THE SECURITY REVOLUTION

Creating a Culture of Security

PEOPLE, NOT FIREWALLS, ARE YOUR COMPANY'S FIRST LINE OF DEFENSE

There's nothing that gets people's attention like handing them a crisp $100 bill.

That's how William Hugh Murray remembers a colleague rewarding an employee who followed the corporate security policy and challenged Murray's friend for strolling around the building without his required security badge. "People start asking other people about their badges, and the wearing of badges gets good really quick," chuckles Murray, a Certified Information Systems Security Professional (CISSP), consultant with TruSecure Corp. in Herndon, Va., and Corporate Secretary of (ISC)², the International Information Systems Security Certification Consortium, a non-profit security training and standards organization based in Framingham, Mass.

That's an example of the kind of creative, consistent reinforcement necessary to forge a culture of security — a work environment in which employees at all levels understand and commit to the need to protect the enterprise not just from physical security breaches, but also virtual intrusions from hackers or viruses. More than just a cost of doing business in the post-9/11 world, creating a culture of security can actually boost productivity and profits by reducing downtime and system outages, says Hal Tipton, CISSP and former president of (ISC)².

But to achieve these business benefits, senior executives must foster awareness of security risks through education, training and consistent enforcement of proper policies. Everyone from the CEO to the accounts payable clerk must commit to following proper security practices.

DEFINING YOUR CULTURE

Creating a culture of security is no different than creating a "culture of quality" or a "culture of customer service." The initiative can come from anywhere in the organization — in this case, likely the CIO or Chief Security Officer. But senior management — whoever has the authority to administer recognition and rewards — must promote the change by consistently communicating the business implications of security, and enforcing security policies. At each step in the management hierarchy, says (ISC)²'s Murray, supervisors must evaluate and reward those who report to them based on their adherence to good security practices.

And there's no room for breakdowns. If an employee goes to a manager to report a security lapse and is brushed off, that staffer won't speak up again. Similarly, if management preaches the importance of passwords but then casually hands out the same temporary password to every new employee, "The immediate message is that management doesn't take this very seriously," Murray says.

"MAKING CHANGES IN ANY ENVIRONMENT NEEDS TO BE INCREMENTAL, AND IT NEEDS TO BE DONE CONTINUOUSLY. YOU CAN'T JUST HAVE A SECURITY AWARENESS PROGRAM THAT RUNS FOR TWO MONTHS."
— JOHN COLLEY, VP/DIRECTOR (ISC)²

The need for top-down leadership — and to ensure security spending is focused on the most critical risks — is reflected in the rise of chief security officers (CSOs). These new executives boost efficiency and security effectiveness by coordinating security efforts across the organization, managing outsourcing contracts and mapping security measures to real business risks, says Steve Hunt, a Vice President at Giga Information Group in Chicago. He knows of about 80 CSOs who report to the CIO level or higher and who coordinate security across all types and sizes of businesses. Hunt expects companies to increase spending on security software by 5 percent this year. "However, in 2002 proportionally more money is being spent on management personnel than in previous years, as part of an effort to ensure security spending delivers business benefit. The move to CSOs is part of this trend, and is working," Hunt says.

CIO
Custom Publishing
Advertising Supplement

DOING DUE DILIGENCE

BASIC STEPS TOWARD CREATING A CULTURE OF SECURITY IN YOUR ORGANIZATION

- **Identify who is responsible** for designing and implementing your information security policy.
- **Communicate** that policy with on-going awareness and training programs; establish clear expectations for managers and employees.
- **Create and test** a business continuity program to ensure survival of critical data, equipment, and networks and to keep valuable employees.
- **Identify and control** critical systems with password management, installation of security patches and fixes of common vulnerabilities. Links to external networks may require encryption, firewalls, authentication and/or intrusion detection systems.
- **Stay vigilant** with security reviews, audits, and vulnerability assessments. Monitor vendors and the Web to stay current on latest threats.
- **Make sure** the board of directors and corporate officers annually review the status and outlook of your information security program.
- **Provide adequate training** and encourage certification of your security staff.

Source: (ISC)²

REMINDERS AND REINFORCEMENTS

Micki Krause, Director of Information Security at a healthcare company on the West Coast, recently saw firsthand how easily security breaches can occur. She hired outside auditors to test her company's security awareness, and the auditors had a few concerns. In one case, auditors found staff members testing a new system had accidentally exposed the network to outside hacks. In another, auditors posing as support staff were able to get 16 of 22 employees to reveal their user IDs and passwords.

Subsequently, Krause plugged the holes in her organization's security procedures — and just as importantly, she also rewarded the six employees who refused to disclose their IDs and passwords to the fake "support staff." But her experience illustrates that even with top-down awareness, creating a culture change doesn't happen overnight. "Making changes in any environment needs to be incremental, and it needs to be done continuously," says John Colley, a London-based Vice President and member of the board of directors of (ISC)². "You can't just have a security awareness program that runs for two months."

Giga's Hunt recommends an ongoing security-awareness process that includes:

- Identifying critical information assets and risks
- Crafting a security policy
- Implementing, administering and auditing the policy
- Continually reassessing risks.

To ensure a culture of security, security proponents and managers may also have to change some of their own behavior. Too often they get discouraged after a security proposal is rejected by senior management because the risk may not be enough to justify the cost. "You've got to understand `no' is a perfectly appropriate answer," says Murray, especially since budget conditions, or management's perception of the risk, are subject to change. Department managers who have a budget all got it the same way — "They asked for it and got told `no' a lot," he says. As long as the risk and cost are explained, it's up to the business managers to decide whether the cost of the security plan is too high. But Murray feels it is up to him to keep raising security concerns so business managers can decide how much to spend to reduce their risks.

Most companies aren't doing enough to create a culture of security, says Bruce Murphy, CISSP and CEO of Vigilinx, Inc., a provider of managed security services, consulting and security related information in Parsippany, N.J. "They don't understand the value, since it is hard to quantify" the hard-dollar return on security spending. Many companies also underestimate the importance of people and processes in creating a culture of security, he says.

Krause concurs, saying creating a culture of security involves communication, rewards and incentives. "In fact, security is not just technology, it's really people and processes."

The Big Picture

INFORMATION SECURITY PROBLEMS ARE GLOBAL, BUT SOME REGIONAL SOLUTIONS ARE UNIQUE

Among the greatest security challenges now facing senior executives worldwide are:

- The increasing sophistication of network security threats, and the speed at which they change.
- The ongoing need to educate staff about the importance of information security.

And although some nations and agencies are crafting unique local solutions, studies show that most businesses are not doing enough to overcome these common global problems.

Among recent research findings:

- **Senior Leaders Recognize the Threat.** In a fall 2001 survey of 459 CIOs and business managers, Ernst & Young found that 70 percent of respondents cited ever-changing and increasingly sophisticated security threats as their top concern. Employee awareness of security threats was the number two challenge, cited by 66 percent of the respondents.
- **Most Companies Aren't Doing Enough to Fight Back.** In a summer 2001 survey conducted by *CIO* Magazine and Cambridge-Mass.-based digital security firm @stake, two-thirds of respondents said they did not have a well-defined company-wide security policy or plan.

Faced with this disconnect between awareness and response to global security threats, organizations such as the International Organization for Standardization (ISO) and (ISC)² are working to create new international security standards. The European Commission has even unveiled a plan that would send hackers and writers of computer viruses to jail for years.

But just as vital as policy-making is education — making global business leaders aware of the risk of embarrassing and costly security breaches, as well as potential shareholder lawsuits that could hold senior management personally responsible for such breaches.

SAFEGUARDING PRIVATE DATA

Intrusions and viruses aren't the only issues on the minds of global business leaders. Regional privacy laws are also a concern — and they vary by nation. In the U.S., for example, the Health Insurance Portability and Accountability Act (HIPAA) prescribes strict standards for how healthcare providers must protect patient information. But other privacy standards are less clearly defined in the U.S. and elsewhere, and inconsistently enforced from country to country. The only way to stay on top of and within these standards, global security experts say, is for companies to designate staff in each of their global marketplaces to understand individual countries' rules and ways of doing business so processes can be adapted to meet those local requirements.

Some examples of regional variances: some European countries have different definitions for what constitutes a legally acceptable digital signature for an online transaction. And while the European Union's Data Privacy Directive prevents the collection of most personal data unless the consumer authorizes it, the laws that define "informed consent" vary widely from country to country, says John Colley, Vice President of (ISC)², in London. "What may be perfectly legal in the [United Kingdom] may be illegal in Germany, or vice versa," he says.

Enforcement can also vary across global regions. For example, while Hong Kong has adopted an ordinance similar to the EU's privacy directive, it relies on companies to police themselves rather than on the stricter government enforcement found in Europe.

To cope with the differing global requirements, many companies that do business both in America and in Europe have established "safe harbors" in which they promise to safeguard private data about EU consumers under the laws that apply in those consumers' countries. But rather than using technology to provide special safeguards, says Colley, the safe harbors are usually "legal constructs more than anything else, based on trust and business expediency" between trading partners.

LEADING THE CHARGE

Mindful of global security threats — and the diversity of regional solutions being deployed against them — several international agencies are at work on various information security standards.

The International Standards Organization (ISO) in December 2000 released its ISO 17799, which it calls "a comprehensive set of controls comprising best practices in information security." The 10 CISSP domains, which are closely related to the ISO control areas, include:

- Access Control Systems and Methodology
- Applications and Systems Development Security
- Business Continuity Planning (BCP) & Disaster Recovery Planning (DRP)
- Cryptography
- Law, Investigations & Ethics
- Operations Security
- Physical Security
- Security Architecture and Models
- Security Management Practices
- Telecommunications and Network Security

Clearly, there is no single solution to eliminate the global security threat, but increased awareness and action will minimize risk.

WHY SPEND ON SECURITY?

HOW TO JUSTIFY COSTS AND SHOW BENEFITS

Potential costs of lax security:

- Lost sales due to system downtime
- Loss of proprietary customer or product information
- Drop in stock price due to security breach
- Shareholder lawsuits over lax security
- Customer lawsuits over loss of privacy
- Regulatory penalties

Potential benefits of strong security:

- Increased sales and productivity
- Tighter integration with customers, suppliers
- Increased customer loyalty
- Competitive advantage over less secure competitors
- Lower premiums on "hacker" insurance

Source: Strategic Directions

ALIGNING SECURITY AND BUSINESS

10 QUESTIONS TO ASK YOURSELF ABOUT SECURITY:

1. Does your board of directors recognize that information security is a board-level issue that cannot be left to IT alone?
2. Is there clear accountability for information security in your organization?
3. Can your board members articulate an agreed set of threats and critical assets? How often do you review and update this?
4. Do you know how much is spent on information security and what it is being spent on?
5. What would be the impact on the organization of a serious security incident?
6. Does your organization see information security as an enabler? (For example, by implementing effective security, could you enable your organization to increase business over the Internet?)
7. Has your business assessed the risk of getting a reputation for slackness in security?
8. What steps have you taken to ensure that third parties will not compromise the security of your organization?
9. How do you obtain independent assurance that information security is managed effectively in your organization?
10. How do you measure the effectiveness of your information security activities?

Source: Ernst & Young

The ROI of Certification

SECURITY CERTIFICATION ISN'T JUST A COST; IT'S AN INVESTMENT

An hour a day, seven days a week, for nine months. That's the time commitment made by Chuck Bianco, a 17-year security veteran, in preparation for his Certified Information Systems Security Professional (CISSP) certification in November 2001. "I'm as proud of that certification as anything else I've done in business," says Bianco, Manager of IT Examinations for the U.S. Treasury Dept. in Dallas. But more than just new credentials and personal pride, this certification has given Bianco a strategic new position at a key time in his enterprise's battle against information security threats.

People such as Bianco are a hot commodity these days. In an increasingly security-conscious world, CIOs need professionals like Bianco who have the certified skills to secure corporate data and systems. And although certified security personnel do cost more money, the ROI is pretty clear, experts say. "You're buying protection in case of a shareholder lawsuit resulting from a security problem," says David Foote, President and Chief Research Officer at research and consulting firm Foote Partners in New Canaan, Conn." Boards of directors are getting involved, and they realize a high-profile Web breach, or a privacy breach, could harm the reputation of a company and impact revenues," Foote says. "By saying you have the CISSP on staff, you can show you took prudent and reasonable precautions — you did the best you could," Foote says.

The CISSP certification is granted by the International Information Systems Security Certification Consortium (ISC)², a non-profit security association in Framingham, Mass. The certification is "like a badge of honor" that promises its holder can be trusted, says Victor Keong, a partner in the Security Services Practice of Deloitte & Touche in Ontario, Canada. "When we do security consulting, the customer's prime concern is `are my secrets safe?'" Certification can help assure them the security professional they hire is not himself a hacker, he says.

Along with three years of practical experience, CISSP exam applicants need in-depth knowledge of the 10 domains within (ISC)²'s Common Body of Knowledge (CBK). The CBK is a central, standard list of key security knowledge. Domains within the Common Body of Knowledge include security architecture and models, cryptography, operations security, access control systems, and law and ethics. Hal Tipton, a former (ISC)² president, describes the CBK as the topics a security professional "needs to know enough about so they can carry on an intelligent conversation with their peers."

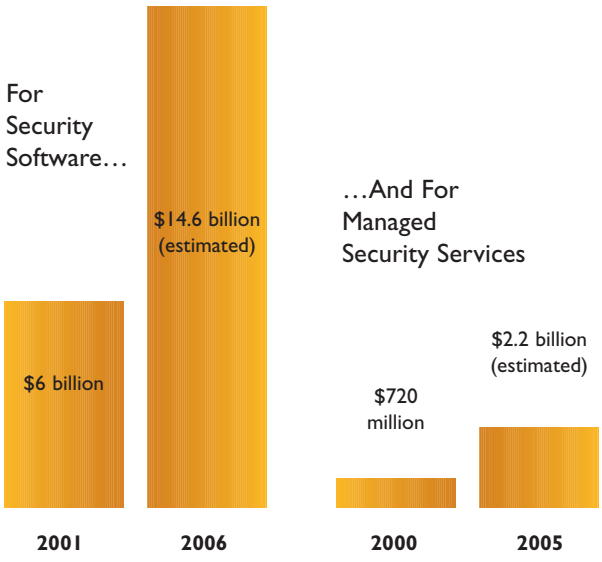
(ISC)² also offers review courses and online study guides for its certification exams.

More than showing off the proper skills, security certification tells an employer a security professional is truly knowledgeable and experienced in the field, rather than someone who has just read some books and can use the proper buzzwords, says Tipton, who is now a Security Instructor and Administrator of security training programs.

Employing certified security professionals also helps protect senior management, which can be held personally liable if they fail to take proper security precautions required by law, he says.

"Top management doesn't have the time to really study all these things and understand what the requirements are," Tipton says. "That should be up to the qualified security people on their staff, and certification is a way of being assured they are properly qualified." ■

WORLDWIDE SECURITY SPENDING ON THE RISE



Source: International Data Corp.

YOUR RESOURCE FOR MORE CISSP INFORMATION

Contact us at:

(ISC)² Inc.

PH (888) 333-4458 (North America)
(727) 738-8657 (North America)

FX (727) 738-8522 (North America)

EM info@isc2.org

W www.isc2.org

When contacting (ISC)², please provide your name, full mailing address, telephone and fax numbers, and your e-mail address.