INTERHACK

Interhack
5 E Long St 9th Fl
Columbus, OH 43215

VOX +1 614 545 HACK
FAX +1 614 545 0076
WEB http://web.interhack.com/

Incident Handling: When The Breach Occurs

C. Matthew Curtin, CISSP

Thursday, July 23, 2009

Reputation is made or broken not on whether an incident takes place, but how well the incident is handled. Thus, every security program includes a component on incident handling. Effectively handling adverse events requires planning and practice, paving the way for sound execution.

What is an Incident?

An *incident* is generally any adverse event, which by its nature also implies that the event is unscheduled. Worse, the organization generally cannot know the scope, duration, or impact of the event until after resources are mobilized for response. As used in computer security, an incident is defined as "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices."[1]

An incident can take many forms. It can be exposure of the organization's operational capability, reputation, or money. In my experience, incidents typically include all of these in varying degrees.

[1] Tim Grance, Karen Kent, and Brian Kim. Computer security incident handling guide. NIST SP 800-61, January 2004. [online] http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

Incidents Are Not Technical Problems

By and large, information security professionals have historically come from inside of the information technology (IT) groups, and have focused extensively on the avoidance of security-related failures. More than thirty years of failure avoidance theory has failed to produce *systems* that avoid failure, leading some to look more broadly at the issues.

Some in the literature have looked at economic models, attempting to find acceptable failure rates, methods to limit the impact of failure, and systematic approaches to deploying systems that, quite simply, don't surprise the people who rely on them.[2]

Incidents, however, are not ultimately a technical problem: they threaten their organizations' resources and reputation. Security

[2] Howard F. Lipson and David A. Fisher. Survivability - a new technical and business perspective on security, 2000 . [online] http://www.cert.org/archive/pdf/busperspec.pdf; R. Anderson. Why information security is hard-an economic perspective. In *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual*, pages 358–365, 2001; and Matt Curtin. *Developing Trust: Online Privacy and Security*. Apress, November 2001

breaches themselves have a high (and increasing) cost.[3] Privacy breaches have a negative albeit short-lived impact on market value.[4] Interestingly, research has found correlations between some industries and breach types.[5]

Incidents Pose Risk to the Chief Information Officer

Another study released this year showed that incidents are of concern among C-level executives. CIOs might not be surprised to discover that other senior executives will think them responsible for protecting sensitive information. CIOs should note, however, that among senior executives, CEOs have the most trust in their organizations' ability to avoid such incidents.[6]

Thus, the first question for CIOs arises: are you properly managing expectations with your management?

Incident Response Is a Cross-Discipline Effort

When an incident occurs, it's often (but not always) something that takes place within infrastructure that's part of IT. Incidents of data exposure that come from system compromise, lost computing equipment, and lost data storage equipment are common examples.

Incidents are different from routine operational mistakes in that they expose the organization in particular ways. For example, exposing customer data may impact the organization's reputation and customers' future buying decisions, and possibly fines from the U.S. Federal Trade Commission.[7] Exposing payment card data may cause revocation of the organization's Payment Card Industry Data Security Standard adherence certification and fines to be levied.[8] And of course, where there is apparent harm, litigation will follow.[9]

Responding to an incident therefore requires the expertise of people who can protect the organization from harm arising from these aftershocks. Efficient response will be a single coördinated response effort. Here we consider some of the *dramatis personæ*.

Counsel Attorneys can determine exposure arising from failure to uphold law, contract terms, and what remediative action is required to avoid further exposure.

Security Expert An outside security expert—as recognized by the courts, and with litigation experience—can opine on the efficacy of controls and response, bridge the gap between IT and legal resources, and protect internal resources from

[3] Larry Ponemon. Fourth Annual US Cost of Data Breach Study, January 2009b

[4] A. Acquisti, A. Friedman, and R. Telang. Is there a cost to privacy breaches? An event study. In *Workshop on the Economics of Information Security (WEIS)*, 2006

[5] C. Matthew Curtin and Lee T. Ayres. Using Science to Combat Data Loss: Analyzing Breaches by Type and Industry. *I/S: A Journal of Law and Policy for the Information Society*, 4(3), Winter 2008-09. URL http://web.interhack.com/publications/breach-taxonomy/

[6] Larry Ponemon. Business Case for Data Protection Study of CEOs and other C-level Executives, July 2009a. URL http://www.ouncelabs.com/writable/resources/file/business_case_for_data_protection_070809.pdf

Loss Type	*Frequency*
Media	9.57%
Hardware	29.14%
Compromise	21.58%
Disposal	7.12%

Table 1: Proportion of 'IT-related' loss types, without regard to industry
Source: Curtin and Ayres, 2008

[7] Jaikumar Vijayan. FTC imposes $10M fine against ChoicePoint for data breach. Computerworld, January 26, 2006. URL http://www.computerworld.com/s/article/108069/FTC_imposes_10M_fine_against_ChoicePoint_for_data_breach

[8] Dan Kaplan. Visa: Heartland, RBS WorldPay no longer PCI compliant. SC Magazine, March 13, 2009. URL http://www.scmagazineus.com/Visa-Heartland-RBS-WorldPay-no-longer-PCI-compliant/article/128762/

[9] The Chubb Corporation. Technology Companies Are Exposed to Security Breach Litigation, January 8, 2007. URL http://www.chubb.com/corporate/chubb6156.html

exposure through deposition. Furthermore, if engaged by counsel, the work of the expert might fall under the domain of *attorney work product privilege*, making it unavailable to opposing attorneys in litigation or regulatory action even under subpœna.

In-House SMEs Subject matter experts from your own business can help those who shield the organization from outside threats such as litigation quickly understand how things work specifically in the organization. They will know the history necessary to understand not just *what* but *why*. These include both technology SMEs and those with expertise in lines of business.

Public Relations If the organization needs to explain itself publicly or to its customers, PR will need to be prepared to do so in a way that is honest and appropriately communicative, while not providing basis for undue panic or additional exposure. Furthermore, if the story leaks and someone from the press calls to ask about it, you will want PR to be prepared with a statement that will not exacerbate the situation. Within public relations there is a specialty known as *crisis communications*.[10] Likely you'll want to ensure that you have such special expertise at the ready.

[10] K. Fearn-Banks. *Crisis communications: A casebook approach*. Lawrence Erlbaum, 2007

In a crisis situation, you will want to turn to people that you know and can trust. That means that people you know and trust need to cover the range of disciplines needed to remedy a problem. **The second question for CIOs: have you established good working relationships with your peers in legal, HR, PR, and operations?**

Incident Recovery Is a Long-Term Effort

Recovery isn't "complete" after the crisis has passed. The question of how the incident took place will require understanding enabling factors. Were systems not kept up to date on patches? Was there a weakness in software that was developed in-house? What are those root causes, and how can they be assessed? How much of the budget needs to be diverted away from 'offensive' action toward defensive?

In many cases, a combination of weaknesses created the condition for the vulnerability that ultimately led to the exposure. These will likely come from such diverse areas as procedural weaknesses, policy gaps, insufficient training, and perhaps even a lack of vigilance. Once those conditions are identified, they will need to be addressed.

Budgeting with cost-benefit analysis using net present value has been shown to be effective.[11] Once budgets are approved however, follow-through will be needed to ensure that the expected results are being achieved. Models for assessment will need to be in place to give you—and therefore your organization—the assurance that it needs that it is striking the proper balance between enabling the business and protecting the business.

The third question for CIOs: is your organization prepared to follow immediate tactical action with strategic action?

[11] Lawrence A. Gordon and Martin P. Loeb. Budgeting process for information security expenditures. *Communications of the ACM*, 49 (1):121–125, January 2006. ISSN 0001-0782

Effective Incident Management Starts Before the Incident

No one expects to win on game day by running on to the field, then figuring out the rules of the game, how many people are needed, what positions each will play, and setting a deadline on when to score a goal. Teams win by understanding their game and by practicing together as a team, getting to know one another, seeing how to use one anothers' strengths, and how to cover one anothers' weaknesses.

In many organizations, disaster recovery plans are in place, and are tested with some frequency. The same kind of exercise can be tremendously valuable. Working with an outside computer expert, your attorneys, and other players who will spring to action in the event of a breach will help to ensure that your team knows its game, and comes prepared to win.

The important thing always to keep in mind is the end state: a 'win' might not be finding a 'bad guy' and bringing him to 'justice.' It might mean repelling an attack, preventing a loss of a hard drive from turning into a breach, or simply ensuring that the business is not unduly distracted from taking care of its customers.

The fourth question for CIOs: does your organization maintain proper preparedness for adverse events?

An organization that is prepared for an incident, having created plans that are relevant and tested and people who are trained and prepared, will need to run through the process. The plan might not survive first contact with the enemy, but the team that planned together and drilled together will be able to find its way through. Your job as the CIO is to ensure that the objective stays clearly before the team so that they can do the work of taking you there.

1. The breach is identified and reported forward to management in a timely fashion;
2. Management calls counsel and identifies the resources necessary to understand the potential magnitude of the incident;
3. Other resources, including outside experts, in-house SMEs, and PR are mobilized, rôles established, and timeframe to check back established;
4. Management assesses reports from action to determine such issues as whether to report, to whom to report, when to report, and what to report; and
5. Ensure that the breach is contained, evidence is preserved, remediation strategies are developed, and action is memorialized.

Figure 1: Critical Elements in Incident Response

About the Author

C. MATTHEW CURTIN, CISSP, is the founder of Interhack Corporation, a Columbus-based computer experts firm, aiding executives and attorneys facing challenges and opportunities involving the management of information. His work is used to find the right questions to ask and the best answers science can provide. He advises organizations on the use of enterprise-wide cryptographic controls and analyzes information technology and electronic stored information to answer questions that arise in adjudication. Mr. Curtin has appeared as an expert witness in both civil and criminal cases, dealing with everything from electronic discovery to assessment of information technology in practice.

Mr. Curtin maintains a regular academic appointment as a Lecturer at The Ohio State University's Department of Computer Science and Engineering, teaching courses in the Common Lisp programming language and operating systems. He is the author of *Developing Trust: Online Privacy and Security* (Apress, 2001) and *Brute Force: Cracking the Data Encryption Standard* (Copernicus Books, 2005). He can be reached at cmcurtin@interhack.com.

Bibliography

A. Acquisti, A. Friedman, and R. Telang. Is there a cost to privacy breaches? An event study. In *Workshop on the Economics of Information Security (WEIS)*, 2006.

R. Anderson. Why information security is hard-an economic perspective. In *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual*, pages 358–365, 2001.

The Chubb Corporation. Technology Companies Are Exposed to Security Breach Litigation, January 8, 2007. URL http://www.chubb.com/corporate/chubb6156.html.

C. Matthew Curtin and Lee T. Ayres. Using Science to Combat Data Loss: Analyzing Breaches by Type and Industry. *I/S: A Journal of Law and Policy for the Information Society*, 4(3), Winter 2008-09. URL http://web.interhack.com/publications/breach-taxonomy/.

Matt Curtin. *Developing Trust: Online Privacy and Security*. Apress, November 2001.

K. Fearn-Banks. *Crisis communications: A casebook approach*. Lawrence Erlbaum, 2007.

Lawrence A. Gordon and Martin P. Loeb. Budgeting process for information security expenditures. *Communications of the ACM*, 49(1):121–125, January 2006. ISSN 0001-0782.

Tim Grance, Karen Kent, and Brian Kim. Computer security incident handling guide. NIST SP 800-61, January 2004. [online] http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf.

Dan Kaplan. Visa: Heartland, RBS WorldPay no longer PCI compliant. SC Magazine, March 13, 2009. URL http://www.scmagazineus.com/Visa-Heartland-RBS-WorldPay-no-longer-PCI-compliant/article/128762/.

Howard F. Lipson and David A. Fisher. Survivability - a new technical and business perspective on security, 2000 . [online] http://www.cert.org/archive/pdf/busperspec.pdf.

Larry Ponemon. Business Case for Data Protection Study of CEOs and other C-level Executives, July 2009a. URL http://www.ouncelabs.com/writable/resources/file/business_case_for_data_protection_070809.pdf.

Larry Ponemon. Fourth Annual US Cost of Data Breach Study, January 2009b.

Jaikumar Vijayan. FTC imposes $10M fine against ChoicePoint for data breach. Computerworld, January 26, 2006. URL http://www.computerworld.com/s/article/108069/FTC_imposes_10M_fine_against_ChoicePoint_for_data_breach.