MEETING EXCEPTIONAL SECURITY CHALLENGES

Focus on IT Spending and the Right Hires

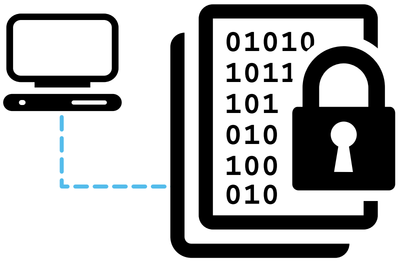
MODIS

PROTECTING YOUR DATA IS A PRIORITY AND A CHALLENGE

In the wake of the recent Sony data breach, customer and company privacy issues have become a hot topic in the media and the tech sector. The Sony incident and other widely covered consumer-facing data breaches experienced by Target, Home Depot, JPMorgan Chase and others have had a significant financial impact on these companies.

Experts are projecting that both the number of incidents and the cost of dealing with data breaches will increase in 2015. To combat these attacks, businesses must respond with a heightened awareness of cybersecurity as well as increased spending on enterprise security as needed. Designating high-level executives to lead security and hiring certified security experts are among the best practices for stronger IT security in 2015 and beyond.

TABLE OF CONTENTS



MODIS

December 2013: Target kicked off a wave of major data breaches with the announcement that data from as many as 70 million consumer credit cards had been stolen during the holiday shopping season.[i]

Estimated cost: $148 million, with an increase of 9.3 percent in mean cost over last year. [ii]

April 2014: The widespread Heartbleed security bug left more than 10,000 of the most visited websites vulnerable, exposed millions of personal passwords and data, and resulted in the theft of 4.5 million records from one of the country's largest hospital networks.

Estimated Cost: Unknown, but millions of companies and individuals were affected.

HIGH-PROFILE HACKS

Throughout 2014, news of cyberattacks of all kinds and their rising costs topped the headlines. A quick review of the most high-profile hacks:

September 2014: After detecting a data breach on September 2, Home Depot announced that 56 million consumer credit cards and 53 million email addresses since April 2014 might have been compromised.

Estimated Cost: $43 million in Q3 2014 alone.

July 2014: An attack on JPMorgan Chase & Co. netted information from 76 million customers and 7 million small businesses. [iii] While use of the information has yet to be discovered, some security experts reasoned it was one step in a larger planned attack. [iv]

Estimated Cost: Unknown at this time.

November 2014: The massive Sony Pictures Entertainment hack released personal and confidential information including addresses, salaries and emails of Sony employees, freelancers and celebrities. The breach has also resulted in diplomatic issues for the United States government.

Estimated Cost: Expected to exceed $1 billion.[v]

December 2014: Staples, Inc. disclosed that as many as 1.16 million credit card numbers had been stolen from 119 stores, in a hack running from July through September of that year.

Estimated Cost: Unknown at this time.
Furthermore, Albertsons Stores, Neiman Marcus, Michaels, PF Chang's and Goodwill were among other companies that experienced theft of company and/or consumer data last year.

Because of these highly publicized data thefts covered in the media, hacking has intruded into public consciousness. Gallup found that Americans were more worried about having their credit card information stolen than they were about being raped, murdered or mugged. [Vi]

According to a study recently completed by Ipsos MediaCT, 62 percent of Americans say they're concerned about who "owns" their data or files stored in the cloud, compared to 53 percent just three years ago.

Those fears are not unfounded: According to SafeNet's Breach Level Index for the third quarter of 2014, there were 320 reported data breaches between July and September – 46 percent of which involved identity theft. [Vii]

THE HIGH COST OF HACKS

Cyberattacks cost American companies time and plenty of money. The Ponemon Institute's 2014 Global Report on the Cost of Cyber Crime found that the average cost of cybercrime among the large U.S. companies participating in its survey was $12.7 million–the highest of any country in the survey. [Viii]

It's important to note that, while retailers and consumer-facing companies received the most media attention, cybercrime affects virtually every industry. In fact, according to Ponemon, retail and healthcare are far down the list of 14 sectors incurring the costs of data theft. The energy sector bore the highest average annualized cost of cybercrime, at $26.5 million; defense was nicked for $21.9 million; third on the list, the financial services sector bled $20.8 million on average.

Retail, by contrast, was eighth on the list of 14, spending an average of $8.6 million to recover from cybertheft; consumer products, twelfth on the list, spent $6.8 million to make good; and healthcare, at thirteenth, bled $6 million. It's also worth noting that the costs to the retail sector more than doubled over 2013.

DAMAGES FROM BREACHES

Increased IT spending is just one financial expense incurred due to a data breach. Companies may also be subjected to additional costs such as providing credit monitoring services to affected customers and legal expenses arising from class action lawsuits and paying settlements. Soft costs in the form of bad publicity and loss of trust are also a factor.

Expenses to repair and make good to customers: While Home Depot sales did not seem to be impacted, the company reported in its quarterly filing to the Securities and Exchange Commission that other expenses related to the data breach totaled $28 million so far–including costs associated with providing Experian's ProtectMyID service to affected customers. Target provided a similar service to their customers but did not break out this cost in its SEC quarterly filing.

Loss of consumer trust: Target's fourth-quarter 2013 sales, during the crucial holiday shopping season, were down a staggering 46 percent. It took an entire quarter before Target's sales began to trend upward again, despite purchasing credit monitoring services for all affected customers.

Long-term network damage: Some files residing on the network may be damaged or compromised, resulting in temporary or permanent loss of information. Individual nodes on the network that are damaged can result in reduced connectivity and lower performance until they are restored.

Business interruption: According to The Ponemon Institute, the costs associated with business interruption and lost productivity account for 38 percent of all external costs of a data breach. That figure has increased 7 percent over the past five years. Sony's corporate network was completely shut down for five days following the breach. Soft costs can include severance packages for executives who step down and costs associated with hiring their replacements. Both Target's CEO and CIO stepped down after taking responsibility for the breach.

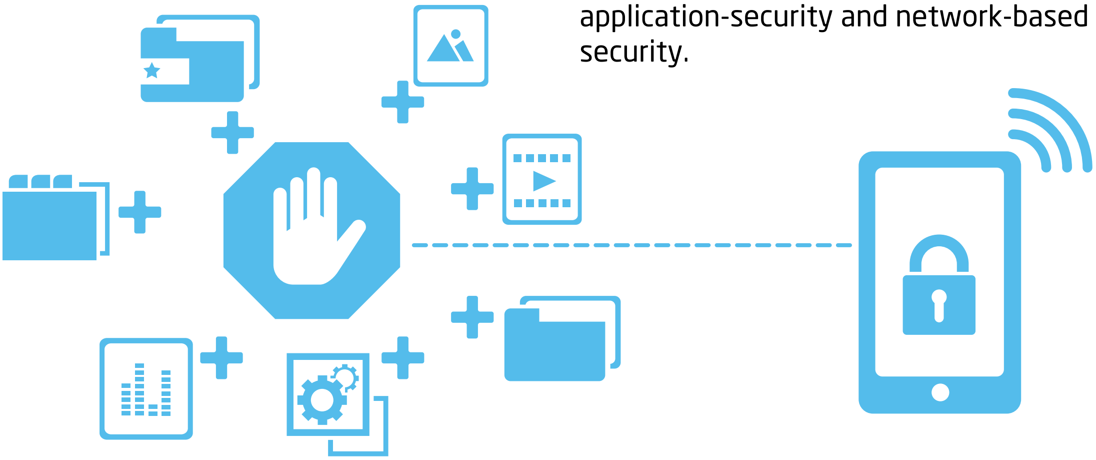
SECURITY GOES MOBILE

New threats are arising with the increase of mobile usage and cloud-based services. The release of celebrity photos stored on Apple's iCloud was the result of a phishing scheme, thus revealing the treasure trove of data available to thieves. There has also been a large increase in mobile transactions: Close to 60 percent of all Amazon purchases were via mobile devices, while mobile commerce accounted for almost a quarter of online shopping on December 2 to 14, 2014. [ix] Mobile shopping could potentially expose more consumer data and put online retailers at greater risk as expansion continues.

Mobile device makers are also implementing near-field communications, or NFC, allowing for the automatic transfer of data –including payments–by tapping one device against another. But the NFC protocol is not inherently secure. NFC transactions must be secured at the application layer–leaving them vulnerable to sloppy coding. As a result, NFC payment readers can be hacked in the same way that Home Depot's and Target's POS machines were.

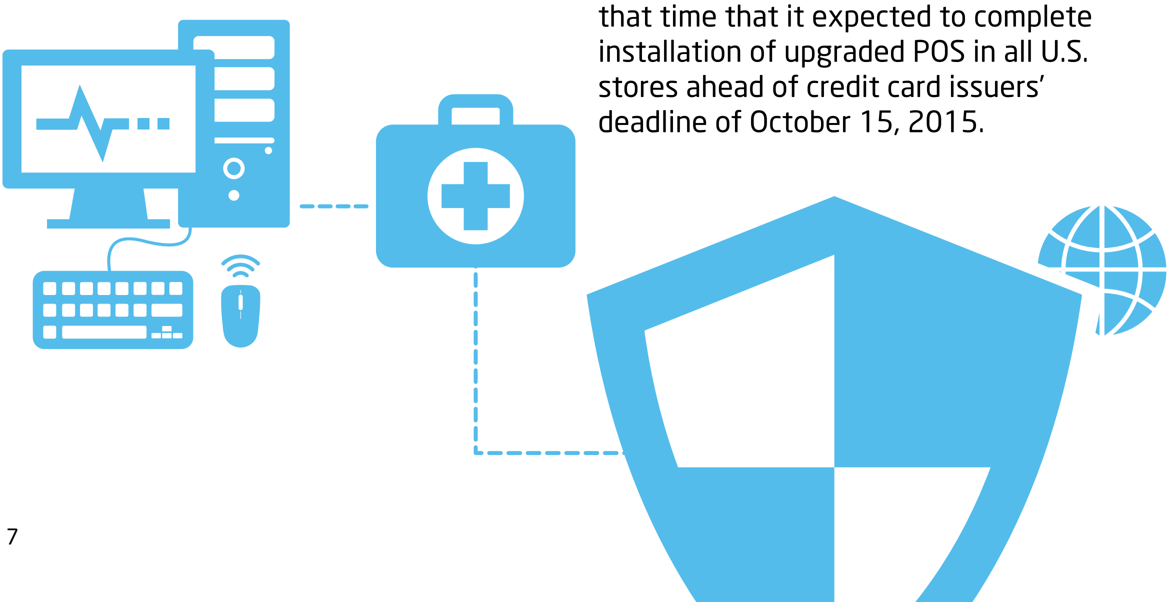
The BYOD trend–business employees using personal devices and applications for work–has also increased exposure to risk. Consumer devices and applications may be less secure than those designed for enterprises. And, as the iCloud hack shows, employees may not exercise the same level of care when using consumer services on their devices, even when they are used for business.

Because of these trends, the practice of security is changing. More security applications have moved to the cloud, driven by BYOD and by the rise in cloud-based enterprise applications and services. In some cases, companies are merging endpoint application-security and network-based security.



HOW BUSINESSES COPE WITH A BREACH

The way a company responds to a data breach seems to be as much a factor of culture as of the technology. Some companies don't reveal the break-in until months later while others seek to minimize the appearance of damage with an immediate response. Security experts agree that the best way for a business to respond is to inform customers as soon as possible, promise to make good on any damages suffered by customers and take responsibility at the highest level of the company. Home Depot has been among the most proactive and transparent in its response. Still, the company faces at least 24 lawsuits, it said in its most recent SEC filing.



Following the September breach of 56 million consumer credit cards and email addresses, Home Depot deployed the following actions:

- Removed affected point-of-sale equipment
- Implemented enhanced encryption of payment data in all U.S. stores
- Sped up the rollout of EMV chip-and-PIN technology that enables POS systems to read encrypted chips on credit cards or mobile phones [x]
- Released a FAQ for consumers
- Offered free identity protection services, including credit monitoring to any customer who used a payment card at a Home Depot store in 2014, from April on
- Provided a team of fraud resolution inspectors to help consumers through September 15, 2015

Impressively, Home Depot accomplished all of this, except for the rollout of new POS systems with EMV technology, by November 4, 2014. The company said at that time that it expected to complete installation of upgraded POS in all U.S. stores ahead of credit card issuers' deadline of October 15, 2015.

ACTION STEPS ALL COMPANIES SHOULD TAKE

Based on the results and takeaways of the aforementioned breaches, there are eight critical steps a company can take to secure operations in this era of heightened threats:

1. Obtain buy-in from key leadership and C-level executives:
When security measures are seen as a hindrance by top executives, they're more likely to be flouted or worked around by the rank and file. On the other hand, when executives prioritize security and take leadership on security initiatives, it creates a culture of security for the entire organization.

2. Create a security governance infrastructure and security management plan:
The Ponemon Institute found that when companies invested in security, appointed high-level security leaders and employed certified and expert staff, overall cybercrime costs were lower. On average, the cost savings of a security management plan was estimated at $1.7 million. Effective plans should include designated incident managers, a defined incident response, updated disaster-recovery plans and a security roadmap. Key security metrics should also be determined and measured regularly.

3. Install security intelligence systems:
Security intelligence analyzes corporate data and network activity in real time in order to identify emerging threats.[xi] Ponemon said its findings suggested that companies using security intelligence technologies were more efficient in detecting and containing cyberattacks. As a result, these companies enjoyed an average cost savings of $5.3 million when compared to companies not deploying security intelligence technologies.

4. Implement an email retention policy:

As the Sony hack demonstrated, a wealth of corporate data may be shared rather indiscriminately via email. Having a defined email retention policy backed up by software applications that automatically alert IT staff and business employees when email content is due to be deleted not only reduces the likelihood of corporate information being stolen, it also demonstrates compliance with Sarbanes-Oxley Section 404 and other information governance standards.

5. Secure brought-in devices:

Cisco's 2012 IBSG Horizons Study of 600 businesses found that 95 percent allow their employees use personal devices for work, and 85 percent of those businesses also provided technical support. Security strategies should prohibit storing passwords used to access the company network on the device itself, require partitioning between corporate and personal applications and data, provide for remote wiping and have a corporate app store of approved mobile applications.[xii]

6. Develop training programs for employee security awareness:

Annual, company-wide training sessions are less effective than more frequent micro training sessions combined with on-going testing, according to Info-Tech Research Group.[xiii] These trainings should include how to recognize phishing and other social engineering attacks, password best practices and general awareness of enterprise security issues.

7. Make security and privacy essential components of new technology adoption:

The technology startup ethos of "release early and often" may be at odds with the security needs of businesses. New technologies should be carefully tested and evaluated with regard to security by specialists within the company.

8. Update POS:

Retailers should plan to move to EMV/chip-and-pin technology point-of-sale systems ahead of the October 15, 2015, deadline set by Visa and MasterCard. With more than 1 billion chip cards already used around the world, the additional level of authenticity provided by the microchip is extra protection for both consumers and retailers.

THE GROWING NEED FOR IT SECURITY EXPERTS

The growing threat of data breaches means that it's more important than ever for companies to hire IT staff with security expertise. Moreover, new skill sets are emerging and evolving in response to the changing security environment.

When the Cloud Security Alliance polled 40 experts in cloud security, it found a vast need for privacy and data-protection principles in the development of cloud, Internet of Things and big data solutions. Security ranked seventh on a list of organizations' most significant IT investments for 2014, according to the Society for Information Management's IT Trends Study.[xiv]

Budgets for data security are also rising. YL Ventures, a start-up investment firm with a security focus, believes these publicized events comprise only a small part of the overall exposure to losses emanating from cyber incidents. YL estimates that in 2014, business lost hundreds of billions of dollars due to cybercrime. The venture firm has also seen many companies dramatically increase their cybersecurity budgets for 2015, and it expects that these allocations will continue to trend upward in coming years.

Relevant Regulations and Standards

Here are some of the commonly used standards and rules for security of corporate and personal data:

ISO/IEC 2700 - 2706: Cover the design, implementation and measurement of information security management systems

FISMA: The Federal Information Security Management Act of 2002 applies to federal agencies

NIST: The National Institute of Standards and Technology special publication 800 series was originally written for federal agencies; it provides advice on security best practices that also applies to businesses.

HIPAA: The Health Information Portability and Accountability Act's Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used or maintained by healthcare providers, insurers and other entities.

Sarbanes-Oxley Section 404: This act created new standards for corporate accountability. Section 404 addresses the management and evaluation of the internal security controls of public and private companies.

PCI DSS: The Payment Card Industry Data Security Standard is a proprietary information security standard created to reduce the risk of fraud for companies that work with the major credit card brands.

THE HIRING OUTLOOK

According to the U.S. Bureau of Labor Statistics Occupational Outlook Handbook, the projected job growth for information security analysts of all kinds through 2022 is 37 percent – much faster than average. Moreover, Computerworld's 2015 Forecast survey found that 28 percent of respondents are planning to hire for security in the next 12 months.

As businesses evolve to meet new security challenges, several jobs and skill sets have increased in demand:

Data Security Analyst

Data Security Analysts are largely responsible for being a first line of defense in protecting systems from security breaches. Not only do they install and maintain security software, these analysts also monitor network activity to identify and resolve any security violations or potential threats that may arise.

This position requires individuals with strong research and communication skills as well as the ability to multitask and a thorough understanding of IT hardware, software and information security issues. The SSCP or CISSP information security certifications are often required for Data Security Analyst.

Systems/Application Security Analyst

The primary objective for Systems/Applications Security Analysts is identifying weaknesses that may leave current systems vulnerable to cyberattack. By evaluating what is in place and suggesting security enhancements based on those findings, these analysts are valuable asset to any data security department.

Effective Systems/Applications Security Analysts have an innate interest in staying up-to-date on hacking trends, security certifications such as SSCP or CISSP and an extensive knowledge of IT hardware, software and information security issues.

HIPAA Security Analyst

Specific to the Health IT sector, the HIPAA Security Analyst has an emphasis on complying with Federal HIPAA regulations. Similar to Data Security Analysts, HIPAA Security Analysts also install and maintain security software, monitor network activity and resolve any security violations that may put an organization at risk for a HIPAA violation.

Substantial knowledge of HIPAA laws, standards and best practices as well as Certified Security Compliance Specialist (CSCS) certification are vital for HIPAA Security Analysts. Additionally, the ability to work cross-functionally to design and implement security initiatives is necessary.

Security Administrator

One of the broadest security verticals, Security Administrators are responsible for addressing an array of security concerns. From implementing network security policies to monitoring network usage, this key position protects the network from unauthorized access and resolves access issues.

An effective Systems Administrator has in-depth technical knowledge of Intrusion Detection Systems, encryption, SSL, VPN, IPSec, TCP/IP, DNS and web security architecture. Strong communication, analytical and organization skills are also necessary in this position.

Data Security Manager

Data Security Managers oversee security systems to protect data from unauthorized access and perform assessments on security risks. They're responsible for creating and implementing policies and procedures for identifying, recording and addressing security violations.

Due to the nature of the position, the ability to manager others and significant ingenuity is required. Data Security Analysts are often promoted to this position, as extensive experience is necessary.

IS Security Manager

The IS Security Manager is responsible for developing and overseeing the information systems security within an organization. This position also manages IT security analysts to ensure that all applications are functional and secure.

This individual leverages creativity and latitude and maintains an extensive knowledge of IT security best practices and procedures. Strong communication and management skills are also required.

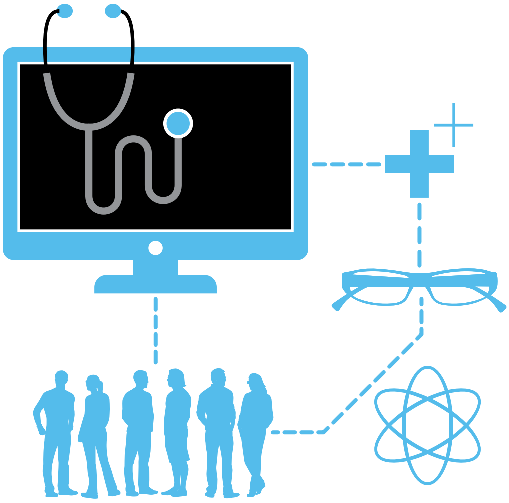
WHAT IS THE VALUE OF THESE IN-DEMAND SKILL SETS?

Download our 2015 Salary Guide for Tech Professionals to find out.
modis.com/salaryguide

HOW IT EXPERTS CAN LEVEL UP SKILL SETS?

At Modis, we've found that employers should look beyond current IT experience when considering new candidates or internal promotions. For example, an interest in technology and a proven track record of personal projects can be more indicative of potential than educational background and years of on-the-job experience for entry-level positions.

Interpersonal skills are also important even among IT security staff. Identifying candidates who are a good cultural fit with a willingness to learn and take criticism well is an important step towards avoiding a costly bad hire. In the high-stress, high-stakes field of IT security, another crucial hiring strategy is to seek out candidates with a positive attitude will help them rise to challenges without burning out.



Security Certifications

Certified Information Security Manager (CISM) was introduced by the Information Systems Audit and Control Association for enterprise security professionals with at least five years experience.

Certified Security Compliance Specialist (CSCS) includes training on HIPAA, FISMA, Sarbanes-Oxley Section 404, ISO 27002 and PCI DSS.

Certified Information Systems Security Professional (CISSP) is offered by the International Information Systems Security Certification Consortium for enterprise security professionals with at least five years experience in at least two security domains.

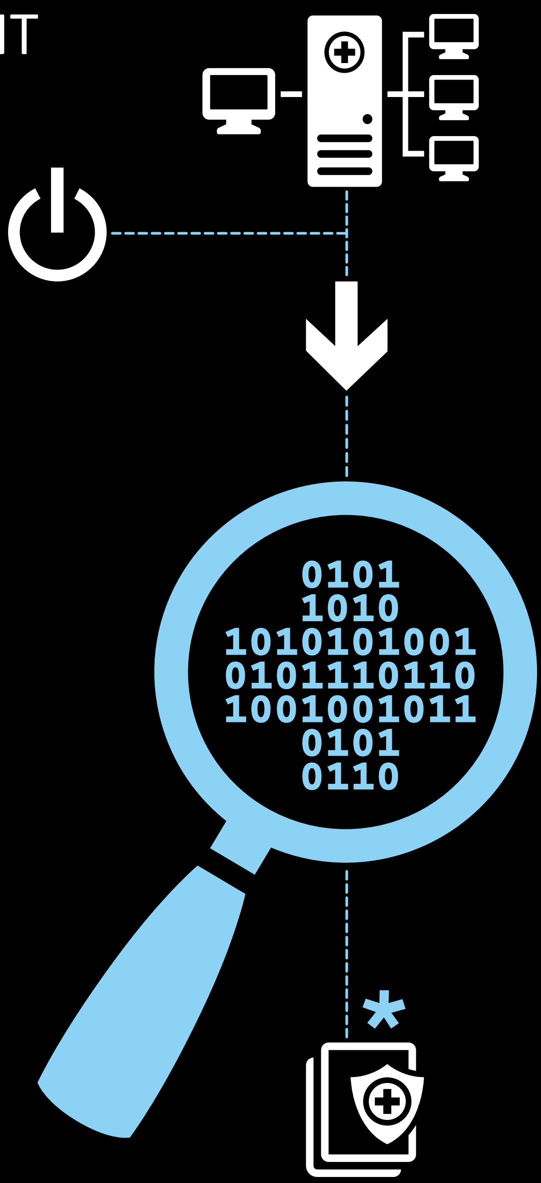
Certified HIPAA Security Professional (CHSP) is specific to HIPAA privacy and security rules

GIAC Security Essentials is the SANS Institute's entry-level certification is awarded after passing a written test.

CompTIA Security+ is a credential requiring at least two years of security experience and passing a written test.

Computer Hacking Forensic Investigator (CHFI) includes certification following training by EC-Council for IT personnel in how to investigate cybercrime, how to recover deleted files or partitions and how to gather the necessary evidence to prosecute.[xv]

PARTNER TODAY TO PREVENT TOMORROW'S THREATS



Not only do advances in technology lead to changes in behavior among consumers and employees, they also lead to new kinds of threats. To meet these challenges, businesses should regularly evaluate and update their security strategies and practices.

At Modis, we can be your partner in identifying skill gaps among current IT staff and hiring experienced, exceptional IT talent to fill these valuable roles to make your IT strategy a reality. To learn more or get detailed information about salary ranges, job descriptions and market demand, please contact your local Modis representative today.

[i] https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ#q5888

[ii] http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html?_r=0

[iii] http://secfilings.nasdaq.com/filingFrameset.asp?FileName=0001193125%2D14%2D362173%2Etxt&FilePath=%5C2014%5C10%5C02%5C&CoName=JPMORGAN+CHASE+%26+CO&FormType=8%2DK&RcvdDate=10%2F2%2F2014&pdf=

[iv] http://www.usatoday.com/story/tech/2014/10/02/jp-morgan-security-breach/16590689/

[v] http://www.sileo.com/sony-data-breach-grows-by-25-million-1-billion-price-tag/

[vi] http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx

[vii] http://data-protection.safenet-inc.com/2014/11/infographic-data-breaches-by-the-numbers-q3-2014/#sthash.utrTSxMe.dpbs

[viii] 2014 Global Report on the Cost of Cyber Crime. http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/

[ix] http://blog.custora.com/2014/12/holiday-shopping-is-heating-up-online-orders-up-16-5-over-2013/

[x] Ibid.

[xi] http://securityintelligence.com/defining-security-intelligence/#.VKr62_Z0xjo

[xii] http://www.apperian.com/wp-content/uploads/downloads/2012/04/Protecting-Corporate-Data-in-the-BYOD-Environment.pdf

[xiii] http://www.infotech.com/research/ss/provide-it-security-training

[xiv] http://c.ymcdn.com/sites/www.simnet.org/resource/collection/7A70D436-28BA-4E88-B958-C86941C704C3/2013_SIMposium.pdf

[xv] http://www.eccouncil.org/Certification/computer-hacking-forensics-investigator