Dismantling the Security Disconnect

By Neill Hopkins

As phishing, pharming, spam, SPIT, viruses, and other assorted nefarious threats to information technology (IT) networks and operations continue to proliferate, organizations across all sectors of the economy say they have heightened their security preparedness. Yet a disconnect remains between talking the security talk and walking the security walk.

According to research conducted in 2005 by the Computing Technology Industry Association, nearly 40 percent of organizations surveyed experienced a major IT security breach—defined as one that causes real harm, results in the loss of confidential information or interrupts business—within the last six months. The number of serious IT security breaches remained consistent over the last three years.

Even more alarming, human error, either alone or in combination with a technical malfunction, was blamed for four out of every five IT security breaches, the study found. That figure is not statistically different from last year's study.

Organizations rely more on the Internet than ever before, making the storage and housing of personal account information and proprietary data even more vulnerable to identity theft and data corruption. Though security software has become increasingly more advanced in its ability to detect security threats to networks, applications and operating systems, hackers are sophisticated enough to reverse engineer patches and launch counter-offensives to vulnerable systems within 48 hours. Even the most sophisticated security software solution, which can provide 24 hours of security detection and assessment, cannot replace fully the need for IT security awareness and training in the workplace.

Clearly there is recognition of the importance of IT security for organizations across all sectors of the economy, especially in large organizations that have multiple points of vulnerability and thousands of employees. Yet organizations may not be doing all they can to counter the threat.

More than half of the respondents (53 percent) to the CompTIA survey indicated that their organization still does not have a written IT security policy. This lack of written IT security policies fosters gaps in security knowledge, especially among end-users.

Even at organizations with written security policies in place, enforcement of security policies continues to be a problem for organizations in every sector. Thus, security assurance continues to depend on human actions and knowledge as much, if not more so, as it does on technological advances.

Though technology-based organizations are faster to adopt technological approaches to IT security and implement security policies for most end-users, security administrators must be continually educated on new threats and solutions to keep pace with the dynamic landscape. Most non-technology based organizations are slower to adopt security software and slower to implement security awareness training to end-users. Security decision-makers without proper training often underestimate the cost and threat of security breaches to their organization. Other decision-makers and executives lack the empirical support to rationalize the needed investment for IT security.

With security on everyone's mind, recognition of professional security certifications can help to focus attention on best practices in IT security. The greater the number of IT professional training and certified in security best practices, the better organizations will be prepared to protect their organization's data, intellectual property and investment in technology.

"Committing to Security," the third annual study published earlier this year by the CompTIA, found that among those organizations who have invested in staff security training, 84 percent feel that their security has improved, up 18 percent from two years earlier. Seventy percent of those who have invested in IT security certification feel the same way. The positive effects of training and certification on IT security are most often described in terms of improved potential risk identification, increased awareness, improved security measures and a generalized ability to respond more rapidly to problems.

Further, training and certification improves security significantly. Eighty-nine percent of respondents reported that major security breaches have been reduced as a result of IT security training and certification.

For those new to security, or for IT professionals wishing to add security credentials to their skills portfolio, there are some essential facts that can help demonstrate where certification fits within the broad category of IT security and workforce development.

Two certifications—CompTIA Security+™ or the International Information Systems Security Certification Consortium, Inc., or (ISC)², Certified Information Systems Security Professional (CISSP®)—predominate today's market. Today, approximately 40,000 people worldwide who work in IT security are certified in either CompTIA Security+ CISSP®, the two leading vendor-neutral security certifications.

Vendor neutrality is important because it means that the certifications are based on industry accepted and recognized practices and standards, not on vendor-specific products or technologies. This better prepares an IT professional to work in the multi-vendor environment that is common in most organizations today.

CompTIA Security+ tests for security knowledge mastery of an individual with two years on-the-job networking and security experience. The certification is designed to validate that an individual has mastered critical practices for communications security, infrastructure security, cryptography, and operational and organizational security. Typical job titles for a professional with this level of experience would be security administrator or security specialist. This person will be responsible for hands-on tasks, such as installation, support and basic upgrades to the

IT security infrastructure. They also are prepared with a good set of foundation-level skills that are necessary to progress to much higher level roles and additional responsibility in the IT security arena.

The (ISC)² CISSP certified security professional has mastered management concepts and theories behind IT security, and possesses the knowledge of the policies and procedures that should be developed and implemented by organizations. The candidate for a CISSP must master accepted standards in ten subject areas based on the (ISC)² common body of knowledge.

While a whole host of other certifications exist at various levels to validate particular specializations, small organizations may want their internal network administrator to study for and earn the CompTIA Security+ certification to ensure the organization's fundamental information protection. Small organizations can also request that their external IT services provider employs personnel who are CompTIA Security+ certified.

Mid-sized to large organizations will probably have both CompTIA Security+ implementers and CISSP managers on staff so that all security needs are met. Vendor personnel should be appropriately certified as well.

Another benefit to an IT professional having CompTIA Security+ is that it is integrated into certification tracks from Microsoft, Symantec, IBM, and others, thus shortening the time and lowering the expense of moving toward greater specialization. (ISC)² offers similar advantages through its advanced concentrations in security architecture, engineering, and management is geared toward senior CISSPs.

The strongest rise in security training, according to the CompTIA survey, has been among directors (+15 percent) and executive staff (+8 percent). The financial industry has the highest proportion of respondents (18 percent) who indicated that 50-100 percent of their IT staff have received security related certifications, compared to only 4 percent for government. In the IT and education sectors, organizations invested in certifying only a select few IT staff. Sixty percent of IT respondents indicate their IT staff received no security certifications, compared to 43 percent for the education sector.

While vendor and technology-specific training continues to dominate training and certification across respondent organizations, vendor-neutral training increased by 10 percent over the past year, while domain-specific security training and certification show a 7 percent decline since 2003.

Though 61 percent of respondents indicate security training is not a requirement at their organization, employers are choosing to train their relevant IT staff, evident in the fact that required security experience at organizations has actually decreased by 6 percent over the past year. Employers recognize that highly-skilled or experienced security staff is difficult to find in the marketplace, especially with the customized skills appropriate to their business needs. The truly committed and well prepared security professional, especially one who possesses strong communication and management skills and has validated security knowledge through certification, should find that there are few limits to the career possibilities in the ever-developing field of IT security.

With current economic conditions continuing on an uncertain course, cost remains a common theme for most organizations; and it is not unreasonable to assume that cost will continue to be a key stated driver of behavior in all decisions regarding security for the foreseeable future.

The trend in computer security investment as a percentage of the IT budget has remained constant over the past year. Almost half of respondent organizations in the CompTIA study appropriate 5 percent of their IT budget to computer security, while those designating between 20-50 percent of their IT budget in this way stands at 1 percent. About one in ten designate no IT budget to computer security.

With regards to security training as a percentage of IT security budgets, a sizable portion (39 percent) do not spend anything at this time, the portion of those organizations spending between 20-50 percent remained constant at 13 percent. For companies with annual revenue of $10 million or higher, the median investment in computer security as a percentage of the IT budget is 5 percent, while the median value for companies with annual revenue of less than $10 million is 8 percent. This shows the cost challenges that smaller companies face in order to implement technological solutions or training for IT security.

This is especially true among small and mid-sized businesses (SMBs), those with 500 or fewer employers, who have traditionally lagged in security spending. Not long ago security was an afterthought for many SMBs. A firewall or anti-virus software was the extent of their security preparedness. They've now come to realize—in some cases, under catastrophic circumstances—that securing voice and data communications and networks is not just for the Fortune 500.

SMBs are increasingly facing IT and network issues similar to those of larger companies. Operators of these businesses are waking up to the fact that without secure, reliable networks and communications systems, their livelihood is at risk.

A recent survey of 300 SMBs in the United States commissioned by CompTIA and conducted by research firm IDC found that problems with electronic or phone business communications occur on at least a monthly basis at 60 percent of these businesses. More alarmingly, 70 percent of those occurrences had a material impact on business, either by putting the viability of the business at risk, causing business to be lost, or requiring extra care for customers.

Though training and certification requirements are still uncommon for new hires, 13 percent of respondents in the CompTIA security survey indicated that their organizations plan to implement security awareness training for employees and end-users in 2005. One in four respondent organizations have considered security awareness training but still have no plans to implement any related program. A larger portion (30 percent) still has not even considered security awareness training.

For companies with annual revenue of $10 million or higher, the median expenditure for in-house security awareness training and education is $20,000. For companies with annual revenue of less than $10 million, the median expenditure for its own security training and education is $2,000. Respondent organizations are much more likely to invest time and resources into developing in-house security awareness training for end-users and non-IT personnel.

Most respondent organizations have no formal approach to assessing the return on investment (ROI) in IT security. In fact, operational continuity and the number of security breaches are the two most common informal approaches used to assess ROI. Only one in five respondents indicated a cost-to-benefit analysis is applied to assess ROI for IT security. These real and perceived improvements in security are accompanied by some hard numbers when the ROI from training and certification are addressed in the study.

Among respondent companies with annual revenue of $10 million or higher, the median value of estimated ROI for training is $50,000, while the median value for ROI for certification is $32,500. For respondent companies with annual revenue of less than $10 million, the median value of estimated ROI for training and certification is $5,000.

Considering the level of ROI mentioned by those who have invested in training and certification, companies generating smaller revenue will have a greater challenge rationalizing the security investment needed over other priorities they currently face. Technological solutions such

as antivirus software and firewalls may seem sufficient until a security failure that equates to a massive financial loss occurs. For larger revenue generating companies, the financial links are clearer, but need to be better exposed among the non-investor minority. There are still a significant amount of companies and organizations that have not recognized the massive potential for loss due to a security failure. The benefits of security awareness and training are still largely intangible to these groups.

To be truly effective in preventing and combating security threats, organizations need to take further steps by spreading security awareness and knowledge from a select group of IT staff to larger portions of their employee base. Decision-makers and executive level staff must become better informed about the real costs of security breaches; and the real return on investment (ROI) available with both security training and certification.

The best security technology in the world won't work without appropriate human intervention, the skills of implementers and the vision of managers to properly deploy and apply it.

For more information on CompTIA Security+ visit http://www.comptia.org/certification/security/?nav=quick. For more information on CISSP, visit https://www.isc2.org/cgi-bin/content.cgi?category=7.

NaSPA member Neill Hopkins is the vice president of skills development for the Computing Technology Industry Association (CompTIA), a global trade association representing the business interests of the information technology industry. Mr. Hopkins oversees the association's professional certification programs as well as regional and national programs aimed at promoting career development in technology professions.