

Assuring Global Information Security Across the Organization

Author: Martin Bean, COO, New Horizons Computer Learning Centers

While international security agencies work from a broad definition of “security,” they have rightfully focused on protecting critical infrastructure -- water supplies, food supplies, airports and other transportation centers. Importantly there is also acknowledgement that the reliability of information networks such as the Internet and telecommunications infrastructure is equally significant to global economies. There is growing awareness among high-level officials that there is just as much risk from a breach of information system security than there is from any of the other physical infrastructure elements.

So how do we as a global business community address the need to protect our IT critical infrastructure in a united way? What good is it to protect your own organization or your own department when we all share common networks that are open to disruption?

Most of the attention historically has been in the area of hardware and software. As those of us in the industry know, however, the reality is that the vast majority of information security breaches are caused by human error. Our real-world experience shows that rather than hardware or software, it's the “brainware” that needs to be the focus of our attention. The level of sophistication of the tools being used to create security breaches and the speed of attack are growing exponentially. You only need to take a look at the headlines in today's IT, security and even general press to see these episodes reported with increasing frequency and severity, backed up by statistics and industry experts.

According to an industry survey conducted earlier this year by the Computing Technology Industry Association (CompTIA), 84 percent of the nearly 900 organizations who participated in the survey blamed human error either wholly or in part for their last major security breach. Nearly six in ten organizations (58 percent) stated they have experienced at least one major IT security breach – defined as one that caused real harm, resulting in the loss of confidential information or interrupted business operations – in the previous six months.

Further, organizations said training and certification significantly improved their security. Results showed that when a company trained at least one in every four IT employees in security fundamentals, it was 20 percent less likely to suffer a departmental security breach.

It may sound simple, but it is a fact: most companies and agencies lack the basic policies and enforcement of information assurance across the organization. Based on results from the CompTIA survey, only a slight majority of organizations (51 percent) have a written IT policy in place. IT security policies are more common in the financial services industry (62 percent), government (58 percent) and education (41 percent) sectors. IT organizations are the least likely industry sector to have a security policy in place – only 35 percent do, according to the survey.

The solution? The first step is to systematically start training people in how to do a better job securing information. Second, as an industry we need to drive home the global benefits and positive consequences of properly secured information. ISSA members and others in the information security industry are in an ideal position to address the “brainware” issue and take a leadership role in driving organizations toward a training-centric information assurance model.

Looking at an organization, there are three key populations to be considered:

1. Executive Level: management and board members
2. IT Professionals: the technical level including the network administrators and those people that protect the infrastructure
3. Knowledge Workers: every single person who touches the computer inside the security framework of an organization, which extends through the supply chain to the entire economy.

Executive Level

In the C-level suite and board room, it is important that an organization's management team is educated as to how much risk their companies or government departments are under if they don't take the necessary steps to protect their information security.

A major issue driving board room and executive awareness is regulation. In the U.S., regulation is coming in the form of the Sarbanes-Oxley law, HIPAA compliance mandates, and other pieces of legislation. This should awaken board rooms across America to the need to do a better job of protecting their information security. To reinforce this, it is essential that executives get behind these initiatives, just like in any other changes initiative within a corporation or department. Without executive buy-in and sponsorship, organizations are doomed to non-compliance and the entanglements that follow.

IT Professionals

The second population that needs to be addressed is the hundreds of thousands of trained IT professionals who have installed and maintained our network infrastructures, but have not kept pace with the enormous escalation in the frequency of security breaches and increased vulnerability of the systems.

Retraining is important, including building and maintaining an on-going set of training programs to ensure that IT professionals are kept up-to-date with the latest vulnerabilities, the patches and fixes put in place and that they are really capable of mounting protection programs. This would ensure that their infrastructure is not only protected as best they can, but in the event that a new breach is observed, they are able to respond in a timely enough fashion to actually protect their organization.

Knowledge Workers

The third population that plays a critical role in an organizations' information assurance model is the knowledge worker. The average person who touches a computer has no understanding of the plethora of tools and software packages that may create vulnerabilities in their company. It is as simple sometimes as not writing a password on a post-it note, or not realizing that launching an instant messaging product or a third party, web-based email tool can actually open up security

vulnerabilities into the organization. Every knowledge worker must take personal responsibility for the piece of information security that they control.

Only by taking care of those three distinct populations can an organization even begin to address the most significant problems they face in information security and that is from human error caused by a lack of understanding or appropriate training. According to the CompTIA survey, among those companies who have invested in staff security training, 80 percent feel that their security has improved. Seventy percent of those who have invested in certification feel the same way. The positive effects of training and certification are seen in improved potential risk identification, increased awareness, improved security measures, and an ability to respond more rapidly to problems.

What does a Security Professional look like?

The U.S. Department of Defense and related security agencies are moving toward defining what an IT security professional looks like and what needs to be done from a training perspective. However, the government only controls roughly 15% of the critical infrastructure; the remaining is in the hands of the private sector. To really take a hold of information security, we are going to need an army of appropriately trained and qualified professionals that we entrust with managing of our critical information technology infrastructure.

One of the big problems that exists today is that there hasn't been enough energy placed on the public and private sector coming together to actually look at what the IT security professional looks like, building the appropriate training taxonomy, and making sure there is a governing body that sits over those people to ensure they are continually trained and updated. That is especially important in the event of an attack when speed of response is absolutely critical. Without having a named population of appropriately trained IT security professionals who are all speaking the same language, it becomes very difficult to mount a counter protection program by being able to rally all of those people to respond in a timely fashion.

ISSA has taken a great step forward in helping to guide this process by establishing its Generally Accepted Information Security Principles (GAISP). Chartered with providing a means to unify and harmonize information security efforts and measure their success,

fully implemented GAISP enables a translation of existing regulations, standards, and accepted practices into logical strategy and detailed tactics that can be implemented by any organization.

Every one of us needs to make a personal commitment to support this concept. Much more needs to be done at the grassroots level to unite public and private sectors to further define, support and encourage the information assurance professional. We all must work together by systemically attacking it at three levels inside the organization. We must champion the IT security professional and put an international governing body in place to keep them trained on an on-going basis. If we set up these necessary systems, when security breaches occur, all levels can then be galvanized and rallied as quickly as possible.

Martin Bean is a noted training industry authority and is COO of New Horizons Computer Learning Centers, named the world's largest independent IT training company by IDC in 2003. Featuring the largest sales force in the IT training industry, U.S.-based New Horizons has over 2,100 account executives, 2,400 instructors and 2,100 classrooms around the globe. For more information, visit www.newhorizons.com.