Strategic Goals Drive Security Priorities

By Bob West, CEO, Echelon One

We are at a unique point in history. In the midst of the most severe economic downturn since the Great Depression, we face another significant challenge.

Our technology infrastructure has significant vulnerabilities and with technology at the foundation of most organizations, businesses could cease to function if their systems were compromised. What would happen if a major financial institution lost its ability to conduct business? What if medical records were tampered with and patients received medication that would normally help them but now caused a life-threatening allergic reaction?

These scenarios are realistic and are issues senior executives and board members are not speaking about or well-versed in for a variety of reasons. In this, and future special sections, we will communicate the security and risk issues we face, why they are relevant to leadership teams and what can be done to address these issues.

This is a period of great adversity and in these times opportunities also arise. We believe that by addressing security along with economic issues globally, we can create an environment that is resilient, transparent and will allow us prosper over the long term. Along with the other compelling topics, this special section features several fictional scenarios written by best selling author, Richard Clarke who believes that truth is better told in fiction, and fiction is the best way to appreciate the potential consequences of a cyber breach.

Section Sponsors

Echelon One, LLC
Executive Security Intelligence

RSA CONFERENCE 2009
APRIL 20-24 | MOSCONE CENTER | SAN FRANCISCO

New Security Threats and Vulnerabilities Render Traditional Security Moot

In recent months, CIOs have been subjected to a shock about the vulnerability of their enterprise systems. "We're hearing this wherever we go: public sector, private sector, universities," says Raimund Genes, CTO Core Tech & Anti-Malware with Trend Micro. Genes attributes the scary new security environment to a number of causes.

- Advances in web-based threats and changes in user habits seem to have galloped past the ability of traditional security technologies to protect current systems.
- Cash-strapped CIO staffs tend to react to a new generation of threats rather than pro-actively preparing for them.
- The global recession has made the bad guys—malware writers—hungrier than ever.

However, while security threats are increasing in frequency and severity, most technologists are behind the curve in how they meet new security risks.

"For example," explains Genes, "many large enterprises regard email attachment scanning as their mainstay protection from outside threats. That may have been an adequate measure to take four or five years ago. But our data shows that in the current environment, over 60 percent of malware on enterprise networks come from phishing-type http links in email."

Moreover, today's threats are driven by a profit motive. "Criminals today, don't just want to wreak havoc…they want to monetize their malware. As with all criminal enterprises, they do not want to be caught or disturbed in the process. So they operate under the radar."

The good news is that there are technologies that can help. Trend Micro will be demonstrating these at this year's premier security event, RSA Conference. New endpoint security solutions powered by the company's cloud-client security infrastructure, the Trend Micro Smart Protection Network, block threats in the cloud, before they have a chance to reach corporate networks and endpoints.

What The Corner Office Needs To Know About Information Security

For years – and despite a steady and concerted effort to communicate the contrary – C-level executives and business unit leaders have seen security as a necessary evil. It is a mindset that a growing number of industry experts say should change...particularly as organizations respond to the current economic environment. But if this change is going to happen, the security profession must be associated with delivering business value.

“Executives need to start thinking of Information security as an enabler of business processes instead of a barrier to progress,” says Michel Emelianoff, VP Enterprise Security Solutions at Alcatel-Lucent. “A mature eco-system of network access controls is necessary for good security as well as good governance, risk and compliance management,” he says.

By integrating data protection and accountability into new business processes, security professionals can not only protect key resources, but also allow organizations to pursue new opportunities with a higher level of confidence.

“For instance, at Alcatel-Lucent, we have developed technologies and processes that ensure individual users connect to network resources in a consistent and compliant manner,” explains Emelianoff. “This allows enterprises to create profiles that automate the privileges and responsibilities users have across the enterprise based on their role within the organization. It is how you ensure that a supply chain specialist in an enterprise with a $25,000 per day transaction limit can’t game the system and spend $50,000 per day.”

Cyber Threats: Fact or Fiction?

Stealing Secrets: Corporate Battles

General Cars had worked for years on developing the latest in eco-friendly vehicles. The release date was fast approaching for the Bolt, an electric car whose state-of-the-art design and cutting edge engineering was predicted to revolutionize the automobile industry and make GC billions of dollars in revenue. Six months ahead of the Bolt’s scheduled release, Mizdo, the major Asian automaker, released a car with a similar engine to the Bolt. GC deduced that Mizdo was able to infiltrate its system and gain access to sensitive design information about the Bolt. Having been undercut in the market, GC stock prices plummeted and the company lost millions in revenue.

This capability allows security and risk managers to deliver tremendous business value to the organization. But it also means that the image of the information security professional needs to change.

Enabling and empowering the increasingly mobile workforce offers an excellent opportunity to demonstrate the business value that security departments can bring to bear for organizations.

“Today, a laptop goes missing every 53 seconds, and newspaper headlines scream of lost and compromised data” says Emelianoff. “Alcatel-Lucent has developed technology that enables enterprises to manage and secure mobile laptops and the data they contain 24x7, regardless of the power state of the laptop and regardless of end-user participation.

“We can then allow executives to control how these devices are used in the field. And if an asset is lost or stolen, we can take control of the data remotely and immediately. This means improved visibility, reduced risk, and increased policy compliance. That is business value.”

To learn more about how available security technologies can address strategic business issues, visit Alcatel-Lucent at the RSA Conference, April 20-24 in booth #317.

40 Million
Credit Card Numbers Stolen from TJX

98,930 Affected In
Forever 21 Data Breach

Johnson, Globe Staff

Trojan horse
captures data on
2,300 Oregon
taxpayers ■ 5C

has been active
appears to be getting warmer by tomorrow's end.

continued on page 12C

Hotel Chain Falls
Victim to 14,000
Data-Stealing
Malware incidents

is hard to secure, and it's

University of Indianapolis
Hacked: 11K Student,
Faculty, Staff Records Stolen

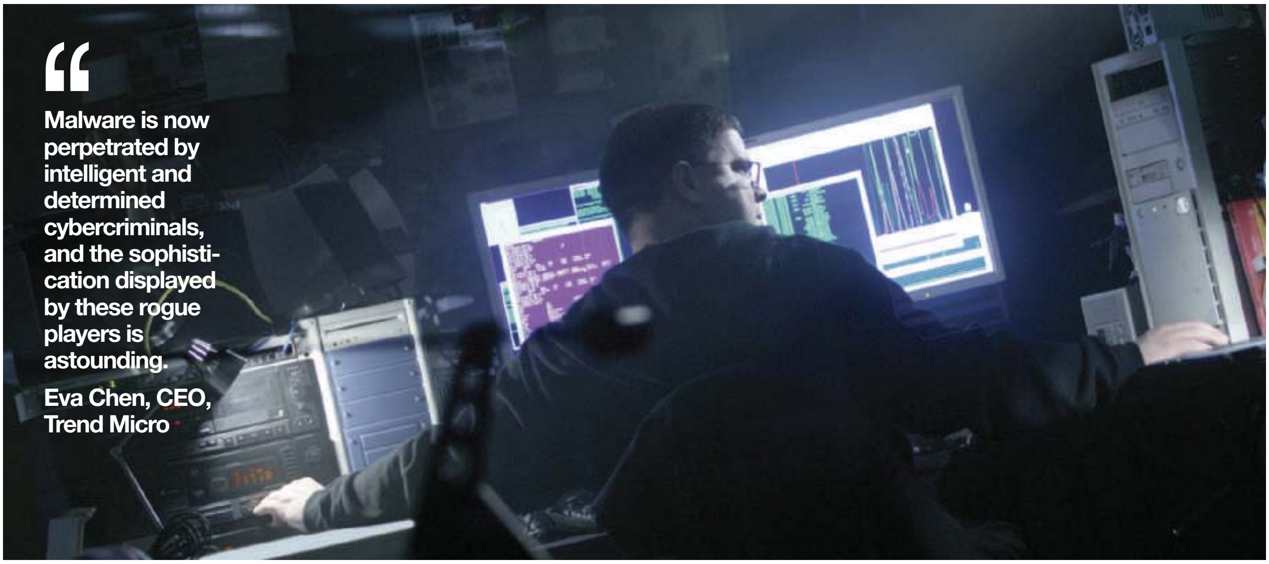
4C

BUSINESS

6,700 Data-Stealing Malware Infections
Plague US Healthcare Company

Information Security: An Executive Guide

Protecting Brand Reputations as Well as Information Resources



> "Malware is now perpetrated by intelligent and determined cybercriminals, and the sophistication displayed by these rogue players is astounding.
>
> Eva Chen, CEO, Trend Micro

Companies today are not only inter-dependent economically, they are interconnected technologically.

The security implications of this are extreme. A breach can not only threaten the integrity of information systems, but can seriously compromise carefully crafted relationships and reputations.

"That is why information security has become such a strategic concern," explains Eva Chen, CEO of Trend Micro. The task before security professionals and business unit managers is daunting, however, as the nature of threats and vulnerabilities become more complex and devious.

"Malware is now perpetrated by intelligent and determined cybercriminals," she explains. "And the sophistication displayed by these rogue players is astounding."

Cybercriminals now use multiple threat vectors to propagate and manage their attacks. They assault business and consumer networks via the web, e-mail, and other forms of digital communication that provides hackers with a way to embed illegitimate code onto unsuspecting computer systems. Because the threats are integrated and coordinated, it is no longer enough to put in place point solutions for each type of attack. Instead, organizations need an equally coordinated defense.

"That is why Trend Micro has developed an enterprise security strategy that is based on what we call the 'Smart Protection Network,'" says Chen. "We have developed a way to correlate threats from multiple vectors by analyzing and providing protection against multiple components of an attack. We are able to effectively integrate feedback from our anti-spam, anti-malware, webcrawlers, honeypots and other technologies to provide a current and coordinated security risk management posture," she points out.

By combining messaging, file and web security services, businesses get the benefit of integrated threat intelligence across all three threat vectors. The result is real-time protection against the largest possible number of threats in the fastest possible time.

Cyber Threats: Fact or Fiction?

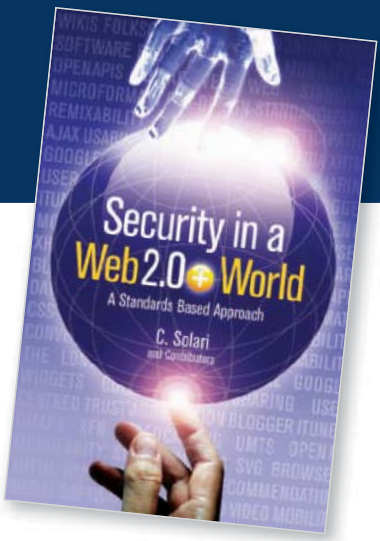
Counterfeit Drugs: Risk Of Contamination

An e-mail with an attachment was sent to an employee at Callusp, a large pharmaceutical company that produces a widely used blood thinner, called Hepatin. Clicking on the attachment in the e-mail released an insidious piece of code that exfiltrated sensitive data out of Callusp and directed it to a terminal in Canada. It was unclear what the hackers wanted – the patent and formula of the drug or something more malicious and lethal. Either way, the cyber vulnerabilities of Callusp proved to be destructive to the company's profitability.

To learn more about how these security technologies work together in integrated products, solutions and SaaS service offerings, visit Trend Micro at the RSA Conference, April 20-24 in booth #2017.

Web Sites to Watch

www.alcatel-lucent.com
www.trendmicro.com
www.us-cert.gov
www.scmagazine.com
www.secureitlive.com
www.rsaconference.com



Security in a Web 2.0+ World by C. Solari

NNetwork convergence, cloud computing, and other phenomena of the Web 2.0 era are exposing ICT security to new and dangerous threats and causing a re-evaluation of traditional security methods.

In Security in a Web 2.0+ World, noted network security expert Carlos Solari and co-authors explore the current systemic vulnerabilities of information systems and make a strong case for taking a rigorous standards-driven approach to designing security into products at the very earliest stage of their development.

Security in a Web 2.0+ World looks at the perplexing issues of cyber security and provides a guide to information security and standards in the Web 2.0+ era. Solari highlights new security standards (ISO/ITU) that provide manufacturers and developers with a means to create products and services that can meet the challenges to security posed by emerging technologies. By implementing standards-based development, companies are able to demonstrate the level of maturity their security solutions have achieved and instill confidence in their customers.

Lead author Solari joined Alcatel-Lucent Bell Labs in 2006 after spending nearly 23 years in some of the most highly trusted operational roles within the U.S. government: Army Officer, FBI Senior Executive and White House CIO. In his current role as VP, Quality, Reliability and Security at Alcatel-Lucent, Solari applies the breadth of his experience in national security, law enforcement and public safety to addressing security in a Web 2.0+ world.

Meet the author and pick up a free signed copy of 'Security in a Web 2.0+ World' at the RSA Conference, April 20-24 in Alcatel-Lucent booth #317

Sandra Toms LaPedis Area VP/GM, RSA Conference

Can you talk about the importance of gathering industry professionals at a major venue?

Anyone who has engaged in face-to-face dialogue with an industry colleague will tell you that no technology can replicate the relationship-building power of those interactions. In talking to our attendees, we have learned that people specifically come to RSA Conference not just for the important content and programming, but to talk with peers, meet industry luminaries, and join impromptu hallway discussions. Especially for the information security industry – one that changes daily – timely education is the most critical component in understanding the security issues that matter and how to react to them.

What trends are you seeing in the security industry with respect to how people consume information and how is web 2.0 Changing the landscape?

Today there are myriad ways for information to be created and shared. Recently, the information security industry has seen dozens of groups crop up on LinkedIn and Facebook, an entire network of security bloggers emerge and a dramatic increase of relevant conversations on Twitter.

For us, 2008 was the first year that RSA Conference offered media credentials to bloggers. We also utilized Twitter in 2008 and will "tweet" more around the 2009 event to effectively connect with our attendees. RSA Conference has its own LinkedIn and Facebook group pages where members can connect, discuss trends and receive Conference updates.

What is different this year at the RSA Conference and what sets it apart from past years?

A goal for RSA Conference 2009 is to demonstrate how innovative our industry can be. As such we've created Innovation Sandbox, an exciting new program where participants can explore the technologies that promise to transform information security. Attendees can collaborate on solutions to tomorrow's security challenges, preview products still in development and vote for the most promising ideas and technologies.

"Dozens of groups crop up on LinkedIn and Facebook, an entire network of security bloggers emerge and a dramatic increase of relevant conversations on Twitter.