THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

COLLEGE OF INFORMATION SCIENCES AND TECHNOLOGY

THE CASE FOR THE ENTERPRISE SECURITY ARCHITECT

EILEEN CHEN
SPRING 2013

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in Information Sciences and Technology
with honors in Information Sciences and Technology

Reviewed and approved* by the following:

Brian H. Cameron
Executive Director, Center for Enterprise Architecture Initiative
Thesis Supervisor & Honors Adviser

Edward J. Glantz
Professor of Practice
Faculty Thesis Reader

* Signatures are on file in the Schreyer Honors College.

Abstract

Cyber-attacks have been on the rise and more and more organizations today are realizing that security is vital for success. Enterprise security architecture can be used to align security architecture with organizational goals to build effective and efficient security architectures. Although past research has established the need for enterprise security architecture, there has yet to be an established career path for the enterprise security architect. This thesis examines the concepts and importance of enterprise architecture and enterprise security architecture, and discusses the multiple roles of the enterprise security architect. This thesis also includes a proposal of a career path for the enterprise security architect with the hope that it will serve as a basis for future development of the career path of the enterprise security architect and increase interest in the career and field.

Table of Contents

List of Figures

List of Tables

Acknowledgements

There are many people to thank for helping me complete this thesis but I'd like to personally thank the following. Without their time and effort in helping me, I would not be able to complete this thesis.

- Dr. Brian H. Cameron, my thesis supervisor and honors adviser for his help, guidance, and expertise throughout this whole process.
- Dr. Edward J. Glantz for volunteering his time to read and provide guidance and expertise on this thesis.
- Eric McMillan for his help with understanding the complex concept of enterprise architecture.
- The Schreyer Honors College for giving me an opportunity to pursue this topic and write a thesis.
- Rebecca Alt for her constant support and motivation throughout this whole process.
- My family and friends for providing me with amazing support and motivation to finish this thesis.

Chapter 1: Introduction

Apple, Sony, CitiBank, Google, Facebook, and NBC: all impressive companies but what do these organizations have in common? They are all victims of recent cyber-attacks ("Recent Cyber Attacks," n.d.).

Cyber-attacks have been on the rise and although more and more organizations today are realizing that security is vital for success, focusing only on the technology of security will not create effective and efficient security architecture for the organization (Sherwood, Clark, & Lynas, 2005; Shen, Lin, & Rohm, 2009, p. 9). Security technology usually does not consider the organization's business operating models (Shen, Lin, & Rohm, 2009, p. 9). Enterprise architecture (EA) aligns a business's strategic vision with its information technology (Daniel, 2007). Employing an enterprise security architect (ESA), who understands both the concepts of EA as well as the security architecture (SA), can provide secure solutions and services that can help improve, or even build, the security of the enterprise. However, some organizations do not consider the enterprise security architect position as part of the main architectural team; some do not even have enterprise security architects. In the $(ISC)^2$ (International Information Systems Security Certification Consortium) staffing survey, it took 36% of organizations three to six months to fill an open security position (Holland, Balaouras, & McKee, 2012). One of the reasons for this is that there is a lack of knowledge available about the career of enterprise security architects and enterprise security architecture, overall.

This thesis aims to describe the job of the enterprise security architect and establish a clear path for the enterprise security architect in hopes that there will be more knowledge about and interest in the position, ultimately helping to decrease the growing number of cyber-attacks.

Chapter 2: What is Enterprise Architecture?

Although the history of enterprise architecture can be traced back to almost thirty years ago, the concept of EA is still is an emerging trend that is the key to enable the enterprise and add value to the organization. The initial idea of EA was to fix two problems: organizations spending too much money to build complex IT systems and poor alignment of expensive, complex IT systems with business need. There was a growing distrust between business and technology departments. Both claimed not to understand each other and as a result, the organizations reacted to changes in the business environment too slowly and inadequately (Cameron, 2011). Despite having two initial purposes for EA, there is still no single, accepted definition. For the purpose of clarifying the concept of enterprise architecture, several prominent definitions follow below. The first group of definitions refers to EA being explained as a business process and the second group of definitions refers to EA being explained as a noun.

EA as a Process

According to Gartner:

> "Enterprise architecture is the process of translating business vision and strategy into effective enterprise change by creating, communicating and improving the key requirements, principles and models that describe the enterprise's future state and enable its evolution. The scope of the enterprise architecture includes the people, processes, information and technology of the enterprise, and their relationships to one another and to the external environment. Enterprise architects compose holistic solutions that address the business challenges of the enterprise and support the governance needed to implement them," (Lapkin et al., 2008). In this definition, Gartner explains EA as a strategy and mainly focuses on where an organization is going and how it is going to get there.

The Federation of Enterprise Architecture Professional Organizations (FEAPO) defines EA as:

> "a well-defined process for conducting the enterprise-wide analysis, design, planning, and implementation needed for successful execution of strategy. Enterprise Architecture applies architecture principles to analyze the components, the structure and connectivity of different parts and layers of the enterprise and identify their relationships to each other and to the strategy of the organization," (Federation of Enterprise Architecture Professional Organizations, n.d., p. 2). Again, EA is described as a process in FEAPO's definition and focuses on strategy planning and implementation.

EA as a Noun

Carla Pereira and Pedro Sousa define EA as:

> "Enterprise Architecture is a framework or 'blueprint' for how the organization achieves the current and future business objectives," (Pereira & Sousa, 2004).

Likewise, The Institute or Enterprise Architecture Developments defines EA as:

> "…a complete expression of the enterprise; a master plan which 'acts as a collaboration force' between aspects of business planning such as goals, visions, strategies and governance principles; aspects of business operations such as business terms, organization structures, processes and data; aspects of automation such as information systems and databases; and the enabling technological infrastructure of the business such as computers, operating systems and networks" ("Enterprise Architecture Good Practice," 2009).

In both of these definitions, EA is explained as a noun, instead of a process. EA is a plan on how to incorporate all aspects of the enterprise from a current state to a future state. It also describes a collection of artifacts, documents, and other outputs of the EA process.

Despite the existence of multiple definitions of EA, EA can take an enterprise from its current state to a more beneficial future state. The benefits of enterprise architecture can be

summed up using three words: better, faster, and cheaper (Ambler, n.d.). EA can provide the organization with a holistic view so that members can understand all the components within the enterprise including how components interact with each other and how a component is impacted by changes in the environment. By having a holistic view, EA can bring together information from all different domains and standardize processes and systems across the organization. It translates and combines information from different domains into a common language that everyone in the organization can understand. As a result, EA can align business and IT as well as bring business and technology into closer partnerships. Morale and focus on the organization's overall goals will increase as organization members understand more about the enterprise as a whole, instead of just their own domains.

Enterprise Architecture Frameworks

Several enterprise architecture frameworks exist. Wikipedia defines an EA framework as "an architecture framework which defines how to organize the structure and views associated with an enterprise architecture," ("Enterprise Architecture Framework," n.d.). The five major frameworks that are often used are The Zachman Framework, The Open Group Architecture Framework (TOGAF), The Department of Defense (DoD) Architecture Framework (DoDAF), The Federal Enterprise Architecture (FEA), and The Gartner Practice. All five of these approaches try to make it easy to understand all the different parts of the organization and how those different parts are related or aligned with the overall strategy of the organization.

Chapter 3: What is Enterprise Security Architecture?

According to Len Fehskens, EA is broken down into four different stacks: infrastructure/technology, applications, information, and business. As seen in Figure 3.1, security is "an attribute that has to be implemented across the enterprise as a whole in a consistent way," (Fehskens, 2010).

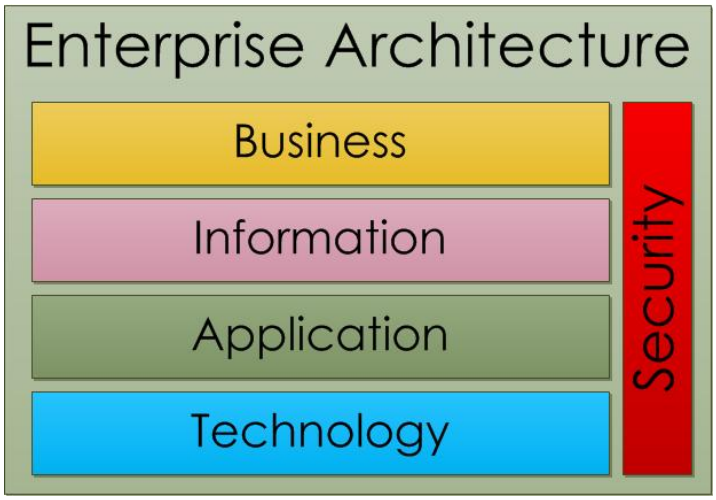

Figure 3.1 Enterprise Architecture with Security Attribute

Below are several definitions of Enterprise Security Architecture (ESA).

Tahajod et al defines ESA as:

> "a cohesive security design, which addresses the requirements (e.g. authentication, authorization, etc.) – and in particular the risks of a particular environment/scenario, and specifies what security controls are to be applied where." They also mention that "developing an security architecture allows organizations to identify the business, IT and compliance elements that must be secured to achieve key objectives and goals, and provides key stakeholders with the ability to plan and prioritize strategic IT security

> investments pertinent to technology implementations, process enhancements and user awareness initiatives" (Tahajod et al, 2009).

SANS Institute describes the objective of ESA:

> "to provide the conceptual design of the network security infrastructure, related security mechanisms, and related security policies and procedures. The enterprise security architecture links the components of the security infrastructure as one cohesive unit," (Arconati, 2002).

Tom Scholtz, vice president of Gartner, describes ESA as:

> "the policies, processes, components and systems that encompass an enterprise security program. Security architectures ideally provide more insight into how data and devices are secured and more choices in how they can be used," (Parizo, 2007).

Fujitsu defines ESA as:

> "documentation of a systematized view of a corporation's security approach, clearly delineating the basic technical approach to information security," (Fujitsu Enterprise Security Architecture, 2007).

Despite having multiple different definitions of enterprise security architecture, ESA looks closely into how security will affect the enterprise and is a valuable asset to many organizations today.

The Sherwood Applied Business Security Architecture Framework

There are many articles that introduce how an organization would integrate security into different enterprise architecture frameworks. Some ESA frameworks are mere collaborations of multiple frameworks. One prominent framework that is often used in conjunction with other frameworks such as TOGAF, is the SABSA (Sherwood Applied Business Security Architecture) framework. SABSA specifically regards enterprise security architecture. The official SABSA definition is "SABSA is a model and a methodology for developing risk-driven enterprise

information security architectures and for delivering security infrastructure solutions that support critical business initiatives," ("SABSA Overview," n.d.).

As seen in Table 3.1, the SABSA model is broken down into six layers of security architecture: contextual, conceptual, logical, physical, component, and operational. Each layer represents a different view of a player in the business system.

The Business View	**Contextual Security Architecture**
The Architect's View	**Conceptual Security Architecture**
The Designer's View	**Logical Security Architecture**
The Builder's View	**Physical Security Architecture**
The Tradesman's View	**Component Security Architecture**
The Facilities Manager's View	**Operational Security Architecture**

Table 3.1 The SABSA Model for Security Architecture Development

Another view of the model, seen in Figure 3.2, shows the operational security architecture layer placed vertically across the other five layers because operational security issues arise in each and every one of the other five layers ("SABSA Model," n.d.).

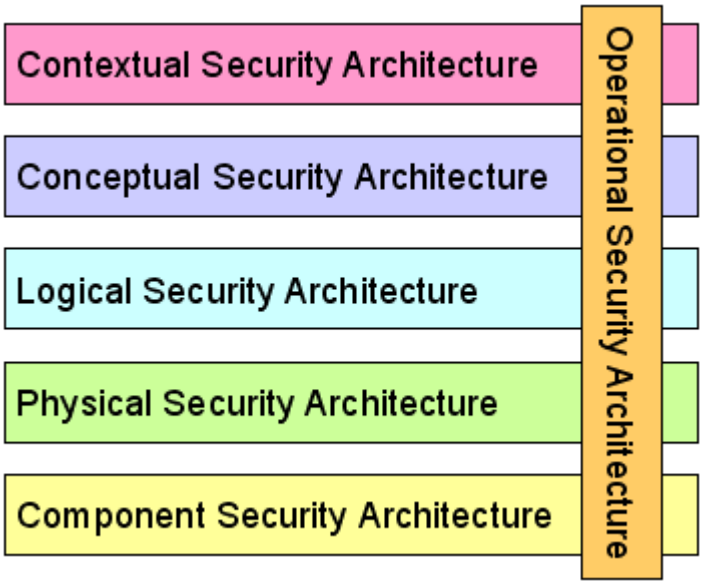

Figure 3.2 The SABSA Model for Security Architecture Development

The SABSA framework also has a detailed analysis of each of the six layers, called the SABSA Matrix. The matrix represents a model and if one can address and cover all the questions raised in each and every one of the cell, one can be confident that their security architecture is complete. In this matrix, seen in Figure 3.3, six questions, similar to the Zachman Framework, are asked at every layer ("SABSA Matrix," n.d.):

(1) *"What* are you trying to do at this layer? – The assets to be protected by your security architecture.

(2) *Why* are you doing it? – The motivation for wanting to apply security, expressed in the terms of this layer.

(3) *How* are you trying to do it? – The functions needed to achieve security at this layer.

(4) *Who* is involved? – The people and organisational aspects of security at this layer.

(5) *Where* are you doing it? – The locations where you apply your security, relevant to this layer.

(6) *When* are you doing it? – The time-related aspects of security relevant to this layer."

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organization and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetimes and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and the User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management and Support	Security of Sites, Networks and Platforms	Security Operations Schedule

Figure 3.3 The SABSA Matrix for Security Architecture Development

The SABSA framework also includes many other elements such as the SSM, Process, Lifecycle, and Business Attributes, which is not discussed in this thesis.

Chapter 4: Why Is There A Need For Security Architecture?

The majority of organizations today said they don't have enough security staff to handle their current demands (Wilson 2013). A majority of organizations today also said the shortage of skilled staff is contributing to the incidence of breaches in their organizations (Wilson 2013). Similarly, a survey conducted by B2B International on behalf of Kaspersky Lab showed that 58% of the IT professionals surveyed highlighted a lack of resources in both security staffing and budget (*Global IT Security Risks*, 2012). Seen in Figure 4.1, the top three obstacles to advancing the security departments are shown to be lack of budget, IT security understanding with budget holders, and sufficient knowledge from the IT personnel to deal with these threats.

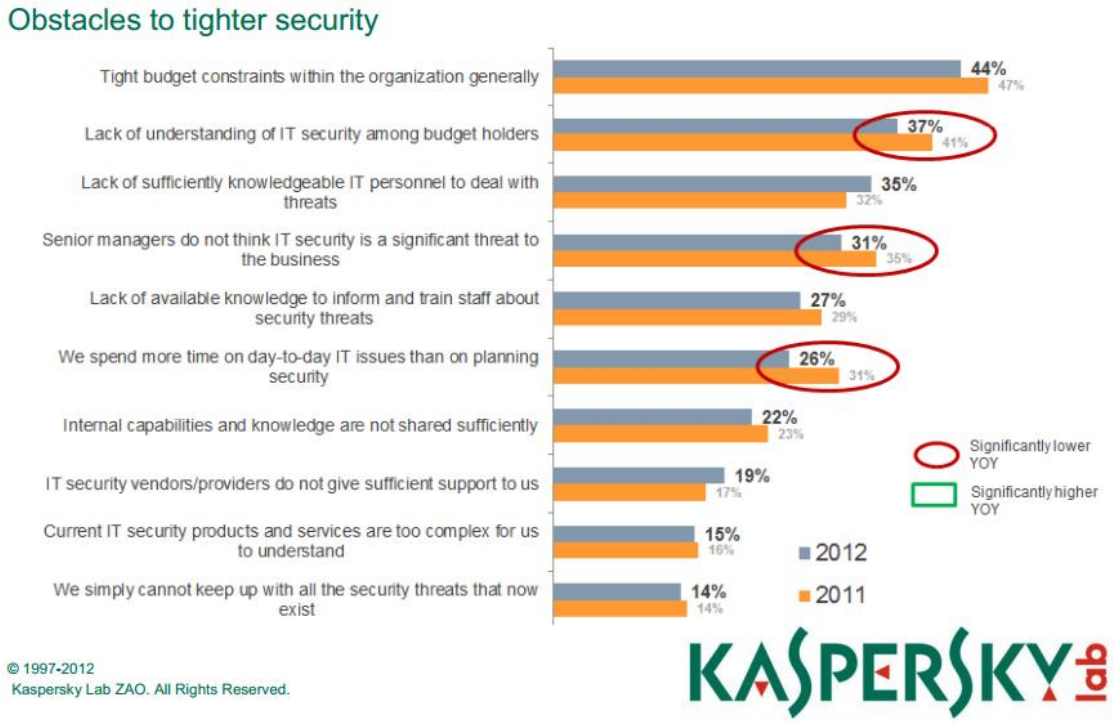

Figure 4.1 Kaspersky Lab Global IT Security Risks: 2012 "Obstacles to tighter security"

Most security specialists in the organization have a very narrow range of experience and knowledge. Often they are limited to just network protection. Enterprise security architectures know how to extend security knowledge into each layer of enterprise architecture (Szakal, 2012).

While industry experts say that in the past two years, there is an estimated growth of more than 600,000 people in the global security work force. Industry will still need to add nearly 2 million more jobs during the next three years in order to keep up with demand (Wilson, 2012a). Hord Tipton, executive director of $(ISC)^2$, said that there are many companies still struggling with hiring security professionals. "It often falls to human resources people, but they don't always know what questions to ask," he observed. "They need to understand what tools that the candidate has used, what specialized areas they have experience in, and what certifications they have. Hiring security people is not always an easy process," (Wilson, 2012a). Also, there is currently no established career path for the enterprise security architect. Having a career path established for both the individuals who look to join this career and the individuals who look to recruit enterprise security architects can give both groups a better idea of what the job entails and how to be effective at the job.

Chapter 5: What is the Role of the Enterprise Security Architect?

According to Forrester Research, a security architect (SA) is "technical role responsible for ensuring that the design of business solutions meets security and compliance mandates. The SA partners with stakeholders across the organization to securely achieve the functional requirements of business initiatives. The SA is the technical authority on information security architecture within the organization," (Holland, Balaouras, & McKee, 2012). Generally, the security architect develops, maintains, and improves the security processes across the enterprise. As it may be obvious, the security architect wears a lot of hats. After researching and analyzing many documents, articles, publications, as well as resources from a number of organizations who provided information pertaining to their EA career paths, this thesis will define below the different roles the SA can play in an organization.

Role 1: Planning the Alignment of Security with Business Strategy

As mentioned previously, there exists the problem with the gap between IT and business. The security architect, in this role, supports the business by creating visions and strategies that will align the enterprise's security architecture with the overall business strategies. The security architect would first partner with various stakeholders across the organization. This may include suppliers, security users, department managers, clients, and other key stakeholders. The security architect and stakeholders would then develop both short and long-term strategic goals for the security architecture visions, standards, and principles that would help guide the enterprise in making the best business decisions possible with regards to security. This also includes the team evaluating current security strategies already in place and making sure that they align with both technology and business needs.

Role 2: Evaluating, Designing, and Enforcing Policies

The security architect reviews security policies, procedures, standards, guidelines, and best practices. Once the policies are defined, the security architects assist management in enforcement of those policies throughout the enterprise.

Role 3: Designing the Security Architecture

Once the team has finished with the holistic view of the enterprise in regards to security with its visions/strategies and policies, they can start designing security solutions that addresses business needs. This can be for information assurance, cyber security, applications, service centers, data centers, and many other aspects of the business. They may develop protection services (authentication and authorization of systems), detection services (monitoring and auditing), and response services (incident response and forensics) ("Security Architect," 2012).

Role 4: Ensuring Compliancy

The security architect, in this role, makes sure that the design of the security architectures meets security and compliance mandates as well as relevant laws, regulations, policies, standards, or procedures such as information security, health and safety, privacy acts, maintenance, etc. (DoD EA Career Path Working Group, 2012). The SA also is included in any audit and compliance efforts. Lastly, the SA creates appropriate security and compliance metrics to evaluate the security architecture and present its current standings and risks to senior management from an information security and regulatory compliance standpoint.

Role 5: Identifying, Communicating, and Mitigating Risk

The security architect, in this role, consistently and aggressively seeks and identifies security risks in the enterprise. Once risks are identified, the SA informs management of those risks and the implications it brings onto the business. They also provide management with countermeasures so that the business can take as many risks to reach their overall goals (Tahajod,

Iranmehr, & Darajeh, 2009). Management would ultimately decide what to do with the risks and leaves the responsibility of mitigating or responding to the risk with the SA.

Role 6: Being the Security Lead

In this role, the security architect is the lead of security within the organization. Essentially, the SA is the "go to" person for any security need. They analyze the current technology environment, security industry, and market trends to identify any critical problems that may impact the enterprise as well as develop solutions to mitigate those problems. The SA also leads improvements of techniques, methodologies, and deliverables in regards to the security of the enterprise. They are the subject matter experts to business, operations, and technology teams on security related topics. They will take the lead in any enterprise security environment and inform others about current security standings, trends, and needs.

Chapter 6: Who Does the Enterprise Security Architect Work With?

While the security architect is a very crucial position, they do not work alone. Often, they are found within the EA team, as it is not found as a formal practice area in most organizations (Cameron). "The actual number of security architects within the EA team varies largely between organizations. Gartner research indicates that many organizations start with one full-time equivalent (FTE) responsible for information security within the EA team. This number occasionally grows depending on the nature of the security planning activities in the organization (and the maturity of the security architecture and EA practices in general). It is obviously also dependent on the size and scale of a given organization," (Scholtz & Byrnes, 2010). According to a survey conducted by Forrester in 2011, 43% of EA groups have security architects whereas in 2010, it was 39% (see Figure 6.1).

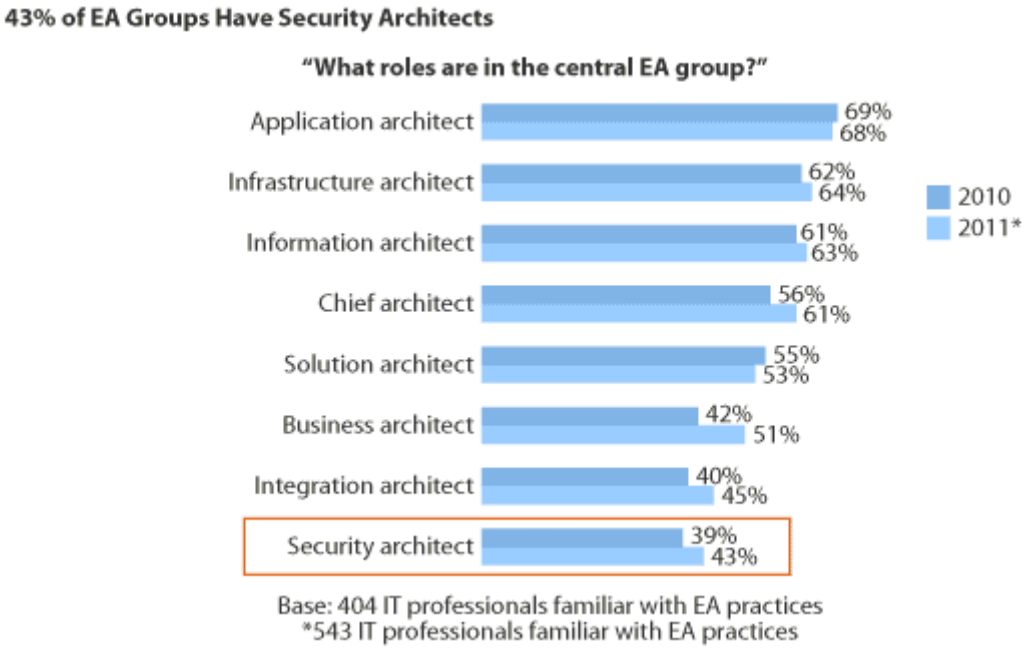

Figure 6.1 What roles are in the central EA group? (Forrester Research Inc., 2011a)

For those EA groups that do contain security architecture, it's the second most complete part of the overall EA program. Sixty one percent of those EA groups that do contain security architecture have implemented at least a moderate amount of security architecture in the EA program, making security architecture to the be the second most complete part of the EA program (see Figure 6.2).

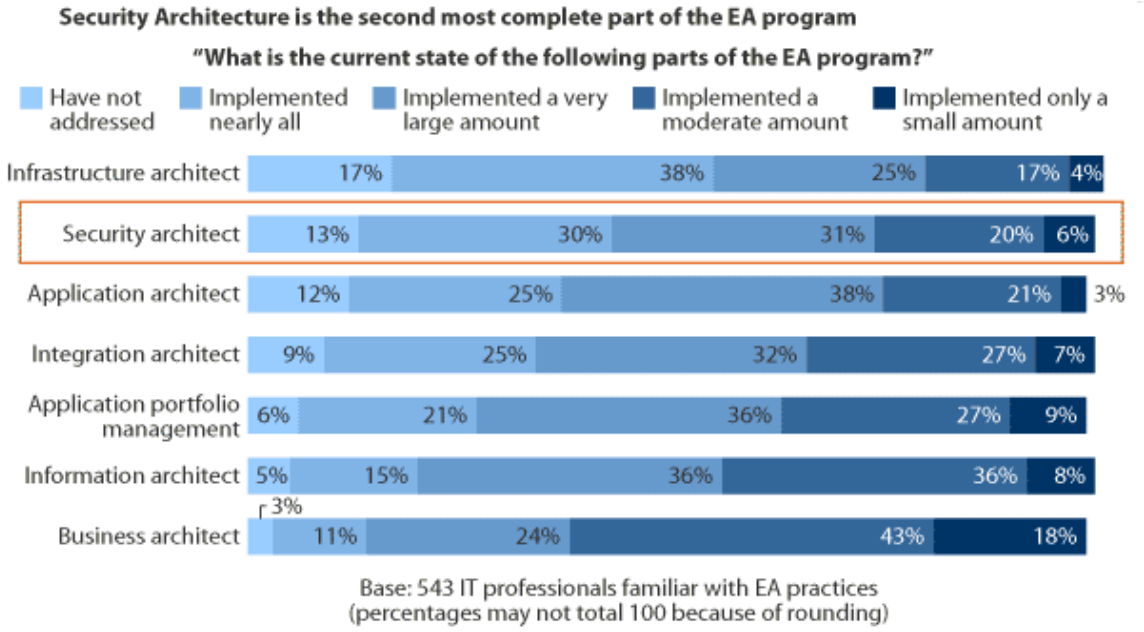

Figure 6.2 What is the current state of the following parts of the EA program? (Forrester Research Inc., 2011b)

According to Forrester, when the security architect is within the EA team, it reports primarily to the chief information security officer (CISO) but also works under the manager of EA. When the security architect is within the security organization, the CISO oversees the director of SA who oversees the infrastructure and application security architects. In other organizations, the security architects could also report to the rest of the EA team as well as the security and risk leadership team. Security architects mostly work closely and build strong relationships with CISO, EA team members responsible for overall organizational architecture,

key stakeholders from the organization as well as technical architects, solutions architects, and security specialists. The SA can also collaborate with various information security subject matter experts during architecture activities or security specialists to develop models, principles, and templates. While some organizations have teams of security architects responsible for specific disciplines, some organizations have one security architect responsible for all disciplines.

Chapter 7: Why Is There A Need For Security Architecture?

The 2012 Global State of Information Security Survey conducted by PricewaterhouseCooopers (PwC), CIO Magazine, and CSO Magazine found that more than 9,600 global executives, 41 percent of US respondents had experienced one or more security incidents during the year of 2012. Antivirus firm Symantec had estimated that the direct financial loss and cost of remediating attacks in 2011 was at $338 billion (Ackerman, 2013). Kaspersky Lab found that half of the companies they surveyed around the world lacked awareness of cyber security threats ("Companies Worldwide Lack Awareness," 2012). An Ernst & Young's global security survey reported that 31% of organizations have experienced a higher number of security incidents in the past two years than they have in the years prior (Wilson, 2012b).

It's clear that security should be extremely important to the success of an organization. However, network and application security itself is not enough; an organization needs enterprise security architecture. Michael Fey, the chief technology officer at McAfee said, "Security is now a boardroom level discussion… The stakes are high, and businesses require a new model that gives them a comprehensive picture of their entire IT infrastructure. The industry has been built on a historical thought process that will not support the demands of the future. We must move to having a real-time understanding and response capability if we are to meet the needs of the future," ("McAfee Outlines Strategy for Future," 2013). Additionally, "organizations are implementing incremental improvements to their information security capabilities to provide short-term solutions -- without tackling the issues associated with the overall information security threat… The need to develop a robust security architecture framework has never been greater," (Wilson, 2012c). Even though there is the need, 63% of organizations say that they do not have security architecture frameworks in place. Only 16 percent of respondents report that their

information security function fully meets the needs of the organization (Wilson, 2012b). The value that architecture provides is irreplaceable. It establishes a comprehensive view of the current state and a future view of the organization wants their security practice to look like. Kevin Riggins, an Enterprise Security Architect from a Fortune 500 Financial Services Organization said, “It’s really hard to figure out how to get somewhere if you don’t know where you are in the first place.” Rarely are the current state and the target state the same and a lot of change is required to get to the target state. The architecture defines the path to get there (Riggins, 2013). Also, enabling an enterprise security architecture has many benefits including improving cost effectiveness, communication, and risk management (Thorn, Christen, Gruber, Portman, & Ruf, 2008).

Chapter 8: What is the Career Path for the Enterprise Security Architect?

This section of the thesis describes the technical skills, interpersonal skills, business management skills, educational competencies, and expert experience the enterprise security architect should have.

Technical Skills

The technical skills required for an SA will vary from organization to organization and from team to team based on its own size and maturity. Some organizations will have generalist SAs who will need to know a broad range of security while other organizations will have specialist SAs who will need to know a specific domain of security such as application or infrastructure. Yet, some general technical skills that the security architect should know are: integrated risk management, information systems/security, and enterprise architecture. Integrated risk management is defined as the "ability to integrate information security risk assessments with other IT, operational and (increasingly) enterprise risk management activities" (Scholtz, 2011). They must know when and how to assess risk situations, decide what specific assessment tools, methods, and approaches to use, and apply it. Information security risk management must be integrated with existing IT risk management practices. The SA must also have expert knowledge of security principals and technologies. According to the DoD Architects' Competency Framework, having information systems/network security knowledge (knowledge of methods, tools, and procedures, including development of information security plans, to prevent information systems vulnerabilities, and provide or restore security of information systems and network services) met the overall importance criterion (DoD EA Career Path Working Group, 2012). It deemed needed for the job and required at entry because it will not be acquired through

formal training, such as classroom, on the job, or field training. This competency also will need development. Information Technology Requirements Analysis, which is the knowledge of the principles and methods to identify, analyze, specify, design, and manage functional and nonfunctional (for example, security, availability, maintainability) requirements and includes translating functional requirements into technical requirements used for logical design or presenting alternative technologies or approaches, had also met the overall importance criterion and deemed the need for development. Software Applications Security, the knowledge of methods, tools, and procedures used to design and build security measures into software applications to prevent vulnerabilities, maintain or restore security of information systems, and defend against unauthorized access to software applications and data, also met the overall importance criterion and deemed the need for development. The SA should also have expert knowledge of cyber security principles, current technologies, and trends in the industry, such as cloud hosting, big data, mobile, web services, and platform technologies, and have experience in developing technical solutions that lead the industry. The SA must also have the ability to think like an attacker. They must be able to shift between offensive and defensive viewpoints in order to identify threats and vulnerabilities in a system and seek ways to exploit them (Holland, Balaouras, & McKee, 2012). Additionally, the SA must be able to take complex technical information and security terminology and translate it into simple business terms to be understood across all levels of the organization. Lastly, the SA should have a sense of what enterprise architecture is about and have the ability to think about architecting for the extended enterprise. The SA has to architect a security architecture network that is integrated into the enterprise architecture.

Interpersonal Skills

As mentioned previously, the security architect will constantly be working in teams. The SA should be able to create and maintain strong relationships with the stakeholders, teammates, and vendors at all organizational levels (Holland, Balaouras, & McKee, 2012). They must be able to effectively work in a team to deliver high performance and customer satisfaction. Because the security architect frequently has to work with other people as well as communicate information to other team members, it is important for the SA to have good soft skills. Effective and strong verbal, presentation, and written communication are extremely important. In the past, many information security and technology professionals were often seen as to only communicate with other IT professionals in a very complex technical language. However, in today's business world, the SA must be able to communicate effectively with senior management, team members, and people in other disciplines outside of IT or security, integrating the technology world with the business world, and making the complex very simple for everyone to understand. One security architect said, "SAs must be able to present security risks in a way that people can understand. They must be able to identify with the stakeholder whom they are speaking with and assess their knowledge level. Don't assume; assess and begin the discussion at the right level." (Holland, Balaouras, & McKee, 2012).

Another interpersonal skill the SA should possess is strong influence and persuasion. According to a survey on global IT security risks conducted by B2B International on behalf of Kaspersky Lab, there is a lack of a clear understanding among senior managers as to why IT departments exist ("Companies Worldwide Lack Awareness," 2012). The SA has to prove the importance of security as well as the risks and proposed solutions to organization executives. They need to negotiate, persuade, and influence to sell their ideas and benefits to others in the enterprise that need to be educated about security issues.

As said before, the SA defines and develops the security architecture in an enterprise in regards to the current trends/issues in the industry/market as well as uprising risks and threats, which are problems to the enterprise. The SA must have strong problem-solving skills. They must be able to identify, analyze, and resolve problems; additionally, they should lead the solutions to successful completion (Holland, Balaouras, & McKee, 2012).

Other miscellaneous skills the SA should possess are high energy and clear passions for the job. It is more likely for a SA to perform better if they are happy and excited at what they are doing. The SA's personal values should align with the corporate values. The SA must be willing to travel internationally and have experience dealing with different nationalities and cultures.

Business Management Skills

To ensure that the security architecture aligns with the overall business strategy, the SA should have a broad overview of business fundamentals and think in business terms at all times (Holland, Balaouras, & McKee, 2012). They should understand at least the basics of business as to be able to translate technical terms into business terms. After all, the enterprise security architecture surrounds the overall business strategy.

Educational Competencies

At an entry level security architect position, usually a degree level qualification in information technology or related field is required. After an analysis of multiple security architect job postings on several job posting websites, it was found that a bachelor's degree in computer science, MIS, or related fields are preferred although employers do look at equivalent experiences. However, having a master's degree is ideal. As one chief information security officer (CISO) observed, "It would be much more valuable if my security staff enrolled in MBA courses, rather than in post-graduate information security qualifications," (Scholtz, 2011).

Enrolling in a Masters of Business Administration (M.B.A.) program or other business management courses are also encouraged.

In addition to further education, security architects are also encouraged to go to training courses and seminars outside information security to expand their knowledge set. SAs should aim to learn more about risk management, scenario planning, enterprise architecture, EA methodology used by the organization the SA is employed at, basic marketing theory, and financial planning skills (i.e. cost-benefit analysis, net present value calculation). SAs should also take courses that would improve their communication and presentation skills, since they play such an integral role in the success of the SA position.

SAs can also further their training and knowledge by attaining certifications. After analyzing many security architect job postings, suggested certifications are Cisco Certified Security Professional (CCSP), Checkpoint Certified Security Administrator (CCSA), Expert (CCSE), SANS Global Information Assurance Certification (GIAC), or other major vendor sponsored security certifications.

Expert Experiences

It is also good to keep in mind that "a laundry list of certifications is nice, but practical skills are required to be successful in the role," (Holland, Balaouras, & McKee, 2012). Many employers look for years of experience when considering candidates for the security architect position. The SA should have hands-on experience designing and implementing security solutions and implementing enterprise Security management processes, procedures, and decision supports. Positions like Cisco System's Cloud Services Security Architect and Rent-A-Center's Senior Security Architect require a minimum of 7 years of experience with information security or security related fields, whereas KForce's IT Security Architect position requires 8-10 years of experience. However, CSZNet, Inc's security architect position require at least 15 years of expert

knowledge in the information security field. CSZNet, Inc's security architect role requires at least 15 years of setting IT security standards and providing security policy guidance/publication in large enterprises. Intuit's security architect position requires at least 5 years of experience with security architecting or engineering.

Chapter 9: Closing Thoughts on the Future of Enterprise Security Architecture and the Career of Enterprise Security Architect

Cyber threats and attacks will never stop. It is no longer the matter of *if* an organization will get hacked or attacked, but rather the matter of *when*. According to the Kaspersky survey of Global IT Security Risks 2012, only 59% (less than two-thirds) of respondents feel that they are more or less prepared for cyber threats (*Global IT Security Risks*, 2012). As the number and intensity of these attacks occurring, organizations will realize that enterprise security architecture needs to be implemented or improved, if already implemented. There should be increased spending on security and that doesn't only mean for a security system to be put in place to defend against the attacks. Security budget should include hiring competent security architects to establish an effective architecture. Once senior management increases the budget on security architecture development, more enterprise security architects will be hired. According to the 2013 $(ISC)^2$ Global Information Security Workforce Study, the average age of the security professional today is over 40 years old and only 12% of them are female (Wilson 2013). Hord Tiptop said, "We need efforts in the industry and in the schools to get more young people involved, and more women." Using the career path that this thesis proposes, recruiting teams can look for individuals that exemplify the ultimate enterprise security architect. There will be an increase of women in the security field. With the increasing popularity of this field, educational institutions will need to change their curriculums to incorporate concepts of enterprise architecture as well as enterprise security architecture. Possibly an enterprise architecture major can be established with concentrations of enterprise security architecture. Students can be more prepared to go into these enterprise security architect roles and the years of experience required for job consideration will decrease in job postings. Additionally, with an increase interest in enterprise security

architecture, perhaps more models and frameworks will be developed so that organizations can improve their architectures and feel more prepared for cyber attacks.

References

Ackerman, R. R. (2013, February 1). Cyber attacks: A growing threat to the U.S. economy [Blog post]. Retrieved from Xconomy website: http://www.xconomy.com/san-francisco/2013/02/01/cyber-attacks-a-growing-threat-to-the-u-s-economy/

Ambler, S. W. (n.d.). Agile enterprise architecture. Retrieved March 16, 2013, from http://www.agiledata.org/essays/enterpriseArchitecture.html

Arconati, N. (2002). *One approach to enterprise security architecture* [White paper]. Retrieved March 16, 2013, from http://www.sans.org/reading_room/whitepapers/policyissues/approach-enterprise-security-architecture_504

Byrnes, F. C. (n.d.). Overview: Who is responsible for security architecture? Retrieved from http://www.gartner.com/id=689610

Cameron, B. (2011). *Enterprise alignment* [Web-based Lecture]. Retrieved March 16, 2013, from Introduction to Enterprise Architecture website: https://online.ist.psu.edu/ea/topic1d

Companies worldwide lack awareness of cyber threats. (2012, November 22). Retrieved March 16, 2013, from http://www.kaspersky.com/about/news/virus/2012/Companies_Worldwide_Lack_Awareness_of_Cyber_Threats

Cybersecurity: The new business priority. (n.d.). Retrieved March 16, 2013, from http://www.pwc.com/us/en/view/issue-15/cybersecurity-business-priority.jhtml

Daniel, D. (2007, March 31). The rising importance of the enterprise architect. Retrieved March 16, 2013, from http://www.cio.com/article/101401/The_Rising_Importance_of_the_Enterprise_Architect

DoD EA Career Path Working Group. (2012, March 23). *DoD architects' competency framework guide: New tools for career development and management*. Retrieved March 17, 2013, from http://www.dodenterprisearchitecture.org/program/Documents/eb_DoD_Architecture_Career_Guidance_mar_24_2012_(5)wjo_(5)_(2).docx

Enterprise architecture framework. (n.d.). Retrieved March 16, 2013, from http://en.wikipedia.org/wiki/Enterprise_architecture_framework

Enterprise architecture good practice guide first international open standard in EA. (2009, January). Retrieved March 16, 2013, from http://www.enterprise-architecture.info/EA_Standards.htm

Federation of Enterprise Architecture Professional Organizations. (n.d.). *A common perspective on enterprise architecture* [Microsoft Word].

Fehskens, L. (2010). *The emerging field of enterprise architecture, why it is a critical role, and what EA professionals do for an organization* (Interview by Penn State College of Information Sciences and Technology) [Video file]. Retrieved from https://online.ist.psu.edu/ea/topic1b

Forrester Research, Inc. (2011a, December 14). What roles are in the central EA group? [Chart]. Retrieved from http://www.forrester.com/Rick-Holland#/Job+Description+Security+Architect/fulltext/-/E-RES61549

Forrester Research, Inc. (2011b, December 14). What is the current state of the following parts of the EA program? [Chart]. Retrieved from http://www.forrester.com/Rick-Holland#/Job+Description+Security+Architect/fulltext/-/E-RES61549

Fujitsu enterprise security architecture. (2007, May). Retrieved March 16, 2013, from http://jp.fujitsu.com/solutions/safety/secure/concept/esa/files/ESA5010P.pdf

Global IT security risks: 2012. (2012). Retrieved April 1, 2013, from http://www.kaspersky.com/downloads/pdf/kaspersky_global_it-security-risks-survey_report_eng_final.pdf

Holland, R., Balaouras, S., & McKee, J. (2012, June 1). Job description: Security architect. Retrieved March 16, 2013, from http://www.forrester.com/Job+Description+Security+Architect/fulltext/-/E-RES61549

Kumar, V. (2012). The perusal and review of different aspects of the architecture of information security. *IJCSMS International Journal of Computer Science & Management Studies, 12*. Retrieved from http://www.ijcsms.com/journals/Special%20Issue%20of%20Volume%2012,%20June%202012_Vipin%20Paper%202.pdf

Lankhorst, M. (2009). Introduction to enterprise architecture. Retrieved March 17, 2013, from http://link.springer.com/chapter/10.1007%2F978-3-642-01310-2_1?LI=true

Lapkin, A., Allega, P., Burke, B., Burton, B., Bittler, R. S., Handler, R. A., . . . Gall, N. (2008, August 12). Gartner clarifies the definition of the term 'enterprise architecture'. Retrieved March 16, 2013, from http://www.gartner.com/id=740712

McAfee outlines strategy for future of business security. (2013, January 22). Retrieved April 1, 2013, from http://www.darkreading.com/security-monitoring/167901086/security/security-management/240146709/mcafee-outlines-strategy-for-future-of-business-security.html

Parizo, E. B. B. (2007, June 6). Analysts make the case for enterprise security architectures. Retrieved March 16, 2013, from http://www.computerweekly.com/news/2240080856/Analysts-make-the-case-for-enterprise-security-architectures

Pereira, C. M., & Sousa, P. (2004). A method to define an enterprise architecture using the Zachman Framework. Retrieved March 16, 2013, from http://portal.acm.org/citation.cfm?id=968175

Recent cyber attacks. (n.d.). Retrieved March 16, 2013, from http://www.forbes.com/pictures/mhl45gkeg/sony-2/

Riggins, K. (2013, March 3). Winchester house security: Why enterprise security architecture matters. Retrieved April 1, 2013, from http://www.infosecramblings.com/2013/03/03/winchester-house-security-why-enterprise-security-architecture-matters/

SABSA matrix. (n.d.). Retrieved March 16, 2013, from http://www.sabsa-institute.org/the-sabsa-method/the-sabsa-matrix.aspx

SABSA model. (n.d.). Retrieved March 16, 2013, from http://www.sabsa-institute.org/the-sabsa-method/the-sabsa-model.aspx

SABSA overview. (n.d.). Retrieved March 16, 2013, from http://www.sabsa-institute.org/the-sabsa-method/sabsa-overview.aspx

Scholtz, T. (2011, August 15). Develop the key competencies required by the new security team. Retrieved March 17, 2013, from http://www.gartner.com/id=1767214

Scholtz, T., & Byrnes, F. C. (2010, February 23). Collaborating for effective security architecture. Retrieved March 17, 2013, from http://www.gartner.com/id=1307113

Scholtz, T., & Kreizman, G. (2008, june 5). Architecting security: Different approaches. Retrieved March 17, 2013, from http://www.gartner.com/id=687607

Security architect. (2012, June 1). Retrieved March 17, 2013, from http://www.qgcio.qld.gov.au/qgcio/projectsandservices/ictworkforcecapability/Pages/SecurityArchitect.aspx

Sessions, R. (2007, May). A comparison of the top four enterprise-Architecture methodologies. Retrieved from http://msdn.microsoft.com/en-us/library/bb466232.aspx

Shen, Y.-T., Lin, F., & Rohm, C.E. T., Jr. (2009). A framework for enterprise security architecture and its application in information security incident management. *Communications of the IIMA*, *9*(4).

Sherwood, J., Clark, A., & Lynas, D. (2005). *Enterprise security architecture: A business-driven approach* [Google eBook]. Retrieved from http://books.google.com/books?isbn=157820318X

Szakal, A. (2012, December 28). Security architects or security architecture? Retrieved April 1, 2013, from https://www-304.ibm.com/connections/blogs/government/entry/security_architects_or_security_architecture8?lang=en_us

Tahajod, M., Iranmehr, A., & Darajeh, M. R. (2009). A roadmap to develop enterprise security architecture. *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5402639&isnumber=5402499

Tapadinhas, J. (2012, October 19). How to meet the security challenges of mobile BI. Retrieved March 17, 2013, from http://www.gartner.com/id=2205715

Thorn, A., Christen, T., Gruber, B., Portman, R., & Ruf, L. (2008, September 29). *What is a security architecture?* Retrieved March 17, 2013, from http://www.isss.ch/fileadmin/publ/agsa/Security_Architecture.pdf

Wieringa, R., Van Eck, P., Steghuis, C., & Proper, E. (2009). *Competences of IT architects* (2nd ed.). Retrieved from http://www.scribd.com/doc/22310251/Competences-of-IT-Architects

Wilson, T. (2012a, September 11). Security skills shortage creates opportunities for enterprises, professionals. Retrieved April 1, 2013, from http://www.darkreading.com/identity-and-access-

management/167901114/security/security-management/240007115/security-skills-shortage-creates-opportunities-for-enterprises-professionals.html

Wilson, T. (2012b, October 29). New threats necessitate shift toward security architecture, risk management. Retrieved April 1, 2013, from http://www.darkreading.com/risk-management/167901115/security/security-management/240012456/new-threats-necessitate-shift-toward-security-architecture-risk-management.htm

Wilson, T. (2012c, December 27). Rethinking IT security architecture: Experts question wisdom of current 'layered' cyberdefense strategies. Retrieved April 1, 2013, from http://www.darkreading.com/risk-management/167901115/security/security-management/240145324/rethinking-it-security-architecture-experts-question-wisdom-of-current-layered-cyberdefense-strategies.html

Wilson, T. (2013, February 25). Businesses feel impact of IT security skill shortage, study finds. Retrieved April 1, 2013, from http://www.darkreading.com/cloud-security/167901092/security/security-management/240149286/businesses-feel-impact-of-it-security-skill-shortage-study-finds.html

ACADEMIC VITA

Eileen Chen

27-11 Corporal Kennedy St.

Bayside, NY 11360

Education

B.S., Information Sciences and Technology, May 2013,

Penn State University, University Park, PA

Minor in Supply Chain and Information Sciences and Technology

Honors in Information Sciences and Technology

Honors and Awards

- David Suarez Memorial Scholarship, Deloitte Consulting/Deloitte & Touche, Jul 2011
- Society of Distinguishing Alumni Trustees Scholarship, Penn State University, Aug 2012
- Bunton Waller Scholarship Aug 2012
- Burstin Family Scholarship in IST Aug 2012
- Colfelt Scholarship, Penn State University, Jan 2013
- Deans List, Penn State University, All Semesters

Academic-related Experience

- Research Assistant to Dr. Brian H. Cameron, Executive Director of Center for Enterprise Architecture Initiative (Fall 2011 to Fall 2012)
- Teaching Intern for IST 240: Introduction to Computer Languages (Fall 2011)

Other Activities/Interests

- Penn State Panhellenic/IFC Dance Marathon Hospitality Captain (Fall 2012-Spring 2013)
- Penn State Panhellenic/IFC Dance Marathon Technology Captain (Spring 2011-Spring 2012)

- Bee House, Special Interest THON Orgnization, Administrator (Fall 2009 – Spring 2012)
- Delta Gamma Sorority, Director of Electronic Communication (Spring 2010 – Spring 2011)
- LeaderShape Institute Graduate (Spring 2011)

Employment History

- PwC, Security Consulting Associate Intern (Summer 2012)
- Penn State University Residence Life, Resident Assistant (Spring 2012 – Spring 2013)
- Penn State ITS Lab Consulting, ITS Lab Consultant (Spring 2011 – Fall 2011)