

SECURITY IS BETWEEN THE PNEUMATIC CHAIR AND THE KEYBOARD



Peter Hillier, CD, CISSP, ISSPCS

You don't need to be reminded that the bulk of security related incidents that you face are sitting in your own office chairs. Although between the years the 2001-2004 CSI-FBI Computer Crime & Security Survey noted that "unauthorized use of computer systems" was on the decline, with regard to financial losses, the same survey has noted an increase in 2005. Insider abuses of Net accesses were still attributed at 56%, up from 53% in the previous year. In attributable loss, the overall numbers showed a decrease in 2005 to \$130 million from \$141 million, but \$130 million is a very significant figure! A tremendous number of security issues are attributed to this area and it stands to reason you should have more control.

While respondents of the survey all noted in favour of security awareness, the material did not gauge exactly how many were actually conducting an awareness program.

WE MUST DO MORE

Your organization's Acceptable Use Policy is not enough! You may force personnel to read it, and even have an acknowledge button for them to click on the corporate intranet, but they'll rarely remember or adhere to the content. Why? Because you cannot measure its success. Also, it is safe to say you cannot change an adult's personal habits with an electronic document.

Of course appropriate policies remains the supporting tenet of any awareness program, but if you really want to mitigate the number noted above, you have to demonstrate some thought leadership on the inside of your organization. In the end you'll need less Acetaminophen.

A great deal of effort goes into protecting the perimeter; at least it should. Hardening firewalls, intrusion detection sensors, servers and protecting other sensitive assets are key. You should consider your personnel resources as an extension of that perimeter. After all, they are the weakest link in the infrastructure; the most susceptible to security

issues and basic human instincts. Without the proper tools in place (policy, procedures, awareness, education) they are ill-prepared to be an extension of a proper security program.

EXAMPLES

Some of the goals of your Security Awareness Program should be to:

- Put information security and its importance in the forefront of your staff's mind.
- Spread YOUR ORGANIZATION'S information security policy and awareness throughout corporate ranks.
- Get management on the same page as the security department and the staff with executive targeted components.
- Build security awareness into the technical and development teams.
- Think differently. Create a paradigm shift in the way YOUR ORGANIZATION'S staff views its business process and how it should be protected.
- Make Security Awareness enjoyable for everyone. Get significant 'buy-in' from the entire corporate target audience.
- Target the three major groups within your organization:
 - ❖ Management
 - ❖ Technical Staff
 - ❖ All other workers and business partners.
- Build Cyber Security, Physical Security and People Security into a coherent approach where the goal is to teach behavioural and environmental awareness according to company goals and policies.

So, what's in it for you? You'll all ask this question at some point. Why would you spend the money on an IT Security Training program? Let's put it in language you'll appreciate. Like the marketing adage "you've got to spend money to make money", there is a distinct Return on Investment from your security spending as well.

RETURN ON YOUR INVESTMENT

While Security ROI can be a contentious issue in and of itself, here's a top five ROI list, or "What's in it for me list" I developed with some input from a good friend and fellow security guru, Winn Schwartau (www.interpactinc.com) who works and lives in Florida:

- Increased security and audit compliance. This means lower fees by your auditors and lower insurance rates. Target the CXO's;
- Lower development costs and application deployment when building security in from the beginning. Target the Techs and Execs;
- Less security snafus: viruses, worms, etc. when staff is trained to detect and report security events: Target - entire staff;



- More home security tips, protect family from ID theft etc: bring good habits to work and safeguard network from remote users. Target: entire staff.
- Less downtime, fewer investigations, more network resiliency, create human firewalls and human IDS.

MEASURE SUCCESS

When developing policies and processes around an IT Security training program, it is equally important to measure its success. Note the following tips:

- Announcing your awareness program from a high management level.
- Ensure existing security policies and procedures are current, complete and have been announced to all staff.
- Lead by example. For instance, a new user is more likely to choose secure passwords if the initial password assigned to him is strong and unique like 'yT56Bc3c' rather than something weak and common like 'welcome'.
- Demonstrate management's continuing commitment through follow-up procedures such as:
 - routine desk checks,
 - before and after awareness measurement quizzes, and
 - checking for poor network passwords.
- Illustrate the importance of secure practices by making regular announcements of actual external security breaches that happened due to poor security awareness.
- Consider including security awareness as part of the formal evaluation process.
- Consider implementing a security improvement suggestion program to further demonstrate management's commitment.

Like any area of improvement and given how stretched our resources are, the earlier you demonstrate leadership in the area of security training, the sooner you will realize a return and see some relief.

EVENT MANAGEMENT

Like so many other issues that crop up in an organization, for the most part the bulk of security issues can be handled at the lowest possible levels. Not unlike a harassment complaint, which can be often resolved with some minimal mediation between the affected parties, so too can security events by communicating with your personnel.

We are continuously inundated with statistics reminding us that the highest numbers of security-related incidents come from inside the organization. You take your personnel resources for granted; they are all loyal and trustworthy, otherwise you would not have



hired them in the first place. However, you still find yourself dealing with issues around inappropriate use, malfeasance, etc. The exposure of these types of incidents can be extremely more damaging than that of a distributed denial of service. You can react appropriately to the latter and it is considered to be a normal risk when conducting business on the Internet. The former, however, can cause irreparable damage to reputation, market share and shareholder perceptions that can result in staggering losses.

All these headaches for want of a formal policy and guidance for employees that demonstrates leadership, responsibilities and accountability for actions. Sounds like a much easier pill to swallow.

After all, it's all about managing risk. You have countless more employees than you do firewalls, so it is implement to implement the appropriate security program as you would a firewall and maintain it as you would the firewall rule sets.

Don't wait for the "teeth" from legislation to catch up to you. Demonstrating some due diligence and leadership can help reduce the number of internal incidents you will have to respond to and at the same time increasing the base of security-minded personnel who will mentor new generations of employees.

Peter is a Senior IT Security Consultant with CGI's Information Systems and Management Consultants in Ottawa, Canada. He served a 20-year career in the Canadian Armed Forces in a variety of Security and Intelligence roles, which culminated with strategist and management roles within the DND Computer Incident Response Team. Currently assigned as the Business Growth Lead for CGI's Managed Security Services, he is responsible for the strategic directions of CGI's Security service, Business Development, and partner relations. A Certified Information Systems Security Professional, Peter is also the founder and past President of the Ottawa Chapter of the High Technology Crime Investigation Association. Peter can be reached at peter.hillier@cgi.com.

