Improving Enterprise Security

Security is a balancing act. Enterprises need security that is appropriate to the risks to their information assets; to attain that goal, they must find the right mix of people, processes and technology.

Perfect security is impossible, but enterprises should aim to provide a level of security appropriate to their business and operation needs. Security is achieved by a balanced focus on three factors: people, processes and technology. It can't be attained by focusing on any one of these factors to the exclusion of the others. This issue of the Security and Privacy Spotlight examines how enterprises can improve their security by strengthening one or more of these elements.

Any enterprise that wants to make significant improvements in security must take a broad view of its information assets and understand their value, and the threats and vulnerabilities to and of these assets. It's very easy for an enterprise to focus on countermeasures that address a specific, topical risk — for example, physical attacks by recently terminated employees — to the detriment of overall security. At best, such initiatives can divert resources; at worst, they can create a false level of confidence or even introduce new vulnerabilities. In short, an enterprise must not lose sight of the big picture.

People

People often are the weakest links in security initiatives. To solve this "people problem," enterprises can:

- Sufficiently improve employee attitudes toward security by encouraging them to behave more responsibly

- Look for a way to "save people from themselves" by exploiting technology that reduces the human factor in security

John Pescatore posed this question to Gartner's security, privacy and risk research community: "If you had $100 per user to spend on one thing to increase the level of information security at your company, what would you spend it on?" The community was evenly split over the answer: one half favored investment in stronger authentication; the other half favored user awareness and education. He argues the case for stronger authentication in "It's Time to Get Smart About Smart Cards" (COM-13-9590); Conal Mannion provides a counterpoint in "Policy, Process, Awareness ... and Smart Cards" (COM-14-3807).

Kristen Noakes-Fry looks at a different problem with the human factor in "Unmasking Social-Engineering Attacks" (TG-15-1287), which considers various attacks that exploit human nature and suggests how enterprises can protect against them. As with many security issues, the solutions combine people, processes and technology.

Processes

An information security policy is a keystone for all enterprises. However, although many enterprises have policies and may even train employees on them, very few foster a culture of security awareness that promotes the recognition and reporting of security issues. In “Building a Security-Aware Enterprise” (https://www.gartnerg2.com/research/rpt-0102-0010.asp?SID=40434), Rich Mogull describes the management initiatives that are required to create a security-aware culture based on a model that is surprisingly close to home.

Technology

Information technology is a key enabler for all enterprises, and successfully and *securely* implementing new technology is crucial to e-business and the net-liberated organization. Roberta Witty considers how the enterprise can successfully manage risk exposures associated with the use of technology across the entire project life cycle for all technology products, services, delivery channels and processes in “Elements of a Successful IT Risk Management Program” (SPA-15-1752). She defines information security requirements and explains how to implement enterprisewide policies in “Information Security Policies” (DF-15-2327).

In “Enterprise Smart Cards: Securing Buildings, PCs and Corporate Networks” (SEMC-WW-DP-0090), Andrew Phillips looks at how enterprises can leverage investment in “smart cards” by combining information system access control and physical access control in the same device. This is a good example of how a single technology can have multiple security benefits. Nevertheless, successful implementation must take account of people and processes: however strong a technology, it can’t in itself address all of an enterprise’s security needs.

For enterprises looking for outsourcing security solutions, Alain Dang Van Mien provides a review of the “Big Four” network and systems management (NSM) vendors — BMC Software, Computer Associates, Hewlett-Packard and IBM — in “The NSM ‘Big Four’: Security Dynamos or Dinosaurs?” (DF-14-5598).

Features

“It’s Time to Get Smart About Smart Cards” (COM-13-9590). Using smart cards for corporate PC security. **By John Pescatore**

“Policy, Process, Awareness ... and Smart Cards” (COM-14-3807). Contrasting user education and awareness with smart-card security. **By Conal Mannion**

“Unmasking Social-Engineering Attacks” (TG-15-1287). How employees can be manipulated into breaking enterprise security, and how to prevent it. **By Kristen Noakes-Fry**

“Building a Security-Aware Enterprise” (https://www.gartnerg2.com/research/rpt-0102-0010.asp?SID=40434). Integrating security into the enterprise’s structure and culture. **By Rich Mogull**

“Elements of a Successful IT Risk Management Program” (SPA-15-1752). Building an IT risk management program. **By Roberta Witty**

“Information Security Policies” (DF-15-2327). Defining information security requirements and implementing consistent policies enterprisewide. **By Roberta Witty**

“Enterprise Smart Cards: Securing Buildings, PCs and Corporate Networks” (SEMC-WW-DP-0090). How to avoid the pitfalls of smart-card implementation. **By Andrew Phillips**

“The NSM ‘Big Four’: Security Dynamos or Dinosaurs?” (DF-14-5598). NSM vendors and their security products, market positions and methodologies. **By Alain Dang Van Mien**