Avoiding I.S. Icebergs

Part four of "Audits, Assessments & Tests (Oh, My)" delves into information systems auditing, the often maligned but always necessary practice of evaluating technologies and security procedures to ensure they work as intended. (BY DAN SWANSON).

INFORMATION SECURITY EDITOR'S NOTE: This is the final installment of a four-part series on information systems security testing. This article explores the audit's assurance role regarding information security and outlines approaches and methodologies. As with all Secure Strategies articles, this feature is targeted to the beginner infosec professional, though more experienced practitioners will also find it useful as an update on what's available and in use today.

Imagine you're the captain of the R.M.S. Titanic, standing on the bridge as it steams across the frigid North Atlantic under a moonless sky. The ship's architect boasted of her invincibility, but you still station hands on the bow as lookouts for icebergs drifting in the black waters. After checking your course and issuing instructions to the crew, you retire for the evening, assured all is well.

Several hours later, you're shocked out of your slumber by terrible vibrations and a horrific wail of buckling metal. Your worst fears are confirmed when you reach the bridge; the ship struck an iceberg despite your precautions. At this point, it doesn't matter how or why it happened; the damage is done and your ship is going to the bottom.

What does this have to do with information security? The same scenario could happen to any organization that deploys security technologies and policies but doesn't audit its systems and personnel compliance. Routine, independent reviews of security systems and procedures not only ensure an organization has adequate protections in place, but confirm that they are working as designed-and that employees are using them effectively. Audits will highlight an organization's strengths and weaknesses, and make recommendations for improvement.
An audit of the Titanic's systems would have revealed if the ship was going too fast, or if a design flaw prevented it from turning quickly, or if the freezing ocean water made the hull's inferior alloy brittle. For an IT-dependent organization, an audit is a tool for ensuring you're secure, on course and steering clear of danger.

**Defining Tasks**

Although security still lags in priority compared to other business functions—particularly those that generate revenue—many organizations are now investing huge sums of capital and resources into information security. Management is beginning to recognize the legions of barbarians probing systems for weaknesses and waiting for a mistake to exploit. Just look at what happened last month with Western Union. Admins doing routine maintenance accidentally left a credit-card database unprotected, and a few hours later more than 15,700 customer credit-card numbers had been stolen.

Security is essential since the fate of many organizations rests on the integrity of their digital information. Auditing is the mechanism that management can use to ensure the company's information is guarded effectively, that employees are adhering to policies and procedures, and that new products and services are incorporating security into their basic design. Auditors are not ubiquitous inspectors that delve into every nook and cranny of an organization's systems. Rather, an auditor will examine select policies, procedures and functions for individual system performance, or conduct a series of select reviews and extrapolate the results to develop an overall picture of the organization's security posture.

How an audit is approached depends greatly on who wants the audit and the purpose behind it. A HR director may want to know how many former employees still have access credentials, and how long the accounts remained active. An IT director may want the same information, but will also want to know the level of access and if these accounts have been used since the employees left the organization. A technical security audit may test intrusion detection systems (IDSes) to check if they are performing as designed and if the organization has policies for addressing new threats. A general organizational audit requested by upper management could cobble together pieces of the previous examples to develop a global picture of the organization's overall security.

Some may perceive the tailoring of results as pandering to the ones paying the bill, but such targeting of the final analysis is critical to the audit process. Above all else, audits should identify areas needing attention and provide recommendations for improvement. If the manager, division vice president or board member doesn't understand the audit report— or, if it doesn't address his or her area of concern—the exercise is meaningless.
Standards of Measure

Auditors will often use the same tools and methodologies as penetration testers and assessors when conducting a review of systems and procedures. It makes sense for an auditor to test an organization's perimeter to ensure that the firewall is strong, or that databases are appropriately segregated from the Web server. The difference between auditing and other security evaluations is that it measures the outcome against prescribed standards of performance.

There is no one standard for electronic or physical security. Even the smallest organization will have multiple physical and technical security systems, making specific standards applicable only to specific applications, policies and processes.

The yardstick used by auditors can be anything from the performance expectation of an organization to government regulations to generally accepted industry standards. If managers want to know the effectiveness of the company's password-protection policy, for instance, the standard of measurement would be the number of employees adhering to and violating the policy. For applications such as authentication systems and firewalls, the audit could measure their effectiveness against the manufacturer's specifications. Or, for those seeking ISO 9001 or BS 7799 certification, an audit will examine an organization point by point to see how well it stacks up to the standard's specifications.

For the health care industry, for example, audits will be a critical component for ensuring compliance with the Health Insurance Portability and Accountability Act (HIPAA), which prescribes specific standards for ensuring patient confidentiality and the electronic transmission of medical data. Health care organizations that fail to comply with these federal regulations will face criminal charges and huge fines. Hospitals, physician groups and insurers will likely use audits to evaluate their systems against HIPAA requirements and use the results to make improvements.

Standards and measurements are critical to an audit. Without a baseline for gauging performance, there is no way an organization can judge the effectiveness of its systems or plot a course for improvement.

Auditing Methodologies

While auditing is an evaluation of compliance to set standards, there's no one-size-fits-all method for conducting such an assessment. Auditors will use different approaches to evaluate security systems based on an organization's objectives and system configuration. Both the area being evaluated and the purpose for the review dictate the audit approach.
The four basic approaches to security auditing are an organizational audit, results-based audit, point-in-time audit and an extended-period audit. Each method focuses on different functions and scope to produce reports ranging from a snapshot of a specific application's performance to a system-wide evaluation of security effectiveness.

An organizational audit reviews the frameworks an organization has in place for managing security and protecting vital assets. It seems obvious, but many organizations fail to adequately support security functions on par with growth or changing circumstances. Other organizations that perceive their security systems as functioning well will sometimes allow their quality control to lapse.

Auditors conducting an organizational audit will check the systems and applications, but are really looking to see if security and IT managers are using best practices to keep their systems operating effectively. Sure, SSL meets the company's B2C e-commerce needs today, but does the organization have a strategy for developing more robust authentication systems in response to greater privacy needs?

During an organizational audit, an auditor will meet with management teams and key personnel to develop a list of security programs and resources, evaluate the current security threats facing an organization, and review the security successes and failures for a given period. Based on the outcome, the audit report will highlight the organization's strengths, flesh out its weaknesses and make recommendations for maintaining best practices and eliminating shortcomings.

A results-based audit is an approach in which the auditor reviews the security knowledge and practices within individual business units. By assessing the security understanding of unit managers and staff, an auditor can gain a sense of the overall security program's effectiveness.

Once an organization has made a commitment to security, it wants to ensure the investment is not being undermined by poor practices. Quantifying results can range from evaluating the security education program to assessing how different business groups incorporate security into their daily operations and functions. Are employees guarding against social engineering? Are DBAs changing default admin passwords? Is the R&D team thinking about security measures for the next generation of the company's flagship product?
Results-based audits are especially important to e-commerce enterprises, which operate in an environment with constantly changing security threats. The Western Union breach happened because the IT staff disabled database-encryption protocols and left the network connected to the Internet while performing routine maintenance. Western Union said it was an isolated incident, but security experts pointed out several flaws—all human error—that could have contributed to this incident. An audit in this case may have revealed some of the flawed practices. Technology is only as effective and secure as the people flipping the switches.

A **point-in-time systems audit** employs diagnostic tools, often the same tools used by an organization’s IT staff (as well as outside hackers) to gauge the effectiveness of a security maintenance program and probe for unknown weaknesses in the organization’s defenses. Many organizations become comfortable with their internal evaluation methods and fall into a routine of diagnostic tasks that reveal few weaknesses. An independent audit, using the same tools, can sometimes find overlooked security gaps.

The fatal flaw in most antivirus programs and intrusion detection systems is that they typically react to yesterday’s threats. Malicious users are constantly coming up with new vectors of attack to penetrate defenses and capture digital goodies. IT professionals may believe their security measures are working as intended, and for today’s risks they may be right. But when tomorrow’s attacks appear, today’s defensive measures may be inadequate to the task.

An auditor shouldn’t find many gaps in an organization that has an enthusiastic security staff on the payroll. After all, most infosecurity professionals understand the evolution of threats. What an independent auditor brings is a fresh perspective to judging systems’ performance. An auditor looks at applications from a different perspective, comparing their use in the host organization to that in peer organizations, and makes recommendations for better use of existing resources. Using best practices sounds like a cliché, but organizations sometimes need to hear an independent voice to keep them on the straight and narrow.

An **extended-period audit** is a measure of quality assurance of security systems and personnel over a period of time. Similar to an organizational audit, this method uses an initial audit of a number of systems to establish a baseline. Over the course of weeks or months, successive audits will measure the organization’s progress in correcting problems and improving performance.
While other forms of auditing measure current conditions and operating effectiveness, an extended-period audit attempts to predict future performance based on current practices. IT professionals will cringe at the thought of such a complacent statement, but the goal of this audit is not to say, "If an application or policy works today, it will work just as well tomorrow." The auditor is looking for evidence that the organization has good practices for addressing changing circumstances, threats and technology. How the organization updates itself is the key indicator for future performance.

The extended-period audit is a useful tool in the development of new products and services. When developing a new e-commerce venture, an audit can be performed to see if security measures (and the appropriate level of security) have been included. As products progress from design to development to release, periodic audits can help determine if an appropriate level of security is being built into them.

The results of an extended-period audit will either confirm the security staff's effectiveness or reveal shortcomings for management to address. If few problems are found and the organizational environment remains unchanged, a successful extended-period audit can be a good indication of continued smooth sailing.

Audits are not confined to these basic forms. Different audit approaches reveal different views of an organization's security effectiveness. An organization can tailor an audit to meet its specific needs. When conducted in concert, the four methods can produce a comprehensive view of an organization's overall security posture.

**Independent Perspective**

Just as finance departments have comptrollers and auditors to keep expenditures in check with budget allocations, executive management and security departments need an independent arm that checks the effectiveness of security policies, procedures and systems.

Organizations should have an internal auditor or auditing team acting as a quality-control mechanism for systems' performance and operations. While IT managers and security staff will make performance and progress reports on their activities to management, an auditor should file unbiased reviews of security.

Internal auditors will typically judge security performance based on accepted standards, report successes and problems independently to management, make recommendations to the IT staff for improvements and ensure problems are resolved in a timely manner. Having this function in place may help IT staffers anticipate new security problems or identify security flaws in products before they're pushed to market.
Not every organization has the luxury of internal audit capabilities. Outside auditors and consultants are often used by organizations with a small staff or limited security expertise. Those embarking on large auditing projects may also require third-party help. Independent auditors should enhance the function of internal teams, since they should offer skill sets not present in the organization's internal audit team.

There's no right or wrong answer for who should do auditing, so long as it's done by auditing professionals who use accepted standards.

**The Case for Auditing**

In Austin Powers, comedian Mike Myers's parody of the '60s spy genre movies, the character Dr. Evil decides to kill his swinger nemesis by putting him on a machine that slowly dips him into a pool of ferocious, mutant sea bass. It's painfully obvious to everyone that Austin Powers can easily escape the situation, but Dr. Evil dismisses their warnings and departs assuming all will go according to plan.

Naturally, Powers escapes and thwarts Dr. Evil's plans. The scene works for Myers's purposes, but such cavalier attitudes in the infosecurity world could mean the life or death of an organization. Assuming security systems are functioning as designed and employees are following policies without auditing checks is worse than having no security.
Some Conclusions

1) Auditing is management's tool for making sure the entire organization has the resources, systems and processes for maintaining effective and efficient security. An audit will tell management that business units understand the importance of security and adhere to policies, whether key systems are secure and if programs are in place for continually updating and improving safeguards against internal and external threats.

2) Senior executives may not understand the technical threats posed by crackers, vulnerable systems, hostile code and intentional or accidental employee misuse. But they know a lot about losing market position and the consequences of compromised customer information.

3) Auditing is an assurance tool for management to know that all that can be done is being done.

4) Appropriately supported security and routine auditing provides a certain level of assurance that an organization's security functions are proactive and effective against current and future threats.

Unlike Captain Edward J. Smith, who allowed the Titanic to steam blindly into the dark, executives with strong auditing functions can steer their enterprises clear of deadly icebergs.

DAN SWANSON, CMA, CISSP, CISA, CAP is the AVP of Professional Practices at the Institute of Internal Auditors (IIA) in Altamonte Springs, Florida. Dan was previously a Winnipeg-based management consultant and is a frequent writer on IT audit and management practices. Dan is also a past Winnipeg chapter president for both IIA and ISACA organizations and has chaired ISACA International's publication committee. He has also been the chair for the Information Protection Association of Manitoba (IPAM) - a security officer user group dedicated to improving security management practices.