Got Security?

Protecting Critical Assets in an Age of Cyber Intrusions

By Chuck Adams, Cisco Internet Business Solutions Group (IBSG)

Today, our information and communications technology (ICT) infrastructure, along with the data it collects, stores, processes, and shares, is among our most critical strategic resources. Individuals, enterprises, and nations increasingly depend on ICT to find their way, pay bills, conduct business, and collect taxes. We have come to expect anytime-anywhere connectivity to people and information through mobile phones, wireless technology, web conferencing, instant messaging, social networking, and a growing list of other technologies.

From online banking, to electronic medical records, to virtual classrooms, to national defense networks, this "always on" capability is transforming the ways we work, live, play, and learn.[SM]

The more dependent we become on ICT to run our lives, our companies, and our nations, however, the higher the stakes in the event of an attack on our information systems. This paper will take a brief look at some of the ways intrusions on commerce and infrastructure are targeting nations and global organizations, and will suggest a strategic approach to securing our critical resources.

> "Information has become a strategic resource that may prove as valuable and influential in the post-industrial era as capital and labor were to the Industrial Age."
>
> "Cyberwar Is Coming!"
> John Arquilla and David Ronfeldt
> International Policy Department

Keeping Ahead of *This Week's* Threat

Government information systems are continually probed by outsiders millions of times a day. While many of these scans do not trigger problems, federal agencies reported more than 16,000 threats in 2008, a threefold increase from the year before.[1] In July 2009, a powerful denial-of-service attack overwhelmed U.S. and South Korean computers for days, targeting numerous government agencies, the White House, the Pentagon, and the New York Stock Exchange.

As Russian troops rolled into Georgia during the conflict of August 2008, a seemingly coordinated cyber attack was carried out by unknown civilians, jamming Georgian websites and communications. Many of the civilian computers used in the attack had been taken over by a "botnet" that caused them to unwittingly bombard targeted websites in a denial-of-service attack.[2] As the first anniversary of the conflict approached, Twitter, Facebook, and other social networking sites were brought to their knees for several days by an attack that targeted a Georgian blogger.

Not all security breaches are so malicious, but they can be just as dangerous, as we saw in June 2009 when a document detailing information on nuclear sites was inadvertently posted on the U.S. Government Printing Office's website.

Security threats can come from anywhere—from a careless employee, a teenage hacker, a serious criminal, or a terrorist organization. And they can threaten our most critical resources. According to a report in the Foreign Policy Journal, the energy infrastructures of the United States and other countries have been attacked by cyberspies, as well as by criminals hoping to extort money.[3]

Generally, there are two broad types of cyber intrusions: structured and unstructured. Structured intrusions are targeted attacks carried out by hackers-for-hire with malicious intent. Unstructured intrusions tend to be pranksters or people seeking to enhance their hacker reputations. We can think of these attacks as the "graffiti" of the information age—someone saying, "I was here, and you didn't catch me." If many organizations today are unable to control even the unstructured attacks, what chance do they have against deliberate, rapidly evolving, targeted attacks?

Opportunity: Build Trust, Build Value

When we think of cyber intrusions, what comes to mind for most people is identity theft, infection by viruses, loss of privacy, denial of service, or loss of information integrity. While all these are examples of specific kinds of vulnerability, the primary asset we need to protect is the value of the Internet.

The value of the Internet and our information systems is based primarily on the trust people have in them. If we look to electronic medical records and other e-healthcare initiatives to help bring down the cost of healthcare, people must have confidence that their health records will remain confidential. If we electronically transfer vast amounts of money among financial organizations, people must know that the transactions are secure. If an individual types his or her social security number in order to pay a bill online, he or she must trust that this information will remain private. If people distrust the basic security of these actions, they will stop using these systems, diminishing the value of the Internet and the advanced technologies that make these activities possible.

Preserving this value by building trust in Internet technologies is a responsibility that the entire community of users must bear.

With every threat, there is an opportunity to rethink the ways we secure our critical assets. Today, our opportunity—and challenge—is to create a comprehensive risk-management strategy that preserves trust and value at the personal, corporate, national, and global levels. Since any system is only as secure as its weakest link, it becomes imperative for each of us

to take ownership of what is under our direct control, and to work toward a broader risk-management approach through industry standards and other cooperative efforts.

First, Take Charge of Your Own House

In many organizations, security is built around a patchwork of "protect and defend" products and tools. Critical functions such as continuity, disaster recovery, compliance, and other physical and cyber security programs remain largely independent of each other and, in worst-case scenarios, isolated from the rest of the organization.

With annual global losses associated with cyber security attacks exceeding US$1 trillion,[4] it is clear that this fragmented approach to security is not working. Information technology leaders need to step back and take a broad look at their overall security strategy, not just react to the specific challenges raised by each new incident. They should develop an all-encompassing, unified risk-management vision aligned with all functional areas to accomplish core organizational objectives and to preserve the confidentiality, integrity, and availability of all critical resources. As we align security policy with larger organizational objectives, we have an ideal opportunity to fundamentally strengthen our overall approach to security and to embed more resiliency into the core of our operations.

The challenge and opportunity for security leaders is to show that their teams have the skills needed to harvest accurate, actionable, and timely information from the cyber realm. They can be most effective when they use these skills in the broadest ways, using well-chosen technology tools to help them collect and analyze the data.

Broaden the Focus with Cross-Sector Cooperation

The cyber world we all share does not recognize firm corporate or national boundaries, so we need international standards and cooperation to effectively protect the Internet in a "borderless" way. In addition to taking ownership of the resources within our control, we need to establish cross-sector cooperation through public-private partnerships among industry groups, government entities, educational organizations, financial institutions, healthcare providers, and energy providers. There must be broad participation in defining, adopting, and complying with industry standards.

There have been numerous government attempts to coordinate a defense against cyber attacks. The Federal Communications Commission formed a cyber security working group to assess vulnerabilities in the nation's communications infrastructure and make recommendations to address deficiencies.[5] In Europe, an EU agency has published the first pan-European Good Practice Guide on Network Security Information Exchange (NSIE), an attempt to help public and private stakeholders set up NSIEs on a national level to help protect critical communication networks and services.[6]

While some enterprises may look to governments and international organizations for leadership, it is really up to each one to protect its own assets and forge partnerships with others who are willing and able to cast a broader net of protection.

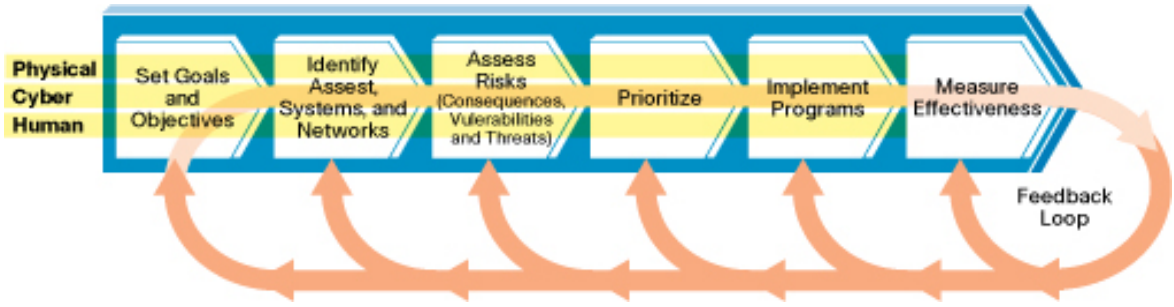
"It's one grid, one global network, and we're all stuck in the same boat. We need to establish some rules."

Dr. James Lewis, Director of the Technology and Public Policy Program,
Center for Strategic and International Studies

Establish a Comprehensive Framework

In its 2009 National Infrastructure Protection Plan, the U.S. Department of Homeland Security (DHS) describes its overall strategy as managing risk by deterring threats, mitigating vulnerabilities, and minimizing consequences. Figure 1 illustrates the DHS risk-management framework, with feedback loops for continuous improvement.

Figure 1. NIPP Risk Management Framework



Source: National Infrastructure Protection Plan, U.S. Department of Homeland Security, 2009

Any organization, regardless of size, should establish a security strategy and framework that are as comprehensive as the DHS approach: set goals, identify assets, assess risks, prioritize, implement programs, and measure effectiveness. Adopt standards and hold all stakeholders accountable for following them.

Conclusion

In a world with broad Internet access and instant global communications, it is impossible to establish iron-clad protection against all cyber intrusions. We can, however, minimize the damage of such attacks by creating a unified risk-management strategy to protect our own resources, and by reaching across public and private boundaries to cast a broader security net. We must begin to consider our organizational risks in a unified and comprehensive manner, take action to address them, and assure our customers, partners, employees, and citizens that our measures are effective. While this is no easy task, the integrity of all our critical information assets and the very value of the Internet depend on our success.

For more information, please contact:

Chuck Adams
Business Resiliency Solutions Manager
Cisco Internet Business Solutions Group
cjadams@cisco.com
+1-512-340-3430

Endnotes

1. FOXNews.com, July 8, 2009.
2. Thomas Claburn, InformationWeek, August 17, 2009.
3. Joel N. Gordes and Michael Mylrea, "A New Security Paradigm Is Needed to Protect Critical U.S. Energy Infrastructure from Cyberwarfare," Foreign Policy Journal, September 14, 2009.
4. "Unsecured Economies: Protecting Vital Information," McAfee, January 2009.
5. TG Daily, September 8, 2009 (http://www.tgdaily.com/content/view/43908/108/).
6. i-policy.org, September 11, 2009 (http://www.i-policy.org/2009/09/enisa-launches-guide-on-mitigating-network-security-vulnerabilities-threats-and-cyber-attacks.html).