The Economics Of Cyber Security

Written by Peter Mills

Malicious cyber activity, from hacking and identity fraud to intellectual property theft, is a growing problem within the global economy. While news reports tend to focus on the impact of cyber crime on consumers, a recent Global Economic Crime Survey, published jointly by the Center for Strategic and International Studies and McAfee, notes that “direct losses to consumers may be the smallest component of the cost of malicious cyber activity.”

Although consumer losses—estimated to be around $1 billion annually—are significant, the McAfee survey points out that malicious cyber activity aimed at businesses may cost the global economy as much as $400 billion each year from stolen trade secrets, stock market manipulation and intellectual property theft—which is by far one of the biggest concerns for companies both large and small.

Hidden Costs of Intellectual Property Loss
The loss of intellectual property and confidential business information is one of the most serious, and hardest to quantify, components of cybercrime. The McAfee report notes that the “actual value of intellectual property can be quite different from the research and development costs incurred in creating it.”

Take, for example, a recent case in which the FBI arrested a Michigan couple for stealing trade secrets related to hybrid technology from a major automobile manufacturer. The couple planned to sell the secrets to a competitor. If they had succeeded, the financial impact on the company would have been far more devastating than the cost of the R&D alone.

While it may be satisfying to see some perpetrators of cyber crime facing jail time, this is still the exception. Many companies victimized by cyber theft may not be aware for years—or ever—that they’ve lost their intellectual property or that someone illicitly accessed their confidential information. In these cases, the McAfee report states, “the victim may not know the reason they were underbid, a negotiation went badly or a contract was lost.”
Better Awareness of the Threatscape

The risks to intellectual property and sensitive information may be growing, but the means of exploitation haven’t evolved that much in a decade, says Doug Steelman, CISO of Dell SecureWorks, a security services provider that helps companies understand what’s happening across their networks.

What has changed, Steelman says, is that companies have a better awareness of the threatscape. “The things that threat actors are doing—for example, spear-phishing exploitation, client-side browser exploitation, Internet-facing web application exploitation, and denial-of-service attacks—are activities they’ve been doing for probably ten years now. I think that what’s increasing is the understanding of what the threat actors are doing.”

That’s good news, he explains, because every organization needs to understand that there is a real risk from a variety of malicious attackers bent on profiting from trade secrets.

“Intellectual property theft is a concern for every company that’s connected to the Internet.”

—Doug Steelman
CISO, Dell SecureWorks

Visibility Helps Prevent Loss

No matter where threats originate, effective cyber security can only be accomplished with appropriate visibility into what’s happening on corporate networks. “It seems intuitive,” Steelman says, “but if you can’t see the threat, you’ve got no chance at preventing an attack.” That means companies need ways to look at and understand network traffic, user Web surfing, e-mail distribution and so on.

Dell SecureWorks security services enable visibility into its customers’ networks, which leads to threat interdiction or, at a minimum, detection, Steelman explains. “Prevention will eventually fail. When it does, organizations must ensure they can see what’s happening on their networks. Otherwise, the way they find out about embarrassing exploitation of their infrastructure is through the press or a visit from law enforcement.”

Obviously, insiders are uniquely placed to get their hands on sensitive information. “That’s very difficult,” Steelman says, “because you’ve consciously made the decision to give someone access, and if they abuse that access to take information or disrupt operations, that can be a more devastating problem.”

Bridging Communication With the C-Suite

While the understanding of the threat vectors is getting better, communication of the threats to senior executives is still lacking. Steelman believes that the C-suite views cyber threats differently than other types of business risks. That’s in part because in the world of cyber security, the language used doesn’t mesh with the language that senior executives are used to hearing.

Steelman says that Dell SecureWorks has developed a cyber security profit-and-loss decision-making framework that communicates in plain language what the C-suite needs to understand. “We call it a common operational picture, or COP. The C-suite understands the language of P&L, but to date there is no ‘cyber P&L.’ Senior leaders usually have to take the word of the security leader briefing them. We believe we have created an operational construct and measurement to enable tactical and strategic decision making with respect to cyber.”
The economics of cybersecurity

1. Test defenses
2. Assess vulnerabilities
3. Invest to reduce risk

Formula for success

Security breaches make the news daily. Theft equates to a loss of data, money, productivity and reputation. Because threats are ever-evolving, your security must too. How do you make headway, not headlines?

Dell SecureWorks has a three-step formula for success. Have a complimentary conversation with an expert security consultant to learn more. Get started now.

Visit secureworks.com/forbes to beg’n.

Dell and the Dell logo are trademarks of Dell Inc. Dell disclaims proprietary interest in the marks and names of others. ©2013 All rights reserved.
“Prized Possessions” in the IP Space

The threat to intellectual property has grown tremendously as companies have transitioned from tangible to intangible assets in a post-industrial, knowledge-worker society, says Chandra McMahon, vice president, Commercial Markets, Cyber Security, for Lockheed Martin’s Information Systems and Global Solutions business.

“There’s a lot more for adversaries to gain by stealing intellectual property than there is from some of the assets that actually get created or manufactured,” McMahon says, because “a company’s prized possessions, regardless of industry, are in the IP space.”

Intellectual property, she explains, can be anything from research and development to manufacturing processes to financial data. “Companies are really looking closely at what they consider their crown jewels in terms of information, and are trying to take action to better protect them.”

No company is likely to be off the radar of cyber attackers, McMahon reports. “I have yet to come across a company that says, ‘I haven’t had to deal with hacktivists or cyber criminals or attacks from nation states.’”

Lessons Learned From Determined Cyber Attackers

As a large federal government contractor, Lockheed Martin not only helps defend government and commercial networks, it also is a target of sophisticated nation-state attacks. McMahon, who previously served as Lockheed Martin’s CISO, says that defending against these attacks, and having high visibility into the attacks against commercial and critical infrastructure customers, means the company has a unique perspective on cyber threats. “It gives us insight into a broad array of adversaries and the different types of tactics and techniques that they’re using,” she explains.

Determined attackers provide the company with a wealth of threat intelligence. “The whole premise to our approach to cyber security is to be able to gather intelligence around the adversaries, around their tactics and techniques, and then use that intelligence so it’s actionable,” McMahon says.

This intelligence is used for the defensive countermeasures that are built into Lockheed Martin’s solutions. In fact, the company has been credited with identifying several zero-day vulnerabilities (previously unknown vulnerabilities that are hard to detect and defend against), and coming up with ways to block these attacks.

The company has established world-class centers focused on research and development in cyber security called the NexGen Cyber Innovation and Technology Center to innovate and collaborate on new defensive capabilities for customers. Today, there are centers located in Maryland, the U.K. and Australia.

The Weakest Link

No matter how well you protect your own information or employee data, intellectual property is ultimately only as secure as the weakest link in the supply chain. McMahon emphasizes that it’s critical to consider the entire “cyber ecosystem” in which information travels or is stored.

Lockheed Martin works closely with its suppliers to ensure they have a heightened awareness of the threatscape and participate in information-sharing programs so that they can adequately defend themselves. “In some cases, we’re looking to help those companies bolster their defenses through the use of Lockheed Martin’s own cyber security services and solutions,” she says.

The threats to intellectual property and confidential business information are real, and the results can be devastating—not only to the companies that suffer the losses, but to the employees of those companies, the communities where they live and work, and the global economy. Being prepared to defend against and mitigate cyber attacks, with the assistance of cutting-edge research, technology and expertise, should be a cornerstone strategy for every company.
With financial institutions facing increasing risk of data loss, identity theft, sabotage and more, the ability to effectively manage cyber risk has become a top priority. Lockheed Martin Cyber Intelligence is helping major financial institutions get cyber smart by integrating it into everything they do—from securing the infrastructure, applications and data they rely on every day to cyber forensics that help predict and change the future. Lockheed Martin Cyber Intelligence: protecting corporate America’s competitiveness.