



- JOHN BREAKEY, NETWORK INDUSTRY COLUMNIST -

Effective Security Posture Starts With People

John Breakey is President of UNIS LUMIN

Although there has been an increase in Information Technology security awareness over the last few years, there has yet to be a corresponding budgetary boost. According to the 2003 InformationWeek U.S. Information Security Survey, only 39% of respondents say they expect to raise security spending this year. The number of incidents is continuing to rise dramatically, with over 76,000 reported to the CERT Coordination Center in the first half of 2003, compared to 82,000 for all of 2002. Yet, the losses are cited as being manageable. Survey respondents reported few occurrences of unauthorized information access, identity theft, or a substantial financial loss being incurred.

While many organizations continue to purchase security infrastructure, they must determine what's appropriate for their needs. There are many categories of products available that can strengthen the security of an organization's IT assets. These include:

- **Firewalls**, which are used to control what types of data, are allowed to enter and leave the corporate network.
- **Virtual Private Networks** allow information to be accessed privately over public networks.
- **Strong Authentication Systems** augment generally weak password-protected systems by requiring an additional form of authentication, such as the possession of a swipe card or tokens.
- **Biometrics** identify users based on their physical properties, such as fingerprints, voice patterns or the properties of one's retina.
- **Antivirus** products prevent malicious software from being executed.
- **Intrusion Detection Systems** can detect attacks while in progress, generate an alarm and take corrective action.

The list above is only a sampling of the most common technologies employed today. Yet, for every product category above, there is a multitude of potential ways to circumvent the controls. Perhaps not too surprising is that effective security policy and awareness is just as important as any of the products used.

When the infamous hacker Kevin Mitnick was asked about his crimes after his release from prison in 2000, he explained:

"People are the weakest link. You can have the best technology, firewalls, intrusion detection systems, biometric devices - and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything."

Although Mitnick's 15 minutes of fame is quickly fading, his comment refers to the fact that all members of an organization must take responsibility for security. All employees should have security as a component of their job description. Of course, if it is a requirement to follow security procedures and best practices, employees need to be educated with this end in mind. Some ways in which non-IT employees must contribute to the information security practice are:

- Awareness and comprehension of the organizations security policy
- Ability to identify systems, data, and procedures they are responsible for maintaining the integrity of
- Understand which roles have legal responsibilities associated with them, beyond the scope of the organizational security policy
- Recognize and ensure that observed or suspected security incidents are reported through appropriate channels immediately
- System malfunctions must be reported immediately

In addition to the dissemination of the Security Policy, some common issues that constantly recur have the most impact on non-technical staff. These issues should be addressed through employee training and frequent communications in order to achieve security awareness level within the organization.

Security awareness topics include:

- **Passwords** are usually the number one weakness in any system that requires authentication. Characteristics of password mishandling include: sharing, choosing easily guessed, written down, and use of the same password on many systems.
- **Social Engineering** is the fancy infosec term to describe con artists. Because people usually want to be helpful, it's all too easy to convince a user to divulge their password to aid in some "testing". Social engineering isn't limited to passwords, as corporate and network information are also requested and used in building attacks.
- **Viruses and Hoaxes** are too often mistaken for each other by end-users.
- **Acceptable Use Policy** usually defines what computer systems (and the Internet) are to be used for. All employees need to understand what is and is not permitted.
- **Remote Access Considerations** are important, as more organizations grant employees the ability to work from home. Extra measures need to be taken to protect the corporation, as it is often extending its perimeter to include employees' homes.
- **Information Classification.** People need to know what they're trying to protect by following the security policy. Information confidentiality should be classified according

to organization-standard structure. This classification should be made by the owner of the information, which is often a non-technical worker.

A common approach to augmenting the knowledge base of the entire organization is to hold security awareness seminars. The objective is to educate a large number of people with regard to issues that may seem irrelevant to their duties at first. Some guidelines to get the most out of these seminars are:

- Keep it short. This isn't the most exciting topic, so the sessions must be kept around 30 to 60 minutes. If that isn't enough time, multiple sessions should be scheduled, perhaps with a month or two of time between sessions.
- Customize sessions according to relevance if possible. Although the policy will be mandated across the organization, examples of its application can be made specific if attendees have similar function.
- Make it interesting. Help attendees identify why information security is important to them.
- Groups should be small enough to allow some interaction. This also helps to accommodate busy schedules by having multiple available timeslots.

The ISO 17799 code of practice is an ideal starting point for developing organization-specific policies and guidelines. It can be used as the framework to build a comprehensive, appropriate information security management program. Larger organizations with an established program may take on this task internally, or may choose to engage a consultant to manage the process. In any case, it's never too early to develop or enhance security practices.



Since 1988, COACH, Canada's Health Informatics Association has provided leadership and guidance in the areas of security, privacy and confidentiality. The 2001 publication gives health informatics professionals the framework needed to develop and implement security and privacy programs. *Guidelines for the Protection of Health Information* reflects the new realities of health informatics as we enter the third millennium and the dawn of the information age.

COACH is proud to offer for purchase the new *Guidelines for the Protection of Health Information*, a valuable reference that no health informatics professional should be without.

Download the order form for the *Guidelines* from the COACH Web site at www.coachorg.com.

COACH, Canada's Health Informatics Association
1304 - 2 Carlton Street
Toronto, Ontario M5B 1J3
Tel: (416) 979-5551
Fax: (416) 979-1144
Toll Free: 1-888-253-8554

