Information Crisis Management

By John C. Checco

Information Crisis Management defines the SOP used when proprietary information assets are compromised, either by network breaches or employee breaches. According to ASIS, "Fortune 1000 companies lost more than $45B from the theft of proprietary information" in a single year[1].

Cockpit Resource Management?

The FAA, in response to the avoidable crash of United Airlines Flight 173 on Dec. 28, 1978, developed one of the first "critical thinking" guidelines for crisis management. Originally known as "Cockpit Resource Management" (and later changed to "Crew Resource Management"), this process is integrated by many emergency services into their Incident Command System.[2] One particular aspect of this guideline that applies to any group of decision-makers is the use of the three "*decision outcome avenues*."

1. **Avoid**: plan to prevent possibilities of a crisis.
2. **Trap**: recognize bad decisions and fix potential problems before a crisis.
3. **Mitigate:** minimize the negative effect during a crisis and investigate post-crisis.

The concept of "decision outcome avenues" applies directly to information security planning. Many organizations spend sufficient effort on plans to avoid and trap breaches, but mitigation is usually not a well pre-planned effort.

Pre-Planning for Mitigation

To plan for an effective post-crisis investigation, an organization needs to plan pre-crisis. *Content-specific planning* addresses the mitigation of direct breaches, intentionally accessing information for dissemination outside its intended audience. *Access-specific planning* addresses the mitigation of indirect breaches, hijacking legitimate information access.

At the heart of this plan lies the explicit determination of informational risk. The organization must first evaluate any information that is considered proprietary. This may mean a substantial effort in collecting information that is subject to scrutiny, but it is a necessary task for every organization. Second, it must classify information according to damage control needed: i.e. source code needs to be under version control, sensitive documents need to be centrally managed, etc. Information that is considered paramount should be in lock-down mode – inaccessible except through physical means, even if it means having a standalone workstation holding the information in a locked room.

Content-Specific Planning

For documents that are considered confidential, companies need to institute a central document repository. Companies that are ISO-9001 compliant should already have this in place. However, additional precautions should be taken.

- The repository should have strict entitlement rules for each user. Proper licensing should be in place for the document management system to allow each user access, rather than a set of shared userids.

- Classification is necessary for all new documents being submitted to the central repository. This need not be a committee review, just a second authority to ensure documents are properly protected.

- Document server storage should be encrypted.

- Authors can request a document in editable form; all others MUST get the document in read-only form. Software utilities, such as Win2PDF, can accomplish this task dynamically as an extension to most document management systems.

- Tracking of highly-sensitive documents, already done on the server side through audit logs, should be augmented with steganography. Steganography is a technique to embed requester information (who, what, where and when) into a document when it is downloaded from the server. A recovered document now provides forensic evidence for post-crisis investigations.

Source code can be similarly managed via a variety of version-control systems. Extensions, such as read-only access and steganography, cannot apply here because of the working nature of source code.

Access-Specific Planning

Of 503 corporations and government agencies polled, 33% cited their internal systems as a frequent point of attack.[3] Intranet-specific safety is comprised of two parts: access and information flow.

- **Access** refers to both *ingress* and *egress* of information systems as well as critical information applications. A plethora of secure login systems are available from smart cards to polymorphic password tokens and biometric devices. *Other factors, such as **auditing**, **actual vs. intended usage** and **ensuring logoff**, are just as important.* Proximity badges, which use short-range RF devices to communicate authorization information to nearby computers, are finding their way into many businesses as a means to provide more security while maximizing user acceptance. Proximity badges are highly recommended as a secondary means of login authorization and for ensuring unattended logoff, although they tend to be misused. In one case, a hospital equipped all personnel with proximity badges for automatic login. “Doctors didn’t like always having to type in a password.[4]” This

particular use of proximity access control systems is troublesome because gives a false sense of security, yet the hospital is considered fully compliant with HIPAA[5] regulations.

- **Information flow** refers to ad-hoc documents and messages exchanged within and/or outside of an organization's network. The popularity of IM and document swapping via email are two prime areas for security review. Companies should augment employees with their own custom IM packages that have the controls to: transmit using a secure protocol and track/log access between outside persons or large transfers. For emailing of documents, encryption is desired, but many times too difficult to use. Solution providers, such as Sigaba, provide enterprise-wide encryption proxies on top of standard internet services. Another promising technology touted by magiQ Technologies, is the use of quantum cryptography as a method to ensure "a message has been securely delivered between two parties – and that no copy exists."[6]

Conclusion

It is important to assess your organization's mitigation SOP for informational losses. The mitigation pre-planning process allows an organization to assess its information liability and decisively take risk. And most importantly, it provides a solid foundation for any post-crisis investigation.

About the Author

John C. Checco (John.Checco@Checco.com) is a member of ASIS and founder of bioChec™ (http://www.bioChec.com), an implementer of IS security solutions.

**** The author is not associated in any way, does not exclusively endorse, nor receives any fees from any of the products/companies mentioned in the article.*

---

[1] American Society for Industrial Security, 2000.
[2] "Crew Resource Management," Dennis L. Rubin, Firehouse Magazine, July 2002.
3 "2002 Computer Crime and Security Survey," Computer Security Institute.
[4] "Security Goes the Distance," George V. Hulme, Information Week, January 13, 2003.
[5] The Health Insurance Portability and Accountability Act of 1996
[6] "Security's Next Steps," Brian Fonseca, InfoWorld, January 13, 2003.