Mixing Technology and Business: The Roles and Responsibilities of the Chief Information Security Officer

Matthew Cho

SANS GSEC Certification
Practical Assignment
Option 1.4 – Research on Topics in Information Security

Summary

Today, information is everywhere and both public and private organizations worldwide have invested large amounts of money implementing information technology in order to address their information needs. While doing so, they have taken a complacent attitude regarding the security of those assets. However, as security has received more attention in the last several years, organizations have realized that they lack a designated an individual with the appropriate authority to carry out the security responsibilities of an organization. With the rise of the Chief Information Security Officer to the executive level, organizations that previously relied on information technology department personnel for security now have an individual dedicated solely to the physical and technical aspects of security for an organization. This research paper describes the roles and responsibilities of the Chief Information Security Officer and the importance of these roles and responsibilities to public and private organizations worldwide. In addition, this paper explains the return on investment and the importance and how it relates to the Chief Information Security Officer.

Information Importance

For today's global economy, optimizing speed and access to information is just one common goal that organizations in both the public and private sector strive to accomplish. Financial companies need to know the latest economic information on Company X to make that billion-dollar transaction, while intelligence agencies depend on top-secret information on Country Y to protect the security of their nation. As a result, it comes as no surprise that within the last decade corporations and governments worldwide have invested heavily in information technology (IT) in order to address their information needs as well as maintain an edge over the competition.

With such a huge focus on implementing the most advantageous IT solution or determining which of the latest and greatest web applications, servers, and databases best suits the mission of an organization, protecting the information held by those assets has always been a second priority. Specifically, minimal concern has been given towards designating a dedicated and qualified individual towards ensuring the complete availability and assured integrity of information. However, within the last several years and mostly during this past year, public and private organizations have grown more conscious of this security management void and have stopped to think about exactly who is responsible for ensuring that the assets which hold their trade secrets, financial data, and/or proprietary information are properly protected.

Information Assurance

A 2002 Global Information Security Survey performed by the Technology and Security Risk Services sector of Ernst and Young found that of the leading organizations surveyed, only forty percent answered that they were confident that they could detect an attack on their IT assets (Ernst & Young). In addition, while seventy-five percent said that they had experienced unexpected unavailability at one time or another, only half responded that they would take the extra step to investigate these incidents. Finally, despite overwhelming evidence that a majority of attacks originate from within, only forty-one percent of those surveyed were concerned about internal attacks on their systems and less than fifty percent had an established information security training and awareness program.

Although these results show that both public and private organizations have made somewhat of an attempt within the past several years at addressing information security within their organization, the results also show that organizations are doing so with very little direction. In particular, issues such as training and incident response, which are management-initiated projects that have an affect on the entire organization, have not been addressed or carried out by a majority of the organizations based on this survey. This only confirms the fact that organizations have completely ignored the management aspect of security and have blindly implemented security solutions with very little delegation of responsibility.

Information Responsibility

As other research sources demonstrate similar results and, at the same time, compromises in security continue to become more significant to an organization’s well being, IT executives and managers are beginning to realize that security responsibilities must be addressed at the management level in order to successfully implement security for any organization. As a result, organizations have taken on an increased strategic executive-level focus on security and have started by ensuring that a capable IT executive dedicated entirely to security is in place. This individual, also known as the Chief Information Security Officer (CISO) bears the full weight of an organization’s security responsibilities and is the first step in the right direction for effective enterprise-wide security.

The Evolution of the CISO

Before there were any CISOs, most organizations relied on only a few professionals in the IT department dedicated to the security of their infrastructure. However, as technology started to replace file cabinets and security no longer consisted of a lock and key, the protection of an organization’s data and resources became an important issue for a wider range of individuals. Not to mention, the events of September 11th and the issuance of the United States Patriotic Act in October 2001, which required that all Federal IT departments employ an individual solely dedicated to IT security, helped push executives to consider security responsibilities for their organization much more seriously.

The armed forces and financial services sector, organizations where a direct and definable impact on the mission could be determined, were the first to actually employ the CISO role (Prencipe). By 2001, a study of 276 financial services, manufacturing, technology, and government organizations discovered that almost half (47%) acknowledged the existence of an employee dedicated to security at their organization (CIO Research Reports). Of that percentage, only a small percent claimed to hold the CISO title, while a majority either continued to share security responsibilities with other IT staff members or the Chief Information Officer (CIO) carried out security responsibilities based on his/her job description. Despite the small percentage, the study indicated that the role of the CISO, was beginning to take hold.

CISO Roles and Responsibilities

According to the latest information, almost sixty percent of the organizations in the United States acknowledge the existence of a CISO dedicated entirely to security (Ware). Responsibilities for these individuals include ensuring proper protection for all physical and technical aspects of the organization. Technical aspects ranging from securing communications, applications, and business systems to performing risk assessments of IT assets exposed to outsiders on the Internet. Physical aspects including non-electronic factors such as physical site access as well as drafting policies and procedures for secure daily operations. Along with overseeing the organization's physical and technical security implementation, CISOs are also responsible for security management activities. These activities may include training others for security awareness, purchasing security products, planning for and managing disaster recovery, developing secure business and communication practices, and ensuring all policies are followed. In addition, CISOs must ensure that security breaches are not a result from any of the changes made in order to protect the organization.

The following highlights some important responsibilities carried out by most CISOs.

- Act as the organization's representative with respect to inquiries from customers, partners, and the general public regarding the organization's security strategy.
- Act as the organization's representative when dealing with law enforcement agencies while pursuing the sources of network attacks and information theft by employees.
- Balance security needs with the organization's strategic business plan, identify risk factors, and determine solutions to both.
- Develop security polices and procedures that provide adequate business application protection without interfering with core business requirements.
- Plan and test responses to security breaches, including the possibility for discussion of the event with customers, partners, or the general public.
- Oversee the selection testing, deployment, and maintenance of security hardware and software products as well as outsourced arrangements.

- Oversee a staff of employees responsible for organization's security, ranging from network technicians managing firewall devices to security guards (Robert Francis Group).

CISO Characteristics

In order to carry out these responsibilities, the CISO must have excellent interpersonal and written communications skills, solid knowledge of electronic and site security issues, and a firm understanding of the organization's business requirements. The CISO must also be able to stay abreast of any new developments in the rapidly changing security environment to avoid serious and/or costly mistakes as well as focus and determine on what actions could and should be carried out for an organization's infrastructure at a given time. In addition, while selling the project, the CISO's leadership abilities and communication skills will come into play to strike a balance between business and security requirements and persuade executives to approve any necessary security projects (Robert Francis Group).

The CISO Need

Based on these responsibilities, a CISO's overall responsibility can seem overwhelming, but it is the exact reason why a dedicated individual is necessary. Establishing a CISO position is an important strategic move that sends a message to customers and partners saying that the organization cares deeply about security, especially if the organization is large and diverse or has been the victim of publicly visible security failures. Other security-sensitive industries that benefit from the employment of a CISO are financial, government, medical, and pharmaceutical organizations. However, there are some organizations that do not need a CISO. These are usually smaller organizations that can delegate responsibilities and adequately address security within their organizational structure. This is perfectly fine as long as the responsibilities are delegated within executive-level management. In other cases, although an organization may need a CISO, they may not have a budget for one. In 2002, the average salary for a CISO was $105,000 (Ware). For organizations that can afford a CISO, the cost is minimal relative to the protection and effective security implementation provided to an organization.

For organizations that are considering hiring a CISO, one major reason for justifying the need is based on the current situation with existing IT management. In comparison, there are many more security related issues that CISOs can accomplish compared to an IT security manager. This is mainly due to the fact that most IT managers are not solely responsible or dedicated to security. Based on job descriptions, IT managers may only be responsible for a piece of security or may juggle many other non-security related tasks in addition to security. On the other hand, the CISO's sole responsibility is security. Therefore, a CISO can concentrate and totally dedicate all efforts to the security of an organization, while security might not even be an IT manager's first priority.

Another reason for justifying the need for a CISO, as well as another difference between CISOs and IT managers, is the fact that the CISO's responsibilities are addressed at the executive level (Robert Francis Group). This difference is particularly important, especially as security is increasingly considered from a more strategic standpoint. Depending on the size of an organization and the perceived importance of security, the CISO usually reports to the CIO or, less frequently, reports directly to the Chief Executive Officer (CEO). Another figure states that almost forty percent of security heads report directly to the CEO, Chief Operations Officer (COO), Chief Financial Officer (CFO), or other officer, while almost a quarter report to the CIO or a top IT executive (Ware).

By having a say at the executive level, CISOs play a role in both the business and technical aspects of security and have more control and influence over the budget and staffing decisions. Essentially, CISOs are needed to play the role of an IT security manager as well as a CEO. Very rarely do IT managers have a say in these types of decisions, which is one reason why they have failed to effectively implement security in line with an organization's mission. Without executive level control, IT security managers face difficulty when bridging the gap between business process demands and security requirements and are powerless with respect to effecting change in the organization's strategic plans.

Managing Security

Once a CISO is in place, the actual job of managing security for an organization requires a great deal of effort and a lot of hard decisions. Security decisions are usually driven by either government/industry regulations or risk management findings (Ware). For government and industry regulations, there is no decision when it comes down to it. A CISO is simply required to invest in security if the organization is not protected according to the standards within an industry or regulations set forth by the government. On the other hand, risk management is where more managerial freedom comes into play. Here, the CISO must ensure that all security risks are appropriately addressed and managed by performing a risk assessment to determine what areas are the most at risk. Based on the findings, CISOs can plan and determine projects to target certain at-risk areas. However, determining which project to implement can be a difficult part of risk management since addressing risk can be handled in numerous ways, such as policy and procedure development, implementation of protective measures, or auditing.

Statistics currently show that existing employees pose the biggest threat to an organization's technology infrastructure. In addition, the need for adequate backup plans and procedures were one of the lessons learned from the attacks on September 11th. Based on this, the top priorities for CISOs in 2003 should include security projects that mitigate the risk posed by exiting employees and unexpected disasters. Projects that address these two issues include employee training and education, security policy enforcement, and/or business continuity and disaster recovery development. In the previous year, CISOs were mainly concerned with electronic attacks such as viruses and unauthorized access, which is evident based on the spending priorities for 2001. Most of the money was spent on security software, services, and hardware (CIO Research Reports).

The Cost of Security

Speaking of money, the CISO must also consider the cost of security when making decisions. The cost for security varies from organization to organization and can be impacted by the size, type, and nature of the business. Obviously, in low-threat environments, security spending is lower. In high threat environments such as financial and military institutions, security spending is higher. For example, in an e-business organization, the need for network security is much higher due to the probability and potential impact of malicious attacks. (Cisco) Therefore, a typical network security implementation consisting of antivirus and firewall products for small quantities of desktops, file servers, and application servers can range anywhere from $100 to $300 per machine. For a larger network, a broader mix of products is required, including technology to identify individuals, manage perimeter security, enable secure connectivity, and manage security policy. Cost for network security products range from $25 per node in small organizations from up to about $85 per node for larger organizations. (Cisco)

The Security Budget

Obviously, the CISO cannot afford to implement every single security initiative to address its security needs, but can pick and choose what projects to implement based on how much IT departments can spend, also known as the security budget. The security budget, which is used to finance all security projects, is determined by the CFO and is based on input from the CIO. The economy also has a direct effect in determining the security budget for an organization. During robust times, CISOs operate under generous budgets and focus on major long-term “big-bang” projects. However, statistics show that these projects usually have high rates of failure and ended up not meeting expectations. During times of recession, security budgets are generally tighter and put CISOs under increased pressure to cut costs and focus on more short-term revenue-enhancing projects (Computerworld). According to one source, organizations will allocate almost 10.3% of their total IT budget to information security in the coming year, up from 9.5% reported in 2002 (Ware). Based on these figures, estimates for 2003 figure that more than one third of companies will have an annual security budget of more than $1 million while almost half will have a security budget between $101,000 and $1 million. The remaining organizations will have a security budget of less than $100,000 (Ware).

The CISO Challenge

Although it seems as if the CISO can simply determine what projects to implement based on the risk findings, calculate the cost of each one, and go ahead one by one until the security budget is all spent, in reality, the decision is not that simple. In fact, the CISO may do a stand-up job of assessing an organization’s risk, but without implementing appropriate security projects that mitigate the risk as well as fit the organization’s business goals, the effort is useless. The CISO must demonstrate his/her ability to perform the security-balancing act of juggling the security needs of the organization with the security budget. Not only must the CISO determine what projects to implement, but he/she must also take the security budget into consideration to see if a security project is worthwhile. One way of justifying a project is by demonstrating that if it is implemented, the result will be fewer security breaches, reduced financial loss, and/or increased customer satisfaction for the organization (Ware). For most public and private organizations today, the method used to determine which projects are worthwhile is by showing a return on the money spent. Most organizations use a traditional method known as return on investment, or ROI. For the CISO, this is the determining factor for what projects will or won’t be approved by the CIO or CFO.

Return On Investment (ROI)

ROI is defined as the measure of return, usually profit or cost saving, that an organization is able to earn for a given use of money. ROI may be used as a way to grade how well an organization is managed. However, in most cases, ROI is used to develop a strong business case for executives as to why a given project or proposal should be accepted of not. A project’s value is determined by the relationship between what the organization will pay (costs) and what it will get back (benefits). The larger the amount of benefit is in relation to cost, the greater the value of the project. Most organizations use one or more financial metrics, which they refer to individually or collectively as ROI. These metrics include:

- Payback Period. The amount of time required for the benefits to pay back the cost of the project.
- Net Present Value (NPV). The value of future benefits restated in terms of today’s money.
- Internal Rate of Return (IRR). The benefits restated as an interest rate.

ROI and the CISO

In terms of security, the same definition of ROI applies, but the calculations are a much more complicated. What makes a security ROI calculation difficult is, not only must CISOs consider and calculate the financial benefits, but they must also consider the non-financial benefits of security investments. When executives discuss the ROI of a security project, they are thinking of the financial benefits such as impacts on the organization's budget and finances such as cost reductions or revenue increases. For example, costs such as replacing servers or paying overtime for a security breach are easy to track. However, the difficulty for CISOs lies within calculating the non-financial benefits of security projects such as an improved image, the loss of customer trust, prevented security breaches, impacts on operations, mission performance, or customer satisfaction. These gray areas, referred to as “intangibles” or “soft” returns, are usually the most significant in terms of cost, but are the hardest to prove (Kaplan).

Unlike financial returns, there are no widely accepted metrics that can be applied in calculating “soft” ROI. Besides, most CISOs aren’t sure what to measure or don’t even know how to measure. According to the 2002 computer crime and security survey from the Computer Security Institute and the FBI, eighty percent of the 503 security practitioners surveyed acknowledged financial losses due to security breaches, but only forty-four percent were willing or able to quantify losses (Kaplan). Another study showed that while a majority of survey respondents reported incidents (defined as security breaches or crimes including viruses and hoaxes that resulted in damage or loss) in the past 12 months, fewer than half (38%) of the IT professionals surveyed could quantify the damages. The ability to show actual figures for a security breach is an extremely important as CISOs vie for security budgets and as companies more frequently negotiate insurance policies for cybercrime. (CIO Research Reports) In some cases, some skeptical CFOs dismiss some security projects because these “soft” returns cannot be quantified. Therefore, “soft” returns are more effectively used as an added benefit on top of ROSI when selling executives.

Before, IT departments and personnel performed very little measurement of the actual ROI of a security project. One of the reasons was because of the level of effort required to develop a comprehensive IT security ROI. However, statistics show that organizations that do perform some sort of ROI calculation for security investments do get more return on their investment via reduced security breaches and increased concordance among CEOs and other officers on the need for security investments. (CIO Research Reports) As a result, organizations are starting to take a stab and calculate a return on a security project, based primarily on the cost of security, the cost of breach, and the probability it will happen (Scalet). For CISOs that absolutely require a comprehensive ROI calculation, there are several commercial methods being tested.

Selling the Project

Although some security projects have an obvious benefit to the organization, there are still some that require approval and a positive ROI can build a stronger case. For those projects, once some sort of positive ROI can be determined, the CISO can approach the executive level with a recommendation on what projects will address the risk of the organization. Here, the CISO should learn what executives are looking for in terms of return and know how the executives want the ROI positioned, either in cash savings, productivity gains, or increases in security. In some cases, an interactive ROI where variables can be changed can help sell a project.

Conclusion

With the rise in security awareness, public and private organizations have turned to the CISO to solve their security issues. Equipped with the technical expertise to implement the necessary security solutions as well as the management authority and business knowledge to make sure those decisions match the mission of the organization, the CISO is necessary for the effective implementation of security for any organization. The CISO's main responsibilities include securing the physical and technical aspects of an organization by managing security, taking in the cost of security, and relating it to the security budget. In doing so, the CISO carefully considers the security requirements of an organization as well as the business requirements in order to address any security risks as well as satisfy the organization's business goals. With the use of ROI, the CISO can further relate the business and technical aspects of security, and convince executives that security is not only necessary, but that it does pay to invest in security.

References

Berinato, S. (2001). Finally a Real Return On Security Spending. *CIO Magazine.* http://www.cio.com/archive/021502/security_content.html

Berinato, S. (December 2002). Calculated Risk. *CSO Magazine.* http://www.csoonline.com/read/120902/calculate.html

Briney, A. (2002). Dollars and Sense. http://www.infosecuritymag.com/2003/mar/cisoroundtable.shtml

CIO Research Reports. (September 2002). Security Spending: How Much Is Enough?. *CIO Magazine.* http://www.csoonline.com/csoresearch/report6.html

Cisco White Paper. The Return on Investment for Network Security. http://www.cisco.com/warp/public/cc/so/neso/sqso/roi4_wp.htm

Computerworld. (March 2001). Prepare for hard times ahead. http://www.itworld.com/Tech/2401/CWSTO58254/pfindex.html

Conrath, C. (September 2002). Taking Stock A Year Later. http://www.itworld.com/Tech/2987/020903takingstock/pfindex.html

Cummings, E. (December 2002). The Art of Uncertainty. *CIO Magazine.* http://www.csoonline.com/read/120902/viewpoint.html

Ernst and Young. Global Information Security Survey 2002.

Heinzl, A. Information Management: Providing Leadership: The CIO. http://www.bwl.uni-mannheim.de/Heinzl/de/downloads/05%20cio2x1.pdf

Kaplan, S. (December 2002). Its Not Easy Being Breached. *CIO Magazine.* http://www.csoonline.com/read/120902/cost.html

Perkowski, M. (August 2001). Security. http://www.cioinsight.com/article2/0,3959,24699,00.asp

Prencipe, L. (October 2001). C-level Security. http://archive.infoworld.com/articles/pe/xml/01/10/22/011022peciso.xml

Robert Francis Group. The Role of the Chief Security Officer. *CIO Magazine.* http://www.csoonline.com/analyst/report903.html

Scalet, S. (December 2002). Risk: A Whole New Game. *CIO Magazine.* http://www.csoonline.com/read/120902/intro.html

Slater, D. (December 2002). Inside the Sausage Factory. *CIO Magazine.* http://www.csoonline.com/read/120902/factory.html

Ware, L. The Evolution of the Chief Security Officer. *CIO Magazine.* http://www.csoonline.com/csoresearch/report35.html

Ware, L. CSOs Prioritize Spending for 2003. *CIO Magazine.* www.csoonline.com