Are We Prepared: Issues Relating to Cyber Security Economics

Dr. Jane LeClair, National Cybersecurity Institute at Excelsior College

Dr. Jane LeClair serves as the Chief Operating Officer of the National Cyber-security Institute (NCI) at Excelsior College in Washington, D.C., whose mission is to serve as an academic and research center dedicated to increasing the knowledge of the cyber security discipline.

Prior to this position, Dr. LeClair served as Dean of the School of Business and Technology at Excelsior College where she led faculty and staff in carrying out the mission and goals of the college and school. During her tenure as dean she oversaw the develop of numerous new programs including six in cyber security, with the establishment of the BS in Cyber Operations and MS in Cybersecurity. Her recent book "Protecting Our Future: Educating a Cybersecurity Workforce" was published in December 2013 by Hudson Whitman Press.

Dr. Denise Pheils, National Cybersecurity Institute

Dr. Pheils has taught networking and cybersecurity topics for associate through doctoral learners on-ground and online. She worked on the faculty panel to help determine the initial NSA Center of Academic Excellence standards for 2 year schools and earned that designation for Owens Community College as one of the first 13 in the nation. Dr. Pheils holds 21 certifications including the CISSP and PMP, and bringing many years of relevant and current work and research into cybersecurity topics. To provide hands-on experience to cybersecurity learners she piloted the Community Project Approach to Teaching Networking and Cybersecurity Topics that partners classes with not-for-profits in the community to accomplish tasks and secure that organization. She is a Fellow with the National Cybersecurity Institute at Excelsior College.

Are We Prepared: Issues Relating to Cyber Security Economics

Introduction

Today, more than ever, we know that the world of cyber security is a major economic issue. We recognize that related security costs may be high, yet we realize that they are a burden that must be the borne if we wish our data to be secure. To ease the effect of those costs on our bottom line, there must be a balance between the risks an organization may take with its data, both that which it generates and that which it is entrusted with, and the cost of protecting that data. Data is not all about financial numbers, it is also sensitive information about customers and employees; personal data such as social security numbers, banks accounts, charge card numbers, email and home addresses. All of this data, financial and personal, has the potential to be leveraged to gain increasingly more information that can be used maliciously. The balance of risks that is arrived at by those making the cyber security decisions will impact the government, stakeholders, the general public, and ultimately the bottom line of the organization.

Background

Make no mistake about it, the cost of cyber security very high. Reporting on a Ponemon Institute study, Kerner, (2013)[8] reports that "the annual cost of cyber-crime in the U.S. now stands at $11.56 million per organization. The 2013 figure is an increase of 26 percent from the $8.9 million Ponemon reported in 2012." (p. 2). Everson, et al. (2010)[5] write that "The network security market, which was $5.1 billion in 2009, has grown at over three times the rate of the enterprise networking equipment market (exsecurity) over the past six years. Given the need for base-line spending and the increase in threats, we expect network security to grow at a 9.7% CAGR from 2009 to 2013 and gain share of the IT budget." (p. 5). Those costs, seen as investments, may not be enough according to some estimates. LeClair, (2013)[9] writes that

"Increasingly, experts are urging that our cyber infrastructure be strengthened to meet these mounting challenges" (p. xii). Sales, (2013)[16] asks "Are individual firms, and society as a whole, investing the right amount in cyber-defense? Most observers believe that firms are under investing—and are missing the mark by a wide margin." (p. 1511). The financial outlay may be steep, but the data needs to be protected, yet accessible.

The long standing security model that is universally utilized by organizations is the 'CIA' Triad. Conklin, (2010)[2] writes that "Enterprise IT security and risk management have long been defined by the confidentiality, integrity and availability (CIA) triad." (p. 76). That model emphasizes that data needs to be confidential, its integrity kept intact, and it must be accessible. (Osborne, 2006)[12] The confidential aspect is readily apparent. An organization generates a good deal of data with regard to its employees, customers and operations. That data needs to be kept confidential at all costs since the release of that information could put much in jeopardy. Likewise, the integrity of the data contained in an organization's computer systems must remain valid, intact and unaltered. The third leg of the triad is accessibility. Data could be easily protected if it were locked in a vault and well guarded, but that would not permit the members of the organization, those with a 'need to know', to have access to the data in the day-to-day operations of the organization. Lack of accessibility would, of course, affect the efficiency and effectiveness of the organization.

Data must be accessible to those people who have a need for it, and yet, by this very accessibility to members of the organization it becomes vulnerable. The vulnerability extends to outsiders who might seek to breach security for personal benefit as well as to malicious insiders

who might seek to do damage for a perceived injustice. Unfortunately, insider threats are one of the main concerns of all organizations, both public and private. Ruppert (2009)[15] notes that "Typically an insider is an employee of the company that has greater access to sensitive information, a better understanding of internal processes, and knowledge of high-value targets and potential weaknesses in security. (p.2). Add to that the often nonsystematic approach to protection that of data, and significant problems and their financial implications can arise.

Financial considerations – Lose of consumer confidence

With the aforementioned in mind, there are three main reasons to focus on the cyber security economics of an organization as they relate squarely to the bottom line. First, if adequate protection measures are not taken, the data may be lost to outside hackers or to employee threats. This in turn affects the bottom line when the organizations name is tarnished. A very recent example is the breach of security at *Target*. At the height of this year's holiday shopping season, *Target* revealed that its security systems had been breached and upwards of 40 million credit card holders could have had their data stolen. The bombshell news sent the value of *Target* stock into decline with an immediate drop of 2%. Finkle (2013)[6] noted that "Target's shares closed down 2.2 percent at $62.15 on the New York Stock Exchange on Thursday afternoon". Analysts noted that "The timing of the [Target] news is particularly bad, said MKM Partners analyst Patrick McKeever. It's right in front of the Saturday before Christmas, the biggest day of the year for many retailers. We do think there could be some negative impact to [quarterly] sales, and there will very likely be a cost, both in dollars and in management time [and] attention." (Cheng, 2013)[1] The investigation of the *Target* breach is just beginning, but by all accounts it could have a serious impact on sales at the organization, reaching untold millions of dollars of

lost revenue and the public's good will. Cheng, (2013)[1] wrote that "…consumers' perception of the company has plunged to a six-year low. Industry analysts say it could take months for nation's No. 2 U.S. discounter's image to recover." *Target* reacted by issuing a statement of apology and a 10% limited discount on sales. (Woodyard, 2013)[17]. But this may be a matter of too little and too late as the personal data is reportedly being offered for sale on the internet already. Crosman (2013)[3] writes that "What is known is that the cybercriminals have obtained the basic account data stored on the magnetic stripes of the credit and debit cards - information such as name, account number and card expiration data. And they're selling the card data on underground websites."

Financial considerations – Civil lawsuits

A second financial consideration is the lawsuits that result from breaches of cyber security. If sensitive data is lost or exposed to the public as we have seen in the recent past, lawsuits and legal fees become a huge bottom line expense. When the personal data of customers is entrusted to an organization, customers expect that their sensitive data will be protected. When it is not, organizations can expect that lawsuits will soon be filed. In 2007 *TJX*, a large discount chain that includes *TJ Maxx* and *Marshalls*, had a significant breach of security that resulted in data from up to 100 million credit cards being stolen. Hackers had intercepted transaction data that TJX was sending via a dated wireless communication system and leveraged the information to gain further information on TJX customers. In that instance, TJX did not exercise 'due diligence' and courts decided against them. The final financial tally on that breach is still being determined, but current estimates are into the hundreds of millions of dollars in loss. (Lynch, 2009)[10] Another example is the 2009 data breach at *AvMed* that is running into the millions. McGee (2013)[11]

noted in an article in *Data Breach Today* that "A class action lawsuit against AvMed, a health plan company, stemming from a 2009 data breach, has been settled for $3 million. The *AvMed* settlement is significant because it awards payments to those who were not actual victims of identity theft because there was an expectation that there would be some sort of data security. (McGee, 2013)[11]

The lawsuits regarding the recent *Target* breach have already begun. Paramaguru (2013)[13] writes that:

> "Target was hit with a lawsuit Thursday amid the news that hackers had breached the retailer's systems and compromised as many as 40 million customers' credit and debt card data. The lawsuit in a San Francisco federal court was filed hours after Target acknowledged the hack, which took place between Nov. 27 and Dec. 15. The lawsuit was filed by a California resident, Jennifer Kirk, who wants to make it into a class-action suit representing other Target customers also affected by the data breach, Bloomberg Businessweek reports." (p. 1).

The lawsuit contends that Target failed to exercise due diligence and did not have in place "reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach". (Paramaguru, p.1)[13]

Financial considerations – Government action for violation of rules and regulations

Finally, if organizations are not following the numerous regulations in place to protect sensitive data, both fines and criminal penalties may be lodged against them. Numerous government rules and regulations govern how data is handled by organizations and fines that will be levied for

violations, including prison terms. There are countless regulations, but some of the more notable ones include: The Health Insurance Privacy Act of 1974, Portability and Accountability Act (HIPPA) of 1996, The Computer Security Act of 1987, The Clinger-Cohen Act of 1996, Gramm-Leach-Bliley Act of 1999, The Homeland Security Act of 2002, Federal Information Security Management Act of 2002, and the Sarbanes-Oxley Act of 2002. (Dennis, et al. 2013)[4] Each of these in turn has attempted to force organizations to strengthen various security aspects of business, industry and government agencies through enforcement. Violations of HIPPA for example can be fines up to $1.5 million per violation and potential jail sentence of up to ten years. Many of the violations in the differing pieces of legislation come from the lack of 'due diligence' by those responsible for security at organizations. In the specific case of TJX, they have agreed to numerous settlements since their breach. Lynch (2009)[10] notes that in one case alone "The bill for a three-year-old computer break-in at The TJX Cos. Inc. got $9.8 million steeper Tuesday when the company revealed a settlement with the attorneys general of 41 states". (p. 14) The 2005 cyber security breach at ChoicePoint was even costlier. Kaplan (2013)[7] wrote that "After the information theft was announced in 2005, ChoicePoint, acquired three years later by Reed Elsevier, settled with the Federal Trade Commission, as well as 44 states. In total, it paid out some $45 million as a result of the breach, and in the process, effectively created a new source of liability for organizations nationwide, one which has sped forward at lightning rates." (p. 1) Kaplan also notes that the Federal Trade Commission is charging the Wyndham Hotel group for a breach in 2008 and is "…seeking unspecified relief for incidents which it said resulted in $10.6 million in phony card charges and other expenses." (p. 2)

Recommendations for enhanced security

To protect the data of an organization and the all important bottom line, a comprehensive cyber security strategy for sensitive data needs to be embraced by organizations. That needs to begin with a top to bottom risk assessment of what the important assets of the organization are, what the threats/vulnerabilities are, what is the likelihood those vulnerabilities will be exploited, and what controls should be in place to attempt to alleviate/lessen perceived threats. A comprehensive education and training program needs to be implemented for the members of an organization that not only trains them, but raises their awareness of the threats to their organization's cyber systems. LeClair (2013)[9] writes that "As we seek to improve our defenses, we also need to recognize the importance of educating our workforce so that there is a seamless transition between educational facilities and industries" (p. xii).

Special emphasis in that program should be on 'social engineering', how to recognize it, and how to deal with such intrusions. Ricart, et el. (2013)[14] note the impact of this threat and writes:

> "According to a 2011 study by Internet security firm Check Point, 48% of the largest international organizations have experienced 25 or more social engineering attacks in the two years before the study, costing the organizations from US$25,000 to US$100,000 per incident. The impact of a social engineering attack can be significant, including theft of confidential information, loss of reputation and loss of competitive advantage" (p.41).

As one of the major threats to cyber security, social engineering is too often ignored or given little attention. Few learning institutions include the importance of human factors in their cyber curriculum and this absence needs to be addressed.

Finally, recognizing that education is the one of the important keys to success of any program, an organization needs to ensure that its senior managers are educated in the field of cyber security, that they are aware of its importance, and provide it with due attention. In many cases, this education can be offered in the form of cyber security courses, certificates and degrees that will enhance their skills in this all important arena. In so doing, when the time comes to assign funding for cyber security, managers who have been made aware of cyber issues will be more likely to include in their budgets adequate funding to provide a layered defense against intrusions – intrusions that will ultimately be very expensive.

Security breaches can affect the bottom line along three primary avenues, through loss of consumer confidence and business, lawsuits from individuals that have had their data stolen, and entanglements with state and federal officials. The costs of protecting the data of an organization can be a daunting one and requires a good deal of research and consideration as to how that cost will be dealt with. However, the costs that are incurred with a data breach can be staggering with the potential to put a smaller organization out of business entirely. A balance needs to be arrived at that is economically feasible yet protects the data utilizing the CIA triad model. Organizations that generate or are entrusted with sensitive data can choose to lessen their cyber security defenses, but as cyber criminals become increasingly sophisticated, they do so at their own risk and might well be advised to at least invest heavily in risk insurance.

References

1. Cheng, A. (2013) Retrieved from the internet on 12/20/2013 at http://blogs.marketwatch.com/behindthestorefront/2013/12/19/targets-card-breach-delivers-a-rude-christmas-surprise/

2. Conklin, W. (2011). "Control systems personnel are from Mars; IT personnel are from Venus". *International Journal of Critical Infrastructure Protection*. 4(2).

3. Crosman, P. (2013) Retrieved from the internet on 12/24/2013 at http://www.americanbanker.com/issues/178_243/40-million-dollar-target-data-breach-has-become-a-card-data-fire-sale-krebs-1064445-1.html

4. Dennis, C., Goldman, D. (2013). Date security laws and the cybersecurity debate". *Journal of Internet Law.* 17(2).

5. Evenson, J., Cofsky, J., Almazan, A. (2010). "Black book: The art of cyber war -- asymmetric payoffs lead to more spending on protection." *Bernstein Global Wealth Management* October. p1-188.

6. Finkle, J. (2013) Retrieved from the internet on 12/29/2013 at http://www.reuters.com/article/2013/12/19/us-target-breach-idUSBRE9BH1GX20131219

7. Kaplan, D. (2013) Retrieved from the internet on 12/24/2013 http://www.scmagazine.com/data-breach-lawsuits-roll-on-as-lawyers-work-to-establish-legal-precedent/article/309439/

8. Kerner, S. (2013). "Cyber-crime costs continue to rise: Study". *eWeek*. 10/8/2013, p2-2.

9. LeClair, J. (2013). *Protecting our future: Educating a cybersecurity workforce*. Albany, NY. Hudson Whitman/ Excelsior College Press.

10. Lynch, M. (2009). "TJX settles cyber-breach case." *Women's Wear Daily*. 197(131).

11. McGee, M. (2013) Retrieved from the internet on 12/24/2013 http://www.databreachtoday.com/settlement-in-avmed-breach-suit-a-6188

12. Osborne, M. (2006). *Managing information security*. Rockland, MA: Syngress Publishing.

13. Paramaguru, K. (2013). "Target sued for credit card hack". *Time.com*. 12/20/2103.

14. Ricart, P., Soulis, F., Nadeau, Y. (2013). Beware of social engineering. *CA Magazine*. 146(8).

15. Ruppert, B. (2009) Retrieved from the internet on 12/20/2013 at http://www.sans.org/reading-room/whitepapers/incident/protecting-insider-attacks-33168?show=protecting-insider-attacks-33168&cat=incident

16. Sales, N. (2013). "Regulating cyber-security". *Northwestern University Law Review*. 107(4).

17. Woodyard, C. (2013) Retrieved from the internet on 12/29/2013 at http://www.usatoday.com/story/money/business/2013/12/21/target-ceo-credit-breach-discount/4157103/