Proceedings of the 13th Colloquium for Information Systems Security Education
University of Alaska, Fairbanks
Seattle, WA June 1 - 3, 2009

Giving Failure a Place in Information Security: Teaching Students to Use the Post-Mortem as a Way to Improve Security

Patricia Logan, Ph.D. and Tracy Christofero, Ph.D., *Marshall University*

Abstract – Despite state-of-the-art technologies and enhanced organizational policies, the security of corporate data is not a guarantee. The possibility of the failure of security, however, is. Given the certainty of failure, it is surprising that information security curricula do not include post-incident reviews to gather the lessons learned from failure and to better prepare students to enter the workforce ready to plan for and manage security incidents. This paper proposes that undergraduate and graduate courses in information security include the topic of failure, and address the performance of a post-incident (post-mortem) review as a best practice.

Index terms – Information security, post-incident analysis, lessons learned, security post-mortem, security education and training

I. INTRODUCTION

State-of-the-art technologies and the application of enhanced organizational security policies have not ensured that information security is a guarantee. Security failure, however, is. Given the certainty of failure, it is surprising that information security curricula do not include post-incident reviews to gather the lessons learned from failure and to better prepare students to enter the workforce ready to plan for and manage security incidents. An incident can be thought of as a violation or eminent threat of violation of computer security policies, acceptable use policies, or standard security practices [1].

Dr. Logan is an Associate Professor of Information Systems, and Dr. Christofero is an Associate Professor and Coordinator of the Technology Management Program for the College of Information Technology and Engineering at Marshall University's Graduate College in South Charleston, West Virginia.

Today's security curriculum is typically heavy on teaching the concepts of attack methodology, malware, human failures, insiders, risk identification, planning and policy, firewalls, IDSs (Intrusion Detection Systems), antivirus tools, scanners, and sniffers. Concepts are taught, students practice using tools, and it is implied that these will be enough to avoid a security incident.

Yet, the reality is that despite the omnipresence of failure, the information security curriculum does not go far enough to prepare students to expect failure and teach them to critically dissect breaches to improve an organization's security effectiveness.

According to the Open Security Foundation, the number of security incidents in 2008 increased by 50 percent and compromised millions of data records [2]. Their data loss database enumerates security breaches by month, year, and type; and leads to the conclusion that there are no silver bullets, or in some cases, that common sense is not always exercised when applying security to a business enterprise. Security cannot be guaranteed, as there are novel methods of attack and intrusion not yet executed and contemplated, and insiders with trusted privileges can penetrate secure systems.

The Computer Security Institute performs annual surveys of security professionals that show that half of the surveyed companies have one to five incidents and 26 percent have five to ten annually, with additional unreported breaches likely [3]. Security professionals and educators realize that failure is inevitable, and although alluded to in many textbooks, information security students are not often prepared to expect and to manage failures. NIST Guide 800-61 revision 1 details how to maximize the lessons learned from a security incident using a post-incident review to identify systemic security weaknesses and deficiencies in policies and

procedures. The *Computer Security Incident Handling Guide* provides practical guidance in how to establish an effective incident response program, analyze and respond to security incidents, and reduce risks of future incidents [4]. Yet, managing failure is more than the identification of incident characteristics and break/fix security repair. As a part of the post-incident process, planning for and managing failure must be explicitly taught to assure that students are capable of strengthening an organization's information security. Equipped with only the technical skills, information security students will assume they are completely skilled and that the repair of the system is the end of an incident. Without appropriate training, even the best students will fail in managing a real-world security incident.

This paper proposes that undergraduate and graduate courses in information security include the topic of failure, and address the performance of post-incident review as a best practice.

II. NEED

One only has to open a newspaper and view current headlines documenting the almost constant loss of personal and financial data due to carelessness and intrusion [4]. The causes of the most recent security breaches continue to fall into the same categories as past ones: improper disposal of data/media (American Express), lost media/laptop (United States Department of Veteran's Affairs), stolen data (Card Systems), fraud (TJX), and hack (Heartland Payment). It is not only careless small businesses that are leaking confidential customer data - it is large, multinational corporations with smart and capable information technology departments and dedicated security professionals with large security budgets that are victimized. It would appear that a large number of well-trained security professionals are still unable to prevent the loss of data. Is there something missing in the information security curriculum that trains our security professionals?

The information security curriculum trains students to identify attack methodologies and signatures, provides information about the threat landscape, enables students to practice with technology tools used to identify and deter intruders, create and design an appropriate security plan, and understand how to repair systems damaged and contaminated from an intrusion. When the penetration of secure defenses occurs, the blame is placed on the victims (end users) rather than assigned to the inadequacies of the defenses provided by the security professionals. Does the quick assignment of blame prevent a thorough post-incident review? Would the post-incident review improve the design of defenses? Would reviewing the failure give the defenders a better understanding of how a failure occurs that could lead to better training of end-users and the design of technologies that are used in prevention? It is not just about the repair and the investigation necessary to appropriately mitigate the harm; it is about the serious and in-depth review of the failures that enabled the data to be compromised. Students should not leave information security courses believing that once repair is complete, that the incident is over. While preliminary assessments of damage can pinpoint a weak link in the layers of defense, a thorough review of the incident and response can often reveal that the weakest link is not always what was originally thought to have been the locus of failure. What the information security curriculum does not do is take the students through a post-incident analysis of a security failure. The current curriculum over-emphasizes capture-the-flag exercises, focuses on technology solutions to implement security, relies on the security of layers of defense, and urges students to quickly assess the blame on the "clueless" users. This approach may leave students unprepared to recommend the changes necessary to protect corporate data assets.

After the adrenaline generated by an intrusion dissipates, the perpetrators are captured or gone, and senior managers have "spun" the incident for their CEOs (and the public if disclosure is required), it is often assumed that having been struck once, they are now immune from further harm. Nevertheless, the question should still be asked: What can be done to prevent this from happening again? Prevention is well-defined and executed in the information security curriculum. Repair and recovery are emphasized as critical post-incident activities. What students miss is the complete picture that exists within the corporation where multiple points of failure exist that enable a security breach. Incident-response teams (IRTs) should have a management perspective in addition to a focus on dealing with the technical symptoms [5].

Post-incident reviews are not intended just for information technology staff. The conclusions and outcomes are relevant across the entire business. For too many organizations, the repair and restoration of a network and the associated business applications is the end of the incident. If any post-incident reviews occur, they often include only the Computer Security Incident Response Team (CSIRT) or the IT staff involved in the repair and restoration of the damaged systems. From a business perspective, a security breach is a serious event that affects profitability, productivity, and public perception – the "3 P's" essential to organizational success and should include the business perspective in any post-incident review.

Including only technical support staff in a post-incident review ignores two important aspects of security incidents: 1) security failures are often failures within established business processes; and 2) there are impacts that affect customers, vendors, and public perception in ways that harm the business that IT staff typically would not have considered. Examining a security incident from a number of perspectives enables the inclusion of these other outcomes from a security breach. Ultimately, the way an incident is processed affects the reputation of the organization. Research indicates that many security incidents relate to people, business policies, and technology. Students must be taught how and when to address these issues and gain experience in the identification and isolation of business events contributing to security failure and remediation. These skills require elements of investigation across business units; artifact gathering; people, policy, and technology analysis; remediation planning; and critical event report writing.

Failures are not always caused or cured by technology. Yet, too many security professionals are obsessed with the tools and the technology, and the current information security programs do not adequately expand that scope. Computer Science and Information Security programs generally focus on the technical aspects of information security. Students gain exposure to incident detection, attack methods, and defensive responses without the business context of the at-risk data. When information security courses are placed in technical programs such as Computer Science, students are often not exposed to the business processes and practices that often contribute to security failures. Leading textbooks may mention remediation, but do not typically include discussion of post-incident review, lessons learned methodologies, or post-incident processes for strengthening security after the failure. For example, one of the more popular textbooks on information security is Principles of Information Security by M. Whitman and H. Mattord. A review of the topics shows that post-incident review as a formal project is not mentioned in any context. Under the chapter in disaster recovery the focus is on preparing to handle a disaster (planning and preparedness). The final chapter in the textbook, "Information Security Management" focuses on monitoring the internal and external environment, vulnerability assessments, and periodic reviews of security defenses. Rehearsals are advocated (war games) where real incidents can be simulated by security staff in order to practice defenses. The glossary of terms at the textbook's conclusion does not define or list "post-incident review" [6].

Protecting data is the goal of a post-incident review. In a 2008 computer security survey, thirty-eight percent of the managers surveyed stated that they experienced one to forty-nine security events in the past year, while another 35 percent said they did not know whether they had been hit [7]. Information security surveys continue to show many areas that are not performed as part of overall security management. Despite technology-oriented gains, there are disturbing trends in the areas of security processes and personnel. For example, encrypting sensitive data makes good sense, and the Payment Card Industry (PCI) Security Standards Council mandates that a firewall be installed to protect cardholder data. Karen Worstell, former Microsoft and AT&T CISO, however, notes that the PCI standard does not address whether a company has processes to ensure that once a piece of technology is installed, it is regularly upgraded or monitored to see how effective it is. "If security stops at PCI, that's not enough," she says [8]. The U.S.-based Hannaford Supermarkets experienced the theft of customer credit and debit card data from December 2007 to March 2008 - a period when the grocery chain was certified as compliant with PCI standards. According to the company, these are "the highest security standards required by the credit card industry" [8]. A post-incident

review could provide the incentive to define and implement the processes that are required to install PCI. Performing a post-incident review and publicizing the outcomes is an effective means of preventing similar security incidents with PCI. The absence of post-incident reviews will negate any protection an IT budget can buy.

The implementation of security continues to be flawed and best practices are incompletely followed. This may reflect on an overall reliance on technology to deliver the silver bullet, and a false sense of protection from additional incidents. Students will certainly experience security failures and must be taught to understand the opportunity a failure presents for security improvements. A component of a post-incident review should also be an evaluation of how risk was assessed for the particular incident. Students should become familiar with the literature in psychology on how risk is determined from the human perspective. In the subject area of information security we assess risk using calculations based on the probability of occurrence. Often we ignore how we rationalize the risk of occurrence for these probabilities [9]. An understanding of how risks were assigned and how professionals assess probabilities of occurrence is a necessary component of any post-incident review because it gets to the heart of how the defenses failed and enabled the incident to occur. The post-incident review is a best practice that can prevent future incidents and when the findings are published can inform the security community in order to prevent the same incident from recurring.

III. PROPOSAL

We propose that the concept of failure be included as a stand-alone unit of study in the information security curriculum and that students should be introduced to the best practice of post-incident review. Instruction should include cases that cover the known types of security incidents with hypothetical situations crafted to allow students to assess the three aspects of security for their contribution to failure: people, policies, and technology.

Including the topic of failure and exercises in post-incident review would introduce and reinforce a number of skills that students at both undergraduate and graduate levels should embrace as a security professional:

- Project planning and management
- Case study analysis
- Risk assessment
- Report writing
- Team work

IT professionals recognize the value of project management as support for risk management. The skills of project planning and management are critical for successful security management. The project management culture emphasizes planning over management. A terminal step in a project plan is a post-implementation review. The goal of this post-implementation review is to: 1) examine what went right; 2) review the problems that negatively affected security performance; and 3) identify the degree to which the goals of the project were met. Many project managers refer to this terminal task as performing a post-mortem. Many companies invested in project management use a specialized form of post-incident review for security breaches: the post-mortem. Goals of this review are: 1) to understand the people, technology and policy failures of a security incident; 2) document for management the necessary steps to prevent a future incident; and 3) develop a project plan for implementing corrective actions. A security post-mortem allows the security project team to review the successes and failures of a project. Post-mortem reviews should be included in the information security curriculum. There should be more than a reference to the need for this as a best practice. It should be tightly coupled with project planning and management skills. Students should be required to develop a project plan for the recommendations that come from the analysis of the case.

Cases are an important way for students and security professionals to practice their security skills. They offer the advantage of happening outside the stressful arena of dealing with a real world security incident. They encourage discussion free from bias, blame, and political influence. Post-mortems performed on hypothetical cases, yield valuable information essential to effectively managing security. Students should expect a case that involves an entire system impacted by the security incident, including business practices that contributed to the incident. This represents an opportunity for student teams to review spending on security,

appropriate deployment of technology, security metrics, and risk management. The post-mortem addresses:

- How an incident happened
- Who, what, how, when, and why
- Information for law enforcement
- Public disclosure details
- Future attack prevention

The focus of the case analysis should be on improving the response and security rather than solving the crime, although that is certainly a by-product of the effort and the ensuing report can be used later in prosecution by law enforcement. Even if the incident was clearly documented at the time, a review of how things could have gone better in order to improve processes, tools, and training for the future is required. These improvements may not prevent all future attacks, but they will assist in preparing the business for the next incident. Students need to learn what artifacts and documentation are important to an understanding of the event and the timeline. Documentation that students should learn to review will include:

- Physical environment
- Email systems
- Applications and specialized utilities
- Backup and restore procedures
- Written policies
- IRT response procedures
- Media and public disclosures

One of the first activities students learn in a case exercise is how to create a timeline. Timelines are useful in ordering events improving future response, and isolating needed artifacts. They also allow students to visually insert players sooner, or later, to see the impacts on the incident and response. The timeline begins with a first report of the incident, which is crucial in assessing the amount of time to respond and provides a good benchmark for future response time monitoring. The mechanism of discovery itself is important. Student teams can review cases, assess how the discovery was made, and use the information to make recommendations for changes. Cases can enable students to perform inter- and intra-incident analysis. Intra-incident analysis of an incident's specifics includes: the software left behind, the elements of trust (web of trust) within the network, log file content, and intruder profiles. Inter-incident analysis attempts correlations with a series of incidents that may be related and predictive. Risk assessment is an important component of a security plan. The purpose of the post-mortem is to learn the security strengths and weaknesses of the processes, so that security may be improved and strengthened. The post-mortem manages risk by forcing a reassessment of the current security plan. Students should learn that assessing risk is not just an annual activity but is required after any changes, including the changes implemented after a security breach.

Students have few opportunities in a technical curriculum to practice report writing. One of the outcomes of the post-mortem exercise is a report that documents the incident for senior management and presents recommendations for remediation. Writing a report that represents large amounts of technical data to a non-technical audience is a good exercise for students, and will improve the ability of students to work as security professionals. Student teams can learn to identify issues (the deltas are the differences between what happened and what should have happened) within the incident and ask: What can be done to remediate? It is important to look at procedures in the security plan that were not followed and the reasons. The report's content would include:

- Recommendations
- Assessment of potential impacts
- Perform a risk assessment
- Define a test plan
- Develop a deployment plan
- Deployment of changes

Working in teams allows students to simulate the team-oriented environment of IT departments. It will provide an opportunity for students to not only analyze a case together but to develop recommendations after the team's discussion, a joint final report, and a project plan to implement the recommendations. Collaborative efforts improve students' ability to work together and share their understanding of security concepts as well as reinforcing the course concepts.

It is unlikely that students will have a real-world opportunity to dissect breaches. Educators can create exercises to simulate these incidents, and students can work in teams to conduct post-mortems on hypotheticals and case studies. If actual security-related cases are not available, a

good source for cases that expose students to a variety of incidents is the Open Security Foundation's data loss database.
The following is an example of how to conduct a post-mortem exercise using a case study.

IV. Case Study

The Case of the Missing Tape

A data tape with state employee personal information slipped out of a package shipped on October 12th by the United Employees Insurance Agency (UEIA) to a Pennsylvania vendor using UPS. The data was not encrypted. The data tape was in a manila envelope secured only by glue on the flap. It was shipped 2-day-ground. The vendor reported it missing on October 16th. Officials believed the package became unglued while in-transit. They did not suspect theft. The employee information was from the UEIA, the Children's Health Insurance Program, and the Access Mid-Atlantic insurance pool.

In a public announcement and a letter to the 200,000 current and former state employee members, state officials advised that personal data was compromised when a backup tape was lost the previous week. The personal information exposed consisted of: names, addresses, phone numbers, Social Security numbers, and marital status. Officials stated that mainframe data processing equipment would be required to access the personal information, and it was unlikely that identity thieves would possess such devices.

A toll-free hotline was set up and state officials recommended that victims contact one of the three major credit-monitoring agencies as a safeguard. State officials meanwhile, attempted to obtain the cooperation of UPS and receive compensation, but were unsuccessful.

The IRT decided to decline a credit watch service for the affected employees, believing that it would set a bad precedent for future incidents (i.e., paying for a credit watch service). Coincidentally, six months later, many employees had their credit card numbers used in an apparent identity theft attempt. Employees complained to the state that they were not provided with credit watch services and that their data was still at risk.

Post-mortem questions:

1. *What would be your first step?*
2. *What artifacts would you collect?*
3. *What was the timeline for actions?*
4. *Who was involved in the chronology of events?*
5. *How was the event discovered?*
6. *What factors made this a security incident?*
7. *Was there a process in place to handle this type of incident?*
8. *Could the incident have been discovered earlier?*
9. *Was anything missing in the response?*
10. *Would there be fall-out from public disclosure?*
11. *What assumptions were made about the risks of this mode of data transport?*
12. *What changes should have occurred that could prevent the incident in the future?*

As you review this case with your students, consider these suggestions for items to focus on:

- *A necessary first step would be to gather a team reflective of the players in the security breach and recovery. The IRT was the IT team in this case.*
- *There was a loss of private data (customer name, address, SSN, medical and dependents) that required public disclosure. Evaluate the employee response and if unknown, suggest a survey of the employees for their reaction. Knowledgeable victims will resent self-serving statements about safety because the data tape required "special equipment" or that the loss wouldn't result in identity thieves or criminals using the information. Media commentary would certainly focus on why the data was not encrypted.*
- *No process or policy existed for assisting victims with identity loss problems or for encrypting data sets.*
- *Angry public employees could cause a backlash. That backlash, in turn, could cause a reevaluation of the response that would make the state officials look unprepared.*

- *The assumptions made about the safety of data transport using a public delivery service were flawed.*

- *Recommendations should include: 1) follow-up with employees; 2) implement hardware level encryption; 3) sending data in a more secure fashion that avoided physical movement; 4) assure agreements were in place for compensation if identity fraud was suspected; and 5) development of a process for helping employees with identity theft.*

V. BENEFIT

Proper post-mortem investigation and analysis is not about repair. It is about security improvement after a failure and involves hindsight: a perfect understanding of an event after it has happened. It is judging the wisdom of decisions in light of information that was not available when the decision was made [10].

Post-mortems are an important part of project management and should be used to manage the extended negative outcomes that result from a security failure. It leads to the identification of the weakest link that led to the security failure, and helps students see the value of the project plan discipline in a post-incident security investigation. Additionally, students are exposed to analysis of systematic failures and learn to isolate failures in documentation.

IV. CONCLUSIONS

Dennis Maynes, chief scientist at Caveon, Inc. "*A good practice in security is learning from your own mistakes. A better practice is learning from the mistakes of others. A best practice is creating processes so that those mistakes are never repeated*" [11]. Teaching security post-mortem analysis as a unit in post-secondary security education is a best practice for assuring that students are not caught dead in the water when investigating real-world security incidents. Security failures may be inevitable, but need not be terminal if post-mortems are taught.

REFERENCES

[1] Grance, T., Kent, K., & Kim, B. (2004). Computer security. *Computer Security Incident Handling Guide (NIST SP 800-61)*. Retrieved March 4, 2009

[2] Open Security Foundation
. (2009). Retrieved March 5, 2009, from http://datalossdb.org

[3] Computer Security Institute. (2008). CSI computer crime and security survey. *CSI Survey*. Retrieved March 6, 2009, from http://www.gocsi.com/forms/csi_survey.jhtml;jsessionid=S40GZJ3FOLZD0QSNDLOSKHSCJUNN2JVN

[4] Information Technology Laboratory (2008, March). Handling computer security incidents: NIST issues updated guidelines. *ITL Bulletin.* Retrieved March 7, 2008 from http://csrc.nist.gov/publications/nistbul/b-March-2008.pdf

[5] http://searchsecurity.techtarget.com/expert/knowledgebaseAnswer/0,289625,sid14_gci1321525,00.html

[6] Whitman, M. & Mattord, H., *Principles of Information Security,* Thomson Course Technology, 3rd Edition, 2009

[7] Eppel, N. (n.d.). Security absurdity: The complete, unquestionable, and total failure of information security. Retrieved March 8, 2009, from www.securityabsurdity.com/failure.php

[8] Nash, K.S. & Greenwood, D. (2008), December 8). The global state of information security 2008. *CIO Magazine.* Retrieved March 7, 2009, from http://cio.co.nz/cio.nsf/depth/6CED47204CFE4A5FCC25750D00746C85

[9] Salavitz, M.(Jan/Feb 2008). 10 Ways We Get the Odds Wrong. *Psychology Today Magazine.* Retrieved April 14, 2009, from http://www.psychologytoday.com/articles/index.php?term=pto-20071228-000005&print=1

[10] http://www.thefreedictionary.com/20-20+hindsight

[11] Maynes, D. (2008, April 7). Hindsight is 20-20: Introducing the security breach post mortem. *Dennis on Data Forensics* [Blog]. Retrieved March 4, 2009, from http://caveon.com/df_blog/?p=40