Wednesday, May 4, 2005

Site Map | About Us | Media Centre | Reprint Services | Mobile | Feedback | Contact Us

itWorldCanada ▸ Subscribe ▸   COMPUTERWORLD★ NetworkWorld★ CIO CANADA itFocus CIO CANADA Government Review it job universe.ca

Enter your **QUICKLINK** number to go directly to that article. [ ] GO!   Advanced Search [ ] GO!

▸ **Knowledge Centres**
■ Enterprise Infrastructure
■ Communications Infrastructure
■ Information Architecture
■ Integrating IT
■ Departmental/End-User Computing
■ Enterprise Business Applications
■ Extended Enterprise
■ Security
■ Voice Data and IP
■ IT Workplace
■ Leadership
■ E-Government
■ Wireless/Mobile Computing

▸ **Content Types**
  IT World Canada Events
  News
  Resources
  Webcasts
  Book Reviews
  White Papers
  Product Reviews
  Careers

▸ **Spotlight on Grid Computing**
  ▪ Articles
  ▪ Events
  ▪ Industry Links
  ▪ White Papers and much more…

PLUS:
▸ **Voices**

▸ **Featured White Paper**

▸

▸ **Featured Book**

▸ **Featured Webcast**

Information Architecture
Identity Management

Page 1 of 1

Bettering your security behaviour
By: Rosie Lombardi
Computer World Canada   (26 Apr 2005)

Everyone knows the rules for losing weight: eat less, exercise more. Knowing the rules doesn't inspire people to change their behaviour. Educating people on how to make two simple rules a part of their everyday habits is a complex public health issue. There are parallels in information security awareness programs: the true objective is not just to impart the rules to users, but to change their behaviour.

Unlike weight loss programs, many users don't even know the basic rules of safe computing. According to the ITAA's Global Cyber Security Survey, 46 per cent of workers say they have either no formal training in information security practices or they learned them through informal channels. Nor are schools providing much training to the next generation of workers. Most students participating in a University of Arizona study described themselves as knowledgeable about protecting themselves from viruses, crashes and other nasties. But almost half reported never having received any computer security training, and the vast majority did not follow basic procedures.

So the workplace is where most people will likely be introduced to security requirements and receive some type of training. But the problem with many corporate awareness programs is that they are too simplistic and typically based on do's and don'ts. "Technology changes frequently and we don't know the don'ts. Users are told not to use the web for x, but in six months, another rule is made for some new threat like spyware, and then users are told not to do y," says Paul K.Wing, co-author of Protecting Your Money, Privacy and Identity. Business and technology environments are dynamic, and expectations of blind obedience to shifting rules are unreasonable in today's workplace.

People need context to understand the point of rules. They need to know the business impact of not following security practices. For example, users may be instructed against sending sensitive content via unsecured e-mail. But people can't understand the problem if they're not provided information about the likelihood that the messaging system might be compromised. And information that may appear innocuous to users can be exploited by hackers, for example, posting a message on a usenet group that reveals information about corporate systems.

"People need examples of how a small lapse or piece of information can

lead to a security breach," says Aron Feuer, president of Cygnos IT Security. "Organizations don't offer clear examples of the impact of a security incident that's tuned to the business or the user's specific function."

Awareness problems are further complicated by privacy issues, which are related to security but add a category of user responsibility beyond the organization to its customers.

"What's common is that people lack awareness of the responsibilities required by privacy legislation," says Brendan Seaton, Chief Privacy and Security Officer at the Smart Systems for Health Agency. "Ethical lapses are a problem: the temptation to browse a famous person's health record, or family and friends, is high. Often people just don't know that it's wrong. The reaction is often, 'But it's my mother – what's wrong with looking?'"

The most intractable behavioural problems involve positive social attributes that are needed in the workplace, like trust and altruism. Countering social engineering, which is the most efficient way to breach security, means reprogramming people's attitudes towards social relationships. "When we do social engineering tests, about 25 per cent to 50 per cent of staff will divulge their passwords to our people impersonating unauthorized users. When we follow-up, the vast majority say, 'I felt uncomfortable answering the question, but I felt it was necessary to do so because I was asked directly,'" says Feuer.

An awareness program needs to teach people how to handle these types of social situations politely but firmly. "Senior executives may not appreciate the value of the little things you can do to train users that prevent big problems. The long-term benefit is phenomenal but the ROI isn't immediate," says Yogen Appalraju, Chief Information Security Officer at Emergis.

A principles-based approach that allows people to develop judgment is more effective in changing behaviour than a rules-based one — it provides the guidelines people need to make the right decisions when they come across something that's not predictable or they haven't encountered before. The principled approach is about getting users to think about how they can behave responsibly in the workplace through the use of customized examples, analogies and what-if scenarios. "We need to bring the values of the real world into the workplace. If you wouldn't give your bank PIN to someone at work, why would you give them your password?" says Wing.

But there are broader organizational issues to consider even in the best of programs. "Assuming awareness training is going to be an effective method without taking a look at the systems you're trying to protect is a set-up for failure. Too much responsibility for security has been moved to users in organizations where systems are too convoluted, complex and interdependent to build a good security posture," argues Feuer.

People who "own" information assets such as finance and HR are responsible for content and held accountable in theory, but in practice

they are not responsible for designing, implementing and maintaining security controls. They may be trained on security practices, but they don't understand the underlying systems or who is responsible for setting data standards.

Says Feuer: "One of the things awareness training should be doing — but doesn't — is to introduce the big-picture security requirements. If it doesn't cover systemic or governance issues, then it's focused on the bottom 20 per cent instead of the top issues. Basic training that doesn't allow users to come back and ask: do we have a policy that tells us how we should use our systems, what method should we use to classify information, and so on — if it doesn't allow users to become managers of their own systems — then from a security perspective, the training is flawed."

Page 1 of 1

Send to a Friend   Rate This Page   Print This Page   Letter to the Editor

Related Content

Articles

Data thefts prompting IT security checks (04/01/2005)

A risk-taking success story (03/01/2005)

OneSign 2.5 simplifies password security (03/04/2005)

White Papers

The importance of building an access strategy
This Yankee Group whitepaper outlines the approach required in migrating your company's access strategy from a reactive model to one that provides ubiquitous access to information and applications for multiple users across different devices.

Value of Integrated Security for Small and Medium-sized Businesses and Enterprise Branch Offices.
Cisco is merging best-in-class network security technology to redefine network security and provide customers with end-to-end network protection.

Platforms for a New Millennium
Download the IDC white paper, "Platforms for a New Millennium: HP's Transition to Servers Based on Itanium Processors." It explains the reasons behind the Integrity server line and how HP is making it easy to change over.

More White Papers

SOA Explained:The Four Abilities of a SOA Registry
Discover how a standards-based SOA registry provides visibility, reusability, adaptability and managability.

SOA Case Study: Amazon Merchant Platform
Discover how Systinet Web services technology helps power Amazon's Merchant Platform, which accounts for more than 20 percent of order placed on Amazon.com.

SOA Case Study: The Hartford Deploy UDDI Registry
In this ZapThink report learn how and why The Hartford deployed an enterprise UDDI registry as part of their SOA.

<u>Aligning Sales Methodology and Technology</u>

Discover how to reap the full benefit of your SFA system by integrating a sales process. This paper provides guidelines for choosing SFA systems, describes how a sales process can improve input, and suggests implementation approaches.

<u>The Four Steps to High Impact E-mail Marketing</u>

E-mail Marketing as a Relationship Strategy is a guide for combining leading customer relationship strategies with the best practices within e-mail marketing. A look at the modern e-mail marketing landscape and an examination of its challenges.

Special Advertising Partners

<u>Bell</u> – <u>7th Annual Bell Wireless Innovation Conference</u>

Don't miss this exciting series of presentations from our industry leading partners. With two Keynote Addresses, an afternoon of Breakout Sessions and a Partner Pavilion open all day, you'll find the information you need to change the way you do business.

<u>HP</u> - <u>ProLiant BL30p</u>

How can the HP ProLiant BL30p blade server help your business adapt to change? Download the IDC White Paper, Adapting to Change: Blade Systems Move into the Mainstream to find out.

<u>HP</u> - <u>Platforms for a New Millennium</u>

Download the IDC white paper, "Platforms for a New Millennium: HP's Transition to Servers Based on Itanium Processors." It explains the reasons behind the Integrity server line and how we're making it easy to change over. Or, read case studies featuring companies profiting from HP Integrity servers right now.

IT World Canada MarketPlace

<u>Covad VOIP Solutions: The New Voice of Business</u>

Save your business up to 40% in telecommmunications costs, increase employee productivity, simplify your network and eliminate frustration with Covad VoIPs fully-hosted, Voice & Data solution. Free onsite assessment for qualified customers.

<u>Security Within - Configuration based Security</u>

Configuration and policy based security systems are a pro-active way to defend against IT security attacks. Click here to request our white papers, "Security Within - Configuration based Security" and "Policy Management vs. Vulnerability Scanning".

<u>GroundWork--Open Source Network Monitoring</u>

Low-cost purchase and deployment, unrivaled flexibility, proven service and support, unmatched simplicity, and no vendor lock in. Tap into GroundWork's open source solution for IT monitoring.

<u>Applications Go 25x faster with Solid State Disk</u>

Texas Memory Systems solid state disks are The World's Fastest Storage(R), with certified results by the Storage Performance Council. Fill in a short information form for a free whitepaper, Increase Application Performance With Solid State Disk.

<u>Dedicated Server Hosting: High Speed, Low Cost</u>

Outsource your web site and application hosting to ServePath, the largest dedicated server specialist on the West Coast. Enjoy better reliability and performance with our screaming-fast network and 99.999% uptime guarantee. Custom built in 24 hours.

Privacy Policy

Bio-IT World   CIO Titles   CMO   ComputerWorld Titles   CSO   Darwin   GamePro
Infoworld
ITJobUniverse   JavaWorld   MacCentral   MacWorld   Network World Titles
PCWorld   Playlist

IDG WorldWide Network