارهای امنیتی تکنیکی می‌بینند که مردم را از کامپیوترهای سازمان دور نگه می‌دارد (Chang & Yeh, 2006). این در حالی است که امنیت اطلاعات چیزی بیشتر از فقط اقدامات امنیتی تکنیکی پیاده سازی شده برای برطرف کردن نیازهای معمول است (Damianides, 2005; Doherty & Fulford, 2006; Keen & El Sawy, 2010; Kim, 2004; Luftman &Ben-Zvi, 2010; Luftman & Ben-Zvi, 2011). امنیت اطلاعات با فناوری اطلاعات فعالیت می‌کند تا امن ماندن محیط به صورت خود کار شده،و همچنین ممانعت از نفوذ خارجی و سوء استفاده داخلی از سیستم‌ها و دستگاه‌ها را تضمین کند (). امنیت اطلاعات به طور ویژه نیاز به سیاست و حکمرانی داشته (Posthumous & von Solms, 2004; von Solms 2006) و یک استراتژی امنیت اطلاعات شامل فعالیتهای ساختار یافته‌ای است که به سیاست و حکمرانی سازمان برسد و نقشه کلی فعالیت سازمان را هماهنگ کند. (White &Bruton, 2011)؛ کارکرد امنیت اطلاعات در یک سازمان برای رسمی کردن استراتژی امنیت اطلاعات است به طوری که یک برنامه برای پیاده سازی حفاظت از اطلاعات و دارایی‌های معنوی سازمان برای اداره کردن کسب و کار (Chen, Kataria, & Krishnan, 2011; Hinde, 2003; Knapp & Boulton, 2006;Mahmood, Siponen, Straub, Rao, & Raghu, 2010) در برابر مهاجمانی که سعی در کپی، حذف، دستکاری یا خراب کردن اطلاعات دارند، به کار می‌رود. نیاز است که امنیت اطلاعات تقریبا یک قدم جلوتر از مهاجمان باشد (Bhalla, 2003; Gupta & Hammond, 2005; Howard & Longstaff, 1998).

۱-۲ مساله تحقیق

در مطالعات گذشته برای استراتژی‌های رسمی امنیت اطلاعات فراخوانی‌هایی انجام شده است که فراتر از پیاده سازی کنترل‌های تکنیکی است (Dhillon, 1995; Herath & Rao, 2009; Ma,Johnston, & Pearson, 2008; Parkin & van Moorsel, 2009; Parakktu, 2010). تاکید برخی محققان بر نیاز به استراتژی‌هایی است که به خوبی توسعه یافته‌اند (Anderson & Choobineh, 2008; Hall, Sarkani, & Mazzuchi, 2011; Kayworth & Whitten, 2010; McFadzean, Ezingeard, & Birchall, 2011; Park & Ruighaver, 2008; Tejay, 2008). همچنین برای فراخواندن امنیت اطلاعات به فعال بودن نسبت به منفعل بودن وجود

www.takbook.com

داشته است (Tejay, 2008). هرچند، تعداد کمی مطالعه وجود دارد که بر روی خود استراتژی امنیت اطلاعات متمرکز شده باشد. هدف از این مطالعه فهمیدن پیچیدگی‌های استراتژی امنیت اطلاعات در یک سازمان مالی بزرگ است.

کاوش در مساله پیچیدگی‌های ابتدایی استراتژی امنیت اطلاعات را در چگونگی تفاوت نقشهایی که یک متخصص امنیت اطلاعات برای عمل کردن برمی‌گزینند و چطور یک سازمان مالی بزرگ برای توسعه برنامه امنیت اطلاعات از طریق استراتژی پیشروی می‌کند را در معرض آزمایش می‌گذارد. دوم اینکه، چگونه یک سازمان برنامه‌های امنیت اطلاعات را ایجاد می‌کند، وسیله‌ای است که به عنوان یک استراتژی امنیت تعریف می‌شود. کاوش بر روی ترکیب استراتژی امنیت اطلاعات و پاسخگویی به مفهوم استراتژی امنیت اطلاعات ممکن است دیدگاهی به درون ساختارش اعطا کند. با نگاه به درون ساختار می‌توان به معین کردن این موضوع کمک کرد که آیا انواع خاصی از استراتژیهای امنیت اطلاعات نسبت به دیگر انواع آن تحت شرایط خاصی ارجح تر هستند یا خیر. اگر این گونه است همچنین می‌تواند برای فهم این مفید باشد که چگونه استراتژیهای امنیت اطلاعات در درون یک سازمان مالی بزرگ تحت مطالعه متفاوت است. سپس با فرض اینکه چندین نوع استراتژی امنیت اطلاعات وجود دارد جستجو به دنبال روشهایی سودمند خواهد بود که یک متخصص امنیت اطلاعات آن روش را از روشهای دیگر برای اجرای نقشهای مناسب در پیاده سازی امنیت اطلاعات متمایز می‌کند.

در دومین بخش، زمانی که متخصصان امنیت اطلاعات یک استراتژی امنیت اطلاعاتی را از دیگری متمایز می‌کند، شخص نقشی راهبردی را برای انجام وظایف ارشد امنیت اطلاعاتی درنظر می‌گیرد. فرآیند انتخاب منجر به کشف نقشهای راهبردی گوناگونی برای متخصصان در حصول به امنیت اطلاعات فراهم می‌کند. جنبه‌های گوناگون نقشها و انتخاب آنها به منظور کمک به فهم بیشتر فرآیند بررسی شده است. این تلاش برای نگاهی به آنچه دیگر نقشها برای دستیابی به امنیت اطلاعات انجام می‌دهند و چه چیزی یک نقش را از نقش دیگر متمایز می‌کند (آیا هر نقش شامل فرآیند رسمی هست و یا نقش بهینه‌ای برای یک استراتژی امنیت اطلاعاتی خاص وجود دارد) استفاده می‌شود.

بحث این مطالعه در مورد موضوعی است که مطالعات گذشته در مورد انتخاب نقش و اکتشاف اینکه چگونه یک سازمان مالی بزرگ نقشها را ایجاد می‌کند، بحثی نکرده اند. بررسی چگونگی استفاده نقشهای مختلف توسط سازمانهای مالی ضروری است. که این می‌تواند به فهم این

www.takbook.com

مساله کمک کند که کدام نوع از استراتژیهای امنیت اطلاعات نسبت به انواع دیگر آن ارجحتر بوده و تحت چه شرایطی.

بنابراین، فهم اینکه چطور یک سازمان مالی بزرگ چند وجهی از داخل تفاوتهایی دارد در رسیدن به امنیت اطلاعات می‌تواند مفید باشد. اکثر واکنشهایی که یک متخصص امنیت اطلاعات انجام می‌دهد به جای اینکه پاسخهای اصولی برنامه ریزی شده باشد در پاسخ به یک عمل هستند. اینطور پاسخگویی منفعل اغلب موجب انتخاب نادرستی به نیازهای امنیت اطلاعات است. برای کاستن مشکل استراتژی‌های منفعل، متخصص امنیت اطلاعات باید استراتژیهای امنیتی موجود را توسط سازمانهای مختلف ارزیابی کند. متخصصان باید استراتژیهای مشاهده شده در سازمانهای دیگر را دسته بندی کرده تا بتوانند جهتگیری درستی را برای حرکت یک سازمان در رسیدن به اهداف برنامه امنیت اطلاعاتی مشخص کنند.

سازمانها به طور خود آگاه یا ناخودآگاه کارهایی را مرتبط با امنیت اطلاعات انجام می‌دهند. نیاز است این فعالیتها درک شوند زیرا این عوامل استراتژیهای سازمان هستند.

Tejay (۲۰۰۸) در مورد اهمیت دادن به زمینه کاری یک سازمان برای رسیدن به موفقیت بحث کرده است. ارتباط بین آنچه استراتژی امنیت اطلاعاتی بدان نیاز دارد و نقش (هایی) که برای عملی کردن این اصول ضروری هستند، باید درک شوند. متمایز کردن نیازمندی-های سیستمهای اطلاعاتی و کسب و کار منجر به زمینه‌هایی می‌شود که از طریق آن متخصصان امنیت اطلاعات استراتژی امنیت اطلاعات را برای رسیدن به اهداف امنیت اطلاعات برقرار می‌کنند. همچنین دانستن این مطلب می‌تواند مفید باشد که چگونه استراتژیهای امنیت اطلاعاتی مختلف که واقعا در سازمانهای مختلف به کار گرفته شده‌اند باعث می‌شود به اهدافشان برسند (McFadzean, Ezingeard, & Birchall, 2007; Mintzberg & Waters, 1985). تا اینجا، هدف تولید مدل نظری برای جمع آوری داده می‌تواند باشد. در فصل ۳، در مورد چگونگی به کار گرفتن داده‌های جمع آوری شده از متخصصان برای ساخت مدل نظری که در سازمانهای مالی بزرگ استفاده شود به طور اجمالی بحث خواهد شد. این مورد ممکن است به مطالعات آینده‌ای کمک کند که در فهم تفاوت سازمانها در به کارگیری مدل برای پیش بینی انتخاب نقش تفاوت دارند. استفاده از مطالعه نظری اصولی با روشهای جمع آوری داده، به داده‌های نوخاسته اجازه می‌دهد که ساختمان یک نظریه را پرورش دهند (Eisenhardt, 1989; Corbin & Strauss 2008).

www.takbook.com

۱-۳ تعاریف

یک ویژگی برقراری توافق، وجود یک هسته مشترک ارتباطی بین تمام ذینفعان است. از طریق ایجاد یک فرهنگ لغت مشترک (دسته بندی تعاریف) با در نظر گرفتن موقعیت‌هایی که تحقیقات دیگر پذیرفته و به اشتراک گذارده‌اند این امر می‌تواند محقق شود (Alter, 2008). یک فرهنگ لغت مشترک به مردم در تبادل اصول و درک مفاهیم به خصوص در زمینه استراتژی کمک می‌کند.

هم گرایی وسیع سیستمهای اطلاعاتی در زمینه مدیریت استراتژی تجاری تاثیر گذاشته (Chan & Huff, 1992) و استراتژی سیستم-های اطلاعاتی را متاثر کرده است (Chen, et al., 2010). بحثهای مختلفی در مورد استراتژی امنیت اطلاعات نیز انجام شده است (Baskerville & Dhillon, 2008; Ezingread, et al., 2005; McFadzean, et al., 2007; McFadzean, et al., 2011). در این فصل بحثی در مورد استراتژی هایی که در کارهای گذشته در سه بخش تعاریف استراتژی کسب و کار، استراتژی سیستمهای اطلاعاتی و استراتژی امنیت اطلاعات انجام خواهد شد.

۱-۳-۱ استراتژی

Gavetti و Rivikin (۲۰۰۵) بیان کردند که استراتژی، انتخاب است، انتخاب بین آنچه باید انجام شود و آنچه نباید انجام شود که بر روی پیامدهای یک سازمان تاثیر می‌گذارد. زمانی که مقاله آنها بر روی انتخاب متمرکز شده بود، تمرکز مقالات دیگر بر روی این موارد بود: دقیقا چه چیزی یک استراتژی است (Alter, 2008; Gavetti & Rivkin, 2005; Mintzberg, 1987a; Mintzberg, Ahlstrand, & Lampel, 1998; Wommack, 1979)، یک استراتژی از چیزی تشکیل شده است (Cohen & Cyert, 1973) و چگونه یک استراتژی شکل گرفته و توسعه می‌یابد (Gavetti & Rivkin, 2005; Wommack, 1979). محققان زیادی مدل‌هایی برای استراتژی اختراع کردند (Dunkerley, 2011; Ezingeard, et.al., 2005; Kankankalli, 2008; McClean & Kark, 2010; Tan, Teo, & Wei, 2003; Ma, Johnston, & Pearson, Rose, 2011) که سعی در دریافت عصاره استراتژی داشت اما هیچ یک از این روش‌ها به طور گسترده پذیرفته نشدند (Markides, 1999). برخی از این مدلها شامل مدل پنج نیرویی پورتر (Porter, 1980)، و مدل هشت نوع استراتژی دیگر که توسط Mintzeberg و Waters (1985)

www.takbook.com

توصیف شدند برای ساختاردهی استراتژی هستند. دشواری تعریف تبین شده را می‌توان با در نظر گرفتن دو جنبه دیگر از استراتژی (ویژگیهای تصمیم گیری با استراتژی و مشکلات حول سطوح مختلف استراتژی) به آسانی توصیف کرد.

دومین زیر مجموعه استراتژی ویژگیهای تصمیم گیری است. این تصمیم گیری بین موارد استراتژیک و غیر استراتژیک در بلند مدت، تاثیرات مورد انتظار، و حرکت جهت‌دار استراتژی توسط تصمیم گیرنده در حین اجرای یک نقشه است (Chen, et al., 2010). سومین جنبه فرا سطحی است که به صورت یک استراتژی عمل می‌کند. برخی سطح شرکتی (Porter, 1980)، سطح مزیت رقابتی (Grant, 2005)، و سطح تخصیص منابع یا استراتژی وظیفه‌ای (Hofer & Schendel, 1978) را مشخص می‌کنند. برخی افراد دیگر استراتژی را به ترتیب به سطوح استراتژیکی، تاکتیکی و عملیاتی از یک استراتژی کامل مانند می‌کنند (Grobler & Louwrens, 2005; da Veiga & Eloff, 2007). هر یک از این انتخابها، استراتژیی را در مدیریت هدایت یک سازمان در نیل به یک هدف تحریک می‌کند.

استراتژی به عنوان نقشه مدیریت عمل، رسیدن به هدفی است که توسط نقاط عطف یا نشانگرهایی که روند رسیدن به هدف را نشان می‌دهند، مشخص شده است (Chen, et al., 2010; King, 1978). در این مطالعه استراتژی در سه حوزه یک سازمان مشاهده می‌شود: کسب و کار، سیستمهای اطلاعاتی و واحدهای امنیت اطلاعات با توجه به سازمان کسب و کار و تجاری (McFadzean, et al., 2007).

۱-۳-۲ استراتژی در کسب و کار

استراتژی در کسب و کار مجموع اهداف، سیاستها و کارهای سازمان است که به شکل نقشه یا الگوی منسجم ظاهر می‌شود (Tejay, 2008). در "استراتژی صنایع" Mintzberg (1987b, In Tejay 2008) استراتژی را با ۵ تا P تعریف کرد، نقشه، ترفند، الگو، موضع گیری و چشم انداز. Mintzberg در این باره می‌گوید:

"... استراتژی می‌تواند به عنوان (۱) یک نقشه (یعنی تعدادی عملیات آگاهانه هدفمند)؛ (۲) یک ترفند (که مانوری خاص است که به منظور بهتر عمل کردن از یک رقیب انجام می‌شود)؛ (۳) یک الگو (رشته‌ای از فعالیتهای محقق شده)؛ (۴) یک موضع (ابزاری برای تطبیق بین یک سازمان و محیط خارجی اش)؛ و (۵) یک چشم انداز (که بین اعضای سازمان به اشتراک

www.takbook.com

گذاشته شده است و محتوای چیزی که نه تنها شامل یک موقعیت است، بلکه روشی عجین شده در درک جهان است (Mintzberg, 1987, In Chen, et al., 2010)."

۱-۳-۳ استراتژی سیستمهای اطلاعاتی

اکثر مطالعات گذشته استراتژی سیستمهای اطلاعاتی را به عنوان رشد سریعی از استراتژی تجاری تعریف می‌کنند که در آن چگونگی محاسبه خروجی سیستمهای اطلاعاتی به منظور افزایش سود است (Chen, et al., 2010).

King (۱۹۷۸) بیان کرده است که سیستمهای اطلاعاتی مدیریت باید با افزایش درآمد، کاهش منابع، و افزایش شهرت مشارکت کنند. در حمایت از این دیدگاه Mata، Fuerst و Barney (۱۹۹۵) بیان کردند که تکنولوژی اطلاعات یکی از منابعی است که با کاهش هزینه‌ها و یا افزایش درآمد مزیت رقابتی را تقویت می‌کند.

Jhonson و Lederer (۲۰۱۰) تعریفی بر اساس تعریف قبلی ایجاد کردند به این شکل که سهم سیستم اطلاعاتی دارای سهمی استراتژیک پنج گانه است: رضایت مشتری، درآمد فروش، سهم بازار، بازگشت سرمایه و بازدهی عملیاتی. به طور کلی، استراتژی سیستمهای اطلاعاتی از استراتژی سازمانی برای افزایش خروجی سازمان و کارآمد ساختن خروجی از طریق سیستمهای اطلاعاتی حمایت می‌کند (Chen, et al., 2010).

۱-۳-۴ امنیت سیستمهای اطلاعاتی

عموما امنیت سیستمهای اطلاعاتی برای امن کردن جنبه‌های تکنیکی و عملیاتی یک سیستم اطلاعاتی برای محافظت از داده دیده می‌شود (Anderson, 2003; de Paula, Ding, Dourish, Nies, Pillet, Redmiles, Ren, Rode, & Filho, 2005; Dutta & McCrohan, 2002; Kim, 2004; Ruighaver, 2008; Vijayan, 2005; Zhang & Bao; 2010). هرچند، کمبود یک تعریف قابل قبول در صنعت برای استراتژی امنیت اطلاعات وجود دارد که مانع از پذیرش یک تعریف متداول می‌شود (Alter, 2008; Anderson, 2003). همانطور که White و Bruten (۲۰۱۱) بیان کردند "استراتژی یک مجموعه هماهنگ از فعالیتهایی است که مقاصد، منظورها و اهداف، یک شرکت را برآورده می‌سازد". این بیان، منجر به مشاهده‌ای توسط Baskerville

www.takbook.com

و Dhillon(۲۰۰۸) شد که در آن عنوان شد که اصطلاح استراتژی بسیار بی قید و شرط در متون به کار برده شده است، با وجود این که نسبتا اصطلاح پیچیده‌ای است.

پیچیدگی را می‌توان در مقاله Mintzberg (1987b) دید که چگونه مدیریت استراتژی را در پنج دیدگاه نقشه، ترفند، الگو، موضع و چشم انداز آزموده است. این تعریف را Baskerville و Dhillon (۲۰۰۸) به ۱۰ روش مختلف برای استراتژی مدیریتی از طریق مکاتب بخشهای تجویزی طراحی و برنامه ریزی و بخشهای توصیفی کارآفرینی، تشخیصی، یادگیری، قدرت، فرهنگ، محیط و پیکر بندی گسترش دادند. هر کدام از اینها به طور جداگانه وجوهی از استراتژی هستند اما با هم (اگر چه با هم تفاوت دارند) درک همه جانبه‌تری از استراتژی و وجوه‌اش می‌دهند (Baskerville & Dhillon, 2008). کلمه‌ای انتخاب شده توسط Baskerville و Dhillon (۲۰۰۸) برای توصیف کردن استراتژی ترکیب شدند اما هیچ اصطلاح خاص یا ترکیبی از اصطلاحات که متضمن همه "استراتژی" باشد نبود که نتیجه آن ترکیبی بود که به اصطلاح استراتژی، مفهوم می‌داد.

۱-۳-۵ استراتژی امنیت اطلاعات

استراتژی امنیت اطلاعاتی که درون یک ساختار سازمانی به عنوان دیدگاه امنیت اطلاعات قرار می‌گیرد سمت و سویی را برای سیاست فراهم کرده، با حکمرانی مشارکت کرده و توازنی برای حکمرانی از طریق تابعیت از قانون را در یک ارتباط هم افزایی از مدیریت امنیت اطلاعات کنترل می‌کند (Klaić, 2010; Posthumus & von Solms, 2004).

روشهای برگزیده برای پیاده سازی یک استراتژی امنیت اطلاعات از انتخاب‌هایی تشکیل می-شود، انتخاب تنظیم و نقشی که استراتژی امنیت اطلاعات را برای مشارکت در "نقشه کلی مدیریت و توسعه امنیت اطلاعات سازمان" اجرا شود (Baskerville & Dhillon, 2008). این تعریف برگزیده استراتژی امنیت اطلاعات است.

این مطالعه شامل مقالاتی است که بیان کرده‌اند استراتژی امنیت اطلاعات باید با استراتژی تجاری تنظیم شود (Caralli, 2004; Dhillon, 1995; Newkirk, Lederer, & Johnson, 2008). در متون چندین مفهوم گسترده برای تنظیم استراتژی تجاری با استراتژی سیست-های اطلاعاتی تعریف شده است (Chan & Huff, 1992; Chen, et al., 2010)؛ اما متاسفانه

www.takbook.com

این افراد مطالعات زیادی در مورد تنظیم استراتژی امنیت اطلاعات نکرده‌اند (Hall, Sarkoni, & Mazzuchi, 2011; McFadzean, et al., 2011).

صنعت، به امنیت اطلاعات به عنوان یک فکر ثانویه نگاه می‌کند که برای بدست آوردن اعتبار یا پاسخ به مشکلات پس از رخداد نقض عهد به کار می‌رود. در نتیجه امنیت اطلاعات به جای اینکه پیاده سازی کنشگرایانه‌ای برای تخفیف مشکلات قبل از منجر شدن به نقض عهد باشد به پاسخی انفعالی تبدیل می‌شود(Hedström, Kolkowska, Karlsson, & Allen, 2011; Hu, Hart, & Cooke, 2007; Scully, 2011).

با تعریف اصطلاحات، هسته اصلی استراتژی تشکیل می‌شود. سپس در بخشهای آتی پوشش استراتژی امنیت توضیح داده می‌شود. فصل ۲ رفتار مطالعات گذشته را در مورد تنظیمات و نقشهای استراتژیک امنیت اطلاعات پوشش می‌دهد. فصل ۳ روش تحقیق انتخاب شده برای تعامل، مشاهده، دریافت و تحلیل اعمال متخصصان امنیت اطلاعات در انتخاب نقشها را معرفی می‌کند و در مورد جمع آوری داده و نتایج جمع اوری داده بحث می‌کند. فصل ۴ داده‌ها را برای ایجاد یک نظریه برای استراتژی امنیت اطلاعات در سازمان‌های مالی بزرگ تحلیل می-کند. و در آخر، در فصل ۵ دستاوردی که در زمینه دانش امنیت اطلاعات بدست آمده بیان شده و توصیه‌هایی برای تحقیقات آینده بیان می‌کند.

www.takbook.com

فصل دوم

مروری بر ادبیات تحقیق

www.takbook.com

۲-۱ مقدمه

از آنجایی که امنیت اطلاعات زمینه‌ای نسبتا جوان و در حال شکل گیری است، متون تحقیقی طیف وسیعی از امنیت اطلاعات را پوشش داده‌اند (Anderson, 2003; Kritzinger & Smith, 2008). این مطالعه شامل مقالاتی از یک طیف امنیت اطلاعات (حکمرانی، سیاست، مدیریت و پذیرش) است که شامل بخشها و اقلام ذینفعی است که اثر مستقیمی بر روی استراتژی دارند (Klaić, 2010; Kritzinger & Smith, 2008; Ohki, Harada, Kawaguchi, Shiozaki, & Kagaua, 2009; Siponen, 2005b).

۲-۲ مروری بر متون

در بسیاری از مقالات، موضوع استراتژی امنیت اطلاعات مطرح شده است، اما به طور مستقیم بررسی نشده است. نویسندگان به طور مستقیم با بحث در مورد استراتژی خود را درگیر نکرده‌اند، اما مراجعی را به عنوان دیدگاه و دستاورد یک نقشه کلی مدیریت و توسعه امنیت اطلاعات تزریق کرده‌اند (Bhalla, 2003; Damianides, 2005; Doherty & Fulford, 2005; Doherty & Fulford, 2006). محقق مراجعی را به طور مستقیم و غیر مستقیم برای استراتژی امنیت اطلاعات مشخص کرده و آنها را با اصطلاحاتی که در جدول ۱ (منابع تعریف) آمده است دسته بندی کرده است.

شکلگیری استراتژی امنیت اطلاعات در برگیرنده چشم اندازی به دیدگاه رهبر و سازمان است (Salmela & Spil, 2002). استراتژی امنیت اطلاعات نتیجه دریافت اهداف، منظورها و اولویتهای دیدگاه و تطبیق آنها با استراتژی سازمانی است (Moen & Norman, 2000; Salmela & Spil, 2002). مراحل بعدی در فرآیند توسعه استراتژی امنیت اطلاعات شامل در نظر گرفتن اهداف استراتژیک، تاکتیکی و عملیاتی سازمان است (da Veiga & Eloff, 2007; Grobler & Louwrens, 2005). درجدول ۱ چندین اصطلاحاتی را که استفاده شده و راههایی که منجر به استراتژی امنیت اطلاعات شده است، تعریف کرده اند. در ادامه در مورد اینکه چگونه این منابع تعریف با امنیت اطلاعات و استراتژی امنیت اطلاعات تنظیم شده‌اند، بررسی می‌شود. این تعاریف معمولا بر اهداف بلند مدت استراتژیک، میان مدت تاکتیکی و کوتاه مدت عملیاتی نگاشت می‌شوند. استراتژی امنیت اطلاعات به سه بخش تقسیم می‌شود که به پرسنل اجازه تعقیب در محدوده‌های زمانی کوتاه، متوسط و بلند را می‌دهد (King, 1978;

www.takbook.com

(Mintzberg & Waters, 1985; Wommack,1979). محکها یا نقاط عطف کمک کرده‌اند تا نشانه‌هایی برای کارآیی موثر در امنیت مشخص شوند (Allen, 2005; Eloff & von Solms, 2000; McFadzean, et al., 2011; Ohki, et al., 2009). اگر استراتژی امنیت اطلاعات بد عمل کند، مسائل در سازمان مکررا در سطوح تاکتیکی و عملیاتی خود را نشان می‌دهند (da Veiga & Eloff, 2007). مشکلات حتی قبل از پیاده سازی استراتژی امنیت اطلاعات در یک سازمان می‌تواند رخ دهد (Scully, 2011). مشخصه‌ای از این ممکن است نوشتن، تائید و سپس دور زدن استراتژی امنیت اطلاعات باشد پیش از اینکه هیچ کسی طبق آن کاری انجام بدهد (Rose, 2011). در این مورد افراد یا پرسنل مسئول انجام درست ایده‌آلهای استراتژی امنیت اطلاعات هستند بدون اینکه هیچ چیزی راجع به آن بدانند. فشارهای عملی برای رسیدن به نیازمندیهای عملیاتی یا تاکتیکی مداخله کرده و در این موارد استراتژی تا زمان تکمیل اهداف تا حتی سطح عملیاتی کنار گذاشته می‌شوند (da Veiga & Eloff, 2007; Grobler & Louwrens, 2005). عوامل درگیر در این وقایع پیچیده و گسترده هستند.

www.takbook.com

جدول ۱. منابع تعریف

اصطلاح به کار رفته	توضیح	منبع
امنیت سایبری معماری مدیریتی سیاست امنیتی	امنیت بخشی از استراتژی کلی بود	Knapp & Boulton, 2006; McFadzean, Ezingeard, & Birchall, 2007
استراتژی امنیت سایبری	مزایا و معایب آن در استراتژیها به شکل استراتژیهای کنش گرا و منفعل بازگو شد.	Rowe & Gallaher 2006
	"محافظت از داراییهای دیجیتال" مردم و سازمانها	Ghernouti-Hélie, 2010
امنیت استراتژیک شرکت	اندازه گیری شده در هر سطح، منتسب به پذیرش ریسک	Anderson & Choobineh, 2008
استراتژی تضمین اطلاعات	تنظیم با استراتژی مشارکتی برای فراهم کردن بهترین دارایی امنیت و دسترس پذیری اطلاعات	Ezingeard, McFadzean, & Birchall, 2005
امنیت اطلاعات	استراتژی امنیتی به عنوان بخشی از حکمرانی، محرک سازمان	Grobler & Louwrens, 2005
استراتژی مدیریتی	استفاده از مدیریت برای پیاده سازی یک روش استراتژیک امنیتی.	Doherty & Fulford, 2005

www.takbook.com

اصطلاح به کار رفته	توضیح	منبع
	استراتژی مدیریت امنیت اطلاعات و چگونگی تنظیم شدن آن با کسب و کار	Ma, Johnson, & Pearson, 2008
استراتژی استنتاجی	برای فهم سطوح انفرادی و سازمانی استفاده می-شود	Albrechtsen & Hovden, 2009
برنامه ریزی امنیت اطلاعات	با وجود اینکه تعریف نشده است، یک استراتژی برنامه ریزی ریسک شایع شده است.	Straub & Welke, 1998
استراتژی امنیت اطلاعات (با پیشنهادات)	بخشی از حکمرانی امنیتی همراه با مسئولیتهای بلندمدت و کوتاه مدت؛ بخشی از برنامه کلی.	Da Veiga & Eloff, 2007; Shoraka 2011
	استراتژیهایی برای پاسخگویی به ریسک و هزینه‌هایش	Daneva, 2006
	به طور استراتژیک با کسب و کار تنظیم شده: استراتژی امنیت اطلاعاتی تنظیم شده با استراتژی کسب و کار؛ تنظیم با استراتژی کسب و کار برای ترکیب اهداف تجاری و مزایای رقابتی؛ در برگرفتن برنامه تنظیم برای استراتژی مشارکتی؛ فعال کننده کلیدی استراتژی مشارکتی بوده است.	Amaio, 2009; Chang & Ho, 2006; Dynes, Kolbe, & Schierholz, 2007; Hall, Sarkani, & Mazzuchi, 2011; Kayworth & Whitten, 2010; van Niekerk & von Solms, 2010

www.takbook.com

اصطلاح به کار رفته	توضیح	منبع
	کنش گرا در تعیین و تطبیق استراتژی	Arce & Levy, 2009
	باعث ایجاد مزیت رقابتی	Vasiu, Mackay, & Warren, (2003)
	عواملی برای پیش زمینه مفهومی، تهدیدهای متداول، و بررسی موانع	Lomprey, 2008
	استراتژی امنیت اطلاعات از حفاظت قوی برای نگهداری پرونده آسیب دیدگان حمایت می‌کند.	Love, 2011
	مدیرانی که از برآورد ریسک برای پیش‌نویس استراتژی امنیت اطلاعاتی استفاده می‌کنند.	McFadzean, et al., 2007
	استراتژی امنیت اطلاعات به عنوان پاسخ درمان تکنیکی	Park & Ruighaver, 2008
	استراتژی امنیت اطلاعات به عنوان بخشی از ساختار مالی	Posthumus & von Solms, 2004
	استراتژی امنیت اطلاعات به همراه قابلیت‌هایی که کارآیی سازمانی دارند.	Hall, Sarkani, & Mazzuchi, 2010
استراتژی امنیت سیستمهای اطلاعاتی	استراتژی به عنوان بخشی از مدیریت استنباط می‌شود و نه به عنوان راه حل تکنیکی برای پیاده سازی	Dhillon & Torkzadeh, 2006

www.takbook.com

اصطلاح به کار رفته	توضیح	منبع
	استراتژیهایی که به خوبی توسعه یافته‌اند حاصل استراتژیهای متعادل شده استراتژیهای تجاری، سیستمهای اطلاعاتی و امنیت سیستم اطلاعاتی هستند.	Chang & Yeh, 2006
	تنظیم کسب و کار با استراتژی امنیت و همچنین بحث با جزئیات کامل در مورد تجمیع کردن استراتژیک برای حمایت از استراتژی کسب و کار	McFadzean, et al., 2011
استراتژی امنیت IT	ارزیابی ریسکی که منجر به استراتژی امنیت IT شده است.	Goluch, et. al., 2008
	تمرکز تکنیکی بر روی دستگاه‌ها و قفل کردن سیستمها	Doughty, 2003
استراتژی نفوذ استراتژی دفاع در عمق	مقایسه طبیعت با روشهای استراتژی	Oreku & Mtenzi, 2009
استراتژی اطلاعات IT	امنیتی که به طور استراتژیک به دست آمده است	Von Solms, 2006
استراتژی امنیت IT	استراتژی امنیت IT به عنوان بخشی از تحلیل ریسک	Von Solms, 1998a
استراتژی (اجرای قانون)	طراحی استراتژی از ابتدا، سپس ساختن آن	Anderson & Moore, 2006

www.takbook.com

اصطلاح به کار رفته	توضیح	منبع
پیشگامان امنیت	استراتژی تنظیم شده با استراتژی کسب و کار	Booker, 2006
استراتژی امنیتی	فرموله کردن استراتژی امنیتی شامل مردم و فرآیندها	Zhang & Bao, 2010
	مقایسه هزینه و سود با وزن گذاری ریسک	Geer, 2007
	روشهایی برای ایجاد استراتژی از طریق کمیته هایی برای پیاده سازی	Smith, 2004
استراتژی	بخش تجمیع شده کل استراتژی	Ahuja, 2009
	تعریف یک فرمول بر طبق سناریویی رخ داده	Abbas & Hemani, 2010
	حفاظت کنشگرایانه نیاز به استراتژی کنشگرایانه دارد.	Bhalla, 2003
تغییرات استراتژیک	تغییر استراتژیک، اهداف تجاری را به عنوان نیازمندیهای جدید یا قابلیتهای پدید آمده میسر می‌کنند	Werlinger, Hawkey, & Beznosov, 2009

www.takbook.com

امنیت اطلاعات در امر تعیین، تحلیل و همبسته کردن درست عوامل سازمانی کار کرده است تا فرموله کردن توسعه و پیاده سازی امنیت اطلاعات را بهبود دهد (Chang & Ho, 2006; Hu, Hart, & Cooke, 2007; Kankanhalli, et al., 2003; Parakkattu, et al., 2010). در این فرآیند، استراتژی امنیت اطلاعات از بودن فقط راه حلهای تکنیکی برای ورود ایمن و نقاط خروجی از یک شبکه (Ghernouti-Helie, 2010; Hinde, 2003; Seeholzer, 2012; Zhang & Bao, 2010) تبدیل به برنامه‌های کاملا توسعه یافته‌ای از کارها شده است (Aivazian, 1998; Bower & Gilbert, 2007). استراتژی امنیت اطلاعات تا حتی فرای مرحله تشکیل و پیاده سازی بسیاری از محصولات مدیریت امنیت اطلاعات پیشروی کرده است، مثل سیاستها، چک لیستها، کتابهای راهنما، ایجاد ساختارهای حکمرانی چندگانه و مشخص کردن چارچوبهای موثر و موفق (Dunkerley & Tejay, 2009; Eloff & von Solms, 2000; Goluch, Ekelhart, Fenz, Jakoubi, Tjoa, & Mück, 2008, Siponen, 2005b; Zhang, Wuwang, Li, & Zhang, 2010).

سوالی که هنوز باقی مانده است، این است که چرا استراتژی امنیت اطلاعات هنوز به طور صحیح در ساختار سیاست و حکمرانی مدیریت امنیت اطلاعات سلسله مراتبی در یک سازمان کار نمی‌کند. (Cecere, 2011; Dawson, Berrell, Rahim, & Brewster, 2010; Dhillon, 2007; Kotulic & Clark, 2004; McFadzean, et al., 2007; Wang, 2009, Wood 2000). در این مطالعه داده‌های جمع آوری شده در مورد تعاملات متخصصان امنیت اطلاعات و نقشهای منتخب برای پیاده سازی امنیت اطلاعات و تحلیل داده‌ها برای رسیدن به یک نظریه مطالعه می‌شود.

در برخی سازمانها، امنیت در پایینترین سطح (برای دریافت تایید اولیه برای اتصال به شبکه یا کار کردن در شبکه) اجرا می‌شود (Anderson & Moore, 2006; Wang, 2009). پس از آن سازمانها امنیت را به سطح مورد نیاز برای نگهداری تائید برای استفاده عملیاتی واگذار می‌کنند. سپس سازمانها از استفاده ادامه دار خشنود می‌شدند (Dougherty & Fulford, 2005). شاهد، قضیه هستیم که سازمانها جلسات زیادی را در مورد پیاده سازی استراتژی برگزار کردند که با کنار گذاشتن تصمیمهای سخت به پایان رسیدند (Wommack, 1979). سازمان‌ها یک شکل از امنیت را پیاده سازی می‌کنند مثلا برای کنترل تکنیکی امنیت برای رسیدگی به تهدیدات شناخته شده (Damianides, 2005; Gilbert, 2008; Smedinghoff,

www.takbook.com

2005) ولی انتخاب اغلب آنها این است که مدیریت امنیت اطلاعات برای رسیدگی به تهدیدهای ناشناخته قبل از ایجاد استراتژیهای آن نداشته باشند (Anderson, 1993; Butler & Gray, 2006; Dhillon, 1995). به جای آن، سازمانها تنها نیازمندیهای تنظیمی پیاده سازی شده‌ای را که توسط قانون اجباری شده‌اند را اجرا کنند. یک پیش فرض حاکم این بود که امنیت فقط باعث کم کردن سرعت پردازش سیستمهای کامپیوتری می‌شود (Post & Kagan, 2007; Scully, 2011).

برخی عوامل استفاده شده در توصیف این استراتژی، یک روش مدیریتی را در نظر گرفته که در آن، از تهدیدات امنیتی آگاه بودند، اما از باور اینکه وقایع بد ممکن است برای آنها رخ بدهد سرباز زده بودند (Knapp & Boulton, 2006; Scully, 2011). برخلاف تهدیدهای امنیتی، مدیریت به خود مطمئن شده و بر این باور بوده که شکست ناپذیر هستند و از دست رفتن داده برای آنها هیچگاه رخ نخواهد داد (Scully, 2011; Straub, 1990). احتمالا، بزرگترین مانع اولیه از سمت مدیران برنامه ایجاد شده است، کسانی که وظیفه داشتند برنامه‌هایشان را سر موقع، با بودجه پایین و با منابع محدودی که بیش از حد بهره برداری شده‌اند، تحویل دهند که همواره به آسیب امنیتی ختم شده و در نهایت امنیت از بودجه حذف می‌شد یا محدود می‌شود (Hinde, 2000; Kark, 2010; Wang, 2009).

به طور ایده‌آل، استراتژی امنیت اطلاعات توسعه یافته در سازمانها توسط تعامل چندین متخصص امنیت اطلاعات تکامل می‌یابد. تجربیات آنها در اجرای وظایف برای تکمیل سهمشان از استراتژی کسب و کار، استراتژی سیستمهای اطلاعاتی و استراتژی امنیت اطلاعات به کار می‌رود (Anderson & Choobineh, 2008; Hall, Sarkoni, & Mazzuchi, 2011; Knapp & Boulton, 2006; Parakkattu & Kunnathur, 2010). روشی همچون تبعیت، تنها از کنترلهای امنیتی به منظور رسیدن به حداقل سطح امنیت استفاده می‌کند (Dhillon, 1995; Herath & Rao, 2009; Ma, Johnston, & Pearson, 2008; Ma, Schmidt, Pearson, 2009; Siponen, 2006). تبعیت عهده دار برآوردن ضروریات قانونی مثل مصوبه مدیریت امنیت اطلاعاتی فدرال FEDERAL INFORMATION SECURITY MANAGEMENT (FISMA) و مصوبه حمل پذیری و قابلیت حسابرسی اطلاعات سلامتی HEALTH INFORMATION PORTABILITY AND ACCOUNTABILITY

www.takbook.com

(HIPAA) به عنوان مستندات تنظیم شده امنیت اطلاعات شد (Damianides, 2005). چند سازمان دیگری که از روشهای تبعیت استفاده کردند مثل آنهایی که برای سازمانهای مالی از مصوبه Graham Leach Bliley (GLBA) و یا مقررات صنعتی تحت استانداردهای امنیت داده صنعت پرداخت کارتی

(PCI-DSS)PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS برای حفاظت از اطلاعات مالی شخصی استفاده می‌کنند (Al-Hamdini, 2009; Damianides, 2005; Gilbert, 2008; Smedinghoff, 2005). هنوز روشهای دیگری که متخصصان امنیت اطلاعات برای فرموله کردن استراتژی امنیت اطلاعات به کار گرفته‌اند از سازماندهی مجدد ساختار امنیت اطلاعات یا ساختار توابع امنیت اطلاعات در سازمانشان منتج شده‌اند. سازماندهی مجدد برای برآوردن اهداف کسب و کار جدید و یا سیستمهای اطلاعاتی پیشتر از مدیریت قرار داده می‌شوند یا رسیدگی به کمبودهای مشخص شده و به آنها از طریق حرکت یا ساختاردهی مجدد سازمان رسیدگی می‌شود (Avgerou & McGrath, 2007; Cecere, 2008; Hansen, et al., 2011; Kajava & Siponnen, 1996; Kotulic & Clark, 2004).

تبعیت و سازماندهی مجدد پاسخهای جزئی برای مساله اکتشافی تشکیل می‌دهند ولی مطالعه بر روی خصوصیات مفهوم استراتژی نگاه می‌کند (Smith & Medin, 1981). تمرکز آن بر روی پیوند بین تنظیمات نقشهای استراتژیک تحت یک استراتژی امنیت اطلاعات است (Chen, et al., 2010; Corbin & Strauss, 2008; Ezingeard, et al., 2005; Leidner, Lo, & Preston, 2011; McFadzean, et al., 2007; Smith & Medin, 1981). پیوند بین استراتژیها و هر یک از نقشهای استراتژیک خیلی پیچیده و بغرنج است (Leidner, et al., 2011). بحث با توضیحی در مورد خصوصیات مفاهیم استراتژیک و تنظیماتشان شروع می‌شود (Chen, et al., 2010; Corbin & Strauss, 2008). به عنوان یک مرور کلی، تنظیم استراتژی امنیت اطلاعات که در ساختار یک سازمان به کار می‌رود به امنیت استراتژی تجاری سازی و خودکار سازی آن از طریق سیستمهای اطلاعاتی رسیدگی می‌کند. تنظیمی که یک سازمان باید انجام بدهد باید در راستای رسیدن به یک محیط تبادل اطلاعات امن باشد (Howard & Longstaff, 1998; McFadzean, et al., 2011). تنظیم یک استراتژی امنیت اطلاعاتی اهداف، مقاصد و اولویتهای طرح ریزی شده‌ای را برای سازمان فراهم می‌آورد که به آن برای رسیدن به یک محیط تبادل اطلاعات امن نیاز دارد (Bruton & White, 2011; Doherty &

www.takbook.com

(Fulford, 2006; Newkirk, et al., 2008). مطالعات زیادی در زمینه استراتژی کسب وکار و سیستمهای اطلاعاتی وجود دارد که تنظیم اهداف را با ماموریت و دیدگاه در استراتژیشان تحلیل می‌کند (Johnson & Lederer, 2010; Mata, Chan & Reich, 2007; Earl, 1993; et al., 1995; Posthumus & von Solms, 2004; Preston & Karahanna, 2009; Salmela & Spil, 2002; Stanton, Guzman, Stam, & Caldera, 2003; Westerman, 2009). هرچند، تعداد زیادی در مورد تنظیم استراتژی امنیت اطلاعات به سیستمهای اطلاعاتی یا استراتژیهای سطح تجاری بحث نکرده‌اند (Leidner, et al., 2011; McFadzean, et al, 2007; Newkirk, et al., 2008; Tejay, 2008). بحث در بخش بعدی مختص به زمینه‌های تنظیم استراتژی امنیت اطلاعات برای مفهوم استراتژی است.

۲-۳ تنظیمات جاری برای استراتژی امنیت اطلاعات

این بخش در مورد تنظیم استراتژی امنیت اطلاعاتی برای توضیح روشهایی بحث می‌کند که در آنها استراتژی پیاده سازی می‌شود. یک مکتب فکری وجود دارد که سبکهای مختلفی از آن برای پیاده سازی استراتژی وجود دارد. پنج روش برای تنظیم استراتژی امنیت اطلاعات موجود است. اولین استراتژی، استراتژی تجاری است که بدون آن سازمان ممکن است دوام نیاورد. همچنین، یک سازمان نمی‌تواند با وجود فقط یک سیستم اطلاعاتی یا استراتژی امنیت اطلاعات به تنهایی دوام بیاورد. بنابراین، استراتژی امنیت اطلاعات بدون یک استراتژی تجاری ممکن است موجب شکست سازمان شود. چهار روش دیگر تنظیم استراتژی بر روی استراتژی امنیت اطلاعات متمرکز شده است که شامل: کار با استراتژی تجاری هم تراز با استراتژی امنیت اطلاعات به استراتژی تجاری، تنظیم استراتژی تجاری با استراتژی سیستمهای اطلاعاتی، تنظیم استراتژی امنیت اطلاعات با هر دو استراتژی سیستمهای اطلاعاتی و تجاری، اجازه دادن به استراتژی امنیت اطلاعات برای اینکه به خودی خود عمل کند و زمانی که استراتژی امنیت اطلاعات وجود ندارد، عملیات به طور خود آگاه از هیچ استراتژی امنیت اطلاعات برای اجرای ماموریتش استفاده نکند. جدول ۲ برای توصیفی در مورد تنظیمات ارائه شده است.

www.takbook.com

جدول ۲. تنظیمات استراتژی امنیت اطلاعات

استراتژی امنیت اطلاعات	دیدگاه‌های اولیه استراتژی با به کارگیری تعریف 5P Mintzberzg (1987b)	فرضیات مرتبط با فرایند توسعه استراتژی امنیت اطلاعات			فرضیات مرتبط با تاثیر استراتژی امنیت اطلاعات و تاثیر مطلوب آن	فرضیات مرتبط با استراتژی امنیت اطلاعات/ تنظیم استراتژیک تجاری
		نقطه شروع در زمان توسعه استراتژی امنیت اطلاعات	دیدگاه گرفته شده در زمان توسعه استراتژی امنیت اطلاعات	ارتباط بین IS و استراتژی تجاری		
تنظیم با کسب و کار	برنامه سازمان را به طور مستقیم حمایت می‌کند	استفاده از استراتژی تجاری به عنوان راهنما	کسب و کار- محور	استراتژی امنیت اطلاعات با استراتژی امنیت اطلاعات تجاری	تضمین برآورده کردن اهداف همزمان با استراتژی تجاری	استراتژی برآورده شئ
تنظیم با سیستمهای اطلاعاتی	موضع، یافتن جایگاه در سیستمهای اطلاعاتی	از سیستمهای اطلاعاتی به عنوان راهنما استفاده شده	سیستم اطلاعاتی محور	استراتژی امنیت اطلاعات با هر دو توسعه می‌یابد	تضمین برآورده کردن اهداف همگان با استراتژی	کمک به استراتژی ازطریق سیستمهای اطلاعاتی

www.takbook.com

					سیستمهای اطلاعاتی	
تنظیم با سیستمهای اطلاعاتی و کسب و کار	برنامه ریزی و موقعیت، حمایت و یافتن جایگاه	استفاده از هر دو استراتژی سیستمهای اطلاعاتی و تجاری	مبتنی بر سیستمهای اطلاعاتی و تجاری	استراتژی امنیت اطلاعات از هر دو استراتژی سیستمهای اطلاعاتی و تجاری توسعه یافته است	تضمین برآورده کردن اهداف همگام با استراتژیهای سیستمهای اطلاعاتی و تجاری	برآورده شده/ به استراتژی از طریق سیستمهای اطلاعاتی کمک شده است
به خودی خود کار کردن	چشم انداز، تمرکز بر روی نقش جدی قانون	استفاده از قانون و مقررات به عنوان راهنما	کسب و کار و سازمان محور	استراتژی امنیت اطلاعات به طور مجزا توسعه یافته، برآورده کردن نیازمندیهای امنیت اطلاعات	نیازمندی دارایی تعیین شده و آگاهی تضمین شده است	استراتژی نیازمندیها اطلاع داده شده
موجود نیست	تمهید، تغییر مطابق جریان	استفاده از تمهید متخصص امنیت اطلاعات برای استراتژی	سازمان محور	استراتژی امنیت اطلاعات واقعا ایجاد نشده بوده است که موجب عملیات بعد از رخداد یا تحلیل شکاف می‌شود.	فهمی از امنیت فراهم کرده و راهنمایی ISP را دنبال می‌کند	برآورده کردن نیازمندیهای متخصصان امنیت اطلاعات برای استراتژی

www.takbook.com

هر نوع استراتژی، چشم اندازی VISION دارد و ماموریتی MISSIONرا تعریف می‌کند و بر روی فعالیت لازم برای پیاده سازی استراتژی تاکید می‌کند (Anderson & Choobinah, 2008; Cohen & Cyert, 1973; Kankankalli, et al., 2003; Kotulic & Clark, 2004; Mintzberg & Waters, 1987). اکثریت متون نیاز به تنظیم را مشخص کرده‌اند اما تمرکز اکثر آنها بر روی تنظیم سیستم‌های اطلاعاتی با استراتژی تجاری بوده است. مطالعات بسیار کمی موجود هستند که استراتژی امنیت اطلاعات را با یا کسب و کار یا سیستمهای اطلاعاتی تنظیم کرده باشند (Newkirk, et al., 2008; Rudd, Greenley, Beatson, & Lings, 2008; Thompson & James, 2001).

استراتژی امنیت اطلاعات از سیستمهای اطلاعاتی و استراتژی تجاری برای امن کردن اطلاعات کسب و کار حمایت می‌کند (Alter, 2008; Chen, et al., 2010; Stanton, et al., 2003). حفاظت اطلاعات و سیستمهای اطلاعاتی در همه سطوح پیچیده و گسترده می‌شوند (Leidner, et al., 2011). بخشی از فرآیند شبکه ساختن و اتصال اطلاعات Meshingو سیستمهای اطلاعاتی در سختی تنظیم استراتژیها مشخص شده است (Doherty & Fulford, 2006; Segars & Grover, 1998). زمینه‌ای که محققان در مورد آن مطالعه کردند اجماع استراتژی امنیت اطلاعات با استراتژی تجاری (Newkirk, et al., 2008; Tejay 2008) و استراتژی امنیت اطلاعات با سیستمهای اطلاعاتی (Dutta & McCrohan, 2002; Straub & Welke, 1998) است.

یکی از تنظیماتی که استراتژی سیستم اطلاعاتی این بود که استراتژی سیستم اطلاعاتی کاملا با استراتژی تجاری از طریق خودکار سازی پردازش، ورودی، ذخیره و خروجی داده تنظیم می‌شود (Chen, et al., 2010; Stanton, et al., 2003). استراتژی دیگری که در امنیت اطلاعات در مورد آن بحث شده است، تنظیم شدن با استراتژی تجاری از طریق عبور شفاف از استراتژی سیستمهای اطلاعاتی است. این تنظیم سیستم اطلاعاتی تنها با خودکار سازی استراتژی تجاری در نظر گرفته شد (Chen, et al., 2010). نمونه دیگر، استراتژیی بود که در آن استراتژی امنیت اطلاعات فقط یکی از استراتژیها را مثلا فقط استراتژی سیستمهای اطلاعاتی یا فقط تجاری را حمایت می‌کرد که این فقط با یک استراتژی خاص تنظیم می‌شد و دیگر استراتژیها را نادیده می‌گرفت (Caralli, 2004; Hall, et al., 2010; McFadzean, et al., 2011). آخرین نوع استراتژی که به آن استراتژی غیر موجود گفته می‌شود، استراتژیی

www.takbook.com

است که در آن برنامه امنیت بدون هیچ شکل یا فرآیند مجزایی، کاملا به خودی خود اجرا می‌شود. اگر چه در واقعیت جنبه بدون استراتژیی سریعا به پذیرش استراتژی تجاری تبدیل می‌شود، زیرا که امنیت اطلاعات درون یک سازمان و ساختار موجودش اجرا می‌شود.

در جدول۲، پنج ۵ مفهوم تنظیم استراتژی و چگونگی ارتباط آنها با تعریف، فرض توسعه استراتژی امنیت اطلاعات، تاثیر فرض استراتژی امنیت اطلاعات مطلوب و نتایج برآورد شده با استراتژی تجاری کلی به طور خلاصه بیان شد. در ادامه این بخش، جزئیات مفاهیم تنظیم را از طریق انواع استراتژی بیان می‌کنیم.

۲-۳-۱ تنظیم کردن با استراتژی تجاری

در تنظیم با استراتژی تجاری، استراتژی امنیت اطلاعات با استراتژی کسب و کار تنظیم شده است (Caralli, 2004). این اولین مفهومی که چگونه تنظیم استراتژی در داخل یک سازمان انجام می‌شود را تعیین می‌کند (Siponen, 2005b; Westerman, 2009). استراتژی امنیت اطلاعات برای پیروی کردن از آن یا تقویت نیازمندیهای استراتژی تجاری نوشته شده‌اند (Cerpa & Verner, 1999; Hall, et al., 2010; McFadzean, et al., 2007; McFadzean, et al., 2011; Parkin & van Moorsel, 2009). ارتباط امنیت اطلاعات در اصطلاح تجاری در حالی که از امنیت سازمان نگهداری می‌کند، به تنظیم دو استراتژی کمک می‌کند (von Solms & von Solms , 2004; von Solms & von Solms, 2005). چالش در مورد توصیف استراتژی امنیت اطلاعات به زبانی قابل فهم برای مجری تجاری بود تا بتواند امنیت اطلاعات را درک کند (Lindström & Hägerfors, 2009). استراتژی امنیت اطلاعات با اهداف کلی سازمان پی گرفته شد و به کارگرفته شد، این استراتژی از مجموعه نیازمندیهای بیرون از رهبری سازمان برداشت شد (Hall, et al., 2010; Kayworth & Whitten, 2010). همچنین تنظیم با استراتژی تجاری منتج به تضمین رسیدن به همان اهداف استراتژی شد (Amaio, 2009; Lomprey, 2008).

۲-۳-۲ تنظیم کردن با استراتژی سیستمهای اطلاعاتی

استراتژی امنیت اطلاعات از استراتژی سیستمهای اطلاعاتی به عنوان راهنما استفاده کرده است. به عنوان هدف کلی، استراتژی امنیت اطلاعات پشت سر و تنظیم شده با استراتژی

www.takbook.com

سیستمهای اطلاعاتی توسعه یافته است. در حالی که استراتژی سیستمهای اطلاعاتی اغلب با مرکزیت سیستمهای اطلاعاتی بودند، استراتژی امنیت اطلاعات سعی در تضمین دستیابی امن به اهداف استراتژی سیستمهای اطلاعاتی داشت. اهداف سیستمهای اطلاعاتی در جایی که در دسترس بودند به تضمین ابزارهای اطلاعاتی کمک کرد اما گاهی اوقات با نیازهای تجاری امکان داشت که تنظیم نشوند، بنابراین نمی‌توانستند بهترین ارزش را برای سازمان فراهم کنند (Alter, 2008: Chen, et al., 2010; Stanton, et al., 2003).

۲-۳-۳ تنظیم کردن با سیستمهای اطلاعاتی و استراتژیهای تجاری

استراتژی امنیت اطلاعات به عنوان دیدگاه اشتراکی اهداف برنامه امنیت اطلاعات در یک سازمان هم با سیستمهای اطلاعاتی و هم با استراتژیهای تجاری تنظیم می‌شود. در عملکردی بسیار حرفه‌ای، توسط بازدهی‌های بهینه سازی شده بین استراتژی سیستم اطلاعات و استراتژی تجاری برای معین کردن فرصت‌های تجاری و تنظیم آنها، همگام با مناسبترین تکنیکهای خودکارسازی باعث افزایش بهره‌وری و حفظ هزینه تجهیزات می‌شود (Baptista, Newell, & Currie, 2010; Leidner, et al., 2011; Straub & Welke, 1998).

۲-۳-۴ استراتژی امنیت اطلاعات به خودی خود کار می‌کند

تنظیم چهارم پوشش دهنده حوزه‌ای بود که در آن استراتژی امنیت اطلاعاتی تقریبا در یک خلا توسعه یافته و کسب و کار یا استراتژیهای سیستم اطلاعاتی را برای توسعه در نظر نگرفته است (Badr, Biennier, & Tata, 2010). برای تمرکز، صرفنظر از محدودیتهایی که نیازمندی-های سیستم اطلاعاتی و تجاری دارند، توسعه در قلمرو خودش رخ می‌دهد و ممکن است تنها به قانون و مقررات فدرال برای مشخص کردن اینکه چه چیزی هدف و منظور است وابستگی داشته باشد. استراتژی امنیت اطلاعات تمایل دارد تا مجوز دیکته کردن نیازمندیهایی که برای تبعیت از دیدگاه استراتژی تجاری و سیستمهای اطلاعاتی وجود دارد را داشته باشد (Eloff & von Solms, 2000; von Solms & von Solms, 2004).

www.takbook.com

۲-۳-۵ استراتژی امنیت اطلاعات موجود نیست

تنظیم پنجم، کمبود هر استراتژی سازماندهی شده‌ای را از منابع خارجی تجاری یا سیستمهای اطلاعاتی در نظر می‌گیرد (Pfeffer, 1992). استراتژی امنیت اطلاعاتی وجود دارد که به شکل تعاملاتی عمل می‌کند که در این استراتژی به واسطه یک مجری امنیت اطلاعات است که به صورت روز به روز (Mintzberg, 1987b; Mintzberg & Waters, 1985; Porter, 1996; Reich & Benbasat, 2000) و بدون هیچ روش ساختار یافته‌ای در مکان کار می‌کند. مجری دستوری را بدون رسمی کردن استراتژی امنیت اطلاعات در نوشتن یا دیگر کانالهای ارتباطی برای زیر دستان یا نظیرهایش فراهم می‌کند. استراتژی در نتیجه تغییرات دوره‌ای پیوسته دستورات مجری ارشد نشات می‌گیرد. Allen (2005) و Linder، Lo و Preston (۲۰۱۱) تاکید کردند که امنیت نباید نادیده گرفته شود بلکه باید ارائه شود.

۲-۳-۶ خلاصه‌ای از تنظیمات

در جدول ۲ مشخصات همه تنظیمات به طور خلاصه نشان داده شده است. در این جدول جایی که انواع تنظیمات مجزا با هم متقاطع هستند نشان داده شده است. نویسنده شکل جدول را از روی کار Chen, Mocker, Preston, & Teubner (2010) برداشته و آن را برای استراتژی امنیت اطلاعات مرتبط با ساختار تطبیق داده است. در بحث تنظیماتی که ارائه شده‌اند، بیشترین راههای محتملی که در آن یک استراتژی امنیت اطلاعات می‌تواند توسعه یابد پوشش داده شده‌اند؛ با در نظر گرفتن استراتژیهایی که در آن از کسب و کار، سیستمهای اطلاعاتی یا هر دو نوع برای تکمیل مجموعه دو جانبه از اهداف پوشش داده شده‌اند. علاوه بر آن، تنظیم دیگر شامل آماده سازی یک استراتژیی است که به خودی خود اجرا می‌شود تا نیازهای داخلی را برآورده کند، اما از عهده تمام اهداف سازمانی برنمی‌آید. در مورد یک سازمان جدید بدون داشتن استراتژی ممکن است به نظر برسد که تنها موقعیت قابل پیشنهاد نداشتن استراتژی بوده است؛ اما نداشتن هیچ استراتژیی معمولا باعث اجرای کوتاه اندیشانه وظایف شده و در نتیجه دوباره کاری و تلاشهای دوباره شده را می‌طلبد (Baskerville & Dhillon, 2007). بخش بعدی شامل بحث تاثیرات خارجی بر روی استراتژیهای امنیت اطلاعاتی است که از طریق نقشهایی که یک متخصص بر روی استراتژی امنیت اطلاعات اعمال می‌کند ایجاد می‌شود.

www.takbook.com

۲-٤ ارائه تشخیص نقش برای استراتژی امنیت اطلاعات

مطالعات گذشته بر روی سیستمهای اطلاعاتی (Chen, et al., 2010) سه نقش کارآی استراتژی را مشخص کرده است (سیستمهای اطلاعاتی نوآور، سیستمهای اطلاعاتی محافظه کار و سیستمهای اطلاعاتی تعریف نشده)، اما تصمیم گرفتند که در مورد متغیرهای دیگر نقشهایی که در آن استراتژیها اجرا می‌شود جستجویی انجام ندهند.

Leidner، Lo و Preston (2011)، بر اساس مقاله اصلی یک نقش اصلی ساختند. آنها پیشنهاد افزودن نقش تردست (Ambidextrous دو دست توانا) سیستمهای اطلاعاتی را دادند (Leidner, et al., 2011) که این نقش سعی در دریافت واریانس اضافی سه نقش دیگر را دارد. قدم بعدی لازم بر اساس دو مطالعه دیگر با اضافه کردن یک آزمایش نظری قابل کارکردن ساخته شد. تا آنجا، یک استراتژی نظری اساسی می‌توانست به ظهور یک نظریه آزمایش اجازه رسمیت گرفتن ببخشد (Pandit, 1996). در هر دو کار، نویسندگان انتخاب کردند که مطالعه را در حوزه نظری بدون انجام تحقیق واقعی برای اعتبار سنجی پیشنهاداتشان، نگهدارند (Chen, et al., 2010; Leidner, et al., 2011). بعد از آن، آنها پیشنهاداتی را ارائه دادند که می‌توانست منجر به یک مبنای معنوی برای مباحثه در مورد استراتژی سیستمهای اطلاعاتی برای مشارکت در زمینه سیستمهای اطلاعاتی باشد. از آنجایی که مطالعات واقعی شواهد دقیقی را جمع آوری نکردند، این مطالعه داده‌های وسیعی از متخصصان امنیت اطلاعات به دست آورد و با استفاده از یک تحلیل دقیق به اشباع زیر نمونه برداری نظری رسید (Corbin & Strauss, 2008; Creswell, 2011; Devadas, Silong, & Ismail, 2011). این تحقیق از مطالعه موجود استفاده کرد (Chen, et al., 2010) تا اعتبار استراتژی امنیت اطلاعات را در انتخاب نقش استراتژیک واجد شرایط توسط متخصصان امنیت اطلاعات بسنجد.

مطالعات تعاملات رسمی و غیررسمی بین مجریان کسب و کار و مجریان سیستمهای اطلاعاتی مشخص کردند و همچنین آن تعاملاتی که بر روی چگونگی پیاده سازی سیستمهای اطلاعاتی تاثیر داشت را مشخص کردند (Pyburn, 1983; Johnson, 2009). اغلب تعاملات نادر بودند و تنها گاهی برای جلسات ارزیابی یا ملاقات برای بحث در مورد تشکیل استراتژی رخ می‌دادند (Jhonson, 2009). از آنجایی که تعاملات نادر بوده و سیستمهای اطلاعاتی به شکلی دیده می‌شدند که در راستای اهداف تجاری باید می‌بودند، نقشهای استراتژیک دارای شایستگی که

www.takbook.com

توسط کسب و کار پیشنهاد شده بود ممکن بود نتواند همیشه با سیستمهای اطلاعاتی هماهنگی داشته باشد. فرض شده بود که سیستمهای اطلاعاتی به طور کورکورانه دنباله رو کسب و کار بودند (Pyburn, 1983). اگر چه، تعاملات نیاز به هماهنگی و ارتباط برای ایجاد یک استراتژی موثر دارد.

با تعریف یک استراتژی امنیت اطلاعاتی به عنوان پیاده سازی یک استراتژی امنیت اطلاعات مقرر شده، شامل انتخابهایی برای "یک نقشه کلی برای مدیریت و توسعه امنیت اطلاعات یک سازمان" است (Baskerville & Dhillon, 2007). Baskervilleو Dhillon (2008) تشخیص دادن که یک استراتژی خوب امنیت اطلاعات موجب سیاستهای امنیت اطلاعاتی می‌شود که مدیریت امنیت اطلاعات برای پیاده سازی فرآیندها و اجرای امنیت اطلاعات مورد استفاده قرار می‌گیرند. آنها تاکید کردند برای اینکه به اهدافش دست یابد نیاز است یک استراتژی مجتمع برای مدیریت امنیت اطلاعات وجود داشته باشد. شرکت کنندگان در امن سازی اطلاعات باید نقشهایشان و مسئولیت‌هایشان در رسیدن به اهداف به طور واضح تعریف بشود.

نقشهای پیاده سازی شده‌ای که توسط متخصصان امنیت اطلاعات به کار گرفته شدند با هم متفاوت هستند که این تفاوت بر اساس پس زمینه‌های افرادی است که استراتژی امنیت اطلاعات را پیاده سازی کرده‌اند (Ashenden, 2012; von Solms, 2001). برهم کنش بغرنج یک متخصص امنیت اطلاعات با کسب و کار و مجریان امنیت اطلاعات باعث سردرگمی می‌شود (Jhonsn, 2009). بخشهایی از این معما سنجیدن تعاملات انسانی مناسب توسط مدیریت امنیت اطلاعات بود (Ashenden, 2012)، ترجیح‌های رهبر و انتخاب دسته برای بسته بندی کارآیی آنها در استراتژی امنیت اطلاعات تحت برنامه امنیت اطلاعات بود. به عنوان بخشی از این معادله، متخصصان امنیت اطلاعات نقشهای استراتژیک دارای صلاحیت را از مجموعه وسیع دسته بندی شده‌ای که در جدول ۳ نمایش داده شده را بر می‌گزینند. این دسته بندی‌های شامل بالا به پایین، تصویر عمومی، رقیب، تغییر پیوسته، بهترین اجرا، سازماندهی مجدد، ارتباط قدرت و پیروی از قانون هستند. در جدول ۳ مجموع نقشهای اصلی که متخصصان امنیت اطلاعات برای پیاده سازی استراتژیهای امنیت اطلاعات نمایش می‌دهند به صورت یک لیست خلاصه شده است. در پاراگراف‌های بعدی این دسته بندیها با جزئیات شرح داده می‌شوند.

www.takbook.com

۲-۴-۱ بالا به پایین

مکتب موضع گیری فکریThe positioning school of thought به کارآیی استراتژی نگاهی بالا به پایین دارد، در جایی که مجریان برای منفعت بردن از مواضع،کارآیی استراتژی را حرکت داده و جا به جا می‌کنند همانطوری که رهبر تغییر جهت را می‌بیند (Slaughter, Levine, Ramesh, & Pries-Heje, 2006). نقش بالا به پایینی که از بالا به سمت پایین مدیریت می‌شود، مجریان را درگیر تصمیم گیری کرده و دیدگاه آنان را در استراتژی و سیاست گرفته، و بر روی فعالیت تمام پرسنل داخل سازمان حکمرانی می‌کند (Baskerville & Dhillon, 2008; Clark & Sitko, 2008; Dawson, et al., 2010; Kajava & Siponen, 1996; Lederer & Mendelow, 1988; Salmela & Spil, 2002). قدرت تصمیم گیری در رده بالاتر قرار گرفته و رهبری تمام فعالیتها را بر عهده دارد. در این حالت، انتخاب و چند تصمیم به طور مستقیم به عملیات سازمان گره خورده و ملزم به رعایت راهنما و مقررات هستند.

پرسنل اغلب این را به عنوان چتری که از استراتژی شکل گرفته است، درک می‌کنند (Mintzberg & Waters, 1987). جهت گیری‌های سراسری توسط مدیریت انجام می‌شود و جزئیات آن به عنوان اهداف در طی زمان اضافه می‌شوند. (Jones, (2001;Mintzberg & Waters, 1987.

www.takbook.com

جدول ۳. نقشهای استراتژیک واجد شرایط امنیت اطلاعات

نقش استراتژیک واجد شرایط	تعریف	منبع سیستمهای اطلاعاتی	منبع امنیت اطلاعاتی
بالا به پایین	استراتژی به عنوان یک پوسته و داخل آن توسط اهداف فهرست شده مشخص شده است، هدفها و اولویتها در طی زمان اضافه می‌شوند، به استراتژی اجازه توسعه یافتن داخل مرزهای تعیین شده داده می‌شود.		Clark & Sitko, 2008; Jones, 2001; Kajava & Siponen, 1996
تصویر عمومی	تصویر عمومی، تصویری است که با اعتقاد عمومی به عنوان ابزاری که توسط آن امنیت که لزوما نباید مشاهده شود، مقابله می‌کند اما از طرف دیگر به نظر برسد که پیاده سازی شده است. امنیت، یک نمای خارجی می‌شود که بیشتر تمایل به جریمه کردن دارد تا تضمین امنیت.		Anderson & Moore, 2006; Knapp & Boulton, 2006
رقیب	رقیب یا محک برای رسیدن به بهترین شرایط کار می‌کند. رقابت می‌تواند شبیه یک مسابقه تسلیحاتی برای تعبیه کردن استراتژیها برای مقابله با دشمنان باشد. نوآوری یا اقدامات متقابل برای بهتر عمل	Howard & Kilmartin, 2006; Lacity & Hirscheim, 1995	Damianides, 2005; Ohki, et.al., 2006

www.takbook.com

		کردن از یکدیگر منجر به مزیت رقابتی بین بازیکنان می‌شود.	
تغییر پیوسته	استراتژیی که برای تغییر مداوم و غیر قابل پیش بینی تطبیق یافته است. امنیت اطلاعات بر اساس تغییرات مقاصد تهدید کننده و استقرار بد افزارها، خود را تطبیق می‌دهد. استراتژی از یک تکرار سالیانه یا چرخه‌های طولانی‌تر به محیط تغییر عملیاتی تقریبابه صورت روزانه عوض می‌شود.	Bechtold, 1997; Fairholm, & Card, 2009; Huebler, Foster, & Phelps, 2007; Lacey, 2009; Levy, 1994; Valle, 2000; Yarger, 2006	Collins, 2001
بهترین تمرین	بهترین عملکرد تجاری (The Best Business Practices (BPP) سعی در مرسوم کردن و پذیرش بهترین تمرینها در سازمان دارند. استفاده از روشهایی همچون مدل بلوغ قابلیت امنیت اطلاعات برای یافتن بهترین عملکردها.	Keen & El Sawy, 2010; Luftman & Kempaiah, 2008; von Solms, 2006	Kark, Penn, & Dill, 2009; Kark, 2010; Kayworth & Whitten, 2010; Luftman & Ben-Zvi, 2010; Luftman & Ben-Zvi, 2011; McClean & Kark, 2010
سازماندهی مجدد	استفاده از توجیه برای تغییر سازمانی به عنوان یک بحث، از آنجایی که امنیت دارای نقص هایی در گذشته بوده است مدیریت نیاز به تغییر ساختار سازمان داشته؛ با این امید که عکس‌العملهای منفی را از بین ببرد، سازمان را دوباره سازماندهی کند. این		Aivazian, 1998; Norman & Yasin, 2010; Zhang, et. al., 2010

www.takbook.com

		از ISS امنیت سیستم‌های اطلاعاتی برای تشویق تغییر سازمانی استفاده می‌کند.	
ارتباط قدرت	قدرت اعمال شده از طریق استراتژی که رهبری سازمانی را برقرار می‌کند. افراد از استراتژی برای اعمال خواسته و یا تحریک پیروی توسط کارمندان استفاده می‌کنند. قدرت در دو روش به خوبی اعمال می‌شود، برای نیل به اهداف سازمانی و مجبور کردن افراد و سازمانها برای رسیدن به اهداف کوتاه مدت، اما معمولا منجر به ناموثر بودن امنیت در طی زمان می‌شوند.	Dhillon, 2004; Dhillon, Caldeira, & Wenger, 2011; Herath & Rao, 2009; Minztberg, 1985;	Lapke, 2008
پیروی از قانون	پیروی از قانون از قوانین فدرال استفاده می‌کند تا استراتژی امنیت اطلاعات حول ان گسترش یابد. پیروی از قانون خیلی مرسوم است. مردم خیلی درگیر فرآیند آن نیستند به جز اینکه روال‌ها را در طی فرآیندها اجرا کنند.		Damianides, 2005; De Paula, et al., 2005; Gilbert, 2008; Hedström, Kolkowska, Karlsson, & Allen, 2011; Hu, Hart, & Cooke, 2007; McFadzean, et al., 2011; Siponen, 2005b; Siponen, 2006; Smedinghoff, 2005; von Solms, 1998a; von Solms, 1998b;

www.takbook.com

۲-۴-۲ تصویر عمومی

قبلا تصور بر این بود که امنیت اطلاعات باید کاربران و داراییها را از تهدیدهای گوناگون اینترنتی که به سمت کاربران وارد می‌شود حفاظت کند (Huang, Rau & Salvendy, 2010). تصویر عمومی مجبور بود که تصویری امن از محیط اطلاعاتی سازمان به عموم مردم نشان بدهد. این نقش دیگری از متخصصان امنیت اطلاعات بود که استراتژی امنیت اطلاعات را پیاده سازی کنند. تصویر به شکلی به مردم نمایش داده می‌شد که عقیده بر این بود که امنیت نباید قابل مشاهده باشد، اما باید مردم بدانند که پیاده سازی شده است، تا جایی که مشاهده گر باور کند که سازمان امن و مورد اعتماد است (Knapp & Boulton, 2006).

Mintzberg و McHugh (۱۹۸۵) تاکید کردند که استراتژی سازمانی بر روی شکل تمرکز می‌کند اما بادوام نیست. بخشی از نقش تصویر عمومی نمایش پایداری امنیت، تضمین مشتری و کل سازمان از اینکه امنیت اطلاعاتی که به آنها سپرده می‌شود، امن باقی می‌مانند (Jhonson, 2009). امنیت تبدیل به یک رویه خارجی شد که تصویری از امنیت برای مردم ساخت که آنها را از افشا شدن واقعی داده دور نگه داشت (Baskerville, 1993). سازمان بعد از اینکه دچار ضرر تلفات داده شد، بر روی داشتن امنیت تاکید کرد و به جای آن که به اندازه کافی برای پیاده سازی مناسب موارد امنیتی سرمایه گذاری کند، می‌پذیرد که جریمه‌های برآورد شده را بپردازد. هزینه جریمه کمتر از هزینه پیاده سازی درست کنترلهای امنیت بود (Anderson & Moore, 2006).

۲-۴-۳ رقبا

نقش رقبا شامل محک زدن بوده یا رقابتی است که موجب تلاش برای قرار گرفتن در جایگاه بالاتر برای سازمانی است که به بهترین شرایط دست می‌یابد. هر واحدی که رقابت می‌کند، در تلاش است که از لحاظ فراهم کردن امنیت بهتر از دیگران عمل کند (Vannoy & Salam, 2010). امن باقی ماندن مثل مقایسه یک جنگ تسلیحاتی است که استراتژیهایی را ارائه می‌دهد که بتوان بر دشمنان غلبه کرد (Chang & Ho, 2006; Robson, 2005). هر رقیب نوآوری ایجاد می‌کند و اقدامات متقابل نوآوریها توسط دیگر رقبا تولید می‌شود. نمایشی از این موضوع، تاثیر "ملکه قرمز RED QUEEN " است که Robson (2005) آن را توضیح داده که

www.takbook.com

نتیجه رقابت رقبا در برابر یکدیگر بود. این استراتژی تا بدست آوردن بیشترین مقدار سود تلاش می‌کند (Mintzberg, Ahlstrand, & Lampel, 1998; Vannoy & Salam, 2010).

استراتژی امنیت اطلاعات پیشنهاد کند که اهدافی برای دور شدن از بد افزارها داشته باشیم (Chan & Reich, 2007: Chang & Ho, 2006; Mintzberg, Ahlstrand, Lampel, 1998; Tejay, 2008; Vannoy & Salam, 2010). با پذیرش تاثیر "ملکه قرمز RED QUEEN امنیت یک هدف شده و صنعت از آن زمانی سود می‌برد که همه شرکا سعی در حذف تهدیدها داشته باشند. امنیت اطلاعات سعی در سود بیشتر با پیاده سازی مناسب است زیرا رقابت موجب پایین آمدن هزینه شده و نهایتا از تلفات به خاطر نشت داده جلوگیری میکند (Baskerville, 1993; Ohki, et al., 2009; Robson, 2005).

۲-۴-۴ تغییر پیوسته

یک رهبر فکری در زمینه‌های فنی و استراتژیکی سیستمهای اطلاعاتی زیاد شدن آشوب یا تغییرات پیوسته را با فن آوری اطلاعات جدید پیش بینی می‌کند (Costello, 2011).

Costello (2011) بیان کرد که رهبران فن آوری اطلاعات و امنیت اطلاعات باید برای به کار گیری سریع تجهیزات، برنامه‌های کاربردی و خدمات آماده باشند. این تغییرات پیوسته حاکی از آن هستند که جریان عدم دارا بودن قابلیت پیش بینی در محیط یک سازمان نیاز به تغییر استراتژی داشته تا خود را با هر تغییری تطبیق دهند. Siponen & Iivari, 2006

برای کسب و کار، سیستمهای اطلاعاتی و استراتژی امنیت اطلاعات، نیاز است که همگی در برابر تغییر نیازمندیهای مشتریان از طریق ارزیابی‌های سیستم اطلاعاتی و مدیریت اطلاعات واکنش نشان دهند. تغییر پیوسته دشوار می‌شود مخصوصا وقتی که امنیت اطلاعات متناسب با آن نیاز باشد. Slater, 2002 علاوه بر آن اهداف تهدید کنندگان و نرم افزارهایی که به کار می‌برند به سرعت تغییر می‌کنند. Choo, 2011 ممکن است استراتژی نیاز داشته باشد تا تغییرات را از یک دوره چرخشی بلند مدت در زمانهای کوتاهتری انجام بدهد. نظریه تغییرات مداوم، شامل تغییرات غیر خطی و پذیرش بازخوردی است که ممکن است به تغییر جهت برنامه منجر شود، حال چه تغییر ناگهانی بوده (نقاط انشعاب) یا تحولی تدریجی باشد. (Bechtold, 1997)

www.takbook.com

تغییر پیوسته بر روی یک زنجیره کار می‌کند در محدوده بین استراتژی آشکار و استراتژی نوظهور، اما در هیچ یک از دو طرف قرار ندارد.Mintzberg & McHugh, 1985یک شکل از تغییرات پیوسته،ادهوکراسی بود در جایی که یک سازمان در محیطی کار می‌کرد که هم پیچیده و هم پویا باشد Leidner, et al., 2011. همیشه محیط منحصر به فرد بوده و در حال تغییر است Leidner, et al., 2011; Mintzberg & McHugh, 1985. منحصر به فرد بودن در ۵ زمینه تعریف می‌شود، اول اینکه پویا و پیچیده است چون هر خروجی منحصر به فرد است. دوم، خروجیهای مختلف باعث نیاز به استقرار مقادیر برای متخصصان می‌شود. سوم، کارشناسان در تیمهایی قرار دارند تا به مسائل پیش آمده رسیدگی کنند. چهارم، تطبیق متقابل استراتژی از طریق گروه‌های کاری و کمیته‌ها هماهنگ می‌شوند. در آخر، سازمانها توزیع شده و قدرت‌ها توزیع شده تا انجام وظایف توسط کارشناسان در تیمهایی انجام شود .Mintzberg & McHugh, 1985به طور کلی، نقش تغییر پیوسته یکی از تغییرات پیچیده و پویایی است که به طور مداوم در حال رخ دادن است.

۲-۴-۵ بهترین عملکرد

بهترین عملکرد تجاری (BPP) سعی در تضمین نهادینه سازی و پذیرش BBP در سازمان به عنوان یک نقش استراتژیک دارند. سازمان سیاست مقرر را برای رسیدگی به مشکلات امنیتی اجرا می‌کند تا بهترین نتایج را بدست آورد (Dawson, et al. 2010). یکی از روشهایی که پرسنل امنیت اطلاعات در آن پیشرفت کردند، بهترین عملکردهایی بودند که به شکل یک مدل یا روشی برای کاهش ریسک به شکل تکراری انجام می‌شدند (Shariati, Bahmani, & Shams, 2010). Rezakhani، Hajebi و Mohammadi (۲۰۱۱) استانداردسازی را به عنوان روشی از بهترین عملکرد توسعه دادند. آنها استاندارد سازی را در صنعت و نمونه‌های ارجاع داده شده پذیرش استاندارد از طریق برنامه‌هایی همچون کتابخانه زیرساخت تکنولوژی اطلاعات (ITIL)، سیستم مدیریت امنیت اطلاعات (ISMS) مدل مدیریت بلوغ امنیت اطلاعات (ISM3)، سازمان بین‌المللی استانداردسازی (ISO) و کنسرسیوم مهندسی بین‌المللی (IEC) مطلوب کردند (Rezakhani, Hajebi, & Mohammadi, 2011). استفاده از روشهایی همچون چک لیست، مدلهای بلوغ قابلیت و دیگر عملکردها در محدوده محیطهای بهترین عملکرد هستند (Baskerville, 1993; Shariati, Bahmani, & Shams, 2010; von Solms & von Solms, 2005; Zuccato,. مدل بهترین عملکرد را مطابق ۵ سطح بلوغ قابلیت نشان می‌دهد

www.takbook.com

Ahuja, 2009; Kayworth & Whitten, 2010; Luftman & Ben-Zvi, 2010; Xiao-yan,) .(Yu-qing, & Li-lei, 2011

انتظارات کاربر نهایی از بهترین عملکرد هامی‌تواند در محرمانگی داده مشتری، تضمین دقت داده خلاصه شوند (Jhonson, 2009). در مورد سازمان، اعتماد عمومی بهترین عملکرد پیاده سازی شده‌ای است که می‌تواند برای افزایش اطمینان بین شرکا و برآورده کردن نیازمندیهای اعمال شده شرکا استفاده شود (Jhonson, 2009). همچنین هزینه‌ها باید در نظر گرفته شوند چرا که بده بستانی بین واقعا امن بودن و دستیابی غیر امن به BBP وجود دارد که هنوز مانع از هزینه‌های گزاف بر روی امنیت می‌شود. در نهایت، بهترین تمرینها نقشه استراتژیک کلی را برای اهداف تجاری با فراهم کردن بازگشت سرمایه کوتاه و بلند مدت، برآورده می‌کنند.

۲-۴-۶ سازماندهی مجدد

با استفاده از توجیه تغییر سازمانی به عنوان یک بحث، دوباره سازمان دهنده تحت فرض قبلی کار می‌کند که از زمانی که نقص امنیت ایجاد شده، مدیریت نیاز به تغییر در ساختار گزارش دهی سازمان دارد؛ با این امید که واکنشهای منفی را دور کرده یا یافته‌های ممیزی را کاهش داده تا سازمان دوباره سازماندهی شود (Cecere, 2011). چندین بخش به عنوان مشارکت کننده در خرابی بیان شده‌اند که استراتژی در بین آنها قرار دارد (Rose, 2011). مشکل اصلی در استفاده از استراتژی امنیت اطلاعات به عنوان یک ابزار برای تحریک تغییر ساختاری و سازمانی (Aivazian, 1998) این بود که مدیریت ممکن است سعی در استفاده از استراتژی امنیت اطلاعات به عنوان وسیله‌ای برای تشویق تغییر سازمانی بکند (Aivazian, 1998; Kotulic & Clark, 2004). بعضی ادارات در یک سازمان ممکن است ثابت کنند که کارکنان کافی برای برآورده کردن یافته‌های بازرسی ندارند. توصیه‌ای برای انتساب مجدد افراد اطراف سازمان به توزیع مجدد و بهبود نظری کارآیی استراتژی امنیت اطلاعات کمک می‌کند. چارت سازمانی اولین کار دستی بود که با استراتژی امنیت اطلاعات برای ارتباط ساختار و ماموریت استراتژی امنیت اطلاعات استفاده شد (Norman & Yasin, 2010).

استفاده مثبت از سازماندهی مجدد، در مواردی مثل دسترس پذیری منابع می‌تواند دیده شود و می‌تواند برای تضمین پرسنل، نرم افزار و سخت افزار شایسته دوباره توزیع شود و بودجه امنیت اطلاعاتی کافی برای بخشهای مناسب سازمان پرداخته شود (Jhonson, 2009). استفاده

www.takbook.com

مثبت دیگر از سازماندهی مجدد این است که می‌تواند با مرور اولیه بی تاثیر توسط مدیریتی باشد که نیاز به تغییر جهت داراییها به سمت هدف فناوری اطلاعات امن باشد (Emery, 1991).

۲-۴-۷ ارتباطات قدرت

قدرت می‌تواند توسط استراتژی اعمال شود، راهی را در یک سازمان به سمت آن حرکت می‌کند را راهبری کند (Backhouse, Hsu, & Silva, 2006). افرادی از استراتژی امنیت اطلاعات برای اعمال خواسته‌ها و تحریک کارمندان به پیروی از آنان استفاده می‌کنند. به عنوان روشی که در آن استراتژی امنیت اطلاعات می‌تواند به خوبی به عنوان یک ابزار قدرت در سازمان از آن استفاده شود (Mintzberg, 1985; Salancik & Pfeffer, 1977). در گذشته تفهیم شده بود که با مهارت به کار بردن قدرت برای دستیابی به اهداف امنیت اطلاعات برای افزایش قدر و قیمت کلی امنیت است. استفاده از قدرت برای وادار کردن افراد و سازمانها ممکن است باعث رسیدن به اهداف کوتاه مدت شود اما معمولا برای امنیت در طی زمان ناموثر است (Backhouse, et al., 2006; Dhillon, 1995; Dhillon, 2004; Dhillon, Caldeira, & Wenger, 2011). قدرت و قابلیت حسابرسی می‌تواند بر روی توسعه و پیاده سازی امنیت اطلاعات اثر بگذارد. کمبود استراتژی امنیت اطلاعات موثر، منجر به سیاست امنیتی غیر موثر شده که در نتیجه منجر به بی تاثیر شدن امنیت اطلاعات می‌شود (Lapke, 2008; Loveland & Lobel, 2012). اثرات جانبی ناشی از استفاده از قدرت نشان دادند که استفاده از قدرت بر روی پرسنل اثر منفی گذاشته و، تاثیر مطلوبی بر روی اینکه شخصی به درستی رفتار کند، نمی‌گذارد. در عوض زمانی که از دلایل مثبت استفاده می‌شود، کاربران مثبت تر پاسخ می‌دهند (Herath & Rao, 2009).

۲-۴-۸ پیروی از قانون

پیروی از قانون به استفاده از قوانین و مقررات فدرال نگاه کرده است تا کل استراتژی امنیت اطلاعات را در مرکزیت قرار دهد. پیروی از قانون خیلی جهت گرایانه است (da Veiga & Eloff, 2007). مردم به جز اجرای بعضی از روال‌ها و ذخیره نتایج در فرآیند خیلی درگیر این فرآیند نبودند (Hedström, et al., 2011). یک مقاله بیان کرده که در نتیجه نشت داده، چندین مصوبه و قانون برای تضمین تبعیت باید گذرانده شده و به تصویب برسند

www.takbook.com

(Smedinghoff, 2005). پیاده سازی کنش گرایانه کنترل‌ها، پیش درآمدی بر پیروی از قانونی است که بعد از آشفتگی اولیه فعالیت برای توافق است، سازمان به کسب و کار عادی خود بازگشته و امنیت در خط مقدم قرار ندارد (Damianides, 2005; Scully, 2011). مقاله دیگری بیان کرد که کنترلهای فناورانه خوب هستند تا زمانی که مردم درگیر فرآیند آنها نیستند (Hedstom, et al. 2011). اگر مردم، سیاستها و فرهنگ در آن دخیل شوند ریسک امنیتی وجود دارد (Hu, Hart, & Cooke, 2007).

یکی از جنبه‌های مثبت پیروی این بود که این مساله مدیریت ریسک را با کاهش ریسکی که می‌تواند از طریق نشت داده رخ دهد، تضمین می‌کند. تضمین کردن دقیق داده شرکت منجر به تصمیمات آگاهانه مدیریتی می‌شود (Hong, Chi, Chao, & Tang, 2003). تابعیت از قانون منجر به حفاظت از مزاحمان داخلی، آسیب تصادفی یا غرض‌ورزانه از طرف کارمندان و باز داشتن از حملات بالقوه می‌شود (Jhonson, 2009).

۲-۴-۹ خلاصه نقشها

متون تحقیقی شامل اطلاعاتی هستند که منجر به ایجاد هشت دسته بندی ممکن برای نقشهایی شدند که یک متخصص امنیت اطلاعات می‌تواند در نظر بگیرد. در این فصل نقشهای ممکنی که می‌توانستند از این متون دریافت شوند مورد بررسی قرار گرفتند. جستجو در فرآیند انتخاب نقش و تنظیم ممکن داخل یک سازمان بخشی از یک فرآیند توسعه استراتژی امنیت اطلاعات بود (von Solms, 2001). فصل بعدی روش تحقیق منتخب برای جمع آوری دقیق داده و تحلیل آنها برای نظری کردن انتخاب نقشها در انجام ماموریت برنامه امنیت اطلاعات به جزئیات بررسی خواهند شد.

www.takbook.com

فصل سوم

روش تحقیق

www.takbook.com

۳-۱ مقدمه

از بین روشهای موجود برای مطالعه (کیفی، کمی و ترکیبی) در این مطالعه از روش کیفی استفاده خواهیم کرد. به این دلیل روش کمی را انتخاب نکردیم زیرا تعداد کارهای گذشته بر روی استراتژی امنیت اطلاعات و مقیاس اندازه گیری مدلهای شناخته شده کمیاب هستند. دلیل اینکه روش ترکیبی را انتخاب نکردیم زیرا که این روش نیاز به وجود موجودیت‌های قابل اندازه گیری دارد اما هیچ معیار تجربی معینی برای استراتژی امنیت اطلاعات وجود ندارد. انتخاب روش کیفی بر روی این حقیقت تمرکز می‌کند که اطلاعات بر روی استراتژی امنیت اطلاعات کمیاب بوده است (Lapke, 2008; Loveland & Loebel, 2012.). همینطور روشهای تحقیق برای مدلهای به کار گرفته شده و نظریه‌ها حداقل هستند. نظریه جمع آوری داده بنیادی اجازه تحلیل داده را می‌دهد، که این امر با استفاده از روشهای تفسیری مصاحبه‌ها و ساخت مجموعه داده‌ها به دست می‌آیند (Allan, 2003; Corbin & Strauss, 2008). داده‌های زیادی جمع آوری و به طور مفهومی تحلیل شد تا از طریق یک راهکار نظریه بنیادی توسط روش نمونه برداری نظری، کاربرد سازمانی نقش استراتژی امنیت اطلاعات درک شود(Glaser 2000; Lee & Hubona, 2009; Pauleen, Corbitt, & Yoong, & Strauss, 1967; Javinen, 2007; Ransbotham & Mitra, 2009; Yoong, 1996). جمع آوری، تحلیل و مقایسه وسیع داده‌ها دقت را تضمین می‌کند (Lee & Hubona, 2009).

نظریه بنیادی با جمع آوری مصاحبه‌ها و مشتقات به صورت قیاسی کار می‌کند، سپس از طریق مراحل کد گذاری بر روی آنها کار می‌شود تا یک نظریه نوظهور ایجاد شود (Pandit, 1996). مراحل با مصاحبه‌ها و یادداشت برداری شروع می‌شود؛ مصاحبه‌ها با استفاده از روشهای (باز، محوری و انتخابی) کد گذاری می‌شوند؛ و نظریه ایجاد می‌شود (Allan, 2003; Jones & Alony, 2011; Glaser, 2012b; LaRossa, 2005; McFadzean, et al., 2007). در هر گام با کامپایل داده‌های جمع آوری شده و تحلیل داده‌ها، فکر، روال و فرآیند دریافت شده از طریق یادداشت برداری، فهم و دیدگاه‌ها میسر شد. (Charmaz, 2006; Corbin & Strauss, 1990; Corbin & Strauss, 2008; Glaser & Strauss, 1967; Pauleen, Corbitt, & Yoong, 2007; Rich, 2012).

برای مواردی که در حوزه تحت مطالعه، تحقیقات زیادی وجود نداشته و طبیعت مطالعه شامل تجربه انسانی و تعاملات بین آنها برای جمع آوری داده است، نظریه بنیادی خیلی مفید

www.takbook.com

می‌باشد (Corbin & Strauss, 2008; Yoong, 1996). هدف از این مطالعه بررسی ارتباطات بین استراتژی امنیت اطلاعات و نقش(های) ضروری برای اجرای برنامه امنیت اطلاعات به منظور برآورده کردن نیازمندیهای سازمانی امنیت اطلاعات است. همچنین اگر خروجی‌های روش نظریه بنیادی باعث ساخت یک راهکار رسمی برای انتخاب استراتژی امنیت اطلاعاتی شود که فرای پیاده سازی کنترلهای تکنیکی بشود، برای متخصصان امنیت اطلاعات مفید می‌تواند باشد. علاوه بر این، اگر یک مدل بتواند برای انتخاب نقش پیش بینی کننده عمل کند، تشکیل راهکاری کنشگرا برای استراتژی امنیت اطلاعات می‌تواند سودمند باشد. جزئیات بیشتری در مورد تجربیات دقیقی که از طریق مراحل فرآیند جمع آوری داده انجام شده است در بخشهای بعدی: کد گذاری باز، کد گذاری محوری، و کد گذاری انتخابی ارائه می‌شود.

۳-۲ روش تحقیق

روش نظریه بنیادی که در این مطالعه استفاده شده است با تقویت کاوش اطلاعات در اینکه، چگونه یک متخصص امنیت اطلاعات برای انتخاب نقشها تحت تاثیر قرار می‌گیرد و برای اجرای برنامه‌های امنیت اطلاعاتش چه انتخاب‌هایی می‌کند. سوال و جستجوی مصاحبه برای داده به چگونگی رخ دادن ساخت استراتژی امنیت اطلاعات دیدگاهی می‌دهد (Duffy, Ferguson, & Watson, 2004; Wimpenny & Gass, 2000). تحلیل داده منجر به فهم این می‌شود که آیا نوع خاصی از استراتژی نسبت به استراتژیهای دیگر ارجح‌تر است و چگونه نسبت درک آنها به مجریان در بخشهای مختلف سازمانی مثل کسب و کار، سیستم اطلاعاتی و امنیت اطلاعات با هم فرق دارند (Fitzgerald, 2010; Johnson, 2009). همچنین اینکه چگونه پرسنل امنیت اطلاعات بین انواع استراتژی امنیت اطلاعات تمایز قائل می‌شوند، در تاکید این مساله کمک می‌کند. فصل ۲ روش ممکن برای فرآیند انتخاب یک نقش برای اجرای استراتژی امنیت اطلاعات را ارائه کرد. فصل ۴ فرآیند انتخاب را پوشش می‌دهد تا نشان دهد که آیا نقش بهینه‌ای برای یک راهکار امنیت اطلاعات وجود دارد یا خیر. هدف این مطالعه استنتاج یک نظریه از داده‌های جمع آوری شده و تحلیل شده و ارائه یک نظریه نوظهور (Eisenhardt & Graebner, 2007; Glaser, 2012a; Goldkuhl & Cronholm, 2010;Pandit, 1996; Scott & Howell, 2008) است. داده‌ها از طریق مشتقات، مصاحبه، مشاهدات و مستندات جمع آوری شد و سپس کد گذاری صورت گرفت و تحلیل شدند تا

www.takbook.com

نظریه‌ای ایجاد شد که برای اعتبار سنجی بیان مساله و سوالات تحقیق مورد استفاده قرار گرفت (Huehls, 2005; Lee & Hubona, 2009;Wimpenny & Gass, 2000). مفاهیم نوظهور از مراحل کد گذاری در مفاهیم به دسته‌هایی گروه بندی شدند وسپس دسته‌ها یکی شدند تا یک نظریه را تشکیل دهند (Corbin & Strauss 2008;Huehls, 2005). سپس یک نظریه راه‌های انطباق پذیری از نظریه سازی را نشان می‌دهد که چگونه متخصصان امنیت اطلاعات یک نقش را برمی‌گزینند (Fitzgerald, 2010; Siponen, 2005).

به عنوان یورش اولیه در استراتژی امنیت اطلاعات با استفاده از نظریه بنیادی مفید است که فرآیند انتخاب نقش استراتژیک کیفی سنجی توسط سازمان را کشف کرد که ممکن است اثر مثبتی بر روی کارآیی سازمانی داشته باشد. اولین دستاورد یک نظریه به یک سازمان اجازه می‌داد تا نیاز، انتخاب و احتمالا پیاده‌سازی یک استراتژی امنیت اطلاعات را ارزیابی کند. اولین گام برای این فرآیند جمع آوری داده است که در بخش بعدی چگونگی جمع آوری داده‌ها نمایش داده می‌شود.

۳-۳ جمع آوری داده ارائه شده

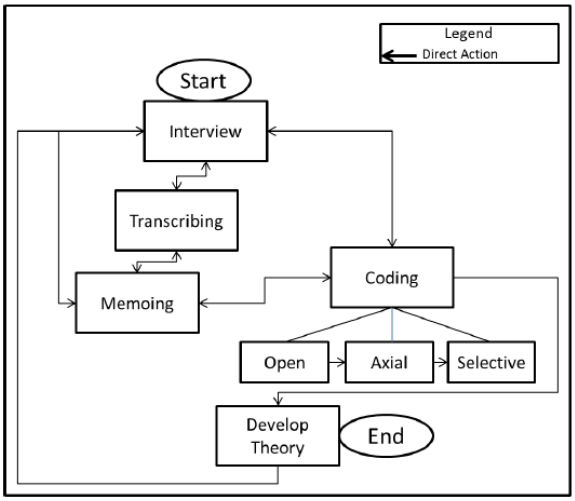
فرآیند جمع آوری داده شامل چندین مرحله در روش نظریه بنیادی است. در شکل ۱ مراحل مورد نیاز برای رسیدن به یک نظریه از روی داده‌های جمع آوری شده نشان داده شده است. برای شروع، محقق مصاحبه‌هایی را با شرکت‌کنندگان انجام می‌دهد. بعد از اینکه مصاحبه‌ها صورت گرفت، توسط محقق رونویسی و مرور شده تا از کامل بودن اطلاعات دریافت شده و منتقل شده برای چاپ در رسانه اطمینان حاصل شود (Duffy, et al., 2004; Wimpenny & Gass, 2000). در طی فرآیند یادداشت برداری، محقق نکات مهمی را که توسط شرکت کننده بیان شدرا به صورت یادداشتهای کوچکی ذخیره کرده تا در فرایند مورد نظر از آن استفاده کند (Charmaz, 2006; Corbin & Strauss, 2008; Stocker & Close, 2013). چرخه بین مصاحبه و یادداشت برداری موجب جمع آوری داده‌های مربوط به بخش مصاحبه شده و منابع دیگر برای جمع آوری داده شامل مشاهدات محقق از محیط کاری شرکت کنندگان می‌باشد (Backman & Kyngaes, 1999; LaRossa, 2005). مشتقات مستند در محدوده مستندات استراتژی، روال‌های اجرای استاندارد و نامه‌های داخلی شامل ماموریت و اهداف توسط محقق جمع آوری می‌شود که موجب کامل شدن داده‌های جمع آوری شده در

www.takbook.com

طی مصاحبه‌ها با مجریان می‌شود. روالی که در مصاحبه انجام می‌شود شامل دریافت اطلاعات و کد گذاری آنها به صورت داده‌های قابل استفاده برای ساخت یک نظریه است (Charmaz, 2006; Corbin & Strauss, 2008).

با نظریه بنیادی تعداد خیلی کمی راهنما با در نظر گرفتن بهترین تعداد موارد برای مصاحبه‌ها وجود دارد (Eisenhardt, 1989; McFadzean, et al., 2007; McFadzean, et al., 2011). در یک منبع برای جایی که داده‌های قبلی تقریبا موجود نیستند، توصیه شده حداقل از پانزده تا بیست مورد برای نظریه بنیادی نمونه برداری شود (Corbin & Strauss, 2008; Creswell, 2011). منبع دیگری توصیه کرده است که این مقدار تقریبا دو برابر (بین ۲۰ تا ۳۰ مورد) باشد (Creswell, 2002). Charmez (۲۰۰۶) از این هم فراتر رفت و بیان کرد که وقتی که تعداد شرکت‌کنندگان کم و حداکثر ۳۰ شرکت کننده مختلف می‌باشد، محقق باید از شرکت-کنندگانش تحقیق و تفحص کند و به مصاحبه‌ها بیفزاید تا به حد اشباع برسد. اشباع زمانی رخ می‌دهد که با جمع آوری و تحلیل قیاسی داده‌ها به نقطه‌ای برسیم که هیچ دسته یا حوزه جدیدی از بحث با مامور ارشد امنیتها یا خوشه چینی داده از مستندات بدست نمی‌آید. زمانی که تخمین زده شد که به اشباع رسیدیم، دیگر نیازی به انجام مصاحبه‌های بیشتر نیست (Charmaz, 2006). محقق در این مطالعه از بیست و پنج نفر شرکت کننده تحقیق کرد که آنها از یک سازمان مالی بزرگ بودند و این کار را به چندین نفر که در دولت فدرال کار می‌کردند نیز گسترش داد، برای این منظور از ۷ فرمانده امنیت اطلاعات (مامور ارشد امنیت) دیگر برای رسیدن به اشباع در دسته‌بندی‌های مصاحبه صورت گرفت.

www.takbook.com



شکل ۱. ایجاد یک نظریه مستدل

Start – شروع
Interview– مصاحبه
transcribing– رونوشت برداری
memoing-یادداشت برداری
coding-کدگزاری
open-باز
axial-محوری
selective– انتخابی
Develop theory– ایجاد نظریه
endپایان
Legend – راهنمای نقشه
Direct actionفعالیت مستقیم

محقق در سازمان حضور پیدا کرده و از شرکت‌کنندگان سطح اجرایی درخواست کرد که در مصاحبه شرکت کنند و از آنان خواسته شد که کپی‌هایی از مستنداتشان که حاوی استراتژی و تکمیل هدف ماموریتشان است به همراه داشته باشند و از سازمان مربوطه اجازه گرفته شد که بتوان عملیات آنها را برای یک مدت زمانی به صورت روزانه در سازمانشان مورد مشاهده قرار دهد (Backman & Kyngaes, 1999; LaRossa, 2005). این مطالعه محقق هیچ مداخله-ای با وظایف حرفه‌ای نداشته و کاملا به صورت گمنام از نظر مقام و مکان در سازمانها عمل کرده است. مصاحبه اولیه از ۱۳ مامور ارشد امنیت و ۲۵ معاونینشان از واحدهای یک سازمان

www.takbook.com

بزرگ تشکیل شد. از هفت مامور ارشد امنیت دیگر و یا معاونینشان از سازمانهای دیگر به منظور رسیدن به اشباع استفاده شد (Charmaz, 2006; Corbin & Strauss, 2008). که برای این منظور از ۴ سازمان دیگر برای رسیدن حد اشباع استفاده شد (Charmaz, 2006).

مامورهای ارشد امنیت زیر واحدهای امنیت اطلاعات اولین مصاحبه شوندگان برای مطالعه نظریه بنیادی بودند.

Jhonson (۲۰۰۹) تاکید کرد که بهترین ترکیب داده، از مجریان با یک مقام یکسان که از سطوح هم نظیر سازمان می‌آیند. زیرا نقاط دید افرادی با سطح یکسان، پس زمینه‌ای مشابه در امنیت اطلاعات در کل سازمان را می‌توان مشاهده کرد (Jhonson, 2009). همچنین، نقشهایی که آنها برای برآورده کردن نیازمندیهای امنیت اطلاعات در واحد سازمانیشان ضروری پنداشته بودند را می‌توان بررسی کرد. باید توجه داشت اگر سطحی در یک بخش سازمانی لازم دیده شود ممکن است در سازمانهای دیگر ضروری پنداشته نشود (Chen et al, 2010). هر سازمان نیازمندیهای ماموریتی متفاوتی دارد. مصاحبه‌ها داده‌های کلیدی را از دیدگاه مدیران سطح بالا برای موضوع استراتژی و نقشهای استراتژیک ایجادکرد " با کشف اینکه مدیران در حال چه اندیشه ای هستند، چرا آنها آن گونه عمل کردند و آنها برای تکمیل مفاد سازمانی چه می‌خواستند" (Vannoy & Salam,2010).

برای اندازه گیری مدت زمان مورد نیاز در هر سایت مورد استفاده برای نظریه بنیادی محقق تعداد، مکانها و بخشهای سازمان مالی بزرگ را بررسی کرد (Corbin & Strauss, 2008; Glaser, 2002). سازمان اصلی که مورد پوشش قرار داده شد به " Branch of the Fatherland شعبه زمین پدری" نامیده شد که شامل ۱۳ زیر واحد کوچکتر بود که هر کدام بخشی از ماموریت کلی سازمان بزرگ را انجام می‌دادند. از این ۱۳ زیر واحد، تعدادی از مامورهای ارشد امنیت و معاونینشان انتخاب ومصاحبه شده و عملیات مستند سازی صورت گرفت. یک خلاصه اظهار نامه ماموریت سازمانی پاکسازی شده از هر واحد جمع آوری شد که بیانگر اطلاعاتی در مورد تعداد، مکان (ها) و ترکیب آنها بود (Pitt, Parent, Junglas, Chan, & Spyropoulou, 2011)، که فقط یک واحد اجازه نداد که اطلاعاتی در این مورد ارائه دهد. برای توضیحات در مورد هر زیر واحد به جدول ۴ مراجعه کنید. پیچیده‌ترین بخش جمع آوری داده در زمان مصاحبه از شرکت‌کنندگان بود. چندین نوع مصاحبه وجود دارد شامل مصاحبه شبه ساختار یافته و مصاحبه پایان باز که می‌توان از بین آنها انتخاب کرد (Allan, 2003; Duffy, et al.,

www.takbook.com

(2004; Wimpenny & Gass, 2000). مصاحبه شبه ساختار یافته،نیاز به محدود کردن اطلاعات بخشی از برنامه کلی امنیت اطلاعات را موثرتر نشان می‌دهد (Charmaz, 2006,Corbin & Strauss, 2008; Duffy, et. al., 2004). دلیل این موضوع این که مصاحبه با پایان باز منجر به جمع آوری حجم عظیمی از داده‌هایی می‌شود که به مطالعه مربوط نیستند و از طرف دیگر مصاحبه ساختار یافته ممکن است موجب جهت گیری بیش از حد شود (Duffy, et al., 2004; Wimpenny & Gass, 2000). بنابراین استفاده از مصاحبه‌های شبه ساختار یافته انتخاب شد.

محقق از پرسنل مجری در زمینه امنیت اطلاعات در زیر واحدهای یک سازمان مالی بزرگ خواست که شرکت کنند. شرکت‌کنندگان موافقت کردند که به سوالات پاسخ دهند و به آنها اطمینان داده شد که پاسخ‌هایشان بدون نام و محرمانه باقی خواهد ماند. به منظور داشتن مصاحبه‌های نامتناقض با همه شرکت‌کنندگان، محقق قوانین پایه مصاحبه در به کار گیری فرم رضایت انجمن مرور سازمانی Institutional Review Board (IRB) را پذیرفت تا به شرکت‌کنندگان مرجعی دهد که تعاملات را در یک محدوده با کران حفظ کند (Allan, 2003; Corbin & Strauss, 2008).

محقق برای هر مصاحبه، از پاسخ به سوالات با ذکر جزئیاتی که رخ می‌داد یادداشتهایی برداشت. فهرست بحثها، یادداشتهای مصاحبه را طبقه بندی کرده تا به محقق در انجام تحلیلها کمک کند. بیشتر مجریان تمایل داشتند که افکارشان را سطح پایین قرار دهند تا گزارشها، مستندات برای مصاحبه‌ها حفظ شود (Jhonson, 2009). با در نظر گرفتن عوامل درک شده توسط آنها با استراتژی امنیت اطلاعاتی که توسط مدیریت سازمان برای آنها فراهم شده و برای بیان انگیزه‌شان از دلسوزی برای امنیت اطلاعات، زمان زیادی در طی مصاحبه صرف شد تا به شرکت‌کنندگان اجازه داده شود افکارشان را شکل دهند (Charmaz, 2006). نکات از طریق یاداشت برداری در اولین فرصت ممکن بعد از انجام مصاحبه صورت می‌گرفت (Duffy, et al., 2004; Wimpenny & Gass, 2000). همچنین محقق تفسیرهای اولیه را بلافاصله بعد آن می‌نوشت (Stocker & Close, 2013). در حالی که هر تلاشی انجام شد تا داده‌های زیادی در طی جلسه اولیه جمع آوری شود، اما این گزینه نیز باز نگاهداشته شد تا در صورت لزوم جلسات متعددی با همه شرکت‌کنندگان در آینده نیز صورت گیرد. (Charmaz, 2006; Corbin & Strauss, 2008).

www.takbook.com

چندین سوال مستقیم و غیر مستقیم از مصاحبه شوندگان پرسیده شد. در این روش از طریق سوالات با انتهای باز در یک مصاحبه شبه ساختار یافته، اطلاعاتی را از مجریانی که در محیط واقعی امنیت اطلاعات کار می‌کنند دریافت می‌شد زیرا که آنها پشتیبان ماموریتهای کسب و کار، سیستمهای اطلاعاتی و سیستمهای امنیت اطلاعات بودند(Allan, 2003; Charmaz, 2006; Corbin & Strauss, 2008; Duffy, et al., 2004). محقق سوالات را با کاوش برنامه ریزی کرد اما هدف او بر پیش انتخاب نقشها، تنظیم‌ها، یا ساختن یک استراتژی نبود. منبع سوالات مصاحبه از دانش کسب شده و بر اساس متون در دسترس و مرور شده در فصل ۲ است. سوالات بر روی کشف چگونگی اینکه مصاحبه شونده نقش خود را در سازمان ایجاد می‌کند متمرکز شده بود. همچنین، در بحث مطلوب بود که مصاحبه شونده بتواند دلایل خودش را برای گرفتن نقشهای خاص بازگو کند. جدول ۵، سوالات استفاده شده، منابع سوالات و اساس شکل گیری یک پاسخ در طی مصاحبه را لیست کرده است. طبیعت نمونه برداری نظری به شرکت‌کنندگان اجازه داد و آنها را تشویق کرد تا در پاسخ‌هایشان آزاد باشند و مسیر خاصی را در بازگویی فهمشان از پیچیدگی ایجاد استراتژی امنیت اطلاعات در سازمانهای مالی دنبال نکنند و چرا نقشهای فردی متفاوت برای اجرای امنیت اطلاعات در واحد سازمانیشان به کار گرفته می‌شود (Corbin & Strauss, 2008). محقق از شرکت‌کنندگان سوالاتی کرد تا جوابها را شفاف سازی کرده و بتواند از پاسخهای انتها باز استنباط کند. در طی فرآیند جمع آوری داده، محقق از رسیدن به نتیجه با شرکت‌کنندگان اجتناب کرد (Corbin & Strauss, 1990; Corbin &Strauss, 2008). تصمیم آگاهانه‌ای که بر روی واقعیت متمرکز شده باشد برای حذف هر درک از پیش پرورش داده شده‌ای استفاده شد (Allan, 2003; Kwok, McCallin, & Dickson, 2012). حفظ فاصله از منابع داده، در جایی که بیشتر شبیه مشاهدات کمی با داده‌های تجربی باشد کمک کرد تا از ایجاد نظریه‌ای که خیلی به داده‌ها وابسته باشد جلوگیری کند (Corbin & Strauss, 2008; Eisenhardt, 1989). هیچ فهرست از پیش درک شده‌ای در جمع آوری پاسخ به سوالات تحقیق یا مساله تحقیق راهنمایی نمی‌کنند (Allan, 2003). مصاحبه‌های انجام شده به این شکل، سختگیری در فرآیند جمع آوری دارند که تضمین می‌کند محقق از جهت‌گیری اجتناب کرده است (Allan, 2003; Corbin & Strauss, 2008; Kwok, et al., 2012).

www.takbook.com

جدول ۴. ویژگیهای زیر واحد شرکت کننده

نام	اندازه (پرسنل امنیت اطلاعات)	بیانیه ماموریت
AXXX	۲۲	مراقبت از سیستمهای بانکداری و پرداخت Fatherland برای تضمین جامعیت. همچنین حفاظت از رهبران مالی، مقامات عالی، مکانهای خاص و رویدادهای Fatherland
UHJY	۲۱۰	به عموم مردم با پاسخگویی، بازیابی و ترمیم تمامی ریسک‌ها کمک می‌کند. به Fatherland کمک می‌کند تا برای موارد اضطراری آماده باشد.
FRT	**	مراقب سیستمهای حمل و نقل Fatherland بوده تا رفت و آمدهای پرسنل آزادانه انجام شوند.
UKO	۱۳۵	قوانین ملی و مدنی Fatherland را برای مرزها، گمرک، معاملات و مهاجرتها اجرا می‌کند.
ERF	۱۷۱	مهاجمان و گروه‌های کمکی به مهاجمان را خارج از Fatherland نگه می‌دارد. تضمین می‌کند که تمامی معاملات عادلانه انجام شده و تمامی قوانین بروکراسی انجام می‌شوند.
CFTY	۲۴۰	نگهبانی ازFatherland در برابر ورود غیر مجاز.
GHY	۵	هر زیر واحد را به طور مستقل برای بهترین اجرا و کارآیی با مشخص کردن حوزه‌ای بهبود و راههای رسیدن به مطلوبیت را اعتبار سنجی می‌کند.
GHJK	۱۴	آموزش نیروهای قانونی برای کمک به آموزش مهارتهایی در مورد ایمنی عمومی تسهیل می‌کند.

www.takbook.com

نام	اندازه (پرسنل امنیت اطلاعات)	بیانیه ماموریت
ERFT	۱۷۷	تضمین می‌کند اصول را آموزش داده و فواید Fatherland به همه پرسنل اطلاع رسانی شده است.
WFRT	۱۰۲	کمک به تضمین جلوگیری از ریسک در سازمان و صنعت Fatherland با روش امنیتی برای تهدیدات فیزیکی و سایبری
WER	۳۹	در همه سطوح دولت تحقیق و توسعه را اجرا می‌کند تا تکنولوژیهای نوظهور را برای حمایت و حفاظت از Fatherland پیدا کند
NKOP	۱۸۱	مسئول سیستمها و تجهیزات فناوری اطلاعات و تعیین و تعقیب معیارهای کارآیی
WDC	۲۱	مسئول حفاظت اطلاعات و آگاهی از مورد سوء استفاده قرار گرفتن

نکته *: نامهای خاص و برخی جنبه‌های عملیاتی برای جلوگیری از فاش شدن، تغییر یافته‌اند.

نکته **: در زمان جمع آوری، FRT فاش نشدن کامل عکسهای پرسنل امنیت اطلاعات را ضروری پنداشت.

www.takbook.com

جدول ۵. اساس شکل گیری سوالات مصاحبه

سوال	منابع	اساس شکل گیری
به نظر شما، استراتژی امنیت اطلاعات چیست؟	Baskerville &Dhillon, 2008; White & Bruton,2011	یافتن و استنباط سطح فهم شرکت کننده از موضوع استراتژی و به ویژه استراتژی امنیت اطلاعات
استراتژی امنیت چه مفهومی برای شما دارد؟ و چه مفهومی برای سازمان شما دارد؟	Hall, Sarkoni, &Mazzuchi, 2010	بیشتر مبتنی بر عقیده است برای استنباط این است که چگونه شرکت کننده کار کرده و چگونه از طریق استراتژی خودش را در راه حمایت از ماموریت کسب و کارش می-بیند.
شما چه نقشی در انجام استراتژی امنیت اطلاعات دارید؟	Johnson, 2009; Johnson & Lederer, 2010	سعی در اینکه شرکت کننده نقش اجراییش را در سازمان ارزیابی کند. مستقیم‌ترین سوال برای معین کردن درک شرکت کننده از نقشش است.
آیا شما می‌توانید بیان کنید که چگونه در امنیت اطلاعات به اولویتهای استراتژیکتان می‌رسید؟	Mintzberg & Waters, 1985	تلاش در بدست آوردن دیدگاهی به فرآیند انتخاب آنها و اینکه چگونه با جهت رهبریشان برای ایجاد استراتژیک کار می‌کنند. شرکت کننده، فعالیتهای خود را ارزیابی کرده و آنها را با اولویت‌هایی که برای رسیدن به موفقیت نیاز است، تطبیق می‌دهد.
آیا شما می‌توانید مدل (زیرساخت یا سیستم) استراتژی امنیت اطلاعاتتان را توضیح دهید؟	Mintzberg & Waters, 1985	تلاشی برای کسب دیدگاهی که شرکت کننده از استراتژی امنیت اطلاعات دارد و اینکه در چه جایی برای استراتژی

www.takbook.com

		سازمانی و سیستم اطلاعاتی مناسب است. شرکت کننده نقشی در برآورده کردن اهداف بیرونی بازی می‌کند.
آیا شما می‌توانید توصیف کنید که چگونه پیاده سازی استراتژی امنیت اطلاعات پیگیری می‌شود؟	McFadzean, et al., 2007; Johnson, 2009	سوالی که سعی در فهم این دارد که آیا آنها معیار معینی دارند یا اینکه چگونه موفقیت رسیدن به اهداف و مقاصدشان را در یک برنامه سازمان دهی شده اندازه گیری می‌کنند. با در نظر گرفتن یک نقش، شرکت کننده راه به سمت موفقیت را دنبال می‌کند و مسیر آن را حفظ می‌کند.
با فکر در مورد استراتژی امنیت، چگونه شما اولویتها را در یک سازمان بزرگ مدیریت می‌کنید؟	Gavetti & Rivkin, 2005	آیا شرکت کننده استراتژی را دنبال می‌کند و از آن به عنوان یک ابزار استفاده می‌کند یا برنامه به درستی که نوشته شده بوده است، کار نمی‌کند. همچنین این سوال نشان دهنده نقش شرکت کننده در توانایی اجرای اولویتها است.
آیا شما می‌توانید توضیح دهید که چه قابلیت‌هایی برای داشتن یک استراتژی امنیت اطلاعات موفق لازم است؟	McFadzean, et al., 2007; McFadzean, et al., 2011	تلاش و استنباط اینکه دیدگاه شرکت کننده از موفق بودن با یک استراتژی امنیت اطلاعات چیست. چگونه آنها به این استراتژی نزدیک شده و چه نقشی را برای موفق شدنش در نظر می‌گیرند.

نکته: برخی منابع از مطالعه استراتژی سیستمهای امنیتی و کسب و کار هستند همانطور که اصول راهبردی برای استراتژی امنیت اطلاعات نیز به کار می‌رود.

www.takbook.com

نمونه برداری نظری به محقق این اجازه را داده که داده‌های تخصصی را از متخصصینی که نزدیکترین اشخاص به فرآیند هستند به طور مستقیم به دست آورده و اطلاعات دست اول برای رسیدگی به مسئله مطالعه کاربردی‌تر است. محقق با استفاده از روشهای نظری بنیادی ساختارگرا سوالاتی را برای استنباط یک داستان و یک تاریخچه از شرکت کننده ساخت بدون اینکه شرکت کننده احساس کند که تحت فشار کاری قرار دارد(Charmaz, 2006; Corbin & Strauss, 2008; Wimpenny,& Gass, 2000). شرکت کنندگان با صداقت جواب دادن به سوالات احساس راحتی بیشتری کردند. به محض اینکه شرکت کننده داده‌هایی را در مصاحبه بازگو می‌کرد، مفاهیم از آن استخراج می‌شدند (Charmaz, 2006; Corbin & Strauss, 2008; Huehls, 2005). همچنین نمونه برداری نظری باعث شد که به خاطر زمینه‌های سازمانی بررسی نشده در مورد برنامه امنیت اطلاعات محقق بتواند مفاهیم عملی مرتبط با مساله و جمعیت را کشف کند که در این مطالعه مورد اهمیت قرار گرفتند (Charmaz, 2006; Corbin & Strauss, 2008;Creswell, 2002; Jirasek, 2012; Mcfadzean, et al., 2007).

جمع آوری داده به تحلیل منجر شده و تحلیل منجر به مفاهیم شده ومفاهیم سوالات را تولید می‌کند. سوالات منجر به جمع آوری داده‌های بیشتر می‌شود. همانطور که تحلیل انجام می‌شود، مفاهیم از آن برداشت شده و اگر سوالات ادامه پیدا کنند، محقق ترتیبی اتخاذ می‌کند تا شفاف سازی‌های بیشتری را از شرکت‌کنندگان دریافت کند (Corbin & Strauss, 2008; Huehls, 2005). چرخه جمع آوری داده تا جایی ادامه می‌یابد که با جمع آوری داده بیشتر و کد گذاری مفاهیم جدید، مفهوم جدیدی از تحلیل آنها استخراج نشود. جمع آوری داده از شرکت‌کنندگان به طور پیوسته انجام می‌شود تا زمانی که به اشباع برسد. اشباع زمانی رخ می‌دهد که "هیچ دسته جدیدی یا تم مرتبطی پدید نیاید" (Corbin & Strauss, 2008). در این نقطه، جمع آوری داده به پایان رسیده است. در بخش بعدی تحلیل داده‌ها، در مورد فرآیند اجرای کد گذاری باز، کد گذاری محور، کد گذاری انتخابی را برای ساخت دسته‌ها بر روی چندین سطح و ایجاد نظریه از داده پوشش داده می‌شود (Allan, 2003;Charmaz, 2006; Corbin & Strauss 2008; Jones & Alony, 2011; LaRossa, 2005; McFadzean, etal., 2007).

www.takbook.com

۳-٤ تحلیل داده ارائه شده

تحلیل داده در جایی اتفاق می‌افتد که کد گذاری انجام می‌شود. نظریه بنیادی از روش قیاسی تحلیل داده استفاده می‌کند که در آن المانهای داده در بین ۲ منبع و از یک منبع با منبع دیگر مقایسه می‌شوند (Allan, 2003; Jones & Alony, 2011, Rich, 2012). این فرآیند با جمع آوری داده از مصاحبه افراد و مشتقات آن و سپس با مقایسه کردن و یافتن تمایز بین مشتقات و مصاحبه‌های جمع آوری شده بدست می‌آید. خروجی این مقایسه‌ها باید دسته‌ها را مشخص کند. دسته هسته‌ای بدست آمده از طریق کد گذاری در شکل ۱ نمایش داده شده است (Allan, 2003; Backman & Kyngaes, 1999; Hallberg, 2006; LaRossa, 2005;Vannoy & Salam). فرآیند کد گذاری شامل سه مرحله تحلیل داده است که از درون به هم مرتبط هستند. شکل ۱ اولین گام کد گذاری باز را نشان می‌دهد که چندین دسته را ساخته و در نتیجه تحلیل در مرحله کد گذاری باز یک دسته اصلی یا هسته‌ای شروع به پدیدار شدن می‌کند (Hallberg, 2006). دومین گام که کد گذاری محوری است، ارتباطاتی را بین دسته‌های تعیین شده برقرار می‌کند و آن را به شکل ساختاری تحلیل می‌کند. در سومین گام که کد گذاری انتخابی است، خروجی‌هایی از کد گذاری محوری ایجاد شده و آنها را به هم متصل کرده تا روایتی از تحلیلها به وجود آورد (Allan, 2003; Corbin & Strauss, 2008; Jones & Alony, 2011; Siponen, 2005a).

به طور کلی، تحلیل قیاسی، استنباطی بوده و منجر به ساخت یک نظریه از روی داده می‌شود (Allan, 2003; Devades, Silong, & Ismail, 2011; Rowlands, 2005). برای کاهش بدبینانه مفهوم در استفاده از نظریه بنیادی، روشهای سختگیرانه‌ای دنبال شده تا قابلیت تکرار شدن داشته باشد که اگر کسی خواست مجددا اطلاعاتی را از داده‌های جمع آوری شده استخراج کند و سعی در ایجاد مجدد همان دسته‌ها داشته باشد بتواند به همان نظریه برسد.

باز کردن منابع و شناسایی این روش به دقت کار برای ضمانت بدست آوردن نتایج یکسان کمک می‌کند. محقق از دو ابزار در این روش استفاده کرد که در مثال‌های مشابه نظریه بنیادی استفاده شده بود که به این ابزارها راهنمای ارتباط شرطی و ماتریس کد گذاری بازتابی گفته می‌شود (Scott & Howell, 2008). راهنمای ارتباط شرطی، یک روال گام به گام برای بدست آوردن و اعتبار سنجی تقسیم داده‌های جمع آوری شده به دسته‌های سطح بالا معرفی می‌کند.

www.takbook.com

ماتریس کد گذاری بازتابی باعث افزایش دقت می‌شود به طوری که در طی مراحل کد گذاری محوری و کد گذاری انتخابی به جمع آوری و تحلیل مقایسه‌ای شباهت‌ها با هم به محقق کمک کرده که این امر موجب شناسایی ویژگیهای نظریه نوظهور می‌شود (Scott & Howell, 2008).

اولین گام در فرآیند کد گذاری باز برای شناسایی مفاهیم، دسته‌ها و خصوصیات از روی مصاحبه‌ها، یادداشت‌ها و یادداشت‌های کد شده است. در طی کد گذاری باز، تحلیل را می‌توان به صورت کلمه به کلمه، یک خط در زمان، دو یا سه جمله‌ای یا کل پاراگراف انجام داده که معانی را در دسته‌هایی خلاصه بندی کرد (Corbin & Strauss, 2008; LaRossa, 2005; Vannoy& Salam, 2010). کد گذاری باز، داده‌ها را جمع آوری کرده، پیش زمینه را ساخته و بر روی کلمات انتخاب شده و به کار رفته تمرکز می‌کند. همچنین کد گذاری باز نگاهی به چگونگی انجام مقایسه‌ها با دسته‌های کشف شده و چگونگی منجر شدن شباهت آنها به قرار گرفتن در گروه‌ها دارد (Allan, 2003; LaRossa, 2005; McFadzean, et al., 2007). راهنمای ارتباط شرطی یک ماتریس ساده است که به برقراری و استخراج دسته بندی‌های اولیه برای استفاده از کد گذاری باز کمک می‌کند. این ماتریس با گسترش تجربه محقق و تفسیر خلاقانه از طریق پرسیدن چندین سوال از داده اجازه می‌دهد تا دسته بندیها توسعه یابند (Scott & Howell, 2008). استفاده مداوم از سوالات برای برقراری دسته بندی‌ها به دقت بررسی داده و تضمین شناسایی همه دسته‌بندی‌های ممکن کمک می‌کند.

Scott و Howell (۲۰۰۸) برای بالا بردن دقت، پیشنهاد استفاده از یک ماتریس را دادند که از طریق سوالات مصاحبه یک چک لیست برای بررسی چگونه ایجاد شدن دسته‌ها ایجاد می‌شود. بعد از گروه بندی اصطلاحات با یکدیگر در دسته‌ها، مرحله بعدی پیوند یا ارتباط بین دسته‌ها را ایجاد می‌شود.

مطلوب است کد گذاری محوری روابط یا پیوند بین دسته‌ها را پیدا کند. اتصالات داخلی دسته بندی‌ها و اینکه اگر اصطلاحات یا عبارات باید به دسته‌های دیگر منتقل شوند در تحلیل کد گذاری محوری، در نظر گرفته می‌شود. در طی مرحله دوم، از طریق اتصال روایتها به هم نواحی مورد علاقه را می‌توان ساخت. کد گذاری محوری به شرایط معمول توجه می‌کند حتی اگر اتصال تداخلی بین دسته‌ها وجود داشته باشند تا در صورت نیاز طبقاتی در داخل دسته بندیها بسازد (LaRossa, 2005; McFadzean, et al., 2007; Vannoy & Salam, 2010).

www.takbook.com

منظور اولیه ماتریس کدگذاری بازتابی، ایجاد دسته اصلی و مفهومی سازی آن با استفاده از همه دسته‌های اقلیت شناسایی شده از داده‌های جمع آوری شده است (Hallberg, 2006; Strauss &Corbin, 1998).

Scott و Howell (۲۰۰۸) مشاهده کردند که ماتریس کدگذاری بازتابی به ساخت دسته‌ها به صورت طبقات تکاملی کمک می‌کند. محقق از ماتریس کدگذاری بازتابی استفاده کرد تا دسته‌ها را از چپ به راست و بین هم انتقال داده و جریان داستان از شروع تا پایان را بتواند نگهدارد زیرا همه دسته‌ها حول یک دسته مرکزی یا پدیده مرکزی قرار گرفته‌اند (Brown, Stevens, Troiano, & Schneider, 2002; Hallberg, 2006). نتیجه نهایی استفاده از هر دو راهنمای ارتباط شرطی و ماتریس کد گذاری بازتابی منجر به پدید آمدن و توسعه نظریه داده می‌شود (Brown, et al., 2002). ماتریس کد گذاری بازتابی کد گذاری انتخابی را تغذیه می‌کند.

کد گذاری انتخابی با تحلیل همه اطلاعات، همه نقشه‌ها را با هم در یک خروجی منسجم‌تر ترکیب می‌کند. داستانی که در پشت داده‌های جمع آوری شده در طی مصاحبه‌ها و مشتقات آن وجود دارد بازیابی شده و از روی فایلها تحلیل می‌شود (Jones & Alony, 2011; LaRossa,2005; McFadzean, et al., 2007; Vannoy & Salam, 2010). سومین گام (کد گذاری انتخابی) جایی بود که داده‌ها تحلیل می‌شدند تا دسته‌ها در دسته اصلی دنبال شده و با هم چگونگی حل مسائل در نظریه نوظهور را تعریف کنند (Hallberg, 2006). آخرین بخش از مرحله کد گذاری انتخابی ارتباطات مابین داده‌ها را بازگو می‌کند تا نظریه جمع آوری شده را نشان دهد (Backman & Kyngaes, 1999; Devadas, Silong, & Ismail, 2011; Siponen, 2005b). با کد گذاری موفق داده، نتایج کد گذاری باز، کد گذاری محوری و کد گذاری انتخابی با جزئیات کامل در فصل ۴ بررسی خواهد شد.

www.takbook.com

www.takbook.com

فصل چهارم

جمع آوری داده، تحلیل و یافته‌ها

www.takbook.com

٤-١ مقدمه

خروجی این مطالعه به عنوان مجموعه داده‌ها، تحلیل آنها و نتایج مراحل پیشروی شده ایجاد شده است. محقق از شرکت‌کنندگان مصاحبه کرده، ورودی‌های مصاحبه‌ها را بخش بندی کرده و نتایج را به شکل نظریه‌ای بر نقشهای فردی به کار رفته در یک استراتژی امنیت اطلاعات هماهنگ کرد. در بخشهای بعدی نتایج برگرفته از مراحل استنباط شده و به هم گره می‌خورند تا از طریق تحلیل استراتژی امنیت اطلاعات یک نظریه برای پیشرفت در برنامه امنیت اطلاعات تولید کنند.

٤-٢ جمع آوری داده

با استفاده از روالی که در فصل ۳ برای انجام مصاحبه‌ها گفته شد، محقق مصاحبه‌هایی با ۳۲ مدیر ارشد امنیت اطلاعات اصلی (CISOs) و معاونینشان (DCISOs) انجام داد. در ابتدا، ۲۵ مصاحبه از واحدهایی از یک سازمان مالی بزرگ انجام شد. هفت مصاحبه دیگر با مامورهای ارشد امنیت و معاونین ارشد امنیت از واحدهای مشابه یا وابسته در سازمانهای مالی بزرگ دیگر انجام شد. جدول ۶ واحدهای وابسته یا مشابه را مشخص می‌کند و مشخص می‌کند که چگونه ماموران ارشد امنیت و معاونین ارشد امنیت Fatherland با سازمانهای دیگر برابری می‌کند (جدول ۴، مشخصات زیر واحد شرکت کننده). جدول ۶ شامل بیانیه ماموریت کوتاه شده‌ای از واحدهای وابسته است و سپس برای اینکه نشان دهد که این واحدها در کجاها به هم شباهت دارند، یک ارجاع به جدول ۴ دارد. در طی هفت مصاحبه دو هدف دنبال می‌شود. هدف اول رسیدن به اشباع در جمع آوری داده بوده است، و برای آزمایش و مشاهده اینکه آیا پاسخهای داده شده در سازمانهای مشابه،شبیه هم بوده‌اند یا خیر. هفت پاسخگو به سوالات خیلی شبیه به هم، پاسخ دادند. جدول ۷ تفکیکی از شرکت‌کنندگان مطالعه نشان می‌دهد که نشانگر این است که پاسخ دهنده مربوط به کدام واحد کاری است و اینکه آیا سازمان بزرگ یا کوچک بوده است و همچنین اینکه شرکت کننده از سازمان مشابهی بوده است یا خیر. هر مصاحبه با ترتیب‌های مشخص شده‌ای با توافقات برقرار شده در (Institutional Review IRB Board) انجام شد. هر فرد در یک محلی، اتاق ملاقات یا یک مکان ملاقات توافق شده که برای مامور ارشد امنیت تعیین شده است توسط محقق ملاقات شد. مصاحبه کننده کل توافقات IRB را پاراگراف به پاراگراف برای هر مصاحبه شونده مرور کرده و از او توافقی در

www.takbook.com

برابر پاسخگویی و دنبال کردن سوالات بدست آورد. مصاحبه‌گر مجموعه یکسانی از سوالات را به یک روش از هر فرد می‌پرسد تا از دقت مناسب آن مطمئن شود (Allan, 2003; Corbin & Strauss, 2008; Lee & Hubona, 2009). مصاحبه کننده متن پاسخها را نوشت و در طی هر جلسه، یادداشتهای از روی مشاهداتش برداشت. بلافاصله بعد از انجام هر مصاحبه، مصاحبه‌گر نکات برگرفته از مصاحبه را می‌نویسد. مصاحبه‌گر در دفتری رویدادهای مصاحبه-های انجام شده برای هر شرکت کننده را نگهداری کرد. به هر پاسخ دهنده یک نشانگر اعداد لاتین به طور دلخواه نسبت داده شد که در جدول ۷ نمایش داده شده است و یادداشت برداری‌های حاصل از مصاحبه‌ها در تحلیل کدها استفاده شدند.

جدول ۶. ویژگی واحدهای وابسته

نام واحد وابسته	نامی برگرفته از جدول ۴، ویژگیهای زیر واحد شرکت کننده	بیانیه ماموریت
LLA	UHJY	با پاسخگویی، بازیابی و ترمیم به عموم مردم در ریسک ها. به کل سازمانها در موارد اضطراری کمک می‌کند.
MSD	FRT	از سیستمهای سطح بالای سازمان نگهبانی می‌کند تا به مردم اطمینان دهد که سازمان امن است.
BAUD*	ERF	اولا، مهاجمان و منابع گروههای مهاجمی را خارج از کشور نگه می‌دارد. نظم را در سازمان تضمین کرده و همچنین تضمین می‌کند که قوانین بروکراسی پیروی می‌شود.
VTEB	WER	تحقیق و توسعه را برای تمام سطوح سازمانی برای یافتن بهبود پدید آمده برای حمایت و پشتیبانی از سامان اجرا می‌کند.
POKE	NKOP	مسئول سیستمها و تجهیزات فناوری اطلاعات سازمان و نشانگر و دنبال کننده معیارهای کارآیی است.
ABC	WDC	مسئول حفاظت از اطلاعات و هوشمندی در برابر خارج شدن اطلاعات از سازمان است.

www.takbook.com

* نکته: آژانس BAUD دو شرکت کننده از یک سازمان داشت.

جدول ۷. اندیس مصاحبه‌شوندگان

Respondent Identifier	A0	B3	C7	D2	E3	F5	G7	H8	I5	J7	K2	K5	L9	M2	M7	N5	P4	P5	Q3	R2	S1	T8	X4	Y4	Z7	Totals
CISO Large Agency														1												1
DCISO Large Agency					1																					1
CISO Small Agency	1					1		1	1		1	1	1		1	1			1	1		1		1	1	14
DCISO Small Agency		1	1	1			1			1							1	1			1		1			9
Total																										25

Respondent Identifier	B8	O9	T5	U2	V8	W3	X9	
CISO Sister Large Agency	1			1	1	1	1	5
DCISO Sister Large Agency			1					1
CISO Sister Small Agency		1						1
Total								7

نشانگر پاسخ دهنده

مامور ارشد امنیت آژانس بزرگ

معاونین امنیت آژانس بزرگ

مامور ارشد امنیت آژانس کوچک

معاونین ارشد امنیت آژانس کوچک

کل

نشانگر پاسخ دهنده

مامور ارشد امنیت آژانس بزرگ وابسته

معاونین ارشد امنیت آژانس بزرگ وابسته

مامور ارشد امنیت آژانس کوچک وابسته

کل

مصاحبه‌گر، مصاحبه‌ها را در یک دوره زمانی چهار ماهه انجام داد. اصل مصاحبه‌ها در دو ماهه اول انجام شدند، زیرا که در این دوره دسترس بودن مامورهای ارشد امنیت در بهترین حالت ممکن بود. برای دو ماهه دوم زمانبندی و دسترس بودن مامورهای ارشد امنیت باعث شد که تعدادی از مصاحبه‌ها طبق برنامه انجام نشوند. نامساعد بودن هوا در عقب افتادن دو تا از مصاحبه‌ها اثر داشت که باعث شد بین انجام مصاحبه تا زمان برنامه ریزی شده برای آنها یک ماه وقفه بیفتد. بیان دقیق زمان رسیدن به اشباع ممکن نیست زیرا فرآیند تحلیل قیاسی همزمان با انجام مصاحبه‌ها انجام می‌شد. همانطور که در فصل ۳ بیان شد زمانی به نقطه اشباع می‌رسیم که هیچ داده جدیدی برای دسته‌های ایجاد شده در طی مصاحبه با مامورهای ارشد امنیت بدست نیاید.

لازم به ذکر است که در طی تمام فرآیند مصاحبه دو مامور ارشد امنیت دعوت شدند که امکان شرکت نداشتند. یکی از آنها با آوردن دلایلی همچون به دلیل مسائل امنیتی و اولویت جلسات

www.takbook.com

دیگر قادر به شرکت در مصاحبه نشدند، از شرکت در مصاحبه سر باز زدند. دومین مامور ارشد امنیت که ابتدا برای انجام مصاحبه موافقت کرده، ولی تماس با وی به قدری خیلی سخت شد. دو مامور ارشد امنیت جدید دیگر در واحدهای سازمان بزرگ به کار گرفته شدند اما به خاطر کمبود تجربه در این زمینه و در سازمان Fatherland بزرگ از مصاحبه آنها منع شد. در نهایت، با مصاحبه از ۳۲ مامور ارشد امنیت به اشباع رسیدیم و به نظر رسید که هیچ مصاحبه دیگری نیاز نیست.

٤-۳ تحلیل داده

محقق با انجام کل مصاحبه‌ها از شرکت‌کنندگان و خلاصه کردن آنها به صورت جداگانه در سطح بالایی از دیدگاه تحلیلی شروع به تحلیل داده‌ها کرد. نتایج اولیه در جدول ۸ نمایش داده شده است که در آن نمایش داده است که هر مامور ارشد امنیت در زمینه‌های عمومی تحت مطالعه قرار گرفته است. تحلیل اولیه چهار زمینه خاص مورد علاقه را در نظر گرفته است. راهکار کنش گرا در مقابل منفعل؛ آیا آنها استراتژی نوشته شده‌ای دارند یا خیر، با چه کسی تنظیم می‌شوند و نقش درک شده شان چه چیزی می‌تواند باشد. همه این اطلاعات در بخشهای از جدول ۸ دیده می‌شود. اولین حوزه این بود که آیا مامور ارشد امنیت برنامه امنیت اطلاعاتشان را به صورت منفعل می‌بینند یا کنش گرا یا ترکیبی از هر دو روش. یک نمونه خاص می‌تواند با پاسخگوی M7 مرتبط باشد که بیان کرد: "استراتژی امنیت اطلاعات نیاز دارد که ریسک تصمیم مدیریتی را که امکان دارد داده را در معرض ریسک قرار دهد کاملا در نظر بگیرد و در برابر آن تصمیماتی کنش گرا بگیرند نه منفعل". دومین حوزه‌ای که در مورد آن سوال شد این بود که آیا مامور ارشد امنیت شکلی از استراتژی امنیت اطلاعات دارد یا خیر یا بیان می‌کند که ضروری نیست. یک مثال نشانگر از یک مورد ایزوله شده از پاسخ دهنده F5 (پرسنل ارتباطات) گرفته شده که گفت: " آن چه ما انجام می‌دهیم این است که بیشتر از اینکه نقشه‌های استراتژیک مامور ارشد امنیت داشته باشیم، آنها را ایجاد می‌کنیم." به عنوان یک معیار کیفی، بیشتر ماموران ارشد امنیت استراتژی نوشته شده‌ای داشتند (یکی از آنها در فرآیند تصویب بود) یا از استراتژی سازمانی سطح بالاتری استفاده می‌کردند مثل استراتژی سیستمهای اطلاعاتی یا استراتژی کسب و کار. مامورهای ارشد امنیت بیان کردند که وجود استراتژی ضروری نیست و بر داشتن استراتژی به عنوان استراتژی تجویزی تکیه داشتند.

www.takbook.com

سومین حوزه نگاهی بر روشی دارد که مامور ارشد امنیت فعالیتهایش را در برنامه امنیت اطلاعات با یکی از اهداف تنظیم می‌کند مثل اهداف استفاده شده در کسب و کار، سیستمهای اطلاعاتی و کسب و کار، سیستمهای اطلاعاتی، امنیت اطلاعاتی که خود به خود کار می‌کند یا امنیت اطلاعاتی که به صورت خاص (هیچ هدفی در رهبری ندارد با مسائل روبرو می‌شود. یکی از مثال‌های استراتژی منتج از کسب و کار از پاسخگوی M2 به دست آمد است که گفت: " نقش من عمل کردن به عنوان یک مجرا برای گماشتگان سیاسی است. من با گماشتگان سیاسی و مجریان نهایی سازمان سر و کار دارم". در چهارمین بخش صفحه گسترده، از اینکه ماموران ارشد امنیت چگونه یک نقش را برای انجام وظایفشان می‌بینند و یا چگونه به آن عمل می‌کنند یک ارزیابی اولیه انجام شد. بعضی بیان کردند که آنها در نقش خاصی عمل می‌کنند و برخی ماموران ارشد امنیت نشان دادند که نیاز است تا چندین نقش کارآ عمل کنند تا آنها به اهداف برآورد شده‌شان در برنامه امنیت اطلاعات برسند (Carter, Grover, & Bennett (Thatcher, 2011; Weill & Woerner, 2013). نقشهایی که از شرکت‌کنندگان به دست آمد شامل بالا به پایین، تصویر عمومی، رقیب، تغییر مداوم، بهترین عملکرد و تبعیت بسیار شبیه به دسته بندیهای مشخص شده در فصل دو بودند.

یک نگاه نزدیکتر به تحلیل کلی این نکته را فاش کرد که برای اغلب بخشها ماموران ارشد امنیتدخودشان را در پاسخ به رهبری کنشگرا می‌دیدند. بیشتر ماموران ارشد امنیت استراتژی امنیت اطلاعات نداشتند. اکثریت قریب به اتفاق آنها با بخشهای کسب و کار سیستمهای اطلاعاتی سازمان کار می‌کردند. آنها کمبود امنیت را مناسب می‌دانستند اما خود از مامور ارشد امنیت یا رهبری کسب و کار پیروی می‌کردند. در نهایت اینکه، اغلب ماموران ارشد امنیت در یک حالت اجرایی دنباله رویی کار می‌کردند. اصلی ترین دلیل روخوانی در بیشتر مصاحبه‌ها این حقیقت بود که در قانون فدرال ماموران ارشد امنیت باید از مصوبهClinger Cohen تحت بخش شناخته شده به عنوان مصوبه مدیریت امنیت اطلاعات فدرال (FISMA) پیروی کنند (Burwell,2013; Corbet, 2014). دیدگاه‌های جداگانه هر مامور ارشد امنیت برای برنامه امنیت اطلاعاتیش در تحلیل کلی اولیه برجسته شد. تحلیل واقعی در این مطالعه با استفاده از کد گذاری انجام شد تا همه ورودی‌ها را از پاسخ دهندگان جمع آوری کرده و آنها را در یک مرور کلی به هم متصل کنند. با استفاده از آنچه در فصل ۳ با آن توافق شد، محقق از روی مصاحبه‌های نوشته شده شروع به کد گذاری داده‌ها کرد. محقق برای اجرای کد گذاری باز،

www.takbook.com

کد گذاری محوری و کد گذاری انتخابی وارد فرآیند کد گذاری از داده‌های جمع آوری شده شد.

جدول ۸. تحلیل اولیه کلی

Strategy	Proactive	Reactive	Have one	Don't have one	Not Needed	Business	Bus/IT	IT	On its own	Ad-hoc	Top Down	Public Image	Competitor	Continual Change	Best Practice	Re-Organization	Power Relationship	Compliance
Respondent																		
A0	X			X			X				X				X			
B3		X		X				X										X
B8	X	X		X					X	X	X			X	X			
C7		X		X			X					X						X
D2		X							X					X				X
E3		X	X				X		X					X				
F5	X	X			X		X			X	X			X				X
G7		X	X	X				X		X	X							X
H8		X		X				X							X			X
I5	X	X					X		X					X	X			
J7		X		X							X			X		X		X
K2		X		X			X				X				X			X
K5	X			X		X						X		X	X			
L9	X								X					X	X			
M2	X		X				X				X			X	X			
M7		X	X				X			X	X							X
N5	X	X		X			X			X	X			X				X
O9		X		X					X		X		X					X
P4	X			X					X						X			X
P5		X			X		X								X			X
Q3		X		X			X				X				X			
R2		X		X			X								X			X
S1		X		X			X		X		X				X			X
T5	X			X		X			X						X			X
T8		X		X						X	X						X	
U2	X		X				X		X					X	X			X
V8	X		X				X		X			X		X	X			
W3	X			X			X							X	X			
X4	X	X		X			X						X	X				X
X9	X			X		X			X	X				X	X		X	
Y4		X		X			X								X			X
Z7		X		X					X	X				X			X	

(سر ستونها از چپ به راست) راهکار- کنشگرا- منفعل- دارای یکی- یکی ندارد- نیاز ندارد- کسب و کار- IT- IT- با خودش است- خاص منظوره – بالا به پایین-تصویر عمومی- رقیب- بهترین تجربه- سازماندهی مجدد- ارتباط قدرت- هماهنگی

www.takbook.com

۴-۳-۱ کد گذاری باز

مصاحبه گر، مصاحبه‌های انجام شده با مجریان ارشد امنیت را به صورت جمله به جمله نوشت. هیچ تغییر یا خلاصه سازی در یادداشت مصاحبه‌ها انجام نشد. محقق از فرآیند کد گذاری باز برای مرور همه جملات جمع آوری شده از مصاحبه ۳۲ مجری مامور ارشد امنیت استفاده کرد. به عنوان مثالی از موشکافی و دقت زیادی که در مصاحبه اجرا شد را می‌توان در برگرفتن یک بخش خاص از مصاحبه به صورت تصادفی و دنبال کردن آن از طریق کد گذاری باز به نمایش گذاشت. بخش انتخابی بخشهای انتخاب شده قسمتهایی از پاسخگوی Y4 در اولین گام تحلیل قیاسی در فرآیند کد گذاری باز بودند که منجر به دسته بندی مصاحبه شد. به ویژه سوال ۶ از پاسخگوی Y4 برای این تحلیل استفاده شد. سوال مصاحبه (جدول ۵، بنیاد سوال مصاحبه) این بود " آیا می‌توانید توصیف کنید که چگونه پیاده سازی استراتژی امنیت اطلاعات پیگیری می‌شود؟" و پاسخگویی Y4 اینگونه بود:

ما پیاده سازی را از طریق تعدادی روش در برنامه مان پیگیری می‌کنیم. اول اینکه آنها از طریق فعالیتهای هماهنگ اندازه گیری می‌شوند به شکلی که یک استاندارد را در نظر گرفته و سیاستها و استانداردها را به صورت چک لیستی از فعالیتها در آورده تا همه اعضایی از تیم که منسوب به آن هستند مسئول اجرای آنها می‌شوند. راه دیگر، از طریق فعالیتهای مدیریتی در درک ماموریت روزانه است و تاییدات باید همراه با فعالیتهای خاصی باشد و فرآیند ارتباط موثری که به مدیران اجازه می‌دهد در مورد فعالیتهایشان در مورد کارمندانشان با بصیرت باشند. راه دیگر برای پیگیری از طریق گزارشهای اجباری یا بازرسی توسط اداره بازرسی عمومی سازمان است. من معتقدم که همه این روشها به ما اجازه می‌دهد که با موفقیت بازدهی و موثر بودن برنامه را تنظیم کرده و نشانگرهای کلیدی را برای موثر بودن استراتژی پیاده سازی فراهم کنیم. در نهایت، بازخورد مشتری را در برآورد پیاده سازی برنامه نمی‌توان کم انگاشت.

محقق از یک فرم دستورالعمل برای گرفتن جمله‌های سوال ۶ از پاسخگوی Y6 استفاده کرد که آنها را به جملاتی تقسیم بندی کرد که در هر سلول جدول ۹ نمایش داده شده است. ستونهای دست چپی جمله پاسخگو را نشان داده و سپس ستون بعدی در سمت راست، اولین مرحله تحلیل قیاسی را نشان می‌دهد که با تکنیک کد گذاری باز ما را به سمت دسته بندی حدکت می‌دهد. تحلیل در کدگذاری باز و یادداشت برداری‌ها از ماموران ارشد امنیت در سمت

www.takbook.com

چپ و مرور کد گذاری باز برای دسته بندی در سمت راست می‌باشد. بررسی‌ها به صورت عبارات ارزیابی کوتاه برای مشخص کردن دسته‌بندی‌ها تولید شدند. این گام پس زمینه تحلیل قیاسی شد که در مرحله کد گذاری باز بر مبنای پیشرفت مداوم انجام می‌شود (Corbin & Strauss 2008; Charmaz, 2006).

جدول ۹. سوال ۶، پاسخگوی Y4

پاسخ به جملات	تحلیل جمله
در برنامه ما پیاده‌سازی از طریق تعدادی روش پیگیری می‌شود.	تعداد راههای پیگیری
اول از طریق فعالیتهای هماهنگ اندازه گیری می‌شوند به شکلی که یک استاندارد را در نظر گرفته و سیاستها و استانداردها را به صورت چک لیستی از فعالیتها در آورده تا همه اعضایی از تیم که منسوب به آن هستند مسئول اجرای آنها شوند	هماهنگی از طریق اینکه چک لیستها یکی هستند
راه دیگر، از طریق فعالیتهای مدیریتی در فهم ماموریت روزانه است و تاییدات باید همراه با فعالیتهای خاصی باشد و فرآیند ارتباط موثری که به مدیران اجازه می‌دهد در مورد فعالیتهایشان در مورد کارمندانشان آگاهی داشته باشند.	کسب و کار متوجه ماموریت شده، تایید می‌کند که کارمندان در مکانشان کار می‌کنند.
راه دیگر برای پیگیری از طریق گزارشهای اجباری یا بازرسی توسط اداره بازرسی عمومی سازمان است.	بازرسی سیستمها برای IG
من معتقدم که همه این روشها به ما اجازه می‌دهد که با موفقیت بازدهی و موثر بودن برنامه را تنظیم کرده و نشانگرهای کلیدی را برای موثر بودن استراتژی پیاده سازی فراهم کنیم.	استراتژی از طریق وارسی و تصویب پیروی از قانون به واقعیت تبدیل می‌شود.
در نهایت، بازخورد مشتری را در برآورد پیاده سازی برنامه نمی‌توان کم انگاشت.	مشتری‌ها در کار کلیدی هستند.

مجموع "درون بافتی in vivo " در ستون سمت راست تلاش دارد تا کلمات خود پاسخگو را تا جای ممکن برای دسته بندیهای تحلیل قیاسی حفظ کند. محقق یک تحلیل موازی را بر روی ۱۷۸۳ جمله از ۳۲ مصاحبه انجام شده، اجرا کرد. بعد از چند مصاحبه اول، مصاحبه

www.takbook.com

کننده حدس زد که واقعا به دلخواه به سوالات مصاحبه‌ای که پرسیده شده‌اند پاسخ دادند. همانطور که در فصل ۳، جدول ۵ مشخص شد، پاسخهای دریافت شده از مصاحبه شوندگان تبادل با ملاحظه‌ای بین مصاحبه کننده و مجریان مامور ارشد امنیت بر اساس نواحی تعیین شده ایجاد کرد.

محقق اطلاعات منتج از تحلیل جمله‌ای در تحلیل اولیه قیاسی کد گذاری گرفته و سپس جملات مشابه را با هم گروه بندی کرد. برای نشان دادن اینکه چگونه پاسخهای جمع آوری شده از یک پاسخگو در گروه بندی کلی جمع آوری شده می‌گنجد، محقق آنها را به شکل جدول ۱۰، گروه بندی تحلیل قیاسی نمایش داد. جدول شامل یک ستون در سمت چپ است که نمایانگر پاسخ پاسخگوی Y4 به سوال ۶ است و ستون سمت راست تحلیل جملات او را نشان می‌دهد. این ورودی‌ها برای دیگر جملات از مصاحبه‌های بعدی در ستون میانی وارد شدند، که نشان دهنده نمایندگان جمع آوری شده کل برای یک دسته ارائه شده از همه مصاحبه‌های انجام شده در فرآیند جمع آوری داده بودند. جملات نمایانگر پاسخهای درون بافتی از مجموع پاسخ دهندگان بود و به این صورت پاسخها جمع آوری شد تا تعداد بارهایی که یک پاسخ تکرار می‌شود را بشمارد. سومین ستون تعداد شمارش‌ها در طی فرآیند از یک گونه پاسخ بود که تا آن زمان رخ داده بود. این تعداد نمایانگر این بود که آیا یک نماینده برای دسته با تعداد رخدادهایی که دارد قابل توجه است یا اینکه تعداد کمی رخداد در طی مصاحبه جمع آوری شده است. این چرخه مقایسه ثابت مداوما در طی انجام مصاحبه‌ها با مصاحبه‌هایی که قبلا صورت گرفته انجام می‌شود. نمایندگان کلی دسته‌ها از جمع آوری تحلیل ۱۷۸۳ جمله پدید آمده در طی فرآیند مصاحبه ایجاد شده و تعداد آنها کاهش یافته تا چرخه کد گذاری باز تکمیل شود.

جدول ۱۰. گروه بندی تحلیل قیاسی

پاسخگوی شماره Y4، سوال ۶	نمایندگان جمع آوری شده از تمامی مصاحبه‌ها با هم گروه می‌شوند.	تعداد بارهایی که از کد گذاری باز اولیه عبور می‌کند
تعداد روشهای پیگیری	ISS یک مکانیزم پیگیر می‌شود)؛ ISS باید روشهای پیگیری را مشخص کند؛ ISS کاربردی بودن را به طور	۱۱

www.takbook.com

	کلی افزایش می‌دهد؛ چندین روش پیگیری؛ چند کاره؛ پیگیری باید به صورت تجربی انجام شود؛ مامور ارشد امنیت رهبران تیم را برای به انجام رساندن ISS پیگیری می‌کند؛ مامور ارشد امنیت روشی برای پیگیری امنیت می‌خواهد؛ مامور ارشد امنیت از طریق بازرسی سیستم پیگیری می‌کند؛ ISS با دنبال کردن همه فعالیتها به پیگیری کمک می‌کند	
تبعیت ازقانون از طریق چک لیستها	چک کردن هماهنگی با استفاده از چک لیستها؛ چک لیست هماهنگ؛ استفاده از چک لیستهای استاندارد برای پیکربندی و تغییر؛ استفاده از چک لیستها برای تنظیم تطابق تجهیزات؛ پیگیری از طریق چک لیستها، استانداردها انجام می‌شود؛ ISS نوعی چک لیست است؛ ISS مستندی برای چک کردن و تعادل است؛ بهترین چک لیست را پیدا می‌کند؛ ما به سمت چک لیستهای خودکار رفته‌ایم؛ دنبال کردن روال پذیرفته شده کلیدی است.	۱۵
درک ماموریت کسب و کار تایید کننده کار کردن کارمند در موقعیتهای مکانی است.	درک ماموریت کسب و کار تایید کننده کار کردن کارمند در موقعیتهای مکانی است.	۱
بازرسی سیستم‌ها به IG	بازرسی سیستمهای به IG	۱

www.takbook.com

استراتژی از طریق استفاده از بازرسی هماهنگ و تاییدات تحقق می‌یابد.	هماهنگی تمرکز یافته است؛ مامور ارشد امنیت فقط از قانون پیروی می-کند؛ استراتژی از طریق بازرسی هماهنگ و تاییدات تحقق می‌یابد	۳
مشتری‌ها در کار کلیدی هستند	امتیاز بندی در اولویتهای بالا؛ مشتری‌ها در کار کلیدی هستند؛ اولویتهای اصلی را با استفاده از خط جدا کننده برای اولویتهای بالا مشخص شود؛ تنظیم نیازمندی‌ها برای امتیاز بندی اولویتها؛ تیم استراتژی آنها را امتیاز بندی کرده و سپس بر اساس بودجه آنها را حذف می‌کند؛ مشخص کردن اولویتهای اصلی؛ سرمایه محرک برخی اولویتها است	۱۰

در این بحث، محقق به استفاده از یک جمله تحلیل شده قیاسی از پاسخ پاسخگوی Y4 به سوال ۶ ادامه داد. تحلیل جمله "تعداد روشهای پیگیری" پاسخ و جا دادن آن در گروه بندی که به آن تضمین هماهنگی یا سازگاری گفته می‌شود در جدول ۱۱ نشان داده شده است.

جدول ۱۱. جمله خام برای خلاصه دسته

جملات خام	خلاصه دسته
مامور ارشد امنیت برآورده شدن هماهنگی را تضمین می‌کنند؛ مامور ارشد امنیت وضعیت جاری و هماهنگی را در نظر گرفته و سپس به سمت جلو حرکت می‌کند؛ مامور ارشد امنیت از طریق خط پایه هماهنگی را تضمین می‌کند؛ مامور ارشد امنیت سیستمها را به منظور	تضمین کردن هماهنگی

www.takbook.com

جملات خام	خلاصه دسته
هماهنگی بازرسی می‌کند؛ مامور ارشد امنیت کوششها برای هماهنگی را رهبری می‌کند؛ هماهنگی پیش فرض است؛ وفاداری به هماهنگی نمایانگر دریافت امنیت است؛ ادامه داده می‌شود تا به هماهنگی دست یافت؛ مامور ارشد امنیت باید مبتنی بر هماهنگی باشد؛ هماهنگی فردی فرای سیستم ISSOها را شکل می‌دهد؛ ISSOها مستقیما هماهنگی را اجرا می‌کنند؛ ISSOها مسئول سیستم هستند؛ همچنین ISS به سیستمهای بازرسی بستگی دارد؛ بسیاری از ISSها در حالت هماهنگی ثابت می‌مانند؛ هماهنگی متمرکز شده است؛ مامور ارشد امنیت فقط از قانون پیروی می‌کند؛ استراتژی از طریق استفاده از بازرسی تطابق و تاییدات تحقق می‌یابد؛ بر برون نگری تمرکز شده است؛ در برخی جاها کمبود هماهنگی وجود دارد؛ هماهنگی برای بررسی امنیت؛ هماهنگی برای پیگیری پیاده سازی استفاده شده است؛ کسب و کار امنیت را مبتنی به هماهنگی می‌بینند؛ خط مبنا توافق شده است و برای رد شدن از ریسک عملی است؛ هماهنگی نیازمندیها را تعیین می‌کند؛ هماهنگی به مشخص کردن کسر بودجه کمک می‌کند؛ هماهنگی هنوز برای برنامه ریزی در مورد امنیت استفاده می‌شود؛ هماهنگی محرک استراتژی است؛ هماهنگی برای اندازه گیری انجام معیارهای ISS استفاده می‌شود؛ ISS باید از قانون پیروی کند؛ ISS از تبعیت برای ISS	(هماهنگی امتیازی برای امنیت ایجاد می‌کند که مامور ارشد امنیت با آن خوب یا بد بودن را مطابق قانون پی می‌گیرد)

www.takbook.com

جملات خام	خلاصه دسته
استفاده می‌کند؛ ISS با هماهنگی پیگیری می‌شود؛ استفاده از کارت ارزیابی متوازن برای اندازه گیری هماهنگی؛ هماهنگی در سراسر به صورت واقعی استفاده می‌شود؛ معیارهایی از واقعه نگاریها ایجاد می‌شود؛ خلاقیت برای هماهنگی؛ ممیزی سیستمها برای IG؛ نیاز است که هماهنگی وجود داشته باشد؛ هماهنگی برای انتها به انتها نیاز است؛ هماهنگی کلیدی است؛ هماهنگی نیاز است؛ برای بهبود هماهنگی کار شد؛ هماهنگی به اندازه کافی برای کار سازمان مناسب است؛ ISS مبتنی بر هماهنگی است؛ ISS هماهنگی و سازکاری است.	

زمانی که از نتایج فرآیند تعداد گروه بندیها به تعداد قابل مدیریتی از دسته‌های ممکن رسید (۳۵ گروه). جدول ۱۲ نتایج تحلیل قیاسی را نشان می‌دهد، جملات را از تمام ۳۲ مامور ارشد امنیت گرفته و پاسخهای مشابه را در گروه یکسانی گروه بندی کرده که نمایانگر داده جمع آوری شده است. هر گروه در جدول نمایانگر ارائه یک دسته است. تعداد گروه بندیهای اصلی یا نمایندگان دسته از کل مطالعه به ۳۵ نماینده اصلی کاهش یافتند. سپس یک ابزار می‌تواند برای تست نمایندگان برای اعتبار سنجی مورد استفاده قرار بگیرد.

Scott و Howell (۲۰۰۸) دو ابزار برای استفاده توسط محققان نظریه بنیادی ایجاد کردند که در تست نمایندگان دسته بندیها مورد استفاده قرار می‌گیرد. اولین ابزار، راهنمای ارتباط شرطی conditional relationship guide (CRG) است که برای آزمایش گروه بندیها مبنی بر جواب به یک سری از سوالات برای قابلیت وجود داشتن دسته ایجاد می‌کند.

www.takbook.com

جدول ۱۲. گروه بندی دسته ارائه شده

دسته	گروه بندی
تنظیم کسب و کار	مامور ارشد امنیت،ISS را با اهداف کسب و کار تنظیم می‌کند. اغلب کسب کار اهدافی را برای مامور ارشد امنیت تنظیم می-کند.
تنظیم کسب و کار و IS	مامور ارشد امنیت با اهداف کسب و کار و IT تنظیم می‌شود.
تنظیم IS	اغلب مامور ارشد اطلاعات، تنظیمات را به مامور ارشد امنیت دیکته می‌کند.
بر مبنای خودش	برخی مامور ارشد امنیتها بودجه خودشان را داشته و اهداف را خودشان تنظیم می‌کنند.
Ad Hoc	ماموران ارشد امنیت هیچ راهنمایی نداشته و اکثرا بر اساس وقوع حادثه کار می‌کنند. از نقشه‌های پروژه به عنوان استراتژی استفاده می‌کنند.
بالا به پایین	برگرفته از مدیریت
تصویر عمومی	کسب و کار از امنیت حمایت نمی‌کند، تصویر عمومی ارزش بیشتری دارد. هیچ پشتیبانی از کسب و کار نیست.
رقیب	به دنبال بهتر بودن از هر کسی در سازمان بزرگ، رقابت
تغییر مداوم	تغییر حتمی است و نیاز به محافظت دارد، انعطاف پذیر، تطبیق پذیر، سریع‌الانتقال
بهترین عملکرد	مامور ارشد امنیت به منظور ساخت بهترین ISSشان برای بهترین نتیجه ممکن به مثال‌های دیگر نگاه می‌کند، تعداد زیادی مامور ارشد امنیت، یک مرتبه ساخته و بارها استفاده می‌کنند، مطابق طرز فکر سازمان
سازمان دهی مجدد	(در حالی که پیشرفت کرده است، اطلاعات زیادی به دست نمی‌آورد)

www.takbook.com

دسته	گروه بندی
ممیزی	برخی ممیزی‌های اجرا شده برای اعتبار سنجی هماهنگ
اندازه گیری و معیارها	نتایج اندازه گیری شده زیاد
تضمین هماهنگی	اکثریت را به هماهنگی وادار می‌کند زیرا که قانون است.
InfoSec Prg	تشخیص یک برنامه کلی که مورد نیاز است
اولویتها	اولویت بندی اینکه چه چیزی در برنامه آنها مهمتر است و ترتیب اولویت چیست
تصور غیر عملی	تشخیص نیاز به دیدن یک هدف و داشتن یک دید برای هر هدف
روش مدل چارچوب	نگاهی به داشتن یک مدل دارد تا برای رسیدن به هدف از آن استفاده شود
به کار انداختن استراتژی	همانطور که توصیه شده استراتژی باید کار کند
Shelfware	باید استفاده شود یا به D2D یا تاکتیکی مبدل شود
اعتماد	مشتریان باید بتوانند به مامور ارشد امنیت اطمینان کنند.
دانش امنیت	شناختن امنیت به عنوان اولین گام در فرآیند
حفاظت	حفاظت از داده و سیستمهای اطلاعاتی
ارتباطات و مشارکت	صحبت کردن و پیام گرفتن برای موفقیت ضروری است.
خرید سهم	تشخیص اینکه خرید سهم از رهبری (کسب و کار/ IT) برای برنامه ضروری است.
اتوماسیون	سرعت تغییر نیاز به خودکار سازی و اتوماسیون یا تسلیم در برابر تهدیدات است.
عملیات و ریسک	InfoSec و ISS مشخص مهمتر از هماهنگی است و باید با عملیات تطبیق داده شود

www.takbook.com

دسته	گروه بندی
مدل	نشان دهنده جا به جایی از عملیات به تهدید است
تهدید، کنش گرا، تغییر	زمانی که به سمت یک استاندارد می‌رود، مامور ارشد امنیت نسل بعدی اجتناب از تهدید را در مخالفت با تعقیب یا سر هم بندی کردن دنبال می‌کند
کارمند واجد شرایط	اگر شما منابع یا اشخاص کافی نداشته باشید نمی‌توانید سازماندهی مجدد را انجام دهد.
ابزارها	اگر منابع- ابزار نباشد نمی‌توانید کار را انجام دهید
آموزش	اگر منابع- آموزش نداشته باشد، نمی‌توان کار انجام داد.
بودجه	اگر منابع- بودجه نداشته باشد، نمی‌توان کار انجام داد.

آخرین گام در بررسی کد گذاری باز از راهنمای ارتباط شرطی استفاده شد (Scott & Howell, 2004). برای هر دسته نماینده، اطلاعات از گروه‌بندی‌ها استخراج شد و در CRG وارد شده به طوری که برای پاسخ سوالات در مورد چه چیزی، چه وقت، کجا، چرا، چگونه طراحی شده بود و اینکه دسته حاصل بر روی نظریه پدید آمده چه پیامدی به دنبال خواهد داشت (Scott & Howell, 2008). جدول ۱۳ یک دسته را برای تضمین هماهنگی نشان می‌دهد همراه با پاسخهایی که به سوالات داده شده است. محقق برای بحث از ابزار نظریه بنیادی در طی تحلیل کد گذاری باز استفاده کرده که ممکن است در آزمایش نماینده‌ها برای اعتبار سنجی دسته‌ها کمک کند.

۴-۳-۲ نتایج کد گذاری باز

همانطور که هر دسته ارائه شده به صورت سیستماتیک با CRG تست شدند، محقق از تکنیک سوال پرسیدن برای سکنی کردن یک راهنمای ارتباط شرطی برای هر دسته اراده شده استفاده می‌کند. هر چرخه تعداد گوناگونی پاسخ تولید می‌کند. بعد از گذشتن از چندین ارزیابی با تحلیل قیاسی، شش گروه بندی اضافی با گروه‌های دیگر ترکیب شده و تعداد دسته‌های منحصر به فرد را به ۲۹ دسته مجزا کاهش داد. دو ستون از جدول ۱۲ دسته‌های تست شده

www.takbook.com

با ابزار CRG را نمایش می‌دهد. با برگرفتن دسته‌ها به مرحله بعدی که کد گذاری محوری می‌باشد، مطلوب است که محقق دسته اصلی یا پدیده مرکزی مطالعه را نتیجه چیری کند. (Brown, et al., 2002; Hallberg, 2006).

www.takbook.com

جدول ۱۳. راهنمای ارتباط شرطی

دسته	چه چیزی	چه وقت	کجا	چرا	چگونه	پیامد
تضمین هماهنگی (عبارت دسته-هماهنگی امتیازی را برای امنیت خوب یا بد از پیگیری مامور ارشد امنیت مطابق قانون فراهم می‌کند)	ISSنیاز به پوشش هماهنگی دارد. هماهنگی شامل چک لیستها است. هماهنگی از طریق تکمیل چک لیستها اندازه گیری می‌شود	زمانی که سیستمها نصب شده‌اند، هماهنگی یک نیازمندی برای عملیات است. خط مبنای استفاده شده توسط اسکنرها برای چک کردن هماهنگی بر روی همه داراییها. چک لیستها بخش اصلی هماهنگی را برای بررسی تضمین استاندارد سازی تشکیل میشود.	هماهنگی بر روی هر دستگاه، سیستم و دارایی متصل به شبکه چک می‌شود. چک لیستها استانداردی برای هر دستگاهی که با آن اعتبار سنجی می‌شوند انجام می‌شود. اسکن کردن دارایی‌ها با کامل کردن پیکربندی استاندارد اعتبار سنجی می‌شود.	بودن استانداردسازی، المانهای سازمانی ممکن است قادر به نصب دارایی‌ها با تمایز پیکربندیها باشند. استاندارد سازی می‌تواند از نصب نسخه‌ها مختلف مخصوصا آنهایی که دارای نقص هستند یا آسیب پذیر هستند جلوگیری کند.	چک لیستها را برای تضمین هماهنگی پیاده سازی می-کند. مرور و به روز رسانی چک لیستها برای تضمین کامل بودن به خصوص بعد از به روز رسانی یا سرهم بندی آسیب پذیری است.	بدون چک لیستها، استاندارد سازی یا تبعیت تضمین سختتر است. بدون اسکن کردن آسیب پذیری تشخیص ضعفها می‌تواند سخت باشد.

www.takbook.com

۴-۳-۳ کد گذاری محوری

در دومین گام از فرآیند کد گذاری نظریه بنیادی که کد گذاری محوری است، محقق به ریز کردن دسته‌های گروه بندیهای اولیه پیش روی کرد و پدیده هسته‌ای یا مرکزی را استنتاج کرد. محقق از مقایسه مداوم در کد گذاری استفاده کرد و هر بار که محقق از داده‌های جمع آوری شده گذر می‌کرد دسته‌ها را یا کاهش می‌داد یا در هم ادغام می‌کرد و مشابهت‌ها را برای ایجاد گروه بندی‌ها بزرگتر با هم ترکیب می‌کرد. برای مثال، محقق به امکان نقشهایی که یک متخصص امنیت اطلاعات می‌توانست اجرا کند نگاه کرد و از روی داده‌هایی که می‌توانستند در چندین گروه بندی با نقش متمایز گروه بندی شوند آنها را کشف کرد. چندین نوع متمایز وجود داشت که توسط پاسخ دهندگان بیان شد همانطور که در جدول ۱۴ نمایش داده شده است.

یکی کردن همه نقشهای مختلف در یک گروه بزرگ باعث ایجاد یک گروه بندی ترکیبی یا نگاشت آن به یک دسته بزرگ به نام نقشها می‌شود. ترکیباتی که محقق آنها را با نقشها بر چسب گذاری کرده است بعدا می‌توانند سطح بالاتر یا ابر دسته نامیده شوند. فرآیند ترکیب کردن بیشتر از طریق تحلیل قیاسی دسته‌ها زمانی به اتمام رسید که ۴ ابر گروه از داده‌ها پدیدار شد. ابر گروه‌های پدید آمده از داده با نام نقشها، تنظیمات، پیچیدگی‌ها و منابع برچسب گذاری شد. این شروع تحلیل هر گروهی است که برای دسته هسته‌ای یا پدیده مرکزی در نظر گرفته می‌شود (Brown, et al., 2002; Hallberg, 2006). محقق مخصوصا هر ابر گروه را به عنوان دسته هسته‌ای ارزیابی کرد.

جدول ۱۴. گروه بندی نقشها در دسته‌ها

پیشنهاد نقش	نامگذاری دسته
مبتنی بر مدیریت	بالا به پایین
کسب و کار از امنیت حمایت نمی‌کند، تصویر عمومی ارزش بیشتری دارد، هیچ حمایتی از طرف کسب و کار نیست	تصویر عمومی

www.takbook.com

پیشنهاد نقش	نامگذاری دسته
به دنبال بهتر عمل کردن از هر کسی در سازمان بزرگ، رقابت	رقیب
تغییر غیر قابل اجتناب است و نیاز به حفاظت داشته، انعطاف پذیر، انطباق پذیر، سریع وچابک	تغییر مداوم
مامور ارشد امنیت به دیگر نمونه‌ها نگاه کرده تا ISS را برای بهترین نتایج ممکن بسازد؛ ماموران ارشد امنیت زیادی بر اساس طرز فکر سازمان یک مرتبه بهترین نتیجه را می‌سازند و تعداد بارهای زیادی استفاده می‌کنند.	بهترین عملکرد
در حالی که پیشرفته است، به کار گرفته نمی-شود	سازماندهی مجدد

گسترش عناوین نمایندگان ۴ ابر گروه، نقشهای منتخب ماموران ارشد امنیت، تنظیمات راهکارهای امنیت اطلاعات، ساختار پیچیده استراتژیهای امنیت اطلاعات و منابع برای اجرای استراتژی امنیت اطلاعات بود. از آنجایی که محقق نمی‌تواند به طور کامل حقیقت اینکه مروری بر متون انجام شده است را نادیده بگیرد، محقق باید این حقیقت را که شباهت‌های بسیاری بین نقشها و تنظیمات موجود است را اعلان کند. با تشخیص این، محقق آگاهانه تنها اجازه می‌دهد که داده‌های جمع آوری شده منجر به ساخت دسته‌ها شوند. دو ابر دسته ارائه شده اول با هم نتایج متون پیشین را بازتاب می‌کنند که شامل چندین نقش بوده است که متخصصان امنیت اطلاعات پذیرفته‌اند که برای پیاده سازی برنامه امنیت اطلاعاتشان در سازمان مالی بزرگ از طریق استراتژی امنیت اطلاعات به کار ببرند (Carter, Grover, & Bennett Thatcher, 2011; Weill & Woerner,2013). دوم اینکه تنظیم استراتژی امنیت اطلاعات در سازمان مالی بزرگ از نزدیک بحث انجام شده در فصل ۲ را دنبال می‌کند که در آن انواع ممکن تنظیمات عمومی استراتژی در یک سازمان نمایش داده می‌شوند (Wagner & Weitzel, 2012). به این نکته باید توجه شود که متون مروری، متونی را در نظر گرفته

www.takbook.com

است که بر روی بخش سازمانهای غیر عمومی متمرکز شده بودند. داده جمع آوری شده در اینجا نشان دهنده امنیت اطلاعات بخش عمومی است که کاملا از سازمانهای مالی بزرگ می‌آیند. نتایج باید کاملا بازتاب تجربه سازمانهای بخش عمومی باشد. برای سومین دسته، تحلیل داده جمع آوری شده بر ساختار پیچیده استراتژی امنیت اطلاعات نگاهی داشت. منابع که چهارمین دسته بودند ممکن بود خارج از حوزه دسته مرکزی باشد. منابع اولا در پایداری تلاشهای استراتژی امنیت اطلاعات کمک کرده و می‌توانند عاملی در محرک نگاهداشتن آن در حالی که متاثر از تغییرات بلند مدت بوده و نه در توسعه استراتژی باشند. چهارمین دسته در چهار پاراگراف بعدی بررسی می‌شود تا از اینکه چگونه هر یک از چهار ابر گروه ایجاد شده‌اند دید کلی ایجاد کند.

۴-۳-۳-۱ دسته نقشهای ارائه شده

اولین ابر دسته‌ها از مجموعه نقشهایی بود که بیان می‌کند ماموران ارشد امنیت باید نیاز به حفظ هماهنگی و سازگاری را در ابتدای صف حفظ کنند و این به خاطر قانون مقرر شده‌ای است که گزارش هماهنگی را برای سیستمی که از کنترلهای امنیتی توصیه شده استفاده می‌کند و به عنوان یک بخش اصلی از شغلشان به کار رفته است ضروری می‌داند (Corbet; 2014). به علاوه، اغلب ماموران ارشد امنیت از نقشهای دیگر برای تفاوت درجات مورد نیاز استفاده کرده‌اند مثل داشتن رهبری بالا به پایین، تضمین تصویر عمومی، رقابت با دیگر سازمانها، راهکارهای همیشه در حال تغییر، پذیرش یا تطبیق بهترین عملکردها و یا در موقعیتهای نادر سازماندهی مجدد برای پذیرش محدودیت منابع.

۴-۳-۳-۲ دسته تنظیمات ارائه شده

تنظیمات راهی را در نظر می‌گیرد که در آن ماموران ارشد امنیت به سمت هدف برای برآورده کردن اهداف کسب و کار و یا سیستمهای اطلاعاتی تنظیم کرده بودند. تنظیمات اضافی به چگونگی اینکه ماموران ارشد امنیت، امنیت را به خودی خود اجرا می‌کنند نگاهی کرده و به کمبودهای روزانه و وقایع رسیدگی می‌کند. برخی ماموران ارشد امنیت نگرانی خود را در مورد اینکه آنها هیچ جهتگیری برای رهبری ندارند ابراز کردند. پاسخگوی T8 (پرسنل ارتباطات) بیان کرد " ما هیچ استراتژی نوشته شده‌ای نداریم. ما همینطور که پیش می‌رویم تصمیم می‌گیریم. ما آن را به صورت مکتوب نداریم فقط آن را انجام می‌دهیم. مکتوب شده نیست و

www.takbook.com

در ذهن پرسنل می‌باشد" که به طور خلاصه کمبود جهت گیری در برخی واحدها را نشان می‌دهد. مامور ارشد امنیت از موقعیتهای منحصر به فرد بهترین را برای رسیدگی به امنیت اطلاعاتشان برمی‌گزینند. این طبقه بندی‌ها تحت ابر دسته‌ها شامل هماهنگی به عنوان کسب و کار، کسب و کار و سیستمهای اطلاعاتی، سیستمهای اطلاعاتی، امنیت اطلاعات بر مبنای خودشان و خاص منظوره AD HOC و بدون امنیت هستند.

۴-۳-۳-۳ طبقه بندی پیچیدگی‌های ارائه شده

پیچیدگیهای استراتژی امنیت اطلاعات در هر مصاحبه به خاطر این است که کل استراتژی برای شروع پیچیده است یا به سادگی این بوده است که یک فرآیند سه مرحله‌ای هر روز استفاده می‌شود. همواره با پیچیدگیهای استراتژی امنیت اطلاعات روبرو هستیم، از کل فرایند ایجاد استراتژی تا پایان آن و آنچه استراتژی باید برای آن تشکیل شود شامل: دیدگاه، نیازمندیهای ماموریت، ارتباطات و مشارکتها، دانستن امنیت، اعتماد، جلب رای و توسعه استراتژی.

۴-۳-۳-۴ طبقه بندی (دسته) منابع ارائه شده

ماموران ارشد امنیت بیان کردند که منابع به عنوان حوزه‌ای برای نگهداری اجرای برنامه امنیت اطلاعات ضروری هستند اما برای اطلاعاتش ضروری نیستند. منابع برای ماموران ارشد امنیت مهم می‌باشند زیرا که برای تضمین پرسنل شایسته‌ای که برای آنها کار می‌کنند مهم هستند، که این اهمیت در کنار نیاز به دسترس بودن آموزش به کار گیری آنها و داشتن ابزارهای امنیتی مناسب برای انجام وظایف روزانه قرار داد. پاسخگوی F5 (پرسنل ارتباطات) بر روی ابزار تاکید کرد: "ابزارهایی که الان تا ۶ ماه آینده استفاده می‌شود و چگونه این موارد با معماری متناسب هستند". دسته بندی دیگری در بین منابع ابر دسته، داشتن بودجه کافی برای حفظ عملیات، خرید ابزارها، گرفتن پرسنل و به روز نگهداشتن مهارتهای امنیتی هستند (اداره بازرسی عمومی (OIG). نتیجه ترکیب دسته‌ها در یک دسته بزرگتر با طبیعتی مشابه تمرکز این مطالعه را،استراتژی به عنوان نقطه تمرکز به سمت ماموران ارشد امنیت به عنوان نقطه مرکزی یا بالا برنده جا به جا می‌کند.

www.takbook.com

۴-۳-۴ نتایج کد گذاری محوری

محقق با استفاده مداوم CRG داده‌های جمع آوری شده و ۳۵ دسته ارائه شده را که از کد گذاری باز به دست آمد مرتب سازی کرد. هر دسته ارائه شده در فرم CRG وارد شده و مورده ارزیابی قرار گرفت. برخی از آنها به این نقطه رسیدند که خیلی شبیه به دیگران هستند و در نتیجه محقق آنها را با هم ترکیب کرد. همانطور که فرآیند پیش می‌رفت، محقق شروع به یکی کردن گروه‌ها جدا ولی شبیه به هم کرد. با ادامه دادن این کار، اولین دسته گروه‌ها تحت گروه بندی نقشها (جدول ۱۴، گروه بندی نقشها در دسته‌ها) حذف شد چون مشابه دسته دیگر بود. از فرآیند مرور CRG از ۲۴ دسته سه گروه بندی دیگر از درون چهار گروه بندی ایجاد شد. جدول ۱۵، ۱۶ و ۱۷ برای دریافت دیگر احتمالاتی که آیا دیگر دسته‌های جدول ۱۲ می‌توانند با یکدیگر ترکیب شوند ایجاد شد. این چهار گروه اصلی: نقشها، تنظیمات، پیچیدگی-ها و منابع از این فرآیند به مرحله بعدی یعنی فرآیند کد گذاری انتخابی رفتند.

جدول ۱۵. گروه بندی تنظیمات در دسته‌ها

پیشنهاد نقش	دسته منتخب
مامور ارشد امنیت اهداف ISS را با اهداف کسب و کار تنظیم می‌کند اغلب کسب و کار اهداف مامور ارشد امنیت را معین می‌کند	کسب و کار
مامور ارشد امنیت اهداف را هم با اهداف کسب و کار و هم با اهداف IT تنظیم می‌کند	سیستمهای کسب و کار و اطلاعاتی
مامور ارشد تنظیمات را به مامور ارشد امنیت دیکته می‌کند	سیستمهای اطلاعاتی
برخی ماموران ارشد امنیت بودجه خودشان را داشته و اهداف را خودشان تنظیم می‌کنند	امنیت اطلاعات
مامور ارشد امنیتها هیچ راهنمایی نداشته و اکثرا بر اساس موقعیت کار می‌کنند. از برنامه ریزی پروژه به عنوان استراتژی استفاده می‌کنند.	هیچ

www.takbook.com

جدول ۱۶. گروه بندی پیچیدگی‌ها در دسته‌ها

پیشنهاد نقش	دسته منتخب
تشخیص نیاز به دیدن یک حذف و داشتن یک دیدگاه برای هر هدف	رویای غیر عملی
اولویت بندی اینکه چه چیزی در برنامه آنها اهمیت دارد و اولویتها به ترتیب کدام است	نیازهای ماموریت
صحبت کردن و دریافت پیام راهی حیاتی به سمت موفقیت است	ارتباطات
تشخیص امنیت به عنوان گام اولیه اساسی در فرآیند	دانستن امنیت
مشتریان باید بتوانند به مامور ارشد امنیت اعتماد کنند	اعتماد
تشخیص جلب رای از رهبری برای برنامه بنیادی است	جلب رای
فرآیند واقعی ایجاد یک استراتژی (سه یا ماکزیمم چهار هدف)	توسعه

جدول ۱۷. منابع گروه بندی شده در دسته‌ها

پیشنهاد نقش	دسته منتخب
نیاز به داشتن سرمایه کافی برای اجرای برنامه	بودجه
باید ابزارهای مناسب برای اجرای بازرسی را داشت	ابزار
نیاز به داشتن افراد شایسته برای استفاده از ابزارها و یافتن ناهنجاری در امنیت	پرسنل
پرسنل نیاز دارند که برای حفظ مهارت‌هایشان آموزش کسب کنند	آموزش

۴-۳-۵ کد گذاری انتخابی

محقق تحلیلهای خود را بر روی داده‌های جمع آوری شده تا آخرین مرحله که کد گذاری انتخابی بود ادامه داد و در این مرحله به این توجه داشت که، چه چیزی استراتژی امنیت

www.takbook.com

اطلاعات را پیچیده می‌کند، چگونه شکل می‌گیرد، چه چیزی آن را حفظ می‌کند، چگونه با دیگر استراتژیها تنظیم می‌شود، و چه نقشهایی را مامور ارشد امنیت برای برآوردن نیازهای برنامه امنیت اطلاعات برمی‌گزینند.

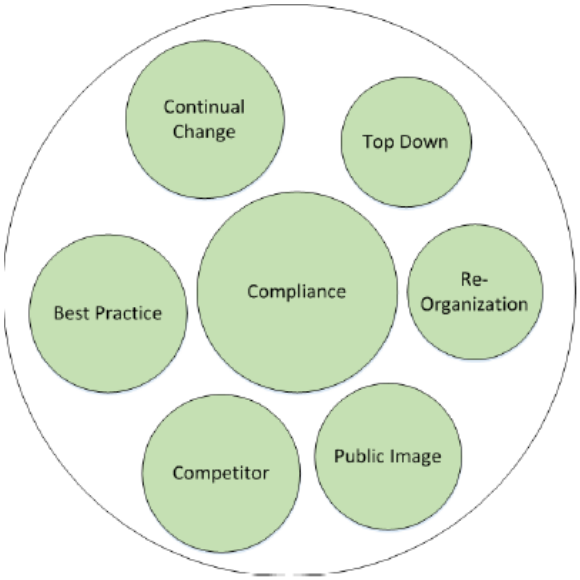
مساله اولیه تحقیق بیان می‌کند که محقق باید داده‌های جمع آوری شده را مرور کند که ممکن است فهمی از پیچیدگی استراتژی امنیت اطلاعات تولید کند. مطالعه باید بازگو کند که چه نقشهای متفاوتی برای متخصصان امنیت اطلاعات وجود دارند و روشهایی که متخصصان امنیت اطلاعات استراتژیها را از یکدیگر متمایز می‌کنند چیست. علاوه بر آن، این مطالعه ممکن است کمک کند تا بتوان تعیین کرد که چگونه استراتژیهای امنیت اطلاعات با هم در یک سازمان مالی بزرگ متفاوت است و چگونه روشی که در آن سازمان ممکن است استراتژی امنیت اطلاعات را راه بیاندازد. چهار حوزه بزرگ از مطالعه استخراج شد که یکی از آنها به نقشها، تنظیمات، پیچیدگی‌ها و منابع نگاهی داشتند. هر یک از آنها برای توسعه دسته اصلی فعالیتهای مامور ارشد امنیت برای به دست آوردن استراتژی کلیدی است.

۱-۵-۳-۴ نقشها

اکثریت ماموران ارشد امنیت بیان کردند که دسته نقش اصلی که استفاده می‌شود هماهنگی است، این دسته برای کار کردن در سازمان مرکزیت دارد. بر عکس آن، اکثریت ماموران ارشد امنیت بازگو کردند که چند تا از نقشهای کم اهمیت به صورت مکرر در دسته استفاده نمی‌شود. نقشهای اصلی که به صورت مکرر توسط متخصصان امنیت اطلاعات استفاده نمی‌شدند تصویر عمومی، رقیب، سازماندهی مجدد و ارتباطات قدرت بودند که از بین آنها ارتباطات قدرت اصلا مورد استفاده نبود. چهار نقش اصلی که مورد استفاده متخصصان امنیت اطلاعات بودند شامل نقش هماهنگی، نقش تغییر مداوم، نقش بهترین عملکرد ونقش بالا به پایین بودند (Seholzer, 2012). شکل ۲ مرکزیت نقشهایی را که مامور ارشد امنیت استفاده می‌کند نشان می‌دهد. هماهنگی یکی از نقشهایی است که همه ماموران ارشد امنیت استفاده می‌کنند (که در مرکز نمایش داده شده است) و بخشهایی با درجات مختلف از نقشهای دیگر در بخش عمومی به کار گرفته می‌شود. ریشه یا هدف برنامه امنیت اطلاعات حفاظت و تضمین محرمانگی confidentiality، تمامیت و جامعیت integrity ، و دسترس پذیری availability (CIA) داده و سیستمهای اطلاعاتی مورد اعتماد امنیت اطلاعات است (Krutz & Vines, 2001). نقش

www.takbook.com

هماهنگی که متخصص امنیت اطلاعات برای طبقه بندی هر سیستم اطلاعاتی استفاده می‌کند مطابق راهنمای منتشر شده توسط موسسه ملی استانداردها و فناوری (NIST) (بخش امنیت کامپیوتر (CSD) است. متخصص امنیت اطلاعات باید از لزومات کارت امتیازی FISMA تبعیت کند (Burwell, 2013; Corbet, 2014).



شکل ۲. نقشها

Compliance -تبعیت
Continual change-تغییرات پیوسته
Top down -بالا به پایین
Reorganization -سازماندهی مجدد
Public image -تصویر عمومی
Competitor-رقیب
Best practiceبهترین عملکرد

متخصصان امنیت اطلاعات بیان می‌کنند که به تغییر مداوم و تطبیق با وقایع نیاز است همانطور که آنها در طی زمان تکامل می‌یابند باید استراتژی امنیت اطلاعاتشان را به روز رسانی کنند. ماموران ارشد امنیت این را در دو روش مشاهده کرده اند. نمایشی از این قضیه پاسخ پاسخگوی E3 (پرسنل ارتباطات) است که بیان کرد: "درون سازمان مامور ارشد امنیت این فرآیند تطبیقی از واقعی سازی اولویتهایی است که می‌تواند تغییر کند... میزان سرعت عملیات،

www.takbook.com

حرکت تهدید، فناوری نوظهور و دیگر عوامل به منظور به واقعیت پیوستن دیدگاه کلی " اول، تغییر مداوم به معنی این است که بخش کسب و کار سازمان به طور پیوسته در حال تغییر روشی می‌باشد که امنیت اجرا می‌کند و به صورت دوره‌ای نیازهای جدیدی در بخش امنیت اطلاعات ایجاد می‌شود که گاهی اوقات بدون هماهنگی قبلی است. پاسخگوی E3 (پرسنل ارتباطات) گفت "اساسا قوانین بنیادی باید اولویت داده شوند سپس ذینفعان می‌فهمند که چه زمانی پوشش بازی را دارند و چه وقت به اولویت بندی نیاز دارند؛ چه زمانی و کجا آنها نیاز به اولویت بندی مجدد در برابر اولویتهای رقابتی دارند" چندین مامور ارشد امنیت اذعان کردند که مدیریتشان در حقیقت چندین بار در طی یکسال تغییر میکند. دومین روشی که ماموران ارشد امنیت توضیح دادند یک راهکار چابک‌تر بود، راهکاری که متخصص امنیت اطلاعات باید به طور مداوم ارزیابی کند تا ببیند که آیا پیشرفتی به سوی برآورده شدن اهداف استراتژی و ایجاد تطبیقات لازم دارد. بسیاری این کار را انجام نمی‌دهند، اما تعداد کمی از ماموران ارشد امنیت از نقشه‌شان استفاده می‌کنند و آن را به صورت دوره‌ای در طی یک دوره سالیانه تنظیم می‌کنند. پاسخگوی P5 (پرسنل ارتباطات) بیان کرد "برخی از اولویتها خارج از کنترل است. سازمان آنها را مشخص می‌کند. مامور ارشد اطلاعات آنها را باید تنظیم کند و باید اهداف سازمانی بالاتری وجود داشته باشد. اولویتها از طریق کانال بالایی تنظیم می‌شود." آنهایی که این موارد را می‌پذیرند، اهداف استراتژیشان معمولا برآورده می‌شود. آنهایی که چنین مواردی را ندارند، اغلب فقط بر اساس موقعیتهای پیش آمده عمل می‌کنند.

متخصصان امنیت اطلاعات بهترین عملکرد را در صنعت بررسی میکنند. بهترین عملکردهای کسب و کار شامل کل محدوده‌ای از فعالیتها است که از استفاده گام به گام دستورالعملهای ساده نگهداشتن کتاب دستورالعمل پایه یا بنیادی (Olsen, 2007) تا تلاش برای رسیدن به سطح پنج ساختار مدل یکپارچگی قابلیت بلوغcapability maturity model integration (CMMI) را پوشش می‌دهد (Bunker, 2012; CMMI Team, 2010). پاسخگوی J7 (پرسنل ارتباطات) با بیان این مطلب افزود "استراتژی امنیت اطلاعات برای من خیلی ساده است، به این معنی که چقدر دقیق و موثر ماموریتمان را به انجام برسانیم. قرار دادن سنگ بناهایی از نقطه A به نقطه B بوده و بدون صداقت، یک فرآیند منطقی نمی‌تواند استراتژی دقیقی داشته باشد..." متخصصان امنیت اطلاعات بررسی‌های لازم را انجام داده و عملکردها را از روی فرآیند مهندسی مجدد و مدلهای موثری همچون برنامه ریزی برای بررسی فعالیت، روش شناسی

www.takbook.com

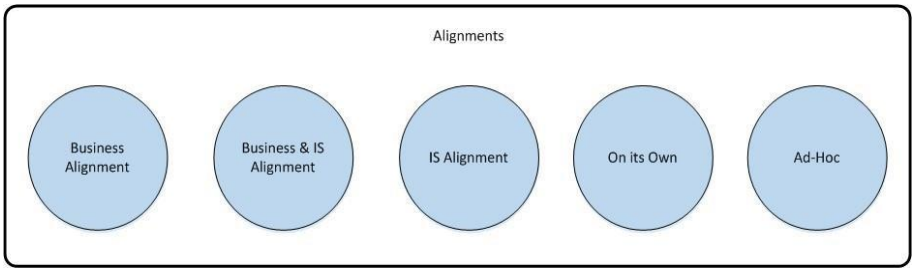
نقاط قوت و ضعف، فرصتها و تهدیدها (SWOT) انتخاب کردند (Moen & Norman, 2009; TeamFree Management Ebooks (FME), 2014). ساختارهای حاصل از بالا به پایین که وجود دارد و باعث می‌شود مامور ارشد امنیت در نتیجه تحریک شدن توسط امنیت اطلاعات یا محرک امنیت اطلاعات با نیروی کاری واکنش نشان دهد. بسیاری از ماموران ارشد امنیت اولویت‌هایی دارند که توسط مدیریت بالاتر به آنها دیکته می‌شود یا آنها را راهنمایی می‌کنند که چگونه باید برنامه امنیت اطلاعات را اجرا کنند. یکی از پاسخگویان با بیان اینکه "اولویتها ممکن است توسط مامور ارشد اطلاعات نیز تغییر کند. زمانی که مامور ارشد امنیت این چنین دستور می‌دهد، پس باید آنگونه انجام شود " به این نکته اشاره کرد که مامور ارشد امنیت می‌تواند مسیر آنها را تغییر دهد. ماموران ارشد امنیت در تحریک نیروی کار برای انعکاس تصویر حاصل از طبیعت بالا به پایین خود مختار هستند که نیروی کار را راهنمایی یا جهت می‌دهد که چگونه باید کارش را انجام دهد. اینها نقشهایی هستند که از مصاحبه‌های انجام شده با ماموران ارشد امنیت سازمانها مشاهده شدند. ابر دسته دیگری که به محقق کردن پتانسیل کمک می‌کند، منابع و روشهایی بود که مامور ارشد امنیت از طریق آنها از پرسنل بهره می‌گرفت.

۴ ۳ ۵ ۲ تنظیمات

برخی ماموران ارشد امنیت بیان کردند که امنیت اطلاعات تنها خرج اضافی است که توسط کسب و کار انجام می‌شود، اغلب به طور آشکار به برنامه امنیت اطلاعات حداقل‌هایی برای قانونهای مقرر شده داده می‌شود و پس از آن به آنها اجازه داده می‌شود که از هر راه ممکنی برای برآورده کردن نیازهای مقرر عمل کنند. این مساله از پاسخگوی S1 (پرسنل ارتباطات) گرفته شد زمانیکه بیان کرد "گرفتن سرمایه با تعداد زیادی اولویتهای در حال رقابت سخت است،زیرا که امنیت اطلاعات مشاهده نمی‌شود، ولی وقتی که اشتباهی رخ می‌دهد، همه نارضایتی خود را اعلام می‌کنند." ماموران ارشد امنیت که به صورت خاص خودشان کار می‌کنند رسیدگی به مسائل را یکی پس از دیگری رها کرده و برای اینکه مشخص شود که آیا کار آنها در برنامه امنیت اطلاعات موفق بوده است یا خیر هیچ برنامه استراتژیک رسمی ندارند. پاسخگوی P5 (پرسنل ارتباطات) با بیان اینکه آنها همیشه قبل از اینکه استراتژی را به کار بگیرند، آتش را دنبال می‌کنند، این مساله را مشخص کرد " وقتی که آتشی شعله ور می‌شود، مهم نیست که کجا اتفاق افتاده است، من همه موارد را کنار گذاشته و آتش را دنبال می‌کنم

www.takbook.com

و پس از اینکه آتش را فرو نشاندیم بر اساس اولویت‌های مامور ارشد امنیت عمل می‌کنیم اما وقتی آتش سوزی رخ می‌دهد ما اول به آتش رسیدگی می‌کنیم." سازمان‌هایی که مامور ارشد امنیت آنها بر مبنای خودش کار می‌کند اگر مامور ارشد امنیت به درستی عمل کند، آنها به درستی کار می‌کنند، اما اگر مامور ارشد امنیت مجبور به انجام وظیفه‌ای باشد که ریسک را در سازمان افزایش دهد، با شکست مواجه می‌شود. شکل ۳ تنظیمات ممکن برای استراتژیهای امنیت اطلاعات را نشان می‌دهد.



شکل ۳. تنظیمات و هماهنگی ها

Alignmentsتنظیمات و هماهنگی ها

Business alignmentتنظیم کسب و کار

Business and IS alignment تنظیم کسب و کار و IS- –

IS alignment تنظیم IS–

On its own– به خودی خود

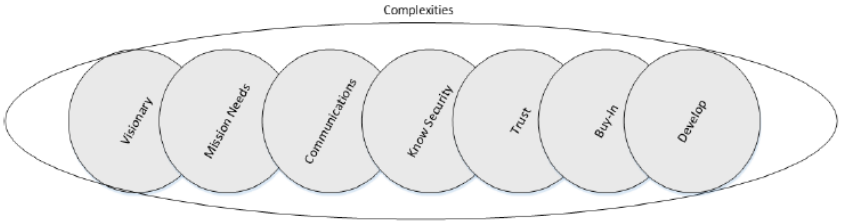
Ad hocخاص منظوره

هر سازمان برای برآورده کردن نیازهای ماموریت خاص خودش به طور متفاوتی عمل می‌کند. محقق یافت که ماموران ارشد امنیت در هر زیر بخش از سازمان بزرگ دارای بخشهایی هستند که مشابه بوده و بعضی از آنها دارای ماموریتی می‌باشند که از کل سازمان بزرگ متفاوت است. هر زیر بخش یا واحد کوچک استراتژی امنیت اطلاعاتش را برای برآوردن نیازمندی ماموریتش تنظیم می‌کند. همه پنج تنظیمات ارائه شده که در فصل ۲ بحث شد در سازمان بزرگ و در بین زیر سازمانهای شرکت کننده کار می‌کردند. دو نوع از بیشترین تنظیمات که استراتژی امنیت اطلاعات با آن تنظیم می‌شدند استراتژی کسب و کار و سیستمهای اطلاعاتی بودند و دوم اینکه تعداد کمی از سازمانها به صورت انفرادی کار می‌کردند که هیچ استراتژی نداشته و هیچ سیستم داخلی به جز اینکه به صورت تاکتیکی برای رسیدگی به بحران‌ها یکی پس از دیگری نداشتند.

www.takbook.com

۴ ۳ ۵ ۳ پیچیدگی‌ها

تعدادی از دسته‌ها در بخشی از تحلیل قیاسی و ترکیب عبارات در طی فرآیند کد گذاری با یکدیگر ترکیب شده و بخشهایی را ساختند که به آن پیچیدگی‌های استراتژی امنیت اطلاعات ابر دسته گفته می‌شود. این ابر دسته به چندین زیر دسته تقسیم می‌شود: دیدگاه، نیازهای ماموریت، ارتباطات و مشارکت، دانستن امنیت، اعتماد، جلب رای و ایجاد استراتژی. هر یک از این زیر دسته‌ها به همدیگر متصل هستند و البته همچنین یک بخش تشکیل دهنده ابر دسته کلی پیچیدگی‌ها هستند. شکل ۴ اتصال زیر اتصال بین بخشهای ترکیب شده را نشان می‌دهد بر اساس اهداف متخصصان امنیت اطلاعات، کسب و کار و استراتژی امنیت اطلاعات باعث استراتژی منسجمی می‌شود.



شکل ۴. پیچیدگی‌ها

Visionary -تصور غیر عملی (رویایی)
Mission needs-نیازمندیهای ماموریت
communication– ارتباطات
Knowing security– دانستن امنیت
trust – اعتماد
Buy in – جلب رای
Developتوسعه

چشم اندازه یعنی دیدگاهی که واقعا مامور ارشد امنیت بر روی آن تمرکز کرده تا سازمان را طی سه تا هفت سال آینده با تعیین ریسک و آگاه کردن رهبر از فعالیتهای ضروری که در مقابله با ریسک لازم است به جای امنی برساند. "ما در چشم‌اندازمان در مسیری که باید برویم به پنج تا هفت سال آینده نگاه می‌کنیم " (پاسخگو A0، پرسنل ارتباطات). مامور ارشد امنیت نیازهای ماموریت را برای تنظیم اولویتهای استراتژی امنیت اطلاعات در نظر می‌گیرد.

او برای تضمین اینکه امنیت در شروع پروژه دخیل بوده با ذینفعانش مشورت می‌کند به جای پروژه‌ای که دچار مشکل امنیتی شده و قرار است امور امنیتی به کار گرفته شود. ماموران

www.takbook.com

ارشد امنیت باید با هر کسی در که سیستمهای اطلاعاتی و کسب و کار دخیل هستند ارتباط داشته و مشارکت کند. پاسخگوی P5 (پرسنل ارتباطات) بیان کرد "امنیت اطلاعات راهکاری جمعی، مشارکتی است که واقعا به ندرت هر سازمانی به آن دست می‌یابد. بنابراین استراتژی امنیت اطلاعات شما یکی از ساختارهای تیمی مشارکتی است که بر روی ارزش واحد کسب و کار متمرکز شده است." ارتباطات باید هر زمانی که شانسی برای بحث در مورد تهدیدها است صورت بگیرد و از این فرصتها برای صحبت در مورد کاهش تهدیدها بهره برد (Scully, 2014).

زمانی که برای بدست آوردن امنیت در شروع چرخه زندگی توسعه سیستم کار می‌کنیم، دانستن امنیت کلیدی است. ماموران ارشد امنیت باید تکنولوژیهای جدید را یافته و همیشه در دانستن اینکه چه چیزی در حال حاضر در شبکه مورد استفاده قرار می‌گیرد، یک قدم جلوتر باشند. قابلیت مامور ارشد امنیت در ایجاد اعتماد، آگاه نگاهداشتن ذینفعان و بدست آوردن اطمینان آنها از اینکه از همه مسائل امنیتی آگاه خواهند شد بسیار اهمیت دارد. پاسخگوی L9، این سوال را در مورد اعتماد مطرح کرد: " چقدر ارتباطات شما و سطح حمایت اعتماد به رهبری شما قوی است؟" به منظور بدست آوردن و نگهداری اعتماد به رهبری، رهبر باید اطلاعات درستی را از مامور ارشد امنیت بدست آورد. مامور ارشد امنیت باید بتواند درون سازمان امنیت را به مجریان عرضه کند و نظر و یا حمایت مجریان سطح بالا را جلب کند. جلب رای در موفقیت استراتژی اساسی است (Hu, Dinev, Hart, & Cooke, 2012). هنر ایجاد استراتژی در ساختن آن از آغاز با استفاده از همه بخشهای پیچیدگی ابر دسته، کوچک نگاهداشتن آن، و در عین حال در برداشتن تمام برنامه امنیت اطلاعات است. مامور ارشد امنیت بیان می‌کند که استراتژی باید به سه یا چهار هدف فراگیر محدود شود. یکی از پاسخگویان به این مساله اشاره کرد "نیاز است که استراتژی امنیت اطلاعات ساده باشد. پیچیدگی، دشمن استراتژی است" (پاسخگوی L9، پرسنل ارتباطات). و پاسخگوی V8 (پرسنل ارتباطات) این مساله را به روایتی دیگر بیان کرد: ".. هفت یا هشت المان به سه یا چهار هدف می‌رسند. سپس ما می‌توانیم به استراتژی امنیت اطلاعات در یک برنامه سه ساله نگاه کنیم." اهداف باید در مدت زمان مشخص شده برای استراتژی قابل دستیابی باشند. و مهمتر از همه، اهداف باید به شکلی نوشته شوند تا بتوان آنها را به صورت دوره‌ای به منظور کامل شدن چک کرد.

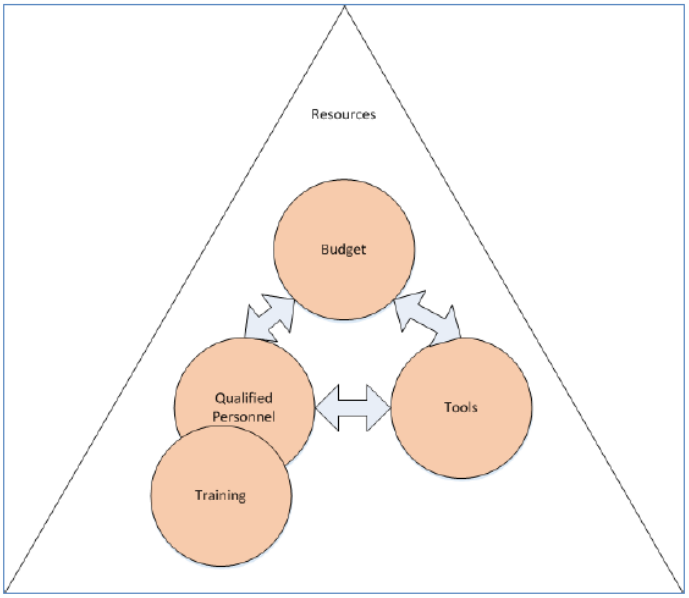
www.takbook.com

یک تحلیل قیاسی از صحبتهای مامور ارشد امنیت نشان داد که پیچیدگی استراتژی امنیت اطلاعات زنجیره‌ای از وقایع است که در هم تنیده شده و به هم متصل هستند. شکل ۵ زنجیره وقایع را نشان می‌دهد که هر واقعه از یکی به دیگری انتقال می‌یابد تا در انتها به انجام برسد. استراتژی امنیت اطلاعات عملیات پویایی است که بر روی چشم انداز مامور ارشد امنیت تمرکز داشته و آن را با اهداف استراتژی مرتبه بالاتر تنظیم می‌کند. توسعه یک استراتژی فرآیندی فعال است که به توجه مداوم نیاز دارد. همچنین برای شکل دادن آن به تنظیم در سازمان و رهبری مامور ارشد امنیت که فعالانه در نقشهای مختلف کار می‌کند نیاز است.

۴ ۵ ۳ ۴ منابع

زمانی که از ماموران ارشد امنیت پرسیده می‌شد "یک استراتژی امنیت اطلاعات موفق به چه چیزی نیاز دارد...." نیاز به منابع را بارها و بارها بیان کردند (جدول ۵ سوال مصاحبه). منابع شامل چهار دسته هستند، آنهایی که آموزش داده می‌شوند، پرسنل واجد صلاحیت، ابزارها و بودجه. مامور ارشد امنیتها درخواست آموزش مجدد برای کارمندانشان را داشتند، مخصوصا آموزش مهارتهای امنیتی اما آنها تاکید بیشتری بر روی آموزش کسب و کار داشتند تا به پرسنل یاد بدهند که چگونه با ذینفعان ارتباط برقرار کنند. پاسخگوی J7 (پرسنل ارتباطات) این موضوع را بیان کرد "... پرسنل واجد صلاحیت برای حمایت از اولویتهای سازمان ضروری است". شکل ۵ نشان می‌دهد که چگونه دسته‌های منابع به هم مرتبط می‌شوند، چگونه با یکدیگر در تعامل هستند و چگونه هر دسته به حفظ ابر دسته کمک می‌کند. یکی از اهداف اولیه مامور ارشد امنیت این بود که آنها باید پرسنل واجد صلاحیت را به کار بگیرند.

www.takbook.com



شکل ۵. منابع

منابعresources
Budget – بودجه
Qualified personnel– پرسنل دارای صلاحیت
tools – ابزارها
آموزشTraining

ماموران ارشد امنیت تشخیص دادند که آنها در حال رقابت با بخش تجاری سازمان هستند، زیرا که آنها می‌توانستند به پرسنل امنیتی که به طور مساوی آموزش دیده بودند بیشتر پرداخت کنند. این مساله حفظ پرسنل با تجربه را برای مامور ارشد امنیت سختتر می‌کرد. ماموران ارشد امنیت متوجه شدند که آموزش پیچیده بوده و می‌تواند موجب مشکل شود به طوری که زمانی که پرسنل در حال آموزش دیدن هستند بسیار خوب عمل می‌کنند، اما مشکل از اینجا شروع می‌شود که به محض اینکه آنها آموزش می‌دیدند بسیاری از آنها می‌توانند به مشاغلی با دستمزد بالاتر بروند. چالش مامور ارشد امنیت این بود که تعیین کند کارکنان به چه مهارتهایی نیاز دارند و سعی کند این فرصت را پیش آورد تا آنها مهارتهای ضروری را به دست آورند تا همه کارکنان را در سطح یکسانی حفظ کنند. ماموران ارشد امنیت می-خواستند که کارکنان بمانند و پیشرفت کنند. برخی ماموران ارشد امنیت می‌خواستند کار راهه شغلی ایجاد شود تا به پرسنل کمک کند تا در مراحل مبتدی، فراگیر، همکار، مربی و

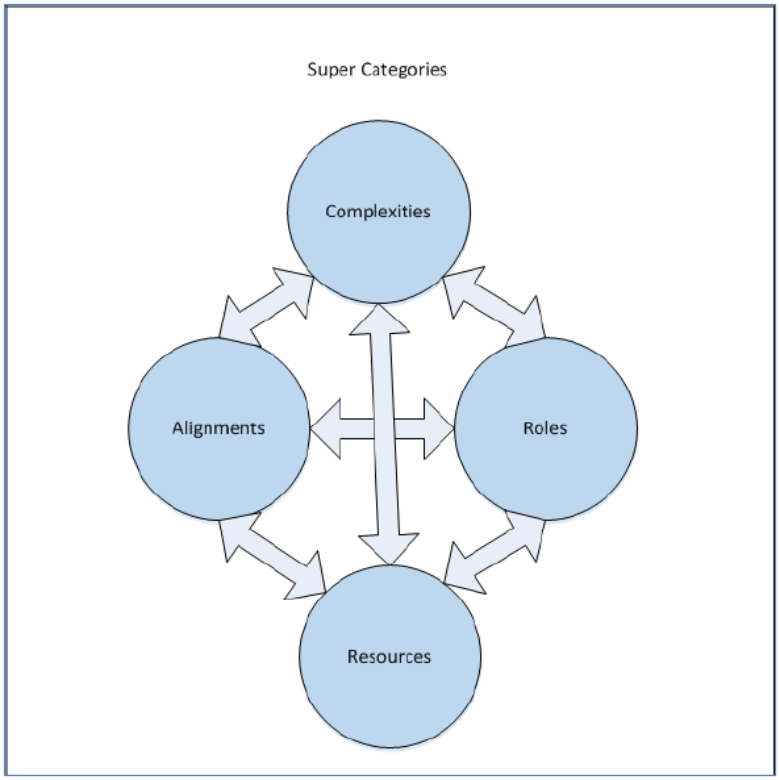
www.takbook.com

سر انجام سرپرست قرار گرفته و پیشرفت کند. مامور ارشد امنیت باید همیشه در پیشرفت افراد کنش گرا بوده و به آنها اجازه دهد تا به بلوغ برسند یا ریسک رفتن آنها به رفتن شغلهای دیگر ادامه داشته باشد. ارائه مشاوره یکی از ملزومات اولیه است. نه تنها مامور ارشد امنیت باید به جایگزینی مامور ارشد امنیت آموزش دهد بلکه باید به آنها توضیح داده شود که در فرآیند تصمیم گیری آنها چه چیزی پیش خواهد آمد. آموزش تازه‌واردها ابزاری برای تفکر انتقادی بوده و اینکه چگونه تصمیمات مامور ارشد امنیت ممکن است به تازه کاران کمک کند و همچنین ارتباط با مدیریت را محکم‌تر می‌کند.

ابزارها همیشه باید تا حد ممکن در برابر بدافزارهای تکامل یافته به روز نگاهداشته شوند. ماموران ارشد امنیت همیشه در حال جستجوی روشهایی برای بهبود ابزارهای نرم‌افزاریشان هستند که این کار را از طریق قابلیتهای افزوده شده یا خودکار سازی انجام می‌دهند تا بتوانند کامل‌ترین استفاده را از ویژگیهای ابزارهای نرم افزاری ببرند. در نهایت، داشتن بودجه‌ای که اجازه دهد امنیت به صورت کارآ عمل کند بسیار مهم است. مامور ارشد امنیت باید کارشناس توسعه کسب و کار شود. مامور ارشد امنیت باید نمونه‌هایی را بتواند بیابد و بسازد که نشان دهد سرمایه‌ای که برای امنیت گذاشته می‌شود بازگردانده خواهد شد، نه در امنیت بلکه به خاطر امنیت و اینکه چقدر سازمان‌ها به خاطر اجتناب از مشکلات امنیتی می‌توانند پس انداز کنند (به عبارت دیگر با حفظ سازمان از معرض خطر استخراج اطلاعات قرار گرفتن، زیرا که این مساله موجب از دست دادن زمان، بهره‌وری، دارایی‌ها و یا حتی امکان نیاز به جایگزینی دارایی‌ها می‌شود). شکل ۵ روشی را نشان می‌دهد که از طریق آن استراتژی امنیت اطلاعات برقرار می‌ماند. در این شکل نشان داده شده است که چگونه همه دسته‌ها در یکدیگر مخلوط شده‌اند تا ابر دسته منابع را تشکیل دهند.

مطلوب است که محقق با تشخیص ۴ ابر دسته اجازه دهد که هر کدام با یکدیگر به شکلهای مختلف تطابق یافته و ببینند که چگونه ابر دسته‌ها ممکن است دسته اصلی یا پدیده مرکزی را تعیین می‌کنند (Brown, et al., 2002; Hallberg, 2006). شکل ۶، ۴ ابر دسته را نشان داده و اینکه چگونه هر کدام از نتیجه دیگری تاثیر می‌گیرند. پیکانها مشخص کننده وابستگی هر دسته به دیگری است. چندین راه برای به هم اتصال دسته‌ها به یکدیگر در یک داستان وجود دارد. فرایند در هم تنیدن و اتصال دسته‌ها به هم با استفاده از کد گذاری انتخابی باید باعث آشکار کردن دسته اصلی شود.

www.takbook.com



شکل ۶. ابر دسته‌ها

Super category ابر دسته‌ها
– Complexities پیچیدگی‌ها
Alignments تنظیمات –هماهنگی
– Roles نقشها
Resources منابع

۶-۳-۴ نتایج کد گذاری انتخابی

در این بخش، محقق از دومین ابزار نظریه بنیادی برای فرایند کد گذاری استفاده کرد که به آن ماتریس کد گذاری بازتابیReflective coding matrix (CRM) گفته می‌شد. مطابق با آنچه Scott و Howell (۲۰۰۸) بیان کردند، بدست آوردن نظریه یا مدل از داده دشوارترین بخش یک فرآیند است. مرحله کد گذاری انتخابی در نتیجه ساختن یک داستان استخراج شده از داده بدست می‌آید. با ارائه داده از دسته‌های جمع آوری شده در شکل دسته‌های جمع

www.takbook.com

آوری شده یک جریان منطقی از ارتباطات استنباط می‌شود که از فرآیند کد گذاری ساخته می‌شود. داستان به این صورت می‌باشد که چگونه همین این ابر دسته‌ها یکدیگر را تغذیه کرده و بر روی داستان مربوطه از نقطه نظر مامور ارشد امنیت تمرکز می‌کنند که چگونه آنها به صورت سلسله مراتبی با یکدیگر کار کرده و در نهایت به یک دسته اصلی منجر می‌شوند (Hallberg, 2006).

برای دریافت نتایج از مرحله کد گذاری محوری، محقق دومین ابزار Scott و Howell (۲۰۰۸) را استفاده کرد که به آن ماتریس کد گذاری انتخابی گفته می‌شود. این ابزار به محقق اجازه می‌دهد که تحلیلهای قیاسی انجام داده تا انتخابها را تقلیل داده تا به دسته اصلی از بین چهار گروه ابر دسته برسد. فرایند RCM به محقق کمک کرد تا یک فرم را برای ضبط فرآیندها، خواص، ابعاد، و زمینه‌ها به دست آورد که برای درک پیامدها CRG پیشنهاد داده می‌شود.

www.takbook.com

جدول ۱۸. ماتریس کد گذاری بازتابی

دسته هسته‌ای	فعالیتهای مامور ارشد امنیت برای دستیابی به استراتژی			
فرآیندها	انتخاب نقش مناسب	تطبیق با تنظیم مناسب	از عهده پیچیدگی‌های استراتژی برآمدن	بدست آوردن منابع کافی
خصوصیات	مشاهده و تطبیق	تنظیم با جهت مناسب	تصمیم گیری آنچه درست است	رایزنی کردن برای کارها
ابعاد	انتخاب اینکه آیا مبتنی بر مدیریت است، با فرض اینکه تصویر عمومی ارزش بیشتری دارد در جستجوی پیشرفت از دیگران، پذیرش بهترین نتیجه که دیگران به دست آورده‌اند، اختراع مجدد ساختار، تغییر همیشگی و یا هماهنگی	استخرج از کسب و کار، سیستم اطلاعاتی یا امنیت اطلاعات بودن یا دارای هیچ جهتگیری نبودن	بازاری برای جلب رای دریافت اعتماد دانستن امنیت داشتن دیدگاه محدود کردن حوزه برقراری اولویتها پذیرش راهکار کنشگرا	داشتن افراد دارای صلاحیت گرفتن ابزارهای کافی برای اجرای وظایف امنیت اطلاعات دریافت آموزش صحیح گرفتن سرمایه کافی برای کامل کردن استراتژی
مفاهیم	پشتیبانی از ماموریت	هماهنگی و تصمیم برای اتصال	برقراری اهداف متقابل	محدود کردن واقعیت
حالتهای فهمیدن توالی	محدود کردن راهکار مناسب	رسیدن به توافق در برآوردن اهداف	همدستی بر روی نتایج	داشتن سرمایه کافی برای بدست آوردن نیازها

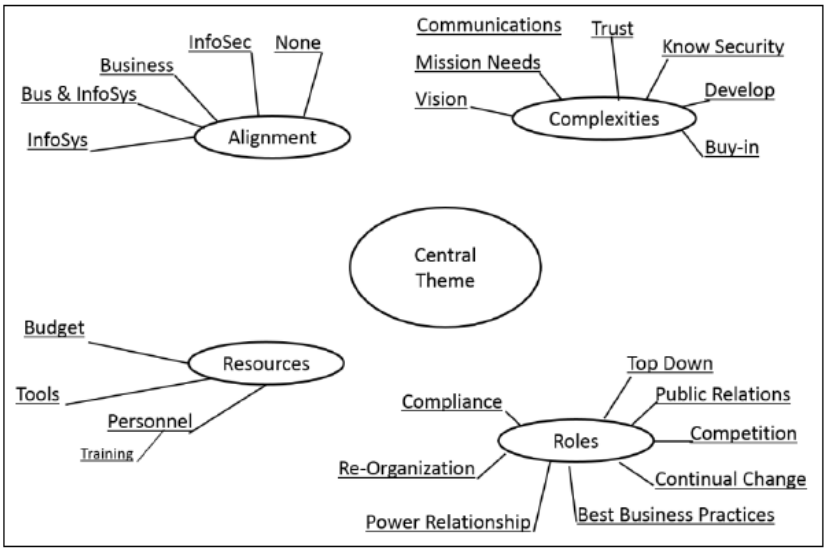
www.takbook.com

RCM چندین تراکنش بین جنبه‌های دسته اصلی (فرآیندها، ویژگیها، ابعاد، مفاهیم و حالتها) را که در ستون سمت چپی قرار دارد با هر یک از دسته‌های اصلی (نقشها، تنظیمات، پیچیدگیها و منابع) در ستونهای بعدی به ترتیب از چپ به راست نمایش می‌دهد. هر سطر یک جنبه از دسته را برآورد کرده و اینکه چگونه در دسته اصلی "فعالیتهای مامور ارشد امنیت برای دستیابی به استراتژی" بازتاب میگرد.

در زمان مراحل پر کردن و برآورد حوزه‌های RCM واضح است که عملیات انجام شده برای رسیدن به خود استراتژی بحرانی‌ترین بخش دسته اصلی است. ماموران ارشد امنیت هسته اصلی برای انجام فعالیتها برای رسیدن به یک استراتژی هستند. جدول ۱۸ روابط پیچیده چهار ابر دسته را در دسته اصلی "فعالیتهای مامور ارشد امنیت برای رسیدن به استراتژی" را نشان می‌دهد. برای ساختن قضیه انتخاب دسته اصلی و نظریه پدیدار شده‌ای که از المانهای RCM به وجود آمده‌اند، محقق از فرآیند کد گذاری انتخابی استفاده کرد (Hallberg, 2006; Pandit, 1996; Scott & Howell, 2008).

محقق از روی داده‌های جمع آوری شده و تحلیل شده روشی را برای نمایش پیشرفت سریع ابر دسته‌های کشف شده ارائه کرد. شکل ۷ تصویری از تقیسمات هر ابر دسته به دسته‌های تشکیل دهنده‌اش در هر ابر دسته نشان می‌دهد. این شکل نشان می‌دهد که هر دسته (زیر آن خط کشیده شده است) به عنوان بخشی از هر ابر دسته (دورش دایره ای ترسیم شده است) که ارتباط آنها با تم یا مضمون مرکزی، هنوز نیاز به ساختار بندی دارد.

www.takbook.com



شکل ۷. نگاشت دسته بندیها

Infosys-سیستمهای اطلاعاتی

Bus & infosys– گذرگاه و سیستم اطلاعاتی

business-کسب و کار

infosec– امنیت اطلاعات

none-هیچ

alignment تنظیم

Vision – چشم انداز

Mission needs -نیازهای ماموریت

communications-ارتباطات

trust – اعتماد

Know security دانستن امنیت

develop – توسعه

– جلب رای جلب رای

Complexitiesپیچیدگیها

Central theme تم یا موضوعیت مرکزی

Budget– بودجه

tools – ابزارها

Personnel – پرسنل

Training– آموزش

resourcesمنابع

www.takbook.com

roles– نقشها
compliance– تبعیت
re-organization– سازماندهی مجدد
power relationship-ارتباط قدرت
top down بالا به پایین
public relations -روابط عمومی
Competition – رقیب
Continual change – تغییر مداوم
Best business practicesبهترین عملکرد کسب و کار

شکل ۶ چگونگی وابستگی‌های موجود بین ابر دسته‌ها را نشان می‌دهد. روش پدید آوری مدل به این صورت است: مامور ارشد امنیت در شروع فرآیند تصمیم گیری وارد می‌شود؛ به این معنی که مامور ارشد امنیت تعریف می‌کند که چگونه نقشها را به کار بگیرد و در تنظیمات نقش داشته باشد، در پیچیدگی‌ها مشارکت می‌کند، و برای منابع رایزنی می‌کند تا ISS تشکیل شود.

محقق به منظور رسیدن به دسته هسته‌ای چهار ابر دسته را با معیارهای خودش مقایسه کرده و تفاوت آنها را سنجیده که بتواند تا حد امکان دسته هسته‌ای یا مرکزی را معین کند. دسته-های لیست شده در جدول ۱۹ به عنوان توالی ۱۲ مرحله‌ای از تکمیل یک نظریه است که تمام ترکیبهای ممکن چهار ابر دسته را پوشش داده است.

با فرض اینکه مامور ارشد امنیت تنها شرکت کننده در یافتن نقشهای استراتژی امنیت اطلاعات باشد که تاثیر مستقیمی بر روی برنامه امنیت اطلاعات دارد، در این حالت سه حوزه می‌تواند موجود باشد که خارج از کنترل مستقیم آنها است: پیچیدگی‌ها، تنظیمات و منابع. منابع خارج از حوزه این کتاب بوده زیرا که ارزیابی آنها مربوط به یافتن نقشهای استراتژی امنیت اطلاعات است. منابع ممکن است برای ارزیابی پایداری و پشتیبانی روزانه فعالیتها مفید باشد. این فعالیت می‌تواند نتایج ۲، ۳، ۴، ۶، ۸، ۹، ۱۰، ۱۱ و ۱۲ را حذف کند. نتایج ۱، ۵ و ۷ ممکن است تنها راههای عملی باشند. از آنجایی که مامور ارشد امنیت با یک نقش شروع می‌کند، خروجی ۱ و ۷ هم حذف شده و بنابراین فقط نتیجه ۵، نتیجه قابل انتخاب برای ارزیابی خواهد بود.

مطالعه برای در نظر گرفتن نتایج ۱ و ۷ بر روی فعالیتهای انجام شده برای حرکت در جهت یک برنامه امنیت اطلاعات برای به دست آوردن محرمانگی، جامعیت، دسترس پذیری داده و

www.takbook.com

سیستمها (CIA)تمرکز می‌کند. تنظیمات ممکن است ورودی‌هایی را از مامور ارشد امنیت دریافت کند اما اکثرا ورودیها از طریق ترکیب تصمیمهای کسب و کار و یا سیستم‌های اطلاعاتی برای حمایت از ماموریت به همراه مامور ارشد امنیت می‌رسند.

جدول ۱۹. جدول نتایج انتخاب

۱	پیچیدگیها	تنظیمات	نقشها	منابع
۲	پیچیدگیها	نقشها	منابع	تنظیمات
۳	پیچیدگیها	منابع	تنظیمات	نقشها
۴	نقشها	پیچیدگیها	منابع	تنظیمات
۵	نقشها	تنظیمات	پیچیدگیها	منابع
۶	نقشها	منابع	تنظیمات	پیچیدگیها
۷	تنظیمات	نقشها	پیچیدگیها	منابع
۸	تنظیمات	پیچیدگیها	منابع	نقشها
۹	تنظیمات	منابع	نقشها	پیچیدگیها
۱۰	منابع	پیچیدگیها	تنظیمات	نقشها
۱۱	منابع	تنظیمات	نقشها	پیچیدگیها
۱۲	منابع	نقشها	پیچیدگیها	تنظیمها

در Lieu با داشتن هیچ تنظیمی، مامور ارشد امنیت ممکن است راهکاری را برای خودش تنظیم کرده یا از تجربه بدون هیچ تنظیمی بهره گیرد که فقط بر اساس موقعیتها عمل کند. بنابراین، تنظیمات باید مهم در نظر گرفته شوند اما در دومین موقعیت مساوی در بالای پیچیدگی‌ها در نتایج قرار داده شوند که نتیجه ۵ را بیشتر اثبات می‌کند.

ممکن است پیچیدگی‌ها در مراحل مختلفی از سه ذینفع در محدوده استراتژی موجود باشد که از سیستمهای اطلاعاتی، کسب و کار و امنیت اطلاعات استخراج شده باشد. استراتژی

www.takbook.com

واقعی از تعامل یا عدم وجود تعامل بین ذینفعان سازمان نشات می‌گیرد. مامور ارشد امنیت استراتژی را بر اساس ورودی‌های ذینفعانش خلق می‌کند. مامور ارشد امنیت باید همه عوامل یا پیچیدگی‌های ساختن استراتژی را که بعدا ممکن است با تنظیمات توافق شده با مدیریت و منابع در دسترس باشند تنظیم کند. بنابراین پیچیدگی‌ها در سومین موقعیت بعد از تنظیمات ولی قبل از منابع قرار می‌گیرد بنابراین نتایج به شماره ۵ محدود می‌شود.

به عنوان دیدگاه جایگزینی از تحلیل قبلی و یکی که از خطوط داستانی برای تحلیل استفاده می‌کند، محقق شروع به دیدن دیدگاه مامور ارشد امنیت به داده‌های جمع آوری شده می‌کند. مامور ارشد امنیت باید داستان را طوری انتخاب کند که در جلسه انتخاب هدف مدیریت پیروز شود و سپس آن را با نقش بعدی ماموریت در سازمانشان با استفاده از منابع مهیا شده تنظیم کند. ماموران ارشد امنیت نتایج خلاصه سازی شده ممکن از جدول ۱۹ را مشاهده کرده و قضیه را با استفاده از نتایج ممکن از ابر دسته‌ها، یکی از بهترین گزینه‌ها را ایجاد می‌کند. بنابراین، هر نقشه به صورت زیر می‌تواند خوانده شود:

- ایجاد پیچیدگی‌های استراتژی امنیت اطلاعات، در نظر گرفتن تنظیم استراتژیک، اجرای نقشهای ضروری، و مهیا شده توسط منابع
- ایجاد پیچیدگی‌های استراتژی امنیت اطلاعات، اجرای نقشهای ضروری، مهیا شده توسط منابع، و در نظر گرفتن تنظیم استراتژیک
- ایجاد پیچیدگی‌های استراتژی امنیت اطلاعات، مهیا شده توسط منابع، در نظر گرفتن تنظیم استراتژیک، اجرای نقشهای ضروری
- اجرای نقشهای ضروری، ایجاد پیچیدگی‌های استراتژی امنیت اطلاعات، مهیا شده توسط منابع، و در نظر گرفتن تنظیم استراتژیک
- اجرای نقشهای ضروری، در نظر گرفتن تنظیم استراتژیک، ایجاد پیچیدگی‌های استراتژی امنیت اطلاعات، مهیا شده توسط منابع
- اجرای نقشهای ضروری، مهیا شده توسط منابع، در نظر گرفتن تنظیم استراتژیک و ایجاد پیچیدگی‌های استراتژی امنیت اطلاعات
- در نظر گرفتن تنظیم استراتژیک، اجرای نقشهای ضروری، ایجاد پیچیدگی‌های استراتژی امنیت اطلاعات، و مهیا شده توسط منابع

www.takbook.com

- در نظر گرفتن تنظیم استراتژیک، ایجاد پیچیدگی‌های استراتژی امنیت اطلاعات، مهیا شده توسط منابع، و اجرای نقشهای ضروری
- در نظر گرفتن تنظیم استراتژیک، مهیا شده توسط منابع، اجرای نقشهای ضروری و ایجاد پیچیدگی‌های استراتژی امنیت اطلاعات
- مهیا شده توسط منابع، ایجاد پیچیدگی‌های استراتژی امنیت اطلاعات، در نظر گرفتن تنظیم استراتژیک، اجرای نقشهای ضروری
- مهیا شده توسط منابع، در نظر گرفتن تنظیم استراتژیک، اجرای نقشهای ضروری و ایجاد پیچیدگی‌های استراتژی امنیت اطلاعات
- مهیا شده توسط منابع، اجرای نقشهای ضروری، ایجاد پیچیدگی‌های استراتژی امنیت اطلاعات و در نظر گرفتن تنظیم استراتژیک

از موارد بیان شده در لیست نشان داده می‌شود که تحلیل می‌تواند به حذف اکثریت اظهارها کمک کند. مجموعه سه مورد اول می‌تواند حذف شود زیرا که "ایجاد پیچیدگی‌های استراتژی امنیت اطلاعات" نتیجه تنظیمات کار کردن با یکدیگر برای رسیدن به توافق نظر است. استراتژی توافقات را جلب می‌کند. مجموعه سه موردی دوم "اجرای نقشهای ضروری" اساس آنچه یک مامور ارشد امنیت در نتیجه تنظیم با یک استراتژی انجام می‌دهد را گرفته که نتیجه اولیه می‌باشد. مجموعه سه موردی سوم "در نظر گرفتن تنظیم استراتژیک" فعالیتی است که یک مامور ارشد امنیت برای هماهنگی رهبری سازمان اجرا می‌کند که آن را با روشی که در آن استراتژی ساخته شده تنظیم کرده و نتیجه تنظیم رهبری در کار کردن با یکدیگر برای رسیدن به توافق است. تنظیمات به صورت پشت سر هم با استراتژی کار می‌کند زیرا که آن راهی است که برای کد گذاری استراتژی به کار می‌رود. مجموعه سه تایی چهارم "مهیا شده توسط منابع" پایداری برنامه امنیت اطلاعات را پس از رسیدن به توافق در بین رهبری برای یک نقش در نظر گرفته و یک تنظیم و یک استراتژی یا یک نقشه برای ارائه یک روش برای دستیابی به استراتژی امنیت اطلاعات کد گذاری می‌شود و این کاری است که توسط مامور ارشد امنیت برای پیاده سازی استراتژی انجام می‌شود. مامور ارشد امنیت باید نقشی را که آنها برای حرکت به سمت تکمیل کردن بازی می‌کنند را انتخاب کند. بنابراین ممکن است نتیجه از دومین مجموعه سه تایی باشد.

www.takbook.com

با نگاه مجدد به دومین مجموعه سه تایی که با کلمات "اجرای نقشهای ضروری" شروع می‌شود. مامور ارشد امنیت تنظیم مدیریت را به عنوان موردی که امنیت به خودی خود، با سیستمهای اطلاعاتی، با کسب و کار یا با مشارکت کسب و کار و سیستمهای اطلاعاتی اجرا می‌شود را بررسی می‌کند به طوری که تشخیص می‌دهد که چه کسی مسئول بوده و در فرآیندی برای رسیدن به نتیجه کار می‌کند. این تنظیمی است که مامور ارشد امنیت برای دستیابی به اهداف برنامه امنیت اطلاعاتیش به سمت آن حرکت می‌کند. پیچیدگیها چشم انداز مامور ارشد امنیت برای بدست آوردن تنظیم و توافق برای بدست آوردن نتایج دلخواه محرمانگی، تمامیت یا یکپارچگی، دسترس پذیری داده و سیستمهای اطلاعاتی است که آنها مسئولش هستند و برای کار کردن با منابع در دسترس مهیا شده برای انجام برنامه امنیت اطلاعات هستند.

روایت نشان داده شده از ماتریس ارائه شده در جدول ۱۹ این است که بهترین نتیجه از یک مامور ارشد امنیت قابلیت او در انتخاب نقش، تعیین تنظیم قابل قبول و تطبیق پیچیدگی‌ها با یک نتیجه دلخواه است. مامور ارشد امنیت در حالی که در حوزه منابع در دسترس کار می‌کند تمام این فعالیتها را انجام می‌دهد. مامور ارشد امنیت باید " نقشهای ضروری را اجرا کند، تنظیم استراتژیک را در نظر بگیرد، پیچیدگی‌های استراتژی امنیت اطلاعات را ایجاد کند و توسط منابع مهیا شود". بحثی که در ادامه آمده است نگاهی به تحلیل داده پس از انتخاب این روایت از ابر دسته‌ها است.

نویسنده نیاز به انتخاب و حمایت عبارتی دارد که بهترین نتایج را از کد گذاری باز و محوری دریافت کند. با استفاده از ماتریس کد گذاری بازتابی، محقق ابر دسته‌ها را ترکیب کرده و متوجه می‌شود که مامور ارشد امنیت یک نقش یا ترکیبی از نقشهایی را که برای اجرای ماموریت امنیت اطلاعات ضروری می‌پندارند را تشخیص داده و انتخاب می‌کند. مامور ارشد امنیت به دنبال تنظیم چشم انداز استراتژی در راستای سازمان است. آنها در سازمانشان ممکن است نیاز به هماهنگی با تجارت، سیستم اطلاعاتی، به خودی خود یا ترکیبی از این سه تا داشته باشند. مامور ارشد امنیت شروع به ساخت استراتژی برای دستیابی به چشم انداز و تنظیم نیازمندیهای ذینفعانی است که از منابع مهیا شده استفاده می‌کنند. با ارزیابی فرآیندها یا شرایط غیر عادی در ماتریس کد گذاری بازتابی مشخص شد که مامور ارشد امنیت نقشهایی را برای پیاده سازی یک استراتژی انتخاب می‌کند. انتخاب نقش به عنوان حوزه اولیه‌ای که

www.takbook.com

مامور ارشد امنیت می‌تواند آن را کنترل کند دیده شده است، زیرا که آنها برای تصمیم گیری در مورد روش‌شان آزاد هستند. انتخاب نقش تبدیل به یک فرآیند پیچیده می‌شود که باید عوامل خروجی تنظیم و استراتژی توسعه یافته برای برآورده کردن ماموریت‌شان در نظر گرفته شود و همچنین باید اهداف سازمانی را حمایت کند. در زمان طراحی روشی که نقش‌شان در سازمان شکل بگیرد ماموران ارشد امنیت بیان کردند که باید برنامه‌شان نگاهی رو به جلو داشته باشد. پاسخگوی Q3 (پرسنل ارتباطات) بیان کرد "استراتژی امنیت اطلاعات به ساده-ترین تعریفش، استراتژی رو به جلویی است که یک رهبر برای رسیدگی به مسائل امنیت اطلاعات امروز و فردا در سر دارد." آنها نیاز دارند که یک استراتژی با یک اندازه قابل مدیریت که شامل سه یا چهار هدف است داشته باشند و نیاز است که این اهداف قابل دستیابی در مدت زمان مشخصی باشند. اکثرا این مدت زمان، در سال مالیاتی تعریف می‌شود که از اول اکتبر تا سی‌ام سپتامبر سال بعد است. استراتژی باید تعریف کند که چه چیزی مهم است و چه چیز باید محافظت شود. همچنین باید یک فرهنگ امنیت پرورش یابد که راههایی را نمایش دهد که در آن جامعه‌ای مشارکتی بین کاربران سازمان را توسعه داده و پرورش دهد. متخصصان امنیت اطلاعات باید در سازمان ارتباط گرا و مشارکت طلب باشند. ترویج و رشد امنیت در میان کل جمعیت سازمان. بخش بعدی مامور ارشد امنیت را به عنوان رکن اساسی سازمان در نظر گرفته و آنها را عامل تصمیم گیری برای روشی که برنامه امنیت اطلاعات توسط نقش، تنظیم و پیچیدگی (استراتژی) در سازمان به آن تکیه می‌کند در نظر می‌گیرد.

٤-٤ نتیجه

بخشهای قبلی دسته‌های استفاده شده توسط مامور ارشد امنیت را در نظر گرفته و راههایی را برای کارو پیاده سازی برنامه امنیت اطلاعاتشان پیدا می‌کنند. در این بخش نهایی، داده تحلیل شده برای تولید مراحلی که یک مامور ارشد امنیت برای پی بردن به نقشش با استراتژی امنیت اطلاعات مطالعه شده است. با استفاده از داده جمع آوری شده، پس از فرآیند کشف مامور ارشد امنیت پی می‌برد که کجا یا چگونه آنها باید با رهبری هماهنگ شود و بهترین نقش را برای شروع انتخاب کنند. اگر پذیرفته شد، مامور ارشد امنیت با کسب و کار و یا سیستمهای اطلاعاتی هماهنگ شده و با توسعه استراتژی مشارکت کرده و یک زیر ساخت استراتژی شکل می‌گیرد. اگر رهبری پذیرای آن نباشد، یا تنظیم به سیستمهای اطلاعاتی تکیه

www.takbook.com

می‌کند و یا با محیط امنیت اطلاعات بر اساس نیازمندیهای معمول هماهنگ می‌شود چرا که مجبور است از قانون تبعیت کند. موقعیت غیر محتملی نیز وجود دارد که رهبری مشارکت نکند و این را دیکته کند که هیچ امنیتی نیاز نیست یا فقط تا یک سطحی که بتوان جواز یا اعتبار نامه رسمی عمل کردن را دریافت کند. در این حالت سازمان در موقعیت خاص منظوره-ای واقع شده به طوری که مامور ارشد امنیت منفعل بوده و به هیچ هدف دلخواهی نمی‌رسد. پاسخگوی J7 (پرسنل ارتباطات) این مساله را به خوبی بیان کرد: "متاسفانه اولویتهای ما بر اساس روشی منفعل است. من اولویتهایی دارم که به طور واضح با رهبری، با کارمندانم، و با دیگران در ارتباط می‌باشم، اما متاسفانه ما کمبود پرسنل داریم، ما نمی‌توانیم این اولویتها را به طور موثری اجرا کنیم و وقتی که موردی اتفاق می‌افتد همه اولویتها به کنار گذاشته شده تا بتوان به بالاترین اولویت رسیدگی شود." داده در مطالعه نشان داده که هیچیک از برنامه‌ها به حد نهایی بدون امنیت، نرسیدند، در برخی موارد برخی ماموران ارشد امنیت نیاز به پیاده سازی سیستم بدون کنترل مناسب بودند، به ویژه جایی که فناوری جدید وارد می‌شد.

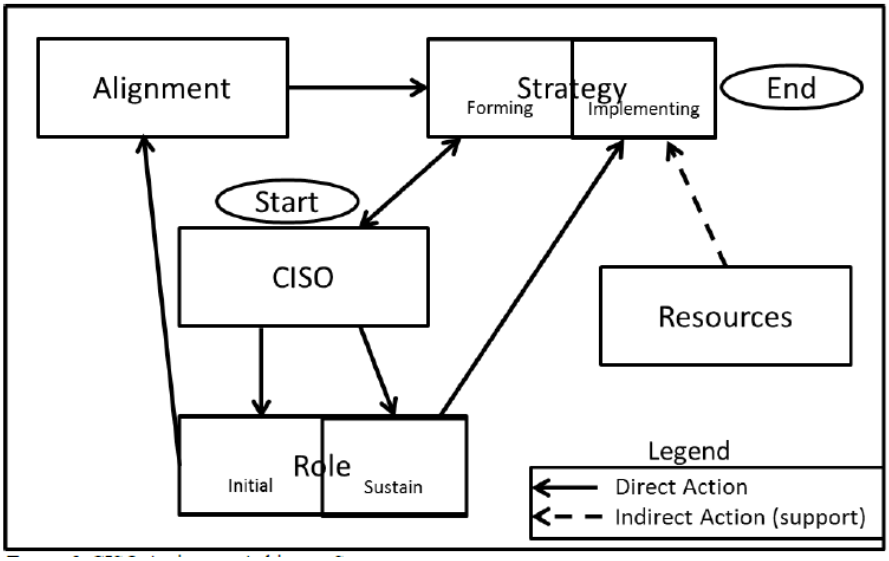
این مورد را به این صورت می‌توان توضیح داد که مامور ارشد امنیت برای تنظیم استراتژی به طور مستقیم با رهبری صحبت می‌کند. از شروع، مامور ارشد امنیت به دنبال این است که موقعیتشان در فرآیند تنظیم کجاست آیا به خودی خود عمل می‌کنند یا با سیستمهای اطلاعاتی یا کسب و کار و یا هر دو.

تشکیل یک استراتژی توسط فرآیند توافق هر سه گروه ذینفع (کسب و کار، سیستمهای اطلاعاتی و امنیت اطلاعات) که با یکدیگر کار می‌کنند توصیه می‌شود یا توسط جهت گیری و توافق بر برخی جهت‌ها انجام می‌شود. یک بحث دیگر زمانی پیش می‌اید که مامور ارشد امنیت در مرحله تشکیل استراتژی است و تعدادی مراحل اضافی ممکن است به رهبری بازگردد زیرا که مامور ارشد امنیت با رهبری بر روی یک مسیر (در مرحله تنظیم) مشورت می‌کند تا زمانی که به توافق برسند. زمانی که استراتژی شکل می‌گیرد، مامور ارشد امنیت اهداف لیست شده را مشخص کرده و برای انتخاب نقشی که استراتژی را برای رسیدن به اهداف پیاده سازی می‌کند تصمیم گیری می‌کند. شکل ۸ فرآیندی که توضیح داده شد را به تصویر کشیده است.

زمانی که تصمیم گرفته می‌شود، نقش انتخاب شده به کار گرفته می‌شود، استراتژی پیاده سازی شده و منابع برای تکمیل پیاده سازی به کار گرفته می‌شود. مامور ارشد امنیت تصمیم

www.takbook.com

نهایی را می‌گیرد که چه نقشی برای کار در راستای اهداف استراتژی باید انتخاب شود و آنها را برای تکمیل برنامه امنیت اطلاعات پیاده سازی کرده تا اهداف توافق شده محقق شوند. منابع به پیاده سازی استراتژی و دستیابی به اهداف کمک می‌کنند. شکل ۸، روش جدید فعالیت را نشان می‌دهد، داستان اینکه چگونه ماموران ارشد امنیت در یک سازمان بزرگ به صورت سیستماتیک کار انجام می‌دهند.



شکل ۸. فعالیتهای مامور ارشد امنیت برای بدست آوردن یک استراتژی

Alignment تنظیم
Strategy استراتژی
forming تشکیل
Implementing پیاده سازی
end پایان
Start شروع
Resources– منابع
role – نقش
Initial -اولیه
Sustain – پایدار
Legend – راهنمای نقشه
Direct action -فعالیت مستقیم
Indirect action فعالیت غیر مستقیم

www.takbook.com

حمایتSupport

به عنوان توضیح مرحله به مرحله فرآیند، مامور ارشد امنیت در ابتدا نقشی را انتخاب می‌کند (اکثر اوقات یکی از نقشهای هماهنگ). مامور ارشد امنیت با ذینفعان در مورد تنظیم، هماهنگ می‌شود. مرحله تنظیم یک فعالیت چرخه‌ای بین مامور ارشد امنیت، نقش، تنظیم، استراتژی (تشکیل) است تا زمانی که ذینفعان استراتژی را تشکیل دهند. به محض اینکه استراتژی شکل گرفت، در دومین بخش مامور ارشد امنیت نقش(هایی) را برای حفظ عملیات انتخاب می‌کند تا استراتژی را پیاده سازی کرده و به طور غیر مستقیم توسط منابع برای دستیابی به استراتژی یاری می‌شود.

چهار ابر گروه دارای وابستگی‌هایی هستند که روابط بین نقشها، تنظیمات، پیچیدگیها و منابع را آشکارا نشان می‌دهد (به شکل ۶، ابر دسته‌ها مراجعه کنید). تقسیمات چهار ابر گروه تحت بخش نتایج کد گذاری محوری پوشش داده شده و در شکل ۷، نگاشت دسته‌ها نمایش داده شده است. استنباط اثر متقابل شکل ۶ و شکل ۷ در شکل ۸ (فعالیتهایی برای دستیابی به استراتژی) نمایش داده شده است. در اکثر سازمانها، مامور ارشد امنیت نقشی را در نظر گرفته‌اند، تنظیمات و منابع محدودی دارند، اما اکثر آنها فاقد استراتژی هستند. آنها اکثرا به حال خود رها شده تا زمانی که اتفاقی رخ بدهد. همانطور که پاسخگوی Q3 (پرسنل ارتباطات) گزارش داد: "اگر جمعبندی کنم، ما هر روز نسبت به حریقها عکس‌العمل نشان می‌دهیم و توانایی آن را نداریم که آن را حفظ کنیم. بنابراین زمانی که شما یک استراتژی امنیت اطلاعات دارید، ممکن است به شما اجازه دهد که کنش گرا عمل کرده و به مسائل رسیدگی کنید."

ماموران ارشد امنیت نقشی را فرض می‌کنند، بسیاری از ماموران ارشد امنیت برای یافتن نقشهای مورد نیاز خودشان در هر موقعیتی به حال خودشان گذاشته می‌شوند. یا مدیریت هیچ مسیری به آنها نداده بنابراین مامور ارشد امنیت استراتژی خودش را ایجاد کرده و یا مامور ارشد امنیت فقط بر اساس موقعیت پیش آمده واکنش نشان می‌دهد. همانطور که در ابر دسته نقشها (به شکل ۲، نقشها مراجعه شود) و همچنین در گوشه پایین سمت راست شکل ۷ نمایش داده شده است نقشی که اکثرا در نظر گرفته می‌شود تبعیت است. نقش تبعیت یک موقعیت مرکزی دارد زیرا که همه ماموران ارشد امنیت مشخص کردند که تبعیت فعالیتی است که باید انجام شود. در این بخش فعالیت مامور ارشد امنیت برای انتخاب نقش اولیه با جزئیات شرح داده می‌شود.

www.takbook.com

اکثر ماموران ارشد امنیتها دارای یک تنظیم هستند. اطلاعات برداشت شده از تحلیل داده جمع آوری شده نشان داد که دو تنظیم اصلی برای ماموران ارشد امنیت وجود دارد. اول اینکه تعداد زیادی از ماموران ارشد امنیت با مامور ارشد امنیت (سیستمهای اطلاعاتی) و کسب و کار تنظیم می‌شوند. این ماموران ارشد امنیت ارتباطی را با رهبری ایجاد کرده و آنها را از ریسکها آگاه کرده و بر روی تصمیمات مشخص شده توسط رهبری پایبند هستند. دوم اینکه، تعداد زیادی از ماموران ارشد امنیت هستند که هیچ تنظیم خاصی نداشته و خارج از فعالیتهای رهبری قرار گرفته و اساسا اینها همیشه براساس وظایف امنیت اطلاعات در حالت منفعل محض عمل می‌کنند. "متاسفانه، اولویتهای ما بر اساس روشی منفعل است" (پاسخگوی J7، پرسنل ارتباطات). آنها همیشه در حال کار کردن بر روی پاک کردن وقایعی هستند که این کار بر خلاف داشتن استراتژی است که از رخ دادن وقایع جلوگیری می‌کند. ماموران ارشد امنیت که تنظیمی ندارند مطلوب است بدانند رهبری در چه مسائلی درگیر بوده و سرانجام می‌توانند به رهبری کمک کند تا تصمیمات آگاهانه‌ای بگیرد، اما از گرفتن نقش در ایجاد سیستم قبل از پیاده سازی محروم شده‌اند. تعداد کمی از ماموران ارشد امنیت بودند که به تنهایی تحت مسیر مامور ارشد امنیت عمل می‌کردند و تنها یک مامور ارشد امنیت بود که به طور مستقیم با تابع کسب و کار، کار می‌کرد. برای اکثر بخشها ماموران ارشد امنیت با کسب کار مرتبط بوده و با آن کار می‌کردند و مامور ارشد امنیت از واحدهای بزرگتر سازمان بود. ماموران ارشد امنیت که در واحدهای کوچکتر از سازمان بزرگ بودند به حال خود گذاشته شده بودند تا خودشان قوانین خود را ایجاد کنند یا همیشه در حال ترمیم موقعیتهایی باشند که مدیریت به خاطر نادیده گرفتن آنها خود را در آن می‌دیدند. همانطور که در شکل ۸ نمایش داده شده است، این مساله تعامل بین ماموران ارشد امنیت، نقشها و تنظیمها را نشان می‌دهد.

زمانی که جلوتررفتیم، ماموران ارشد امنیت بیان کردند که آنها یک استراتژی رسمی ندارند. مامور ارشد امنیت که فقط یک استراتژی غیر رسمی داشت بیان کرد که آنها وقتی برای نوشتن یک استراتژی رسمی نداشته‌اند و آنها به طور ساده وظایف را زمانی که به آنها نیاز است اجرا می‌کنند، و خیلی تاکتیکی وقایع را یکی پس از دیگری پوشش داده بدون اینکه هیچ پیشرفتی در فرآیند داشته باشند. یک مامور ارشد امنیت بیان کرد که آنها استراتژی رسمی داشتند، اما هنوز مورد توافق قرار نگرفته است. پاسخگوی Z7 (پرسنل ارتباطات) بیان کرد "هیچ موردی آنجا نیست، ما سعی در ساختن یک مسیر مدیریتی داخلی برای استراتژی

www.takbook.com

امنیت اطلاعات هستیم، اما هنوز رسمیت نیافته، بنابراین تا زمانی که نهایی نشده است، من وارد جزئیات آن نخواهم شد. " تعداد کمی از ماموران ارشد امنیت گفتند که آنها از استراتژی مامور ارشد امنیت برای خودشان استفاده می‌کنند. این راه ارجحترین کار نسبت به اینکه استراتژی از خود داشته باشند، اما مامور ارشد امنیت بیان کرد که آنها ممکن است استراتژی سازمان بزرگتر را بپذیرند یا حتی تحت مامور ارشد امنیت به عنوان یک برنامه پشتیبان کار کنند. بسیاری بیان کردند که آنها به استراتژی نوشته شده توسط مامور ارشد امنیت اداره مرکزی یا واحد رهبر در سازمانشان مراجعه می‌کنند. همه بیان کردند که استراتژی شامل مقدار زیادی کار دشوار است. کار شامل تیمها، مشارکت، و کارکرد شناسی برای توسعه چشم انداز در برابر نیازهای ماموریت و رسیدن به اهداف امنیت اطلاعات است. بیشتر فرآیند توسعه فراتر از حوزه این مطالعه می‌رود. دستاورد اصلی هماهنگ شدن با ورودیها برای دریافت اهداف، و کد گذاری کردن آنها با دیگر ذینفعان در سازمان است. که این نیاز به کاری سخت برای شکل دهی استراتژی از طریق تعاملات با ذینفعان، ماموران ارشد امنیت و تیمهایی است که برای مامور ارشد امنیت کار می‌کنند.

با داشتن استراتژی چرخه تقریبا تکمیل می‌شود اما تاثیر منابع نقشی را در کشف نقشهای استراتژی امنیت اطلاعات بازی می‌کند. اکثر ماموران ارشد امنیت منابع محدودی دارند. بعضی از آنها سرمایه فراوانی داشته و قابلیت راهنمایی پرسنلشان در مسیر شغلی که برای سازمان بزرگ مفید می‌باشد هستند. اکثرا بودجه‌هایی داشتند که فقط به آنها اجازه می‌داد که دارایی-هایی داشته باشند که در جهت توسعه پرسنل می‌توانستند آن را خرج کنند. منابع فعال سازی حیاتی از قابلیت مامور ارشد امنیت برای اجرای برنامه امنیتی بود. سرمایه پراکنده شده و مامور ارشد امنیت همیشه به رسیدگی به ریسک بیشترین اولویت را می‌دهند. اغلب مامور ارشد امنیت بودجه کافی ندارد ولی کارها را با میزان اختصاص یافته به آنها انجام می‌دهد.

بنابراین، همه فعالیت‌های منسوب به مامور ارشد امنیت برای رسیدن به استراتژی در شکل ۸ نمایش داده شده است. سوال اساسی مصاحبه منجر به ایجاد یک نظریه از طریق فرآیند کد گذاری نظریه بنیادی همه داده‌های جمع آوری شده، شد. داستان پدید آمده از داده‌ها و در نتیجه نظریه‌ای که از روی داده‌ها ایجاد شد با این عبارت مطابقت دارند: مامور ارشد امنیت یک نقش را برای تنظیم با ماموریت انتخاب کرده و یک استراتژی را ایجاد می‌کند (پیچیدگی-ها) که از منابع در دسترس استفاده می‌کند. خلاصه شده این عبارت فعالیت‌های مامور ارشد

www.takbook.com

امنیت برای رسیدن به یک استراتژی است و به عبارتی دیگر مامور ارشد امنیت با تبعیت شروع کرده به عنوان نقشی که با کسب و کار و سیستم‌های اطلاعاتی در تنظیم کردن با ایجاد یک استراتژی کار می‌کند که ریسک ماموریت را با بودجه‌ای که برای پرسنل واجد صلاحیت در نظر گرفته شده تا از آنها برای آموزش کافی حمایت کرده و او را با ابزارهای مربوطه مجهز کند. مامور ارشد امنیت نقش را برای تناسب نیازهای رسیدگی به ماموریت ریسک با مجریان سیستم‌های اطلاعاتی و کسب و کار هماهنگ می‌کند.

www.takbook.com

فصل پنجم

نتیجه گیری، دلالت، محدودیت‌ها و توصیه ها

www.takbook.com

۵-۱ مقدمه

در این مطالعه، تحقیق در مورد بررسی استراتژی امنیت اطلاعات و نقشهایی است که یک مامور ارشد امنیت می‌تواند برای پیاده‌سازی آن را انتخاب کند (Chen, et al., 2010; Leidner, et al.,2011)، چگونه استراتژی امنیت اطلاعات و انتخاب نقش می‌تواند پیشرفت کرده و فعالتر شود (Seeholzer, 2012). این پیشرفت می‌تواند در ایجاد یک پیاده سازی کنش گرای استراتژی مشارکت کند که این کار را از طریق انتخاب نقش مناسب، جهت دهی تنظیم و استفاده از منابع برای رسیدن به اهداف انجام دهد. مطالعات آینده ممکن است نظریه پدید آمده از داده‌های جمع آوری شده در فصل ۴ را اعتبار سنجی کند و مدل منتج از فعالیت‌های مامور ارشد امنیت برای دستیابی به استراتژی را اعتبار سنجی کند.

۵-۲ جمع بندی

نتایج این مطالعه منجر به فهم پیچیدگی‌های استراتژی امنیت اطلاعات در سازمان مالی بزرگ می‌شود. این مطالعه نظریه‌ای را بازگو کرد که می‌تواند به مامور ارشد امنیت کمک کند تا مطمئن شود آیا نوع خاصی از استراتژی امنیت اطلاعات نسبت به شکل‌های دیگر آن ارجحیت دارد یا خیر و چگونه با هم سازگار می‌شوند. این مطالعه با استفاده از مدلی برای کشف سناریوهای خاص که به متغیرهای فراهم شده برای همه ورودی‌هایی که به آنها وابستگی دارد برای ارزیابی اینکه چگونه استراتژی‌های امنیت اطلاعات در سازمان‌های مالی بزرگ متفاوت هستند ممکن است مفید واقع شود. یافته‌های این مطالعه می‌توانند به یک نظریه پیشرفته انتخاب نقش داده شود تا به متخصصان امنیت اطلاعات در انتخاب نقش مناسب برای پیاده سازی برنامه امنیت اطلاعات کمک کند.

نویسنده تاکید کرد که از تحلیل و بررسی متون در دسترس و داده‌های جمع آوری شده چندین نتیجه از تحلیل‌ها می‌توان گرفت. یکی از نتایج مورد انتظار این بود که بسیاری از دسته‌های نقشها که در متون مروری توسعه یافته‌اند، با عنوان نوشته شده است. برخی شرکت-کنندگان نقشها را با نام‌های مختلفی می‌خواندند، اما دسته‌ای که دنبال می‌کردند دارای توضیحات یکسانی در متون مروری بودند. چهار تا از دسته‌های نقش‌ها تا حدودی در سازمان مالی بزرگ بی اهمیت و ناچیز هستند. این نقشها تصویر عمومی، رقیب، سازماندهی مجدد و ارتباطات قدرت بودند. اگر چه دسته‌های مشخص شده در نقشها در سازمان مالی بزرگ ناچیز

www.takbook.com

بودند، ممکن است تحت محیط‌های آموزشی، تجاری یا دیگر بخش‌های خصوصی حفظ شوند. متون بررسی شده چندین مورد در بخش تجاری را دسته‌هایی بی اهمیت عنوان کردند.

بخش متون مروری بر روی تنظیم استراتژی‌ها، دسته‌های یکسانی را با نتایج مختلفی یافتند. اکثریت ماموران ارشد امنیت در بخش خصوصی استراتژی‌های نوشته شده کمتری داشتند که این بر خلاف حالت ایده آل ارائه شده در متون مروری بود. از مصاحبه‌ها عملیات اعتبار سنجی صورت گرفت همانطور که ماموران ارشد امنیت حمایتشان را از استراتژی‌های سیستم‌های اطلاعاتی و تجاری اعلام کردند، کمبود استراتژی امنیت اطلاعات متعلق به خودشان را نشان می‌داد. علاوه بر این مصاحبه ها، کمبود شدید مدل‌ها برای برخورد با استراتژی در داخل ادارات امنیت اطلاعات در سازمان‌ها را نشان داد.

نتایج حاصل از اطلاعات جمع آوری شده بیش از تعاریف امنیت اطلاعات و اطلاعات اساسی در مورد برنامه امنیت اطلاعات بازگو کرد. از آنجایی که آنها هر روز ه برای جلوگیری از نشت و از دست دادن داده به مقابله می‌پردازند و پاسخ‌های اتفاقی به تهدیدهای جدید و بهره گیری از شبکه که باعث می‌شود از هر نقطه ورودی در معرض آن قرار بگیرند بیشتر ماموران ارشد امنیت وارد جزئیاتی در مورد موانع و چالش‌هایی که تقریبا هر روزه با آنها روبرو هستند شدند (Hutchins, Cloppert, & Amin, 2011; OIG, 2012; Suddaby, 2006). جدول ۲۰ (چالش-ها و موانع) چالش‌های اصلی که ماموران ارشد امنیت در سازمانشان با آنها روبرو هستند را گردآوری کرده اند.

برخی ماموران ارشد امنیت به بحث پیچیده‌ای در مورد اینکه چگونه امنیت اطلاعات حمایت می‌شود پرداختند و اغلب بحث را با بیان استراتژی کسب و کار تکمیل کردند و به حوزه‌هایی که مورد انتظار نیست ارزش دادند. برای مثال، در مواردی که امنیت از ابتدا موجود می‌باشد، از هزینه‌های غیر ضروری آتی جلوگیری می‌شود. محقق از مصاحبه‌ها طی یک فرآیند تکرار پذیر که با نتایجی از تمام مصاحبه‌ها بدون جهت گیری از بخش‌های مختلف سازمان بزرگ،استنباط کرد که همه آنها به حمایت از یک برنامه امنیت سازمانی کلی منتهی می‌شود (Duffy, et al., 2006; Hirose, Itao, & Umeda, 2012; Wimpenny & Gass, 2000).

www.takbook.com

جدول ۲۰. چالشها و موانع

پاسخگو	چالش روبرو شده
G7	- کمک به سازمان برای دیدن تصویر بزرگ امنیت اطلاعات اغلب چالش بر انگیز است. اغلب باید روش‌های خلاقانه‌ای را پیشنهاد کرده، بسیار اوقات در پشت صحنه به مشارکت امنیت اطلاعات در سیستم تظاهر می‌شود.
H8	- چالشی که ما با آن روبرو هستیم این است که ما کارهای زیادی هست که باید انجام دهیم، اما بودجه ما به شدت کم است. بنابراین انجام آنها بسیار دشوار می‌باشد. - سعی در تنظیم همه استراتژی‌ها، برنامه‌ها و کتاب‌های راهنمای گوناگون در کل سازمان بسیار چالش برانگیز است. همچنین دولت مواردی را اعلام کرد که هنوز رسیدن به تنظیم و هماهنگی با همه بخش‌ها را سختتر کرده است.
M7	- ما همیشه در حال مبارزه برای بودجه هستیم، بدست آوردن مجوز برای بودجه تجهیزات لازم. مامور ارشد امنیت اولویت بندی‌های مختلفی دارد که چالش برانگیز است.
V8	- من با زیر مجموعه سازمان‌ها چالش دارم. باید استراتژی امنیت اطلاعات را به گونه‌ای بسازم که به اندازه کافی قانع کننده باشد به طوری که دیگران بخواهند خودشان را با ما تنظیم کنند. من آن را در خلا انجام نمی‌دهم. من نمی‌خواهم که آن را فقط در کاغذ بنویسم و آن را تبدیل به یک اجبار کنم، به جای آن سعی دارم که مواردی باشد که آنها از آن استراتژی حمایت کرده و آن را بپذیرند. من باید به آنها فشار بیاورم تا آنها را پشت سر بگذارم. آنها را بیشتر درگیر کنم در این صورت شما می‌توانید آرا را جلب کنید. - اغلب اوقات چالش شغل در اینجا این است که ما همه مسئولیت‌ها و پاسخگویی‌ها را داریم اما ما مجوز و اختیار نداریم. اگر چه مصوبه Clinger Cohen آن را به ما میدهد ولی ما مجوز نداریم. شما باید قابلیت داشتن تاثیر داشته تا آنها را به حرکت در اولویت‌ها و انجام آنها داشته باشید.

www.takbook.com

پاسخگو	چالش روبرو شده
X9	- مشکل در اندازه گیری کمی ریسک می‌باشد.ساخت یک فرآیند تکرار پذیر و چالش برانگیز است. من مدل ارائه شده را برای مشخص کردن ویژگی-های تهدید ساختم، اما من نمی‌دانستم که آیا به نقطه قابل تکرار می‌رسد یا خیر. ساختن فرآیند قابل تکرار دشوار بوده و بدون داشتن فرآیند قابل تکرار سختتر هم می‌شود که بتوان اندازه گیری‌ها و یا معیارهایی برای فرآیند بدست آورد.

۵-۳ دلالت

از آنجایی که در فهم اساسی نقشهای امنیت اطلاعات به کار رفته برای پیاده سازی یک استراتژی امنیت اطلاعات در یک سازمان کمبود وجود دارد، بسیاری از پیاده‌سازیها در سازمانهای مالی، استراتژی امنیت اطلاعات را با راه حل‌هایی که به طور فنی به هم مربوطند، ابزارهای پیاده سازی و نظارت‌های کنترلی رار با هم یکی می‌کنند (Seeholzer, 2012). این مساله با مصاحبه‌های انجام شده پشتیبانی شد به طوری که اکثریت ماموران ارشد امنیت محیط امنیتی خاص خودشان را نشان می‌دادند. در این مطالعه چالش در توزیع اطلاعات ارائه شده است، بنابراین ماموران ارشد امنیت می‌توانند به مجریان در تنظیم اهداف استراتژیک و مقاصدشان کمک کرده و به آنها در ایجاد نقشهایی که در تنظیم قابل توافق می‌گنجد کمک کنند. استفاده از نظریه بنیادی ساختارگرا پیچیده بوده و نیاز به مهارت‌های تفسیری دارد تا بتوان به درستی در داده‌های جمع آوری شده کند و کاو کرد و دسته‌هایی را از بین هزاران سطح پاسخ‌های داده شده توسط مجری استخراج کرد. زمان قابل توجهی نیاز است تا به داستانی منسجم از طریق کد گذاری داده و استفاده از تحلیل قیاسی رسید.

۵-٤ محدودیت‌ها

محدودیت اصلی بدست آوردن پاسخ‌های بدون جهت گیری از شرکت‌کنندگان است. برای هر مصاحبه، محقق مصاحبه را بدون زمانبندی حفظ می‌کرد و به ماموران ارشد امنیت اجازه نمی‌داد که سوالات را قبل از مصاحبه مشاهده کنند، سوالات به صورت لحظه‌ای در زمان بحث بیان می‌شدند. محقق همچنین مرز سوالات را محدود کرد، که به طور واضح در حوزه استراتژی

www.takbook.com

امنیت اطلاعات و نقشهایی که یک فرد می‌تواند برای برآورده کردن اهداف و مقاصدش در نظر بگیرد نگه دارد. تعیین محدوده باعث شد که این مطالعه تنها بر روی سوالات بدون انحراف از موضوع متمرکز شود؛ سوالات اصلی با هر شرکت کننده یکی نگاهداشته شد. همچنین محقق فاصله خود را با شرکت کننده حفظ کرد تا پاسخ‌های بدون جهت گیری را به دست آورد.

محدودیت دیگر، جامعه آماری انتخاب شده بود که تعدادی ماموران ارشد امنیت در محدوده جغرافیایی محدود بودند. تعمیم پذیری به جمعیت بزرگتر یکی از ملاحظات بود به طوری که تحقیق افرادی را که در ناحیه استان انتاریو و آلبرتا قرار داشتند و عموما در شهرهای تورنتو و ادمونتون بودند به کار گرفت. اگر چه این مطالعه از افراد در زیر واحدهای سازمان مالی بزرگ پرس و جو انجام داد، ولی نمی‌تواند نمایانگر کل سازمان باشد. علاوه بر آن، از آنجایی که وفق دادن عوامل کلیدی از همه مطالعات در حوزه امنیت اطلاعات مشکل است، نمی‌توان فرض کرد که همه نقشهای موثر در استراتژی امنیت اطلاعات در این مطالعه نمایش داده شده‌است. می‌توان حدس زد که دیگر نقشها بخشی از این مطالعه نبوده‌اند ولی ممکن است بر روی استراتژی امنیت اطلاعات در یک سازمان اثر بگذارد.

در نهایت، در حالی که شرکت‌کنندگان از عدم فاش اطلاعاتشان اطمینان داشتند و داده به روشی جمع آوری می‌شد که شک و تردید پاسخگو را به حداقل برساند، لازم به ذکر است اطمینان خاطر دادن به پاسخگو از اینکه کاملا سوء ظن نداشته باشد، کاری بسیار دشوار است. همینطور ترس‌هایی نهفته در دادن اطلاعات امنیت اطلاعات به یک منبع خارجی می‌تواند وجود داشته باشد. این فرض به عنوان یک مشکل در انجام مطالعه در زمنیه امنیت اطلاعات دیده شده است (Kotulic & Clark, 2004).

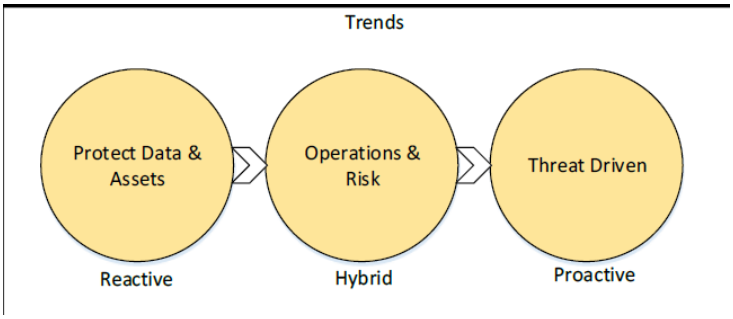
۵-۵ توصیه‌ها

پدیده یا نقشهایی که یک مامور ارشد امنیت باید در نظر بگیرد نیاز به در بر گرفتن چگونگی رسیدگی به تهدیدها، آسیب پذیرها و ضعف‌های معمول در استراتژی امنیت اطلاعات دارد (Ransbotham, Mitra, & Ramsey, 2012). زمینه امنیت اطلاعات بر لبه پرتگاهی قراردارد که از یک دنیای منفعل محض که فقط به تهدیدات زمانی که کشف می‌شوند رسیدگی می‌کند و به سمت یک طبیعت پیشگویی کننده از تهدیدهایی که قبلا با آنها روبرو شده بودند حرکت می‌کند. ماموران ارشد امنیت هم اکنون بر روی راهکارهای منفعل مستند سازی شده که

www.takbook.com

کنترل‌های پیاده سازی شده ایستا برای محافظت از داده و دارایی‌های تحت قلمروشان تمرکز می‌کنند. به صورتی که افزایش محافظت باعث حرکت تهدید به نواحی کمتر محافظت شده می‌شود. برای مثال، مامور ارشد امنیت اصلی سازمان رایزنی کرده تا مجوزی بدست آورد تا ایمیل که بزرگترین نقطه ورود بد افزاراست از طریق ایمیل‌های هدایت شده، دانلود پیوست‌ها و اجرا را بدست آورد. حالا، تهدیدکنندگان منتقل می‌شوند و حملاتشان را از طریق حمله دیگر همچون Heartbleed (Durumeric, et al.,2014) و Bash/ShellShock (Durumeric, et al., 2014) and Bash/Shellshock did (Security Research and Emergency Response Center of AnityLabs (Anity CERT), 2014; Trend Micro Threat Research Lab (TMTRL, 2014) متحول می‌کنند تا بتوانند مجوز ورود به سیستم را پیدا کنند. ماموران ارشد امنیت نیاز دارند تا از راهکاری منفعل به سمت راهکاری کنش گرا تغییر کنند و با آن سازگار شوند. شروع این جا به جایی از پاسخ‌ها به سوالات مصاحبه گردآوری شد، به عنوان نمونه "... چه قابلیت‌هایی برای یک استراتژی امنیت اطلاعات موفق ضروری است؟ "(فصل ۳، جدول ۵؛ سوال اساسی مصاحبه). این سوال یک جا به جایی در پاسخ صورت گرفت که از مامورهای ارشد امنیت که میل به انتقال از راهکار منفعل به نتیجه‌ای کنش گرا داشتند. پاسخگوی M7 (پرسنل ارتباطات) گفت که مامور ارشد امنیت باید "به طور واضح ریسک تصمیمی که توسط مدیریت گرفته شده را در معرض خطر قرار گرفتن داده در نظر بگیرد و این کار را باید کنش گرا انجام دهد و نه یک تصمیم منفعل. " محقق چشم اندازی را در روند حرکت از انفعال در مرحله بین راهکار ترکیبی بین راهکارهای منفعل و کنش گرا به سمت کنش‌گراتر بودن در پیش می‌گیرد. شکل ۹ حرکت از یک برنامه امنیت اطلاعاتی منفعل را به سمت یک برنامه کنش گرا به نمایش می‌گذارد.

www.takbook.com



شکل ۹. روندها

Trendsروندها
Protect data & Assets – حفاظت داده و دارایی‌ها
Operations & risk – عملیات و ریسک
Threat drivenمبتنی بر تهدید
Reactive – منفعل
hybrid– ترکیبی
Proactiveکنشگر

در آینده این تحقیق می‌تواند این چنین گسترش یابد که چگونه نقشها، تنظمیات و استراتژی (پیچیدگی‌ها) با محیط سیال جدید سازگار شود و چگونه این اتفاق رخ خواهد داد. در نهایت، ماموران ارشد امنیت مشخص کردند که برای سالها مدل محیطی سرسختی حفظ شده بود که به آسانی از آن دفاع می‌شد. اما حالا با معرفی ابر، موبایل، داده بزرگ، مجازی سازی و دیگر فناوری‌های نوظهور این محدودیت‌ها دیگر حفظ نمی‌شوند. چگونه مامور ارشد امنیت به الگوی جدید لایه‌های شبکه بر خلاف یک مدل دفاع از محیط پیرامون واکنش نشان می‌دهد؟این مساله می‌تواند یک حوزه برای بررسی و مطالعه در آینده باشد.

ارتباط و اهمیت این مطالعه در افزودن پایگاه دانشی است که در محدوده فهم پیچیدگی‌های استراتژی امنیت اطلاعات و نقشهای نسبت داده شده در روش‌های تطبیقی برای رسیدن به اهداف و مقاصد استراتژی امنیت اطلاعات هستند مساله ایجاد شده در پیچیدگی استراتژی امنیت اطلاعات هنوز برای استراتژی در حال توسعه و انتخاب نقشها برای حمایت از آن مورد بررسی قرار نگرفته است. بخشی از جامعه امنیت اطلاعات که از این پدیده متاثر می‌شوند مجریان امنیت اطلاعات، ماموران ارشد امنیت و دیگر مجریانی هستند که مسئول نظارت امنیت اطلاعات در سازمان هستند. محدوده این مساله برای سازمان‌هایی است که دارای برنامه

www.takbook.com

امنیت اطلاعات هستند و در محدوده کوچکتری در سازمان‌های کوچکتر نیز جوابگو می‌باشد. تمرکز مطالعه بر روی سازمان‌های مالی بزرگ است، اما ممکن است مدل‌های پدید آمده در مقیاس کوچکتری برای سازمان‌های کوچکتر مفید باشد و بتواند متناسب با اندازه هر سازمانی در بخش عمومی تغییر اندازه بدهد. با پذیرش یافته‌ها توسط به کار بردن نظریه ممکن است منجر به تطابق استراتژی امنیت اطلاعات و ایجاد نقش برای سازمان‌ها شود.

ممکن است مطالعات دیگری برای رسیدگی به مساله پیچیدگی تلاش کرده باشند، اما احتمالا به یک نظریه برای انتخاب یک مدل توسعه نقش برای استراتژی امنیت اطلاعات نرسیده‌اند. در اینجا بدون ایجاد نظریه، جاودانگی انتخاب نقش ادامه خواهد یافت، با یک انتخاب منفعل از نقش‌ها برای رسیدگی فوری به مسائل پیش آمده به جای ارزیابی جهت کلی و اکتشاف ریشه به صورت کنش گرا منجر به حذف مساله اصلی می‌شود. داشتن یک فرآیند انتخاب متمرکز می‌تواند منجر به حفظ ثروت و زمان سازمان شود. در نهایت، نظریه توسعه یافته داده به مامور ارشد امنیت این اجازه را می‌دهد که با وضعیت‌های متغیر داده فراهم شده توسط عوامل خارجی تطبیق یابد. زمانی که نظریه در حال ایجاد است و به طور تجربی آزمایش می‌شود، استفاده بیشتر از نظریه برای توسعه معیارها و اندازه‌ها برای قرض دادن به آزمون کمی مدل می‌تواند باشد و شواهد تجربی بیشتر از موثر بودن مدل را فراهم کند.

اغلب برای به دست آوردن نتایج موقت مسیر ساده تر است، تا برای حل مشکل ریشه ای. اجتناب از آن تنها مشکلاتی را که شش ماه تا یک سال بعد به همین ترتیب برطرف می‌شود را مشاهده می‌کند؛ با وجود تغییرات جزئی، از قبیل جدیدترین نسخه ویروس برای فریب دادن از طریق تجزیه و تحلیل اکتشافی در یک برنامه ضد ویروس. Stuxnet followed by Flame (Bencsáth, Pék, Buttyán, and Félegyházi,), and then by Regin (Symantec Security Response (SSR),. ماموران ارشد امنیت و کسب و کار باید به منظور حفاظت از داده‌ها و دارایی‌ها با آنها سازگار باشند که نشان دهنده ماهیت تطبیقی تهدیدی می‌باشد.

این پژوهش، مسئله پیچیدگی استراتژی امنیت اطلاعات را با ارائه یک نظریه ای که اجازه می‌دهد تا عملکرد برای ارزیابی، تجزیه و تحلیل و سازگاری نقش‌ها برای رسیدن به اهداف و برنامه امنیت اطلاعات از طریق استراتژی گفتار، را مورد بررسی قرار دهد. پیاده سازی این تئوری به طور فعال به پیشرفت ماهیت واکنشی چرخه امنیت اطلاعات کمک می‌کند و به یک فرهنگ پیشگیرانه مداوم امنیت در یک سازمان می‌پردازد. پذیرش تئوری و آزمایش اندازه‌های

www.takbook.com

مختلف سازمانی و انواع آن، می‌تواند قابلیت تعمیم دادن و سودمندی آن را در طیف وسیعی از سازمان‌ها اثبات کند. مطالعات آینده ممکن است روش‌های کیفی دیگر را در نظر گرفته و همچنین پیاده سازی بیشتر می تواند به سازمان هایی که تئوری را تصویب می کنند، منجر به ایجاد مدل و تئوری داده های تجربی شود.

۶-۵ خلاصه

این کتاب تحقیقاتی را ارائه داد که پیامدهای آن برای متخصصان امنیت اطلاعات می‌باشد. در یک سطح، سازمان هایی که دارای استراتژی‌های امنیت اطلاعات واکنشی هستند، راهنمایی هایی برای کمک به تلاش‌های خود برای شناسایی نقش تعیین شده برای دستیابی به اهداف و برنامه‌های امنیت اطلاعات خود پیدا می‌کنند. سازمان هایی که دارای امنیت اطلاعات گسترده و نامحدود هستند می‌توانند از یافته‌های خود استفاده کرده تا انتخاب نقش خود را به طور فعال در دستیابی به مقاصد و اهداف تعیین شده در استراتژی امنیت اطلاعات آنها متمرکز کنند. داشتن فرآیند انتخاب متمرکز بیشتر، باعث می‌شودیک سازمان ثروت و زمان بیشتری را حفظ کند. در نهایت، تئوری از داده‌های ناپایدار توسعه یافته به ماموران ارشد امنیت اجازه می‌دهد شرایط داده شده توسط عوامل خارجی با شرایط در حال تغییر،سازگار باشد. استفاده بیشتر از این تئوری ممکن است برای توسعه معیارها و اقدامات برای تضمین تست کمی از مدل،و ارائه شواهد تجربی بیشتر در مورد اثربخشی مدل صورت گیرد.

www.takbook.com

پیوست ها

www.takbook.com

ضمیمه A: سوالات مصاحبه

۱. به نظر شما استراتژی امنیت اطلاعات چیست؟
۲. استراتژی امنیت چه معنی برای شما دارد؟ چه معنی برای سازمان شما دارد؟
۳. نقش شما برای انجام استراتژی امنیت اطلاعات چیست؟
۴. آیا شما می‌توانید نشان دهید که چگونه به اولویت‌های استراتژیک در امنیت اطلاعات می‌رسید؟
۵. آیا شما می‌توانید مدل (ساختار یا سیستم) استراتژی امنیت اطلاعات را توصیف کنید؟
۶. آیا شما می‌توانید توصیف کنید که چگونه پیاده سازی استراتژی امنیت اطلاعات پیگیری می‌شود؟
۷. با تفکر بر روی استراتژی امنیت، شما چطور اولویت‌ها را در سازمان بزرگ مدیریت می‌کنید؟
۸. آیا شما می‌توانید توضیح دهید که چه قابلیت‌هایی برای دستیابی به استراتژی امنیت اطلاعات موفق ضروری است؟

www.takbook.com

ضمیمه B: تحلیل‌های کلی اولیه

جدول ۲۱. تحلیل کلی مصاحبه

(سطر اول از چپ به راست) استراتژی – کنش گرا- منفعل – یکی دارد- هیچ ندارد – نیاز ندارد – کسب و کار – گذرگاه/IT – IT – به خودی خود – خاص منظوره- بالا به پایین – تصویر عمومی- رقیب – تغییر مداوم – بهترین عملکرد- سازمان‌دهی مجدد – ارتباط قدرت – تبعیت

Strategy	Proactive	Reactive	Have one	Don't have one	Not Needed	Business	Bus/IT	IT	On its own	Ad-hoc	Top Down	Public Image	Competitor	Continual Change	Best Practice	Re-Organization	Power Relationship	Compliance
Respondent																		
A0	X			X			X				X				X			
B3		X		X				X										X
B8	X	X		X					X	X	X			X	X			
C7		X		X			X					X						X
D2		X							X					X				X
E3		X	X				X		X					X				
F5	X	X			X		X			X	X			X				X
G7		X	X	X				X		X	X							X
H8		X		X				X							X			X
I5	X	X					X		X					X	X			
J7		X		X							X			X		X		X
K2		X		X			X				X				X			X
K5	X			X		X						X		X	X			
L9	X								X					X	X			
M2	X		X				X				X			X	X			
M7		X	X				X			X	X							X
N5	X	X		X			X			X	X			X				X
O9		X		X					X		X		X					X
P4	X			X					X						X			X
P5		X			X		X								X			X
Q3		X		X			X				X				X			
R2		X		X			X								X			X
S1		X		X			X		X		X				X			X
T5	X			X		X			X						X			X
T8		X		X						X	X						X	
U2	X		X				X		X					X	X			X
V8	X		X				X		X			X		X	X			
W3	X			X			X							X	X			
X4	X	X		X			X						X	X				X
X9	X			X		X			X	X				X	X		X	
Y4		X		X			X								X			X
Z7		X		X					X	X				X			X	

جدول B1 شامل ارزیابی کلی از مصاحبه‌هامی باشد و آنها را در چهار حوزه مختلف دسته بندی می‌کند. اول، برای کنش‌گرا یا منفعل بودن و یا داشتن المان‌هایی از هر یک در طی پاسخ‌هایی که به مصاحبه کننده داده شده است، مصاحبه هر پاسخگو تحلیل شد. دومین حوزه وضعیت پاسخگو را از داشتن یا نداشتن استراتژی و نداشتن نیاز به استراتژی ارزیابی کرده است. با این ترتیب که آیا شخص استراتژی نوشته شده‌ای دارد، آیا یک استراتژی در روند

www.takbook.com

تصویب دارد یا از استراتژی امنیت اطلاعات سازمانی در سطح بالاتر استفاده می‌کند. دو نمونه از بیان اینکه افرادی گفتند که نیازی به استراتژی ندارند از این حقیقت ناشی می‌شد که پاسخگو بیان کرد که آنها از استراتژی مامور ارشد اطلاعات به جای استراتژی امنیت اطلاعات استفاده می‌کنند. سومین حوزه تحت بررسی، ارزیابی تنظیم استراتژی است که پاسخگو سازمان را به سمت آن فرمان می‌دهد که می‌تواند کسب و کار، سیستم‌های اطلاعاتی و کسب و کار، سیستم‌های اطلاعاتی، یا تنظیمات خاص منظوره AD HOC باشد. مثال‌هایی نیز وجود داشتند که یک پاسخگو بیش از یک نوع تنظیم داشته باشد. چهارمین حوزه ارزیابی شده این بود که نقش پاسخگو در پاسخ به سوالات مصاحبه به عنوان یکی از این نقشها یا ترکیبی از آنها توصیف شد: بالا به پایین، تصویر عمومی، رقیب، تغییر مداوم، بهترین عملکرد، سازمان دهنده مجدد، ارتباط قدرت، و یا تبعیت.

www.takbook.com

References

Abbas, H., & Hemani, A. (2010). Addressing dynamic issues in information security management. Information Security Management, 19(1), 5-24.

Ahuja, S. (2009). Integration of COBIT, balanced scorecard and SSE-CMM as a strategic information security management (ISM) framework. (CERIAS TR 2009-21), West Lafeyette, IN: Perdue University. Retrieved from https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2009-21.pdf.

Aivazian, C. (1998). Information security during organizational transitions. Information Strategy: The Executives Journal, 14(3), 21-26.

Al-Hamdani, W. A. (2009). Three models to measure information security compliance. International Journal of Information Security and Privacy, 3(4), 43-67.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. Computers & Security, 28(6), 476-490.

Allan, G. (2003). A critique of using grounded theory as a research method. Electronic Journal of Business Research Methods, 2(1). 1-10.

Allen, J. (2005). Governing for Enterprise Security. (Technical Note CMU/SEI-2005-TN-023), Pittsburgh, PA: Carnegie Mellon University Software Engineering Institute. Retrieved from http://www.cert.org/governance/, 1-81.

Allen, L. M. (2010). A critique of four grounded theory texts. The Qualitative Report, 15(6), 16061620.

Alter, S. (2008). Defining information systems as work systems: Implications for the IS field. European Journal of Information Systems, (17)5, 448-469.

Amaio, T. E. (2009). Exploring and examining the business value of information security:

Corporate executives' perceptions. Available from ProQuest Dissertations and Theses database (UMI No, 3351834).

Anderson, E. E., & Choobineh, J. (2008). Enterprise information security strategies. Computers & Security, 27(1), 22-29.

www.takbook.com

Anderson, J. M. (2003). Why we need a new definition of information security. Computers & Security, 22(4), 308-313.

Anderson, R., & Moore, T. (2006). The economics of information security. Science, 314(5799), 610-613.

Arce, I., & Levy, E. (2009). An analysis of the slapper worm. IEEE Security & Privacy, 1(1), 8287.

Avgerou, C., & McGrath, K. (2007). Power, rationality, and the art of living through so مامور ارشد امنیتtechnical change. MIS Quarterly, 31(2), 295-315.

Backhouse, J., Hsu, C.W., & Silva, L. (2006). Circuits of power in creating de jure standards: Shaping an international information systems security standard. MIS Quarterly, 30(Aug2006 Supplement), 413-438.

Backman, K., & Kyngaes, H. A. (1999). Challenges of the grounded theory approach to a novice researcher. Nursing and Health Sciences, 1(1), 147-153.

Badr, Y., Biennier, F., & Tata, S. (2010). The integration of corporate security strategies in collaborative business processes. IEEE Transactions on Services Computing, 99(1), 1-14.

Baptista, J., Newell, S., & Currie, W. (2010). Paradoxical effects of institutionalization on the strategic awareness of technology in organisations. Journal of Strategic Information Systems, 19(3), 171-183.

Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. ACM Computing Surveys, 25(4), 375-414.

Baskerville, R. L., & Dhillon, G. (2008). Information systems security strategy, a process view.

In D. W. Straub, S. Goodman, & R. L. Baskerville (Eds.), Information Security, Policies: Processes and Practices, Advances in Management Information Systems, Volume 11, (1545). Armonk, NY: M. E. Sharpe, Inc.

Bechtold, B. (1997). Chaos theory as a model for strategy development, Empowerment in Organizations, 5(4), 193-201.

Bencsáth, B., Pék, G., Buttyán, L., and Félegyházi, M. (2014). The cousins of Stuxnet: Duqu, Flame, and Gauss. Future Internet 2012(4), 971-1003.

Bhalla, N. (2003). Is the mouse click mighty enough to bring society to its knees? Computers & Security, 22(4), 322-336.

www.takbook.com

Booker, R. (2006). Re-engineering enterprise security. Computers & Security, 25(1), 13-17.

Bower, J. L., & Gilbert, C. G. (2007). How managers' everyday decisions create- or destroy-your company's strategy. Harvard Business Review, February(2007), 2-9.

Brown, M., & Cregan, C. (2008). Organizational change cynicism: The role of employee involvement. Human Resource Management, 47(4), 667-686.

Brown, S. C., Stevens Jr., R. A., Troiano, P. F., & Schneider, M. K. (2002). Exploring complex phenomena: Grounded theory in student affairs research. Journal of College Student Development, 43(2), 1-10.

Bunker, G. (2012). Technology is not enough: Taking a holistic view for information assurance. Information Security Technical Report, 17(2012), 19-25.

Burwell, S. M. (2013). Fiscal year 2013 reporting instructions for the Federal information security management act and agency privacy management. Executive office of the president, Office of Management and Budget, Retrieved from

http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-04.pdf

Butler, B. S., & Gray, P. H. (2006). Reliability, mindfulness, and information systems. MIS Quarterly, 30(2), 211-224.

Capability Maturity Model Integration (CMMI) Team. (2010). CMMI(r) for development, version 1.3. Carnegie Mellon University, Software Engineering Institute, Technical

Report, CMU/SEI-2010-TR-033, Retrieved from
http://www.sei.cmu.edu/reports/10tr033.pdf

Caralli, R. A. (2004). Managing for Enterprise Security. Software Engineering Institute, Carnegie Mellon University. Retrieved from http://www.sei.cmu.edu/reports/04tn046.pdf.

Carter, M., Grover V., & Bennett Thatcher, J. (2011). The emerging مامور ارشد امنیت role of business technology strategist, MIS Quarterly Executive, 10(1), 19-29.

Cerpa, N., & Verner, J. M. (1999). Case study: The effect of IS maturity on information systems strategic planning. Information & Management, 34(4), 199-208.

Chan, Y. E., & Huff, S. L. (1992). Strategy: An information systems research perspective. Journal of Strategic Information Systems, 1(4), 191-204.

www.takbook.com

Chan, Y. E., & Reich, B. H. (2007). IT alignment: What have we learned? Journal of Information Technology, 22(4), 297-315.

Chang, A. J.-T., & Yeh, Q.-J. (2006). On security preparations against possible IS threats across industries. Information Management & Computer Security, 14(4), 343-360.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, 106(3), 345361.

Charmaz, K. (2006). Constructing grounded theory: A practical guide through qualitative analysis. Thousand Oaks, CA: Sage Publications Ltd.

Chen, D. Q., Mocker, M., Preston, D. S., & Teubner, A. (2010). Information systems strategy: Reutalization, measurement, and implications. MIS Quarterly, 34(2), 233-259, A1-A8.

Chen, P., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. MIS Quarterly, 35(2), 397-422.

Choo, K.-K., R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719-731.

Clark, T. L., & Sitko, T. D, (2008). Information security governance: Standardizing the practice of information security. EDUCAUSE Center for Applied Research, Research Bulletin, 2008(17), Retrieved from http://net.educause.edu/ir/library/pdf/ERB0817.pdf.

Cohen, K. J., & Cyert, R. M. (1973). Strategy: Formulation, implementation, and monitoring. The Journal of Business, 46(3), 349-367.

Collins, J. S. (2001). Pockets of chaos: Management theory for the process of computer security.

SANS Institute InfoSec Reading Room, Retrieved from http://www.sans.org/reading_room/whitepapers/infosec/pockets-chaosmanagementtheory-process-computer-security_602.

Computer Security Division (CSD). (2004). Federal Information Processing Standards

Publication (FIPS PUB) 199. Standards for security categorization of Federal information and information systems. Information Technology Laboratory, National Institute of Standards and Technology, Retrieved from http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

www.takbook.com

Corbet, B. (2014). Annual report to Congress: Federal Information Security Management Act.

Office of Management and Budget, Retrieved from http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy_2013_fisma_rep ort_05.01.2014.pdf.

Corbin, J., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criterias. Qualitative Soامامور ارشد امنیتlogy, 13(1), 3-20.

Corbin, J., & Strauss, A. (2008). Basics of qualitative research: Techniques and procedures for developing grounded theory. (3rd ed.). Los Angeles, CA: Sage Publications, Inc.

Costello, T. (2011). 2011 IT tech and strategy trends. IT Professional,13(1), 61-64.

Creswell, J. W. (2002). Research design: Qualitative, quantitative, and mixed methods approaches. (2nd ed.). Thousand Oaks, CA: Sage Publications Ltd.

Creswell, J. W. (2011). Educational research: Planning, conducting, and evaluating quantitative and qualitative research. (4th ed.). Upper Saddle River, NJ: Pearson Education.

da Veiga, A., & Eloff, J.H.P. (2007). An information security governance framework. Information Systems Management, 24(4), 361-372.

Damianides, M. (2005). Sarbanes-Oxley and IT governance: New guidance on IT control and compliance. EDP Audit, Control, and Security, 31(10), 1-14.

Daneva, M. (2006). Applying real options thinking to information security in networked organizations. Technical Report TR-CTIT-06-11, Centre for Telematics and Information Technology University of Twente, Enschede. Retrieved from http://eprints.eemcs.utwente.nl/5703/01/0000018c.pdf.

Dawson, M., Berrell, D. M., Rahim, E., & Brewster, S. (2010). Examining the role of the chief information security officer (CISO) & security plan. Journal of Information Systems Technology & Planning, 3(6), 1-5.

de Paula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D. F., Ren, J., Rode, J. A., & Filho, R. S. (2005). In the eye of the beholder: A visualization-based approach to information system security. International Journal Human-Computer Studies, 63(1-2), 524.

Devadas, U. M., Silong, A. D., & Ismail, I. A. (2011). The relevance of Glaserian and Straussian grounded theory approaches in researching human resource

www.takbook.com

development. Proceedings of the 2011 International Conference on Financial Management and Economics, 11(2011), 348-352.

Dhillon, G. S. (1995). Interpreting the management of information systems security. Department of Information Systems, London School of Economics and Political Science, Houghton Street, London WC2A 2AE, England. Retrieved from http://csrc.lse.ac.uk/research/theses/dhillon.pdf.

Dhillon, G. (2004). Dimensions of power and IS implementation. Information & Management, 41(5), 635-644.

Dhillon, G. (2007). Principles of information systems security, text and cases. Hoboken, NJ: John Wiley & Sons, Inc.

Dhillon, G., Caldeira, M., & Wenger, M. R. (2011). Intentionality and power interplay in IS implementation: The case of an asset management firm. Journal of Strategic Information Systems, 20(4), 438-448.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. Information Systems Journal, 16(3), 293-314.

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. Computers and Security, 28(3), 189-198.

Doughty, K. (2003). Implementing enterprise security: A case study. Information Systems Control Journal, 2(2003), 99-114.

Doherty, N. F., & Fulford, H. (2005). Do information policies reduce the incidence of security breaches: An exploratory analysis. Information Resources Management Journal, 18(4), 2139.

Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. Computers & Security, 25(1), 55-63.

Duffy, K., Ferguson, C., & Watson, H. (2004). Data collecting in grounded theory – some practical issues, Nurse Researcher, 11(4), 67-78.

Dunkerley, K. D. (2011). Developing an information systems security success model for organizational context. Available from ProQuest Dissertations and Theses database. (UMI No. 3456547).

Dunkerley, K. D., & Tejay, G. (2009). Developing an information systems security success model for egovernment context. Americas Conference on Information Systems, San Francisco, CA, 1-8.

Durumeric, Z., Li, F., Kasten, J., Amann, J., Beekman, J., Payer, M., Weaver, N., Adrian, D., Paxson, V., Bailey, M., Halderman, J. A. (2014). The matter of

www.takbook.com

Heartbleed. Proceedings of the Internet Measurement Conference (IMC), Vancouver, BC, Canada, 1-14.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. California Management Review, 45(1), 67-87.

Dynes, S., Kolbe, L. M., & Schierholz, R. (2007). Information security in the extended enterprise. Proceedings in Americas Conference on Information Systems, Denver, CO, 111.

Earl, M. J. (1993). Experiences in strategic information systems planning. MIS Quarterly 17(1), 124.

Eisenhardt, K. M. (1989). Building theories from case study research, The Academy of Management Review, 14(4), 532-550.

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. Academy of Management Journal, 50(1), 25-32.

Eloff, M. M., & von Solms, S. H. (2000). Information security management: A hierarchical framework for various approaches. Computers & Security, 19(3), 243-256.

Ezingeard, J.-N., McFadzean, E., & Birchall, D. (2005). A model of information assurance benefits. Information Systems Management Journal, 22(2), 20-29.

Fairholm, M. R., & Card, M. (2009). Perspectives of strategic thinking: From controlling chaos to embracing it. Journal of Management & Organization, 15(1), 17-30.

Fitzgerald, T. (2010). Clarifying the roles of information security: 13 questions the CEO, مامور ارشد امنیت, and CISO must ask each other. Information Systems Security, 16(2007), 257-263.

Garg, A., Curtis, J., & Halper, H. (2003). The financial impact of IT security breaches: What do investors think? Information Systems Security, 12(1), 22-33.

Gavetti, G., & Rivkin, J. W. (2005). How strategist really think, tapping the power of analogy. Harvard Business Review, 83(4), 54-63.

Geer, D. (2007). Measuring security. Paper presented at the Metricon 2.0 Conference. Retrieved from all.net/Metricon/measuringsecurity.tutorial.pdf.

Ghernouti-Hélie, S. (2010). A national strategy for an effective cybersecurity approach and culture. Proceedings of the International Conference on Availability, Reliability and Security, Krakow, PN, 370-373.

www.takbook.com

Gilbert, F. (2008). Is your due diligence checklist obsolete? Understanding how information privacy and security affects corporate and commercial transactions. The Computer & Internet Lawyer, 25(10), 13-18.

Glaser, B. G. (2002). Conceptualization: On theory and theorizing using grounded theory. International Journal of Qualitative Methods, 1(2), 1-31.

Glaser, B. G. (2012a). Constructivist grounded theory? The Grounded Theory Review. 11(1), 2838.

Glaser, B. G. (2012b). Stop. Write! Writing grounded theory. The Grounded Theory Review 11(1), 2-11.

Glaser, B. G., & Strauss, A. L. (1967). The discovery of grounded theory: Strategies for qualitative Research. Hawthorne, NY: Aldine Publishing Co.

Goldkuhl, G., & Cronholm, S. (2010). Adding theoretical grounding to grounded theory: Toward multi-grounded theory. International Journal of Qualitative Methods, 9(2), 187-205.

Goluch, G., Ekelhart, A., Fenz, S., Jakoubi, S., Tjoa, S., & Mück, T. (2008). Integration of an ontological information security in risk aware business process management.

Proceedings of the 41st Hawaii International Conference on Systems Sciences, Maui, HI, 1-9.

Grant, R. M. (2005). Contemporary strategy analysis: s, techniques, applications. In D. Q. Chen, M. Mocker, D. S. Preston, & A. Teubner. (2010). Information systems strategy: Reutilization, measurement, and implications. MIS Quarterly, 34(2), 233-259.

Grobler, T., & Louwrens, B. (2005). New information security architecture. Retrieved from http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/046_Article.pdf, 1-12.

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. Information Management & Computer Security, 13(4), 297-310.

Hall, J. M., Sarkani, S., & Mazzuchi, T. A. (2010). Moderating roles of organizational capabilities in information security. Proceedings of the 5th International Conference on iWarfare & Security, Dayton, OH, 427-436.

Hall, J. M., Sarkani, S., & Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. Information Management & Computer Security, 19(3), 155-176.

www.takbook.com

Hallberg, L. R.-M. (2006). The “core category” of grounded theory: Making constant comparisons.

International Journal of Qualitative Studies on Health and Well-being, 2006(1), 141-148.

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. Journal of Strategic Information Systems, 20(4), 373384.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154-165.

Hinde, S. (2000). New millennium, old failures. Computers & Security, 19(2), 119-127.

Hinde, S. (2003). Cyber-terrorism in context. Computers & Security, 22(3), 188-192.

Hirose, Y., Itao, K., & Umeda, T. (2012). Generating a new interview method. Proceedings of the 11th European Conference on Research Methods, Reading, United Kingdom, 161170.

Hofer, C. W., & Schendel, D. (1978). Strategy formulation: Analytical s. In D. Q. Chen, M.

Mocker, D. S. Preston, and A. Teubner. (2010). Information systems strategy: Reualization, measurement, and implications. MIS Quarterly, 34(2), 233-259.

Hong, K.-S., Chi, Y.-P., Chao, L. R., & Tang, J.-H. (2003). An integrated system theory of information security management. Information Management & Computer Security, 11(5), 243-248.

Howard, J. D., & Longstaff, T. A. (1998). A common language for computer security incidents. Sandia Labs, SAND98-8667. Retrieved from www.cert.org/research/taxonomy_988667.pdf.

Howard, M., & Kilmartin, W. (2006). Assessment of benchmarking within government organizations. Accenture, Retrieved from http://www.accenture.com/usen/pages/insightassessment-benchmarking-public-service-organizations-summary.aspx.

Hu, Q., Dinev. T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), 615-659.

www.takbook.com

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security - a neo-institutional perspective. Journal of Strategic Information Systems, 16(2), 153-172.

Huang, D.-L., Rau, P.-L. P., & Salvendy, G. (2010). Perception of information security, Behavior & Information Technology, 29(3), 221-232.

Hübler, A., Foster, G., & Phelps, K. (2007) Managing chaos: Thinking out of the box, Complexity, (12)3, 10-13.

Huehls, F. (2005). An evening of grounded theory: Teaching process through demonstration and simulation. The Qualitative Report, 10(2). 328-338.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Lockheed

Martin Corporation, Retrieved from http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LMWh ite-Paper-Intel-Driven-Defense.pdf.

Jirasek, V. (2012). Practical application of information security models. Information Security Technical Report, 17(2012), 1-8.

Johnson, A. M. (2009). Business and security executives views of information security investment drivers: Results from a Delphi study. Journal of Information Privacy and Security, 5(1), 327.

Johnson, A. M., & Lederer, A. L. (2010). CEO/مامور ارشد امنیت mutual understanding, strategic alignment, and the contribution of IS to the organization. Information & Management, 47(3), 138149. Jones, P. (2001). Organizational information security from scratch - a guarantee for doing it right.

SANS Institute InfoSec Reading Room, Retrieved from http://www.sans.org/reading_room/whitepapers/standards/organizationalinformationsecurity-scratch-guarantee_541.

Jones, M., & Alony, I. (2011). Guiding the use of grounded theory in doctoral studies - an example from the Australian film industry, International Journal of Doctoral Studies, 6(2011), 95114.

Kajava, J., & Siponen, M. (1996) Security management and organizations - bottom up or top down approach? Proceedings of Nordic Workshop on Secure Computer Systems, Gothenburg, Sweden, 1-12.

www.takbook.com

Kankanhalli, A., Tan, B.C.Y., Teo, H.-H., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management, 23(2), 139-154.

Kark, K. (2010). Twelve recommendations for your 2011 security strategy. Forrester database, Retrieved from http://www.forrester.com.

Kark, K., Penn, J., & Dill, A. (2009). Twelve recommendations for your 2009 information security strategy. Forrester database, Retrieved from http://www.forrester.com.

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. MIS Quarterly Executive, 9(3), 163-175.

Keen, P. G. W., & El Sawy, O. A. (2010). Engaging in مامور ارشد امنیت-CxO "Conversations that matter": An interview with Peter Keen. MIS Quarterly Executive, 9(1), 61-64.

Kim, G. (2004). Does security set the right goals? Security Management, 48(6), 182.

King, W. R. (1978). Strategic planning for management information systems. MIS Quarterly, 2(1), 27-37. Klaić, A. (2010). Overview of the state and trends in the contemporary information security policy and information security management methodologies. Proceedings of the 33rd International Convention on Information and Communications Technology, Electronics and Microelectronics, Opatija, HR, 1203-1208.

Knapp, K. J., & Boulton, W. R. (2006). Cyber-warfare threatens corporations: Expansion into commercial environments. Information Systems Management Journal, Spring(2006), 7687.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. Information & Management, 41(5), 597-607.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. Computers & Security, 27(5), 224-231.

Krutz, R. L., & Vines, R. D. (2001). The CISSP prep guide: Mastering the ten domains of computer security. New York, NY: John Wiley & Sons, Inc.

Kwok, K., McCallin, A., & Dickson, G. (2012). Working through preconception: Moving from forcing to emergence. The Grounded Theory Review, 11(2), 1-12.

Lacey, D. (2009). Understanding and transforming organizational security culture. Information Management & Computer Security, 18(1), 4-13.

www.takbook.com

Lacity, M. C., & Hirscheim, R. (1995). Benchmarking as a strategy for managing conflicting stakeholder perceptions of information systems. Journal of Strategic Information Systems, 4(2), 165-185.

Lapke, M. (2008). Power relationships in information systems security policy formulation and implementation. Retrieved from Virginia Commonwealth University Digital Archives http://etd.vcu.edu/theses/available/etd-05052008-164921/.

LaRossa, R. (2005). Grounded theory methods and qualitative family research. Journal of Marriage and Family, 67(November 2005), 837-857.

Lee, A. S., & Hubona, G. S. (2009). A scientific basis for rigor in information systems research. MIS Quarterly, 33(2), 237-262.

Lee, R. M. (2012). The history of Stuxnet – Key takeaways for cyber decision makers. Armed Forces Communications and Electronics Association (AFCEA), Retrieved from http://www.afcea.org/committees/cyber/documents/TheHistoryofStuxnet.pdf.

Leidner, D. E., Lo, J., & Preston, D. (2011). An empirical investigation of the relationship of IS strategy with firm performance. Journal of Strategic Information Systems, 20(4), 419437.

Levy, D. (1994). Chaos theory and strategy: Theory, application, and managerial implications.

Strategic Management Journal, Summer 94(15), 167-178.

Lindström, J., & Hågerfors, A. (2009). A model for explaining strategic IT-and information security to senior management. International Journal of Public Information Systems, 2009(1), 17-29.

Lomprey, G. R. (2008). Critical elements of an information security management strategy. University of Oregon, Applied Information Management, Retrieved from http://scholarsbank.uoregon.edu/jspui/bitstream/1794/7613/1/2008-lomprey.pdf.

Love, V. D. (2011). IT security strategy: Is your health care organization doing everything it can to protect patient information? Journal of Health Care Compliance, 13(6), 21-28, 64.

Loveland, G., & Lobel, M. (2011). Eye of the storm: Key findings from the 2012 global state of information security survey®. Pricewaterhouse Coopers LLP, Retrieved from http://www.pwc.com/giss2012.

www.takbook.com

Loveland, G., & Lobel, M. (2012). Changing the game: Key findings from the global state of information security® survey 2013. Pricewaterhouse Coopers LLP, Retrieved from http://www.pwc.com/giss2013.

Luftman, J., & Ben-Zvi, T. (2010). Key issues for IT executives 2009: Difficult economy's impact on IT. MIS Quarterly Executive, 7(2), 99-112.

Luftman, J., & Ben-Zvi, T. (2011). Key issues for IT executives 2010: Judi مامور ارشد امنیتus IT investments continue post-recession. MIS Quarterly Executive, 9(4), 263-273.

Luftman, J., & Kempaiah, R. (2008). Key issues for IT executives 2007. MIS Quarterly Executive, 9(1). 49-59.

Ma, Q., Johnston, A.C., & Pearson, J.M. (2008). Information security management objectives and practices: A parsimonious framework. Information Management & Computer Security, 16(3), 251-270.

Ma, Q., Schmidt, M. B., & Pearson, J. M. (2009). An integrated framework for information security management. Review of Business, 30(1), 58-69.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., & Raghu, T. S. (2010). Moving toward black hat research in information systems security: An editorial introduction to the special issue. MIS Quarterly, 34(3), 431-433.

Markides, C. C. (1999). In search of strategy. Sloan Management Review, 40(3), 6-7.

Mata, F. J., Fuerst, W. L., & Barney, J. B. (1995). Information technology and sustained competitive advantage: A resource-based analysis. MIS Quarterly, 19(4), 487-505.

McClean, C., & Kark, K. (2010). Introducing the Forrester information security maturity model: A framework for describing and evaluating a comprehensive security program. Forrester database. Retrieved from http://www.forrester.com.

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. Online Information Review, 31(5), 622-660.

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2011). Information assurance and corporate strategy: A delphi study of choices, challenges, and developments for the future. Information Systems Management, 28(2), 102-129.

Miller, D. (1981). Toward a new contingency approach: The search for organizational gestalts. Journal of Management Studies, 18(1), 1-26.

www.takbook.com

Mintzberg, H. (1985). The organization as political arena. Journal of Management Studies, 22(2), 133-154.

Mintzberg, H. (1987). Crafting strategy. Harvard Business Review, 65(4), 66-75.

Mintzberg, H. (1987b). The strategy concept I: Five Ps for strategy. In D. Q. Chen, M. Mocker, D. S. Preston, and A. Teubner. (2010). Information systems strategy: Reutilization, measurement, and implications. MIS Quarterly, 34(2), 233-259.

Mintzberg, H., Ahlstrand, B., & Lampel, J. (1998). Strategy safari: A guided tour through the wilds of strategic management. In R. L. Baskerville, & G. Dhillon, (2008). Information systems security strategy, a process view. In D. W. Straub, S. Goodman, & R. L.

Baskerville (Eds.), Information Security, Policies: Processes and Practices, Advances in Management Information Systems, Volume 11, (15-45). Armonk, NY: M. E. Sharpe, Inc.

Mintzberg, H., & McHugh, A. (1985). Strategy formation in an adhocracy. Administrative Science Quarterly, 30(2), 160–197.

Mintzberg, H., & Waters, J. A. (1985). Of strategies, deliberate and emergent. Strategic Management Journal, 6(3), 257-272.

Moen, R. D., & Norman, L. C. (2000). Evolution of the PDCA Cycle. Profound Knowledge Products Inc., Retrieved from http://pkpinc.com/files/NA01_Moen_Norman_fullpaper.pdf.

Moen, R. D., & Norman, L. C. (2009). The history of the PDCA cycle. Proceedings of the Seventh Asian Network for Quality Congress, Tokyo, JP, 1-12.

Newkirk, H. E., Lederer, A. L., & Johnson, A. M. (2008). Rapid business and IT change: Drivers for strategic information systems planning? European Journal of Information Systems, 17(3), 198-218.

Norman, A. A., & Yasin, N. M. (2010). An analysis of information systems security management (ISSM): The hierarchical organization vs. emergent organization. International Journal of Digital Society, 1(3), 230-237.

Office of the Inspector General (OIG). (2013). Evaluation of DHS' information security program for fiscal year 2012. Department of Homeland Security, Retrieved from http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-04_Oct12.pdf.

www.takbook.com

Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T., & Kagaua, T. (2009). Information security governance framework. Proceedings of the first Workshop on Information Security Governance, Chicago, IL, 1-6.

Olsen, E. (2007). Strategic planning for dummies. Hoboken, NJ: Wiley Publishing, Inc.

Oreku, G. S., & Mtenzi, F. J. (2009). Using nature to best clarify computer security and threats. Proceedings of the eighth annual International Conference on Dependable, Autonomic and Secure Computing, Chengdu, CN, 702-707.

Pandit, N. R. (1996). The creation of theory: A recent application of the grounded theory method. The Qualitative Report, 2(4), 1-13.

Park, S., & Ruighaver, T. (2008). Strategic approach to information security in organizations. Proceedings of the International Conference on Information Science and Security, Seoul, KR, 26-31.

Parkin, S. E., & van Moorsel, A. (2009). An information security ontology incorporating humanbehavioral implications. Newcastle University, Computing Science, Technical Report Series, CS-TR-1139, Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?, 115.

Pauleen, D. J., Corbitt, B., & Yoong, P. (2007). Discovering and articulating what is not yet known: Using action learning and grounded theory as a knowledge management strategy, The Learning Organization, 14(3), 222-240.

Pfeffer, J. (1992). Understanding power in organizations. California Management Review, 34(2), 29-50.

Pitt, L. F., Parent, M., Junglas, I., Chan, A., & Spyropoulou, S. (2011). Integrating the smartphone into a sound environmental information systems strategy: Principles, practices and a research agenda Journal of Strategic Information Systems 20(1), 27-37.

Porter, M. E. (1980). Competitive strategy: Techniques for analyzing industries and competitors. In D. Q. Chen, M. Mocker, D. S. Preston, & A. Teubner. (2010). Information systems strategy: Reutalization, measurement, and implications. MIS Quarterly, 34(2), 233-259.

Porter, M. E. (1996). What is strategy? Harvard Business Review, 74(6), 61-78.

Post, G. V., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. Computers & Security, 26(3), 229-237.

www.takbook.com

Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. Computers & Security, 23(8), 638-646.

Preston, D. S., & Karahanna, E. (2009). Antecedants of IS strategic alignment: A nomological network. Information Systems Research, 20(2), 159-179.

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. Information Systems Research, 20(1), 121-139.

Ransbotham, S., Mitra, S., & Ramsey, J. (2012). Are markets for vulnerabilities effective? MIS Quarterly, 36(1), 43-64.

Reich, B. H., & Benbasat, I. (2000). Factors that influence the social dimension of alignment between business and information technology objectives. MIS Quarterly, 24(1),81-113.

Rezakhani, A., Hajebi, A., & Mohammedi, N. (2011). Standardization of all information security management systems. International Journal of Computer Applications, 18(8), 4-8.

Rich, P. (2012). Inside the black box: Revealing the process in applying a grounded theory analysis. The Qualitative Report, 17(49), 1-23.

Robson, A. J. (2005). Complex evolutionary systems and the red queen. The Economic Journal, 115(504), F211-F224.

Rose, A. (2011). Information security frameworks fail without a supporting management system: Why security is not about controls. Forrester database, Retrieved from http://www.forrester.com.

Rowe, B. R., & Gallaher, M. P. (2006). Private sector cyber security investment strategies: An empirical analysis. Proceedings of fifth Workshop on the Economics of Information Security, Cambridge, UK, 1-23.

Rowlands, B. H. (2005). Grounded in practice: Using interpretive research to build theory. Electronic Journal of Business Research Methodology, 3(1), 81-92.

Rudd, J. M., Greenley, G. E., Beatson, A. T., & Lings, I. N. (2008). Strategic planning and performance: Extending the debate. Journal of Business Research, 61(2), 99-108.

Ruighaver, R. A. (2008). Organisational security requirements: An agile approach to ubiquitous information security. Proceedings of the sixth Australian Information Security Management Conference, Perth, AU, 1-7.

Salancik, G. R., & Pfeffer, J. (1977). Who gets power – and how they hold on to it: A strategiccontingency model of power. Organizational Dynamics, 5(3), 2-21.

www.takbook.com

Salmela, H., & Spil, T. A. M. (2002). Dynamic and emergent information systems strategy formulation and implementation. International Journal of Information Management, 22(2002), 441-460.

Scott, K. W., & Howell, D. (2008). Clarifying analysis and interpretation in grounded theory: Using a conditional relationship guide and reflective coding matrix. International Journal of Qualitative Methods, 7(2), 1-15.

Scully, T. (2011). The cyber threat, trophy information and the fortress mentality. Journal of Business Continuity & Emergency Planning, 5(3). 195-207.

Scully, T. (2013). The cyber security threat stops in the boardroom. Journal of Business Continuity & Emergency Planning, 7(2), 138-148.

Security Research and Emergency Response Center of Antiy Labs (Anity CERT). (2014). A comprehensive analysis on Bash Shellshock. Anity Labs, Retrieved from http://www.antiy.net/p/a-comprehensive-analysis-on-bash-shellshock-cve-20146271/.

Segars, A. H., & Grover, V. (1998). Strategic information systems planning success: An investigation of the construct and its measurement. MIS Quarterly, 22(2), 139-163.

Seeholzer, R. V. (2012). Information security strategy: In search of a role. Proceedings of the Eighteenth Americas Conference on Information Systems (AMCIS), Seattle, WA, 1-18.

Shariati, M., Bahmani, F., & Shams, F. (2010). Enterprise information security, a review of architectures and frameworks from interoperability perspective. Procedia Computer Science, 3(2011), 537-543.

Shoraka, B. (2011). An empirical investigation of the economic value of information security management system standards. Available from ProQuest Dissertations and Theses database (UMI No. 3456209).

Siponen, M. T. (2005a). Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. Information and Organization, 15(2005), 339-375.

Siponen, M. T. (2005b). An analysis of the traditional IS security approaches: Implications for research and practice. European Journal of Information Systems, 14(3), 303-315.

Siponen, M. (2006). Information security standards focus on the next existence of process, not its content. Communications of the ACM, 49(8), 97-100.

www.takbook.com

Siponen, M., & Iivari, J. (2006). Six design theories for IS security policies and guidelines. Journal of the Association for Information Systems, 7(7), 445-472.

Slater, D. (2002). Mistakes: Strategic planning don’ts (and dos). مامور ارشد امنیت, Retrieved from http://www.مامور ارشد امنیت.com/article/print/31106, 1-4.

Slaughter, S. A., Levine, L., Ramesh, B., Pries-Heje, J., & Baskerville, R. (2006). Aligning software processes with strategy. MIS Quarterly, 30(4), 891-918.

Smedinghoff, T. J. (2005). The new law of information security: What companies need to do now. The Computer & Internet Lawyer, 22(11), 9-25.

Smith, E. E., & Medin, D. L. (1981). Categories and concepts, Cambridge, MA: Harvard University Press.

Smith, P. (2004). Developing & implementing an information security policy and standard framework. SANS InfoSec Reading Room. Retrieved from http://www.sans.org/reading_room/whitepapers/hipaa/developingimplementinginformation-security-policy-standard-framework_1401.

Stanton, J. M., Guzman, I., Stam, K., & Caldera, C. (2003). Examining the linkage between organizational commitment and information security. Proceedings of the IEEE Systems, Man, and Cybernetics Conference, Washington, DC, 1-6.

Stocker, R., & Close, H. (2013). A novel method of enhancing grounded theory memos with voice recording. The Qualitative Report, 18(1), 1-4.

Straub, D. W. (1990). Effective IS security: An empirical study. Information Systems Research, 1(3), 255-276.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. MIS Quarterly, 22(2), 441-469.

Suddaby, R. (2006). From the editors: What grounded theory is not. Academy of management Journal, 49(4), 633-642.

Symantec Security Response (SSR). (2014). Regin: Top-tier espionage tool enables stealthy surveillance. Symantec Corporation, Retrieved from http://www.symantec.com/content/en/us/enterprise/media/security_response/whit epapers/regin-analysis.pdf.

Team FME (Free Management Ebooks). (2014). SWOT analysis: Strategy skills. Free Management Ebooks, Retrieved from http://www.free-managementebooks.com/dldebkpdf/fme-swot-analysis.pdf.

www.takbook.com

Tejay, G. (2008). Shaping strategic information systems security initiatives in organizations Available from ProQuest Dissertations and Theses database (UMI No. 3346492).

Thompson, S. H., & James S. K. (2001). An examination of major IS planning problems. International Journal of Information Management, 21(6), 457-470.

Trend Micro Threat Research Lab (TMTRL). (2014). Shellshock: A technical report. Trend Micro Incorporated, Retrieved from http://www.trendmicro.com/cloudcontent/us/pdfs/securityintelligence/white-papers/wp-shellshock.pdf.

Valle Jr., V. (2000). Chaos, complexity and deterrence. National War College, Retrieved from http://www.au.af.mil/au/awc/awcgate/ndu/valle.pdf.1-13. van Niekerk, J. F., & von Solms, R. (2010). Information Security culture: A management perspective. Computers & Security, 29(4), 476-486.

Vannoy, S. A., & Salam, A. F. (2010). Managerial interpretations of the role of information systems in competitive actions and firm performance: A grounded theory investigation. Information Systems Research, 21(3), 496-515.

Vasiu, L., Mackay, D., & Warren, M. (2003). The tri-dimensional role of information security in e-business: A managerial perspective. Proceedings of the Hawaii International Conference on Business, Honolulu, HI, 1-9.

Vijayan, J. (2005). Strategic security. Computerworld. Retrieved from http://www.computerworld.com/s/article/100916/Strategic_Security?taxonomyId=017.

von Solms, B. (2001). Information security - a multidimensional discipline. Computers & Security, 20(6), 504-508.

von Solms, B. (2006). Information security: The fourth wave. Computers & Security, 25(3), 165168.

von Solms, R. (1998a). Information security management (2): Guidelines to the management of information technology security (GMITS). Information Management & Computer Security, 6/5(1998), 221-223.

von Solms, R. (1998b). Information security management (3): The code of practice for information security management (BS 7799). Information Management & Computer Security, 6/5(1998), 224-225.

Wagner, H.-T., & Weitzel, T. (2012). How to achieve operational business-IT alignment:

www.takbook.com

Insights from a global aerospace firm. MIS Quarterly, 11(1), 25-36.

Wang, C. (2009). The underground economy of security breaches. In A. Oram, and J. Viega (Eds.), Beautiful security: Leading security experts explain how they think, (63-72).

Sebastopol, CA: O'Reilly Media, Inc.

Weill, P., & Woerner, S. L. (2013). The future of مامور ارشد امنیت in a digital economy. MIS Quarterly Executive, 12(2), 65-75.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. Information Management & Computer Security, 17(1), 4-19.

Westerman, G. (2009). IT risk as a language for alignment. MIS Quarterly Executive, 8(3), 109121.

White, M. A., & Bruton, G. D. (2011). The management of technology and innovation: A strategic approach. (2nd ed.). Mason, OH:Thomson South-Western, Cengage Learning.

Wimpenny, P., & Gass, J. (2000). Interviewing in phenomenology and grounded theory: Is there a difference? Journal of Advanced Nursing, 31(6), 1485-1492.

Wommack, W. W. (1979). The board's most important function. Harvard Business Review, 57(5), 49-54.

Wood, C. C. (2000). An unappreciated reason why information security policies fail. Computer Fraud & Security, 2000(10), 13-14.

Yarger, H. R. (2006). Strategic theory for the 21st century: The little book on big strategy. Director, Strategic Studies Institute, U.S. Army War College, 122 Forbes Ave, Carlisle, PA 170135244. Retrieved from http://www.StrategicStudiesInstitute.army.mil/.

Yoong, P. (1996), "A grounded theory of reflective facilitation: making the transition from traditional to GSS facilitation", Thesis, Victoria University of Wellington, NZ.

Xiao-yan, Yuan, Y., & Lu, L. (2011). An information security maturity evaluation mode. Procedia Engineering, 24(2011), 335-339.

Zhang, N., & Bao, H. (2010). Design and formulation of security strategy in network. International Conference on Future Networks, Sanya, Hainan, CN, 216-220.

www.takbook.com

Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010). Information risk management framework for the cloud computing environments. International Conference on Computer and Information Technology, Bradford, Yorkshire, UK, 1328-1334.

Zients, J., Kundra, V., & Schmidt, H. A. (2010). FY 2010 Reporting instructions for the Federal Information Security Management Act and agency privacy management, OMB Memo

M-10-15, Executive Office of the President, Office of Management and Budget, Retrieved from

http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m1015.pdf.

Zuccato, A. (2007). Holistic security management framework applied to electronic commerce. Computers & Security, 26(3), 256-265.