

Why End-Users Are Your Weakest Security Link

Four Key Steps to Managing the Threat From Within

November 26, 2007



Why End-Users Are Your Weakest Security Link

Executive Summary

Security experts have for years focused on protecting the corporate perimeter from external threats without realizing that their biggest security threat could be sitting right next to them. While infrastructures and perimeters have been fortified, corporate endpoints and their users have been traditionally overlooked, enabling sophisticated cyber criminals with another entry point into the organization's network. Not only that, employees represent significant risk to an organization's network and data security – whether it is the employee who inadvertently installs malicious code by clicking on a website or an email link or whether it is the employee who steals corporate IP, customer or financial data and sells it to a data broker or takes it to a competitor.

So what is an organization to do? How can organizations effectively manage the risk that is inherent with their employees' use of technology?

This paper examines why end users pose the biggest security risk and outlines key strategies for C-level executives and security staff to effectively address their weakest security link: their end users. Readers will see how Lumension Security customers have been able to seamlessly put controls in place to prevent unwanted end user behavior and also provide the necessary visibility into employee actions. Readers will also learn the fundamental steps to ensure that corporate policies are effectively enforced, which requires a combination of people, processes and technology:

- ▣ Accept the reality
- ▣ Enforce user policies across the enterprise
- ▣ Socialize policies
- ▣ Report on policy enforcement and effectiveness

Why End-Users Are Your Weakest Security Link

Study after study reveals a fundamental truth about the status of IT security today: The biggest threat is not the traditional cyber criminal writing malicious code in a virtual location, but trusted employees sitting within or working outside of corporate walls.

Employees represent a significant risk factor as they are privy to an organization's information and within arms reach of that data. Knowing that infrastructures and perimeters have been fortified, sophisticated cyber criminals have begun to target end users as another entry point into the organization's network.

Endpoints (which include laptops, PCs, servers, terminal services servers and thin clients) and end users have become a major source of disclosure as 70 percent of all serious incidents are sparked by insiders¹. Further research shows that:

- ▣ User error is directly responsible for 50 percent of breaches²
- ▣ Policy violations (intended, accidental and inadvertent) are accountable for 25 percent²

This has not escaped the purview of C-Level executives as 56 percent of CISOs noted employee misuse of corporate data as the most serious IT challenge³.

Users represent a security risk because of several factors:

- ▣ *Expanding corporate boundaries:* Never before have there been so many mobile workers. In the United States alone, more than 44 million were classified as teleworkers (Dieringer Research Group) with more than 100 million teleworkers expected by 2010 (WorldatWork's Telework Trendlines 2007).
- ▣ *The convergence of personal and professional use of corporate endpoints:* As a result of workers becoming increasingly mobile, as well as needing to quickly share and disseminate data, laptops and computers are becoming more personal, loaded with non-business applications, posing the risk of not only

appropriate use, but also potentially exposing your organization to spyware and keyloggers.

- ▣ *Mounting threats that target end user curiosity:* Social engineering tactics such as website or email spoofing, phishing, and many more are used to manipulate end users into performing actions detrimental to the organization's security or divulging confidential information.
- ▣ *Employees moving between competitive organizations:* In today's dynamic business environment, employee movement between companies is the norm, with competitors angling to hire key personnel for their skills as much as for the confidential information they have or can bring with them before leaving their former employer.

The insider threat is real - whether it is the employee who inadvertently installs malicious code by clicking on a website or loses corporate data that was on a removable device; whether it is the employee who steals corporate IP or customer data and sells it to a data broker or takes it to a competitor.

Insider Threats – Malicious Intent

Safeguarding organizations against insiders with malicious intent requires effectively enforcing data access policies and auditing user activity with sensitive and confidential data and systems. The stories that have surfaced on company insiders stealing sensitive data worth millions, if not billions of dollars is a non-stop cycle.

- ▣ "Boeing Employee Charged with Stealing 320,000 Sensitive Files"
A disgruntled employee used his internal access rights to download large amounts of data from information stores he had no legitimate reason for accessing, allegedly transferred these files to a thumb drive and removed them from company property.⁴

Why End-Users Are Your Weakest Security Link

▣ “Rogue DBA Steals, Sells Personal Info”

Fidelity National Information Services Inc. reported that a senior database administrator, one of five administrators with that level of access, sold the personal information of about 2.3 million consumers to a data broker.⁵

▣ “DuPont Data Theft Shows Insider Risks”

A DuPont scientist covertly used the company’s computer systems to steal trade secrets valued at more than \$400 million shortly before joining a rival company. About 22,000 document abstracts were downloaded from DuPont’s Electronic Data Library server and another 16,700 full-text PDF files were accessed.⁶

Insider Threats – User Error

Safeguarding organizations against employee errors or accidents requires policy enforcement so that end users are not solely relied upon to make intelligent security decisions. Most non-malicious employees accidentally make improper choices when it comes to handling corporate data. “98% of data leaks are linked to accident or stupidity,” said Nick Selby, analyst with 451 Group, as told to *ComputerWorld*.

These sentiments are echoed by Mary Smith, information security analyst, with Decatur Memorial Hospital, who in an interview with *PCWorld* called end user blunders her #1 security concern: “Innocent, stupid mistakes by end users; people who don’t mean to cause harm, but they are.”

If you follow the news, you can plainly see why these concerns are so valid:

▣ “Identity Theft May Be Problem for TAMUCC Students”

The personal information of 8,000 Texas A&M Corpus Christi students was recently lost in Madagascar when a vacationing professor took the data with him on a flash drive.⁷

▣ One company conducted a “Social Engineering” experiment, in which 20 USB devices (preloaded with a Trojan that would collect passwords and then email the data to the program’s creator) were planted around office buildings waiting for the unsuspecting pawns. Fifteen of these sticks were discovered and plugged into corporate machines, ultimately compromising the individual and organization’s security.

Key Steps to Enforce End-User Security Policies

Organizations can safeguard against these malicious or accidental employee actions through the combination of people, processes, and technology which together must clearly define and socialize policies, automate policy enforcement and provide detailed auditing and reporting. Below are the fundamental steps that organizations can follow to achieve the desired outcome of enforcing security policy:

Step 1: Accept the reality

A first step to understanding the depth of insider threats is recognizing that employees will always open unsolicited attachments, browse a wide assortment of websites and click on links in emails, instant messages and on the Web, utilize outdated and un-patched versions of software, and plug in personal devices or removable media without understanding or caring about the potential impact of these decisions.

iPods, digital cameras, PDAs and other gadgets continue to see rapid adoption among business users, who can very easily plug a USB keychain with a gigabyte of storage into the back of a corporate PC or download photos from their digital cameras as desktop wallpaper or screensavers. These devices spend most of their lives plugged into far less-secure home computers, making it incredibly easy for employees to unintentionally download a nasty virus or destructive code onto an enterprise machine.

Most users are also not security experts and do not generally understand the criticality of some software and operational vulnerabilities that require immediate remediation. Relying upon end users to rapidly install the latest patches is leaving a lot to chance.

Why End-Users Are Your Weakest Security Link

In a perfect world, written corporate policy would be enough to dictate employees' interactions with technology. While a policy is an important step, the reality is that even the most stringent policies need a solution to support and enforce them. Trying to force policies where the employees are responsible has proven ineffective.

A few years ago, John C. Lincoln Hospitals, a not-for-profit organization with more than 3,000 employees based in Phoenix, struggled with ways to enforce their IT security policies. While the IT organization had extensive documentation that dictated John C. Lincoln's endpoint security policies, specifically around the use of removable media, installation of applications and removal of data from the premises, the IT staff did not have the capabilities to effectively enforce these policies. In fact, enforcement was based largely on the honor system and manual processes to perform audits, which was not effective as employees continued to install unapproved applications and files, including games, mp3s, and instant messenger programs.

"Employees were also adding peripheral devices, such as modems, without our knowledge. The modems were bypassing our firewalls and connecting to programs like AOL. We were not sure what was being uploaded or downloaded. We had people loading games, bringing in term papers and use our machines for other non-work related activities," said Rob Israel, CIO, John C. Lincoln Hospitals.

One specific policy stated that users were not allowed to save anything to a hard drive, even though some employee actions directly violated that policy. For example, one employee inserted a floppy disk and inadvertently exposed John C. Lincoln to the Slammer virus – the pandemic worm that used a known buffer overflow in Microsoft's SQL Server database to generate massive amounts of network packets, overloading servers and routers and slowing down network traffic.

"While we recovered from this, we were continually performing reactive maintenance and combined with frequent news reports of compromised data, it forced us to look for methods that would put some weight behind the written word," said Israel.

Another organization, Booz Allen Hamilton, a For-

tune 1000 firm with more than 100 offices, recognizes that its users cannot be counted on to make the right security decision every time. Their IT environment consists of 350 Windows OS servers and 18,000 workstations, 85 percent of which are mobile users. "I am mostly concerned with users propagating vulnerabilities by misuse of the Internet or email," said Brian Oswald, Booz Allen Hamilton. "No matter how much you educate your users, someone is still going to open an attachment or go to a malicious website they receive via email."

It is clear that policies which rely upon employees to make the right security decisions are wrought with failure. So what can organizations do?

Step 2: Enforce user policies across the enterprise

The next step is to remove the organization's reliance on end users being security experts and to provide a way to develop and enforce policy that enables users to focus on their task at hand, but also reduces the risk of their day-to-day decisions when they interact with technology. This involves understanding which employees need access to specific applications, devices and data, enforcing policies that give users access only to what is required in order to successfully complete their job function and ensuring that the applications in use are up-to-date with the latest patches. This requires buy-in from many different groups in making this determination because forcing all machines into the same strict configuration severely limits the ability for employees to effectively perform their job responsibilities.

Employing technology that automates the enforcement of acceptable resource use while preventing and reporting unacceptable use that could put the enterprise at risk is a flexible, yet secure approach. By using technology to enforce corporate policies and endpoint configurations, organizations can ensure that activities, such as the deliberate or accidental execution of malware and unknown or unwanted applications; reading and writing company-confidential or private data to personal removable media; attaching a PC to the corporate network that may have back-level, vulnerable software installed, are simply not allowed.

By enforcing mandatory baselines for critical patches and configurations, organizations can

Why End-Users Are Your Weakest Security Link

automate the remediation process throughout the enterprise and do not have to rely upon their users, ensuring that proper security configurations are maintained while also taking work off the employee's hands. By enforcing application and device control, organizations can flexibly control execution of specific files or removable devices all the way down to the user level. This automated policy enforcement takes the decisions away from the users and enables them to be focused on the job at hand. If there is a legitimate need for access to an application or for use of a removable device, the policy should allow for a specific user access for a defined or infinite amount of time.

Many organizations require data to be encrypted when transferred to a storage device. Some encryption mechanisms can tie individual users directly to the data and/or to the media itself, preventing anyone else from using it. When this type of device management is paired with application control, you're not only securing the device itself, but you're also preventing those devices from launching dangerous executables, which may endanger the organization's data.

At John C. Lincoln Hospitals, the approach taken was to implement Lumension's Sanctuary endpoint policy enforcement suite. "The ability to manage users in a role-based scenario was one of our core requirements, and this product was one of few that allowed that function," said Israel. "By rolling out Sanctuary to all of our desktops, we were able to set policies based on either a user's role or identity. For example, a user could have full thumb drive access, just keyboard access or access to read from a thumb drive or CD-ROM, but not the ability to save anything to the machine from the peripheral."

"The beauty of the whitelisting approach is that it places control of corporate policy squarely in the hands of the IT administration staff," said Israel. "Only devices authorized as having a viable business use will work on corporate endpoints. It also prevents people from installing software without IT involvement, reducing the risk of software conflicts and assisting with software license compliance."

Ensuring that endpoints have up-to-date security configurations and patches is another way to ensure all systems remain compliant against internal policies without interrupting end user productivity.

"Employing an automated patch management solution keeps external threats from impacting the network," said Oswald. "Before PatchLink Update, we were hit twice by viruses. Since deploying the solution, we have had no threats. The risk of not enforcing patch compliance is opening the door to other vulnerabilities."

Booz Allen Hamilton enforces mandatory baselines for patch compliance related to Microsoft and non-Microsoft patches. Their policy provides guidelines for IT to ensure quality and streamlined processes, which includes process, impact and scheduling.

Knowing that technology is in place to enforce proper user behavior as documented in corporate policies can be quite assuring for the IT staff all the way to the executive management team. However, unless this technology is seamless and policies have been socialized throughout the organization, employee productivity is bound to suffer.

"With ever increasing pressure to make exceptions to the rule for one person or program, it becomes harder and harder to protect our electronic boundaries and information," said Israel. "A CIO must always balance good security procedures with the needs of a particular organization. However, as more data is forced into the electronic age, at what point does convenience have to be overshadowed by security? As such, we strive to make IT as invisible to our employees as possible."

Echoed Oswald, "The policy has to revolve around user awareness so they know what to expect and when to expect it."

Step 3: Socialize policies

Policies must be socialized throughout the organization and must also be enforced as transparently as possible so as not to impede end-user productivity. Without proper socialization and end-user understanding and buy-in of these policies, they will be viewed as a hindrance to productivity and users will find a way to get around them. Though an organization should never expect or rely upon its users to become security experts, engaging in security training and socializing corporate policies is a key step to finding that balance between security and user productivity. In fact, among global financial institutions, secu-

Why End-Users Are Your Weakest Security Link

curity training and awareness was identified among the top five priorities for 2007⁸.

Communication is extremely important in educating the users and preventing disruption in employee productivity or all out rebellion. If end users know what to expect and have time to anticipate the change, there is far more likelihood for minimal impact on end users and infrastructure alike. “Explaining why a policy exists is a key success factor. Policies can not be seen as a stumbling block to progress or your end users will find a way around them. In addition, it is important to limit your policies. Having a hundred policies on security is pointless. Not only will your end users not know them, chances are excellent the IT staff will not. Ultimately, as long as your end users know what you’re doing and why you’re doing it, they’re usually more than willing to help you out,” said Israel.

Repetition and consistency around communicating the policy and the transparent implementation of policy is also important in terms of user acceptance. “Maintaining and enforcing consistent communication is key – we report any issues around the security problems and notify them of any delays,” said Oswald. “It is mandatory for everyone to patch – they’re only notified when there is an issue.”

The pitfall of not having a well communicated policy or well-trained employees? Users will find ways around it. “You have to define and develop policies and communicate across the organization to ensure clear understanding and acceptance,” said Oswald. “The pitfall of not having a well communicated policy is that you’ll have more user error or disregard for the importance of security-driven policies.”

While the IT department is typically responsible for drafting security policy, a best practices approach used by John C. Lincoln includes IT working together with disparate business groups to help shape the policy for maximum effectiveness and efficiency. “Each department has their own unique needs. What may work for one may not work for another,” said Israel. “We try and make our policies flexible enough to accommodate the fact that end users will at times bring in outside technology or programs in order to make their job more productive. We encourage the staff to talk to us and let us see how it could fit in the organi-

zation or what other technologies we may already have that they may not be aware of.”

It is also imperative that the policy is enforced on all levels, especially the IT staff as well, which also helps gain the understanding and buy-in from users. “A lot of times IT organizations will exempt themselves from the policies, so we really made sure that even the IT staff were affected and had to do the paperwork,” said Israel. “They still had to document why they need it and how it was going to affect their job performance. And we made that very clear to the end users. This is not just IT putting themselves above everyone else. We were walking the walk.”

Training and socializing policies should incorporate real life situations to have the desired impact with end users, who typically don’t think about the consequences of their daily interactions with technology. Furthermore, the effectiveness of the training and awareness campaign must be measurable. Making a concerted effort to provide tailored security knowledge and awareness programs to all of employees who comprise an organization’s risk will significantly improve the behavior and understanding of individuals as they will understand the policies and know that these policies are much more than a bunch of words on paper.

Step 4: Report on policy enforcement and effectiveness

The CIO and others within the IT department must have access to a continuous report of the organization’s environment, what policies are working and which ones are not, and adjust policies accordingly. Without that visibility into policy effectiveness it is impossible to know what employees and what employee activities are in violation of corporate policy and if the enforcement that is in place prevented issues from occurring.

“We were surprised when we rolled out Sanctuary at how many devices were out there,” said Israel. “We found devices we didn’t even know about.”

Automated auditing and reporting functions give security personnel the flexibility to conditionally allow certain devices, applications or configurations while still maintaining visibility into user activity. For example, if an organization allows only accounting personnel access to specific finance-

Why End-Users Are Your Weakest Security Link

focused applications, it needs to know if a developer was attempting to gain access to these applications. Either there is malicious intent, or there is a legitimate need whether for long term or for a specific project that person is working on.

“You need systems that can automatically report back violations of policies,” said Israel. “The staff required to conduct routine audits makes extensive policies pointless without the tools to audit and enforce it in a clear and simple manner.”

From a best practices perspective, policy compliance should be reviewed on a regular basis as organizational needs may change and user activities might highlight a policy loophole. This includes continuous surveillance of the enterprise environment and user activities and using the gathered information to update policy as necessary. If you can track who had confidential data, how they used it, and were assured that they could not share it outside of the enterprise, then the organization can learn the effectiveness of its policies and report back to regulatory auditors if necessary. “We get reports every week of infractions to our policies,” said Israel. “On a more detailed basis we conduct monthly, quarterly and semi-annual audits each a bit more in depth or focused on a specific area.”

Comprehensive and continuous monitoring and reporting is also imperative for compliance with specific regulations. For example, John C. Lincoln must show due care with regards to the Health Information Portability and Accountability Act (HIPAA). “It’s extremely important to us for compliance,” said Israel. “The ability to quickly and efficiently understand whether we have to do more investigation if there is an issue or to have that hard that there is no issue and this is how we can show you it’s not.”

Effective Endpoint Security Revolves Around Managing Your End Users

An organization’s end users represent a significant amount of risk due to the proliferation of threats that target individuals and due to the rising value of corporate IP, customer, employee and financial data. Criminal organizations are targeting end users as a way to gain access to valuable data and some internal employees target this data for personal financial gain.

“While it should be the duty of every user to protect the company’s assets, the CIO and their IT departments ultimately will be held responsible for any breach of confidentiality or data,” said Israel. “By proactively taking steps to address device and application control, organizations can ensure that they are protected from data leakage while still enabling employees to use the gadgets and programs they need to perform their regular job functions. The most effective approaches to addressing these challenges involve multiple steps that help companies thoroughly understand what applications and removable storage media are needed and by whom.”

Developing sound policies is a solid first step, but end users cannot be counted on to consistently make the right security decision. Enterprises need to protect themselves from the everyday human error and from the occasional corrupt insider. Through transparent policy enforcement technology which puts substance behind the documented words, socialization of policies and awareness of sound security practices, and continuous and actionable auditing information can organizations take a big step forward in protecting their network and data from the inside out.

Sources:

1. IDC Worldwide Security Products and Services 2007 Top 10 Predictions
2. IT Policy Compliance Group, “Taking Action to Protect Sensitive Data”, February 2007
3. Merrill Lynch Security Software CISO survey, June 27, 2007
4. InformationWeek, “Boeing Employee Charged With Stealing 320,000 Sensitive Files”, July 11, 2007
5. ComputerWorld, “Rogue DBA Steals, Sells Personal Info”, July 9, 2007
6. ComputerWorld, “DuPont Data Theft Shows Insider Risks”, February 19, 2007
7. NBC6, “Identity theft may be problem for TAMUCC students”, June 16, 2007
8. Deloitte, Global Financial Services Industry 2007 Security Survey

Lumension Security™, Inc.

15580 N. Greenway-Hayden Loop, Suite 100
Scottsdale, AZ 85260

www.lumension.com