

Human error at the center of IT Security breaches

By Martin Bean, COO, New Horizons Computer Learning Centers

IT security has primarily been thought of in conventional terms, focusing solely on securing hardware and software. Increasingly, the spotlight is on training the *individuals* who use computers. Statistics show that 80 percent of identified information security breaches are caused by human error due to lack of information assurance knowledge and proper training, as well as the failure to follow security procedures.

According to a recent global survey by Ernst & Young, -- which involved interviews with more than 1,230 organizations in 51 countries – only 56 percent of respondents said they train system users to identify and report suspicious activities.

While many respondents appeared fixated on external threats such as viruses, the more likely threats are those derived from within an organization's growing extended enterprise. Ironically, less than 30 percent listed "raising employee information security training/awareness" as a top initiative for 2004. In addition, only 20 percent of respondents feel strongly that their organizations view information security as a CEO-level priority.

Apparently many employees feel that IT security has no value when there is no visible attack, however because many insider incidents are based on concealment, organizations often are unaware they are being victimized. According to a recent report from the Computer Security Institute and the FBI, an insider attack against a large company could cause an average loss of U.S. \$2.7 million in damages.

The frequency and severity of such incidents are confirming what may seem to be obvious: the single biggest weakness in an organization's infrastructure is people. The

ultimate solution to this problem is the training and re-training of every person in an organization that touches a computer.

Currently, there is no clear definition of an information assurance professional and there is a desperate need for common standards and certification moving forward. The first fundamental change that needs to take place is to move security from being seen as a technology issue to be seen as a behavioral one that has profound consequences for both the reputation of the organization with its customers and prospective customers and for its financial health.

When it begins to be looked at in the same way as organizations do at any behavior in the workplace that opens the organization to bad publicity, litigation or results in confidential information being disseminated, then upper management will see it as their responsibility to enforce and reinforce. This change will be driven by customers who demand that anyone they do business with has secure systems and can maintain data integrity and security and by the financial impact of insecure networks or bad user habits.

There needs to be shared responsibility at senior management level for the creation, dissemination and enforcing of a robust security policy that every employee has a copy of and familiar with the parts that pertain particularly to them. With proper training, people can become the single most important factor in an organization's security defense strategy.

In response to the growing need for information security training and certification, top training organizations worldwide are rallying to help the public and private sector achieve information assurance readiness. More than just training, information assurance readiness is a process that includes protecting key digital assets and capabilities, detecting attacks and malicious actions, responding with rapid notification and reaction, and recovering with disaster and business continuity planning.

A security benchmark study conducted earlier this year by the Computing Technology Industry Association (CompTIA) shows that when a company trains at least one in every

four IT employees in security fundamentals, it is 20 percent less likely to suffer a departmental security breach.

IT security threats that were once infrequent occurrences now happen on a daily basis. Organizations are investing more budget on IT security, specifically on training and certification than ever before. Among the skills acquired is the ability to identify security threats, analyze network security risks, monitor the network for security breaches and respond to network and software-based attacks. Clearly, organizations that require training and certification are much better armed with the critical skills necessary to improve their information security practices.

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.

###