SearchSecurity.com E-Guide

# Identifying and Addressing Evolving Threats

The frequency of data breaches is on the rise and progressive organizations are fighting back. Electronic intruders are becoming more determined and sophisticated in their attacks and today's flat world full of complex relationships makes it difficult to distinguish between internal and external threats.

Read this expert E-Guide and learn what chief information security officers (CISOs) said were their biggest challenges of 2008 and what lies ahead for 2009. This E-Guide will also explain the 4 pillars of an information security strategy, as well as how to make security decisions in a strategic way so that business units will have added value and can be integrated smoothly along with other enterprise initiatives such as compliance.



TechTarget
The Technology Media ROI Experts

SearchSecurity.com E-Guide

# Identifying and Addressing Evolving Threats

## Table of Contents:

# Better Safe Than Sorry: Why You Need an Information Security Strategy, and How to Build One

Nalneesh Gaur and Mike Heindl

Last year, a business disaster of the worst kind—the loss of information kind—struck TJX Companies. When the Framingham, Mass.-based parent of discount retail store chains reported that 45 million of its customers' credit and debit card account numbers had been stolen, it spent more than US$180 million to settle with consumers, banks and network associations. It was an expensive bandage for a wound that could have been easily prevented.

Of course, TJX isn't alone. As reported in "Data Breach: Creating an Organizational Strategy" (InfoSecurity Professional, Summer 2008, page 6), there have been numerous data breaches worldwide. These incidents have brought to light the importance of information security.

Still, businesses remain reactive, responding by allocating valuable resources to tactical measures and standalone compliance efforts. Over time, quick fixes and point solutions become costly and diffi cult to manage due to the complexity of multiple and redundant solutions. What organizations need is a clear and consistent information security strategy.

## New Threats, New Regulations

Globalization makes it easier to conduct commerce anywhere, anytime. It's what New York Times columnist Thomas Friedman refers to as the "flattening of the world." No one could have imagined that this phenomenon would lead to increased crime and cyberterrorism and yet, that's exactly what has happened. Today's flat world is characterized by distributed operations and complex relationships between businesses and providers, all of which makes it difficult to distinguish between internal and external threats.

Still, consumers are increasingly aware of privacy issues and expect businesses to guard their personal data. In fact, 49 percent of consumers expect businesses to protect their information, according to Ponemon Institute's 2007 Consumer Survey on Data Security.

Government expects it, too. In the current environment, lawmakers and industry consortiums have been steadfast in passing regulations that bring information security and privacy best practices to bear. Because many of those regulations require greater accountability on the part of senior management, auditors have become more concerned than ever with verifying compliance. As a result, corporate boards in every industry are getting involved, holding senior executives responsible for security compliance and breaches.

"Today, information security is event-driven by regulatory pressures and the threat of breaches," says the former CISO of a large U.S.-based regional bank. "Unfortunately, most organizations are reactionary."

Another former CISO and the current CIO of an Oklahoma-based non-profit healthcare network provider agrees and says: "Almost three years ago, our information security program was born out of the necessity to comply with

HIPAA [Health Insurance Portability and Accountability Act] security regulations. However, our executives were not content with simply complying with HIPAA; we wanted to adopt information security best practices to comply with any future regulations."

There is no doubt that compliance is a global driver for information security. "We predominantly look at information security from a regulatory perspective," says the head of IT operations risk within a global financial institution's investment management practice. "But our culture, which is driven by a preventative mindset, is another key catalyst for our information security program."

## The Four Pillars of an Information Security Strategy

An information security strategy—and, indeed, a preventative mindset—is essential to modern-day business success because it allows businesses to prioritize their resources when addressing risks. In other words, it gives companies that have invested in various security tools and the tactics with which to use them.

Indeed, while many companies rely solely on technology to confront information risks, doing so can prove inefficient and even harmful. That's because a tools-only approach addresses threats in a piecemeal manner, which may amplify future problems. In the interest of solving problems more holistically, businesses should develop action tactics that are driven by the value of business assets and the probability of business risks, including their likelihood and their potential impact.

Leading global organizations believe that meeting information risks head-on requires an emphasis in four key tactical areas:

1. Strategic and Business Alignment: Businesses must identify information security drivers like applicable regulations, fraud and customer privacy, and then identify business assets, including their respective threats and vulnerabilities. Additionally, companies should review their existing information security initiatives, technologies and trust relationships.

2. Organization and Culture: A successful strategy must incorporate the executive tone; organizational and partner awareness; training needs, skills and competencies; and administrative and functional reporting structures.

3. Management and Governance: Management must focus on how the organization develops policies and standards, manages projects and programs, makes decisions and funds information security programs.

4. Technology: Organizations must establish a precise definition of information security that includes technology needs and standards, and how information security technology is managed. Developing an effective information security strategy requires creating a long-term roadmap with milestones that are prioritized based on risk, compliance needs and cost.

Further, a comprehensive effort requires establishing a program management office (PMO) to lead planning and execution, says the former bank CISO. Planning gives businesses a better understanding of scope, dependencies,

costs and needs. It also helps them budget resources across different groups—for example, operations, technology and information security.

Finally, it helps them reevaluate implementation activities according to competing priorities.

## Transforming Information Security

Although planning your information security roadmap is important, acting on it is critical. After all, to pick the fruits of its strategic labor, your business must move immediately to capitalize on the momentum of its efforts.

To successfully do that, start with right-sizing the scope of your project. Most information security managers mistakenly "over-scope" their initiatives when they ought to be looking for quick wins. Tackle urgent and basic problems before addressing more complex ones. For example, address pending compliance and audit issues on significant systems only before initiating an organization-wide rollout of your solution.

Following your security roadmap will inevitably require change. To help employees and executives cope, consider establishing cultural initiatives to educate and train them on new policies and revised procedures. Where necessary, implement structural changes, which may require recruiting new talent or pooling related job functions to make employees more effective and efficient. Regardless of the changes you make, understanding how your business needs will evolve is essential in leveraging new information security solutions.

Process changes that transcend all initiatives are common, so affected processes must be identified and modified appropriately to ensure that initiatives succeed.

Also critical to success is executive involvement, which requires facilitating an operational relationship between the PMO and the executives who oversee it. "Having executive management on board is paramount to the success of any information security program," says the former bank CISO. "We provided quarterly updates to the board by answering questions such as, 'Are we protected?' and, 'What are the major issues?'"

The CIO of the healthcare network gained executive support with a three-pronged approach that first involved conducting an information security assessment, then implementing the resulting recommendations and finally, educating executive and division heads on information security's strategic nature. "Education came easy in the form of two information security breaches that were small enough to raise awareness but not cause any serious damage to our organization," says the CIO. "We now meet on a quarterly basis with the board and update them with a perspective on the state of information security. We provide them with information security metrics, including a global map that depicts where our threats came from in the last three months, as well as the number of employees, contractors and partners who have successfully passed the information security training."

The head of IT operations risk adds: "We work with the business, legal, compliance, audit, operations and IT groups to articulate the vision and benefits of the information security function. Stakeholder and steering committee meetings serve as the venue, where we share the progress of information security projects, key metrics, risks and issues."

Like all strategies, an information security strategy must be regularly revisited and revised so that it addresses your company's changing business needs, as well as evolving threats and technology advances. "We periodically review the initiatives and are prepared to correct course as needed," says the former bank CISO. "This is necessary to account for budgets and the evolving threats in the business environment. For example, we created and communicated a process to respond to what was, at the time, the emerging threat of phishing."

Unfortunately, information security transformation cannot be achieved overnight; it requires an ongoing commitment, as well as the willingness to persevere through change and resistance. Not ready for the work? Consider the alternative: a costly security breach or debilitating fraud that will bring your company to its knees.

**About the Authors:** *Nalneesh Gaur, CISSP, is a principal, and Mike Heindl is a partner at Diamond Management & Technology Consultants, a consultancy firm with offices in the U.S., India and the U.K.*

# Data Breach: Creating an Organizational Strategy

Bruce Howard

It's hardly surprising these days to read stories about stolen or lost laptops, malicious hacking incidents or data intrusions. Data breaches are occurring with increasing frequency worldwide, across all industries.

According to the nonprofit research group Attrition.org, 162 million records were compromised worldwide in 2007, up from 49 million in 2006. That figure includes the now-infamous TJX Companies breach, in which some 94 million credit and debit card numbers were stolen—by far the largest incident to date. And data breaches take a considerable amount of money to mitigate: The Ponemon Institute, an independent research firm, estimates that in 2007 they cost businesses an average of US$197 per customer record.

Not even the most optimistic experts expect this trend to subside anytime soon. Electronic intruders are only becoming more determined and sophisticated in their attacks. Mike Spinney, principal of SixWeight, a public relations consulting firm and a Certified Information Privacy Professional (CIPP), says, "There are two kinds of companies: those who have experienced a data breach, and those who will."

## A Containment and Contingency Strategy

Organizations must then assume the worst will happen and create a comprehensive strategic plan that minimizes the possibility of a breach occurring and maximizes their ability to curtail it when—not if—it does.

A critical element to the success of such a plan is securing the support of executive business and IT leaders, ideally including the CEO and board of directors. Having an organizational mandate sends a clear message about the importance and necessity of mitigating data breaches. In addition, it smoothes the path toward uniting individuals from across the organization and may make it easier to secure funding for any necessary security technology investments.

Before embarking on a strategic plan, it's essential to create a team—one that includes, if possible, the chief security officer, chief information security officer, and representatives from general counsel, audit, public relations, human relations and other relevant departments.

Hord Tipton, CISSP-ISSEP, CAP, CISA, CNSS and an (ISC)² board member, says, "It is critical to have a CISO on the data breach team—someone who understands the business case and can secure the appropriate funding to ensure the organization has the proper security controls in place."

Furthermore, if the company has offices around the world, it's important that all regions are represented. This ensures a certain level of familiarity with regional or country-specific laws that is useful regardless of where the actual breach occurs.

When it comes to leadership, James Shreve, an attorney with the legal firm of Goodwin Procter, maintains that someone from the legal/compliance side of the house should manage the data breach team. "You want the process

to be unified so the organization is speaking with one voice, following one plan. For the most part, that is done through legal or compliance," he says.

## Forming a United Front

An important factor when establishing the data breach team is the inclusion of both information security and privacy professionals. In fact, due to the urgency of today's environment, many large corporations are already meshing these two disciplines to lead data breach mitigation teams.

Jay Cline, CIPP, president of Minnesota Privacy Consultants and former chief privacy officer of Carlson Companies, says that joint security-privacy operations are now starting to fall under the category of information risk management, with team leaders reporting to CIOs, CFOs or other top executive managers. "I'd say that 10 percent of Fortune 500 companies may have some kind of hybrid model like this," Cline observes.

Privacy professionals can offer considerable expertise and support when it comes to formulating data breach strategies. The International Association of Privacy Professionals (IAPP) says that its members handle matters such as legal compliance, counseling on operational and marketing strategies and the implementation of privacy policies.

A privacy professional is "a leader who understands the technical, legal and operational aspects of gathering, handling and securing personal data," says Orrie Dinstein, chief privacy leader and senior counsel for IT and IP at GECommercial Finance, "and who can establish and maintain a comprehensive strategic vision for handling all personal data of employees, customers and suppliers of an organization in a manner that is legal, secure and ethical, from the point of acquisition through the point of disposition, thereby gaining public trust in the organization's role as custodian of such data."

Consolidating power is not a goal of either privacy or security professionals. They each understand that companies can have security without privacy but cannot have privacy without security. Privacy professionals offer complementary skills that enable them to work with information security teams on breach-related plans, as well as a wide range of projects such as bringing new enterprise applications online and contracting with third-party data management firms.

"Security and privacy go hand in hand," says Jeff Reich, CSO of the information technology hosting firm Rackspace. "Privacy is a deliverable that consumers should expect. One of the most important tools used to produce this deliverable is security. Maintenance of privacy cannot be achieved without solid and consistent security practices and some tools."

He adds that information security professionals provide many of the processes and tools needed to preclude data breaches through the effective use of "preventative controls"—such as software that only allows system access to authorized users.

Chris Zoladz, CIPP, CISSP and vice president of information protection and privacy at Marriott International, agrees that security and privacy professionals bring equal levels of expertise to the table. From his perspective, the strength of information security professionals is in their ability to diagnose and rectify technology security issues

such as firewall misconfigurations or network vulnerabilities. Privacy pros, he says, "are probably better suited when it comes to addressing security issues that are rooted in faulty business processes."

In Zoladz's opinion, these two groups can learn a lot from each other. As he puts it, "I think it is in the company's best interest that there is openness to that learning. The more that privacy pros understand about IT security, the better it is for them personally in their own career development, and the more that IT security pros are familiar with privacy issues, the more complete they are in terms of their own knowledge base and careers."

## Advance Preparation

Once information security and privacy professionals are working together on the data breach team, they, along with other team members from cross-regional and interdepartmental divisions, can begin to formulate a breach prevention and response plan. One of their first steps should be to meet with the organization's board of directors, as well as regulatory and legal entities including law enforcement officials. From these groups, the data breach team should glean a relatively thorough understanding of local, national and international breach notification laws as well as industry-specific compliance regulations.

Some parts of the breach strategy must be coordinated on a regional basis. For example, in the U.S. nearly every state has a unique data breach notification law. The U.K. has taken it a step further with the recent passage of the Criminal Justice & Immigration Act, which enables the Information Commissioner's Office to impose civil penalties on organizations that "deliberately or recklessly" breach data protection rules. Other countries, including Canada, New Zealand and Australia, have issued breach notification guidelines or plan to issue legislation this year or next.

It is important to gather information around industry-specific compliance issues. Some vertical sectors, such as finance and health care, are more heavily regulated with regard to the ways they store, share and secure personal identifying data. Privacy attorneys can add significant expertise in this area.

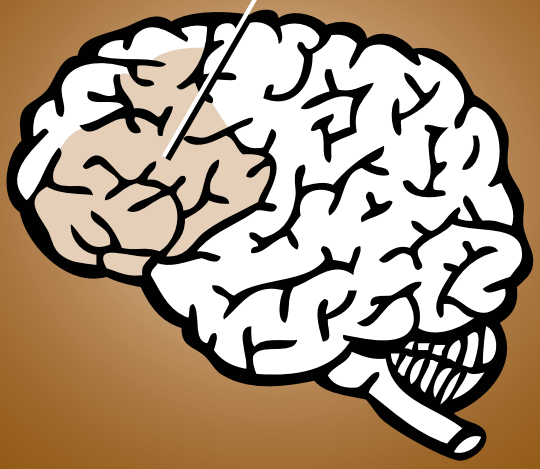
In addition, your organization's public relations officials must be prepared with crisis communications directives should a breach occur. They should be ready to talk with the media honestly and openly about what has happened and the steps being taken to resolve the breach.

## Mitigating the Breach

Now that many countries have established breach notification guidelines or laws, there is often a specified window of time within which an organization must respond—to government officials, law enforcement agencies, business stakeholders, customers and/or consumers—following a data breach. This is where having a strategic plan in place comes into play.

The IAPP estimates that, based on some of the more stringent notification laws in the U.S., the average time to notify parties and resolve a breach is 45 days. This period may vary from industry to industry and from company to company, but it is a reasonable time frame, and it allows the affected organization to remain viable and competitive.

# Memory and the ability to retain stuff.



## Live OnLine, Official (ISC)²® CBK® Review Seminar.

Nothing compares to an Official CBK Review Seminar from (ISC)², unless of course it's Live OnLine, the latest educational offering from (ISC)². From the convenience of your desktop you can enjoy the same award-winning course content*, delivered by our (ISC)² Authorized Instructors, without taking five days out of your busy schedule, or paying travel costs.

And, if working in your PJs is not enough incentive, check out the current special offers at **www.isc2.org/offer**.

*SC Magazine award winner 2006, 2007, 2008

THINK

(ISC)²®

# Looking Back, Looking Ahead: Several CISOs Share Their Biggest Information Security Challenges This Year and Their Expectations for 2009

Anne Taylor

We asked three chief information security officers (CISOs) from around the globe what their most significant security challenges were this past year. Though their answers varied—due to industry, company maturity or organization size—their concerns are similar. They include identifying vulnerabilities, managing compliance, ensuring adequate risk management and demonstrating value to the business.

"All these challenges resonate with me," says Patricia Myers, (ISC)² Board Chair. "They're perennial challenges. When I started ... in the mid-1990s, I was told, 'You have 18 months to create the information security program.' It was very entrepreneurial. [The] budget hadn't been set. We had five people dedicated to it.

"But compliance regulations are much more granular today ... IT departments have more people and different teams—disaster recovery, business continuity, risk management. Technology has not helped us, but rather given us challenges to stay on track. We'd like to draw a line under these issues and say they're fixed, but there's always a new twist and remediation to do."

The 2008 Global State of Information Security study supports this recurring challenges theme. The study is in its eleventh year and—as has been the case for the past decade—when asked to identify the most critical business issues or factors necessitating spending on information security, the majority of respondents point first to business continuity/disaster recovery, followed closely by internal policy and regulatory compliance.

"These are ongoing challenges because as companies grow, change, merge, acquire, they have to reconsider the security impacts of these changes," says study coauthor Mark Lobel, a principal with PricewaterhouseCoopers (PwC). "For example, business continuity has been a factor all along, but it took a huge jump in priority after Sept. 11."

These findings and correlations are subtly echoed in the CISO discussions. Ultimately, though, our three CISOs express optimism about overcoming these challenges—and offer advice based on their own experiences.

## 2008: Looking Back

The need to provide value to the business is a unifying theme among the group. For example, Nelson Novaes Neto, CISO at UOL in Brazil, says ensuring adequate risk management and security metrics management is a challenge his organization faced this past year. He adds that it's clear he needs to work closely with the business to meet organizational objectives.

With regard to risk management, Neto says, "The main challenge for the security area is to guarantee that organizational decisions are supported by a risk management process. But to make that efficient, it is necessary to avoid conflicts between the process and the organization's objectives.

"Security decisions must support business units in a strategic way so that product will have added value," he continues. "Security cannot become an obstacle for the business, impacting the investment and time-to-market. Competition in the global markets demands prompt and transparent development processes."

Similarly, with security metrics management, Neto must justify investments—"a hard task," he says. "We need metrics to be tangible, but to get this, we need to adapt processes and technology in a manner that data is turned into information and the information is well managed."

Sekar Sethuraman, IT security head for Greater Asia with LexisNexis in India, adds: "There is an enhanced need to demonstrate our abilities to significantly add business value." Sethuraman says he must "smoothly integrate the information security program with a number of enterprise initiatives: legal and regulatory compliance; internal business priorities and customer expectations; and enterprise architecture."

Sethuraman's challenges correlate with India's immense growth trajectory in security, and its shift to focusing on information security strategies as they relate to the business—taking a proactive as opposed to reactive approach.

"Companies in India have reported strong, consistent, double-digit gains across virtually every security domain and have taken a strategic approach to security," says PwC's Lobel. "Security efforts of Indian organizations have surpassed those of companies in the United States and we expect this trend to continue given that so many Indian survey respondents expect security spending to increase over the next 12 months."

That's not to diminish the efforts of information security professionals worldwide. Survey respondents across all industries, sectors, countries, business models and company sizes report growth in implementing new security technologies. And 74 percent say that information security spending will either increase or stay the same over the next 12 months.

However, the study found that organizations still struggle with security processes. Lobel says there appears to be misalignment with management's view of security, causing many organizations to fail to capture the full value of their spending.

"Information has become the new currency of business—its portability and accessibility are crucial components of a collaborative, interconnected business landscape," he says. "Organizations need to be prepared to address data security issues, have the proper tools in place, and understand how to use them effectively."

Complicit in this, too, is the need to not just recognize, but also understand the business perspective. Melodi Gates, CISO at Denver-based Qwest Communications, suggests spending "just as much, and preferably more, of your energy on building relationships with key stakeholders across your enterprise than you spend learning the bits and bytes of the latest technical toy. If you have the right relationships with your business, you can always find

a means to accomplish your objectives, and learning those technical means together gives you more credibility with those stakeholders than dictating 'The Answer'."

Neto adds, "We need to be multidisciplinary professionals and great negotiators. We cannot communicate using only technological language; we need to walk alongside the business, with an excellent marketing strategy to sell security. We need to sell security as value-added, positive and strategic; we need to break the paradigm that security generates costs."

## Technical Issues

Outside of business-IT challenges, there are day-to-day technical issues that must be addressed. For example, Gates reports an ongoing need to deal with vulnerabilities: "Keeping up with the high traffic in vulnerability disclosures is a perennial challenge and an important part of our program since we focus on proactively identifying and remediating risks."

Behind the high volume of vulnerabilities, Gates says, is the security research community's continued growth and focus on discovering and disclosing them. "That's generally a good thing when the disclosures are made responsibly, although sadly, that was not always the case in 2008," she says. "Regardless, to run an effective information security program, we had to react quickly to every one of those disclosures and that took time."

Gates' other challenges—balancing resources among programs and obligations, and evolving identity management functions—are the result of Qwest's growing information security program. Her organization is addressing these issues by focusing on "people, process, policy and technology."

Her mantra is strikingly similar to that of Sethuraman. "People are the most important component to the success of an information security program," he says. When establishing an information security strategy, he suggests a sound, solid framework driven by business priorities. And let the business know that its priorities are of critical importance. "If you can establish this reputation, you will soon see greater management commitment and support for the information security program that is so very necessary for its success."

This is the approach he is taking as his organization shifts from meeting internal standards to achieving international ones, such as ISO 27001 and 27002—a significant challenge that he says may be unique to his region.

"Greater levels of outsourcing to India over the last many years and the general practices of various companies have resulted in the general expectation for ISO 27001-compliant systems," says Sethuraman. In addition, he must meet these standards while facing "business pressures for greater cost-effectiveness and for ensuring the global standards are quickly established, even in new centers."

As to information security challenges specific to Brazil, Neto says the most prominent one is defining Internet usage regulations. "Industry and Internet experts in Brazil are discussing with the Brazilian government and other authorities the proposal of self-regulation and a law project for cybernetic crime," he says. "This is a process that may consequently incriminate the Internet service providers and may disturb privacy and free will toward Internet

usage in Brazil. It is a challenge that should be implemented in desirable directions, according to authorities' concurrence and with the agreement of an organized civil society and industry."

## Looking Ahead: 2009

Our three CISOs anticipate a variety of challenges in the new calendar year:
Neto: "A big challenge will be to integrate business continuity management in all organizational sectors, following market best practices. Another huge challenge is working on organizational security awareness, including new policies and providing security training for all development fields."

Sethuraman: "One issue will be identifying new and more cost-effective ways to carry out our information security program. Another is integrating the information security program with other enterprise initiatives in a more efficient manner."

Gates: "In 2009, we expect to focus even more on content-based security through our information governance program. The business requirements vary widely and the technical solutions, especially in data leakage prevention, are still maturing—a familiar theme. And there's always a new threat to consider since, ultimately, information security is an arms race—but that's also what makes it challenging and fun."

There's also the need to consider the economy and its effects on information security strategy.

(ISC)² Board Chair Myers thinks the single biggest challenge will be keeping "security in a steady state in this economy of reduced budgets. Even when you buy security technology or tools, there are still ongoing maintenance and monitoring costs."

Gates concurs. "I expect to see a continued need for vigilance against malicious software and attacks like spear-phishing that are rooted in fraud, along with the ever-present insider threat," she says. "We always seek to maximize the efficiencies of our toolsets, but I also expect to spend even more time on leveraging current solutions to minimize costs."

Cost-effectiveness is key, and security professionals should seek "innovative ways to find new value," says Sethuraman.

However, Neto cautions, "We've got to be ready for a technological investment decision to be cancelled and, furthermore, not let it affect organizational security. Security professionals, in my opinion, must be prepared for any change that may occur in their plans. Our market is in constant mutation and we need to manage security for any situation. For example, your company may acquire another one and you will have to adequately conduct the process of risk management during the joint venture, but also we need to preserve security in this process. We need to be resilient professionals."

# Resources from (ISC)²

(ISC)²
SECURITY TRANSCENDS TECHNOLOGY

Information Security Hiring Resource Center

- Whitepaper: Securing the Organization
- Case Study: Using (ISC)² Certified Professionals
- Global Information Security Workforce Study
- Career Path Brochure
- Hiring Guide

## About (ISC)²

The International Information Systems Security Certification Consortium, Inc. [(ISC)²®] is the globally recognized Gold Standard for certifying information security professionals. Celebrating its 20th anniversary, (ISC)² has now certified over 60,000 information security professionals in more than 130 countries. Based in Palm Harbor, Florida, USA, with offices in Washington, D.C., London, Hong Kong and Tokyo, (ISC)² issues the Certified Information Systems Security Professional (CISSP®) and related concentrations, Certified Secure Software Lifecycle Professional (CSSLP$^{CM}$), Certification and Accreditation Professional (CAP®), and Systems Security Certified Practitioner (SSCP®) credentials to those meeting necessary competency requirements. (ISC)² CISSP and related concentrations, CAP, and the SSCP certifications are among the first information technology credentials to meet the stringent requirements of ANSI/ISO/IEC Standard 17024, a global benchmark for assessing and certifying personnel. (ISC)² also offers a continuing professional education program, a portfolio of education products and services based upon (ISC)²'s CBK®, a compendium of information security topics, and is responsible for the (ISC)² Global Information Security Workforce Study. More information is available at www.isc2.org.

# # #