Ron Rittenmeyer

“Information Security: Striking a Balance Between Risk and Reason”

SMU Management Briefing Series
October 10, 2007

A lot of things come to mind when you think about information security and protecting sensitive data:

- Identity theft
- Medical privacy violations
- Threats to our national security

Cyber-crime has evolved a lot over the years: from hackers merely causing mischief to show off their abilities to criminals stealing millions of dollars online.

The fact is, security breaches within business and government are more common than we’d like to admit, whether they result from:

- Unintentional security errors
- Large-scale cyber-attacks
- Or crimes for profit

You might recall some of these stories:

- At TJX stores, hackers made off with more than 45 million credit and debit card numbers, resulting in a cost to the company of $256 million as of August.

- Cyber attacks on Estonia’s government: Called the “first war in cyberspace.” Estonia alleges these attacks were launched by Russia or Russian sources. They almost shut down the country’s digital infrastructure.

- Monster.com breach, where personal information on 1.3 million job seekers was stolen.

And these are just a few of the breaches that get reported.

Security threats are real and growing, and no one is exempt from them.

Lawlessness in cyberspace has been compared to days of the Wild West. The Wild West pales in comparison, however. It never was this vast, fluid and interconnected.

As bad as **“**Billy the Kid**”** was supposed to be, he never went “global.”

You could get carried away by such news or, worse yet, be taken advantage of because of it. Opportunists might try to capitalize on the fear, uncertainty and doubt, promising so-called quick fixes or silver bullets.

There are no such things.

Short-sighted tactics that lead to knee-jerk reactions are not in the best interest of business or government. What's required is an informed and reasoned approach.

We need to ask ourselves:

- What are the facts and impact behind these threats?
- What can we do to minimize – or prevent – them?

I'd like to offer my perspective as a business leader who's invested in data security across diverse companies in many industries and, as a leader whose business is committed to protecting the information resources of our clients.

During my remarks today, I will:

- Provide you a snapshot of today's security landscape
- Propose a common-sense course of action to improve data security
- Consider what we – as business and civic leaders – can do together to address this

TODAY'S SECURITY LANDSCAPE

Let me start with a snapshot of today's security landscape, with a few things for us to consider.

First, globalization and the Internet are sending your personal information everywhere in the world.

A question for everyone here: Is your data being transmitted through a secured network – and stored securely at both ends? If it's not, your online transactions might travel unprotected through one or more countries – before ever reaching their final destinations.

The Internet seeks the path of least resistance for your data. And that could take it any number of places in transit – some of which are more secure than others. This means you must be prepared for the lowest level of security at any one of those transit points to avoid data loss.

Even something as simple as a customer service call might be answered somewhere across the globe, which means they'll need your personal information in order to help you.

At EDS, we provide a secure connection between EDS and our clients and their IT assets through our Global Services Network. It is built to the highest standards and is used by our Defense Department in some aspects of its operations.

Second, almost every major country has – or will soon have – its own privacy and data protection laws.

These regulations place restrictions on transfers of personal information across national borders. Some regulators apply their laws to even <u>accessing</u> personal information across borders.

Within the United States, we have as many as 39 different state laws regarding notices to individuals affected by certain data security breaches, while the other states have no such law.

Clearly, this is an area crying out for consistency and reason – for the sake of the individual – as well as the companies involved.

In the early days, when a company handed EDS its data, we processed it – simply and securely.

Now, we have to know what your data is and, for example, whether it is subject to export controls or privacy regulations. And, we make sure that the data we handle in countries around the world comply with – or exceed – their respective regulations.

Not doing so can result in potentially serious business issues for our clients, embarrassment for all of us and potentially stiff financial implications.

Third, 125 to 175 new malicious software codes pop up every day. That's according to McAfee, a longtime leader in the IT security space.

The FBI reports that virus attacks continue to be the source of the greatest financial losses.

Some good news, however: Improvements in the IT industry's ability to deal with virus attacks – through widespread deployment of anti-virus solutions and aggressive software patching – are curtailing these losses.

Keep in mind that an unexpected "zero day" virus still could cause billions of dollars in damages worldwide – like we saw with the "Code Red" or "I Love You" viruses.

Currently, EDS identifies and blocks 100,000 intrusions a month for both EDS and our clients.

Vigilance continues to be the order of day.

Fourth, while data breaches are frequent, the U.S. Government Accountability Office suggests that resulting identity theft is limited.

Some sources report that less than 3 percent of breaches result in fraud. However, a data breach that does result in a loss can cost an organization millions of dollars.

The Ponemon Institute – a leading privacy and security research group – reports the average cost of a data breach may result in a loss of nearly $5 million. That equates to about $180 for every lost record.

Looking at the bigger picture, data breaches and identity theft have become organized crime's #1 business. The FBI estimates that cyber-crime has cost the U.S. economy about $67 billion in damages during a 12-month period.

Just for comparison, $67 billion is the annual GDP of Peru.

Fifth, your security level is only as strong as the weakest link in your supply chain.

It's not just about security on your servers and network. Rather, it's about the security standards of your partners – and their partners as well. If they're not secure, they provide potential entries into your systems.

Identifying the electronic interfaces – and verifying the security of trading partners – should be as important as verifying their financial solvency.

Finally, no one has yet to achieve perfect security or 100 percent assurance.

As hard as everyone works to protect data, breaches do occur.

To strive for "perfect" security could mean over-spending if you don't consider the ultimate cost and benefits. Not all information has the same risks of exposure – or poses the same risk if exposed.

The goal, then, should be to achieve a reasonable degree of protection. And that's based on a risk assessment of the information you're trying to protect.

One of the challenges we all face is that the definition of "reasonable" is a moving target. That's because of ever-changing business needs, regulations and security threats.

To stay ahead, business and government must have a sound framework of security policies, tools and methodologies – all of which must move with the times.

So that's the security landscape – not pretty, but something that is addressable.

DEVELOPING AN INFORMED, REASONED APPROACH

So how do we go about developing an informed, reasoned approach?

At EDS, we see security as a proactive defense against anything that threatens a business' – or a government's – stability, growth or performance.

It's more than defending the perimeter these days. It's a culture shift.

It's a business-oriented approach with a broad reach into every aspect of corporate or government operations and planning.

As such, a good security program is a comprehensive one that revolves around people, technology and processes.

Let's take a look at people.

Information security is as much a management concern as it is a technology issue. Training and employee awareness must be implemented to make your security program truly effective.

In addition to security audits, some organizations are investing in – or intensifying – security training for their employees. This includes everything from establishing effective password policies to advanced systems architecture training.

This also includes practicing good physical security, such as locking doors and locking up laptops and CDs. In fact, 70 percent of data breaches result from the loss of off-network equipment, such as a laptop.

The FBI reports a laptop is stolen every 53 seconds … with 97 percent never being found.

At that rate – since you left your office or home to come here – 75 to 100 laptops are now in the hands of a criminal.

Hope all of you locked up your PCs before you left.

However, this is where technology really can make a difference.

Encryption of laptops – and software that electronically wipes a hard drive if someone tries to crack the password – can make information inaccessible when a laptop is stolen or lost.

Encryption, remote data wiping and new "data leakage" technologies must be used to augment and support good security policies.

The greatest data leakage threats actually come from employees … or contractors and other partners. The most common ways sensitive information is leaked – intentionally or not – is through e-mail, instant messaging, Web mail and blogging.

Advanced content scanning and analysis of a company’s outgoing data can help detect the leakage of sensitive or classified information.

Older tools that we have used for years – such as anti-virus and firewall technologies – are "table stakes" for security. In the past, we‘ve seen clients who viewed such tools as being "nice-to- have" items that can be cut when budgets get tight.

This is simply short-sighted and not sound judgment.

Finally, processes and procedures for handling sensitive data are just as important as billing, finance and other operational processes. These include systematic and routine software updates and patches, which can pay huge dividends in preventing security incidents.

Using “zero touch” technology that we jointly developed with Microsoft, EDS can deploy system upgrades to secure an enterprise up to five times faster – and with less risk.

The point is, security needs to be treated and integrated as a standard business process – not something just added on. And should be seen as a three-way strategy of people, technology and processes to protect your operations.

The stakes are high. More and more, it's only a matter of when you will have a data loss through crime or carelessness – not whether you will have one.

All the more reason to make security an integral part of your business plan – from the outset.

Those are some of the basics for developing an informed, reasoned approach.

When it comes down to deciding a course of action, we have to ask ourselves some hard questions:

What's the real impact of a security breach on my business?

The answer depends on your customers and the type of data you deal with. As I said earlier, not all information has the same risks of exposure.

Classifying your data assets by risk level will help focus your security efforts.

Also related to this question are the various rules and regulations you must comply with.

Two that touch our everyday lives the most are:

- The regulations set by the Health Insurance Portability and Accountability Act (HIPAA) for healthcare standards
- And the rules set by Payment Card Industry (PCI) regarding credit card standards

How do you ensure security without hamstringing your operations?

This is a real judgment call.

At one extreme, you can lock your system down so tightly that nothing gets through – including your customers. At the other extreme, your goal to make services and information easily accessible to customers might compromise their privacy and result in loss of data.

In the end, each business has to weigh risk tolerance against operational agility and customer responsiveness.

What kind of a return should business and government expect for their security investments?

First, I believe security is the cost of doing business in our global, online economy – not a discretionary cost we cut when times are tough.

Second, to assess the real benefit of a security program, you have to first monitor user compliance and then measure the impact of each initiative.

Third, being known for smart security practices builds brand integrity. It increases the likelihood your customers and partners will continue to do business with you because they feel safe.

Again, your approach to data security should be an informed and rational one, coupled with a mindset that anticipates and prepares rather than worries and overreacts.

WORKING TOWARD A JOINT SOLUTION

Now, let me address the roles of business and civic leaders in dealing with this difficult, but important topic.

All of us will benefit from improved security if we work together toward effective standards and increased cooperation.

Developing national standards around data security is a step in the right direction.

At EDS, we support the legislation introduced by Rep. Tom Davis (R-VA) and Senator Norm Coleman (R-MN) on government data security breaches.

This legislation asks for a clear definition of the type of sensitive information agencies need to protect, as well as timely notification when sensitive information is compromised and poses harm to individuals.

EDS is working with industry associations to develop a set of principles on what should be included in any national security breach legislation.

Establishing standards will require more leadership within the private sector, which owns 80 percent of the infrastructure. Businesses should not wait on government because:

- They might not like what government comes up with
- Legislation is often too old and out-of-sync with technology once it’s enacted

In closing**,** my objective today was to help you strike a balance between risk and reason around information security – and to leave you a little smarter about the real threats that all of us face.

Let me share with you one more news story.

A few weeks ago, a 23-year-old hacker on his way to federal prison said that breaking into computers was “so easy a caveman could do it.”

In fact, this hacker broke into 15 telecommunications companies – and hundreds of businesses – worldwide before being caught.

And you know what? Most of this could have been prevented with a few simple security measures. But they weren’t in place.

As a result, this hacker and his partner were able to steal – and then resale – Internet-based phone minutes at a discount for a million-dollar net profit.

Whether we’re talking about a couple of high-tech “cavemen” on a crime spree or a seemingly innocent security breach by a child, the results can create havoc – either way.

Thank you.