THE ECONOMICS OF CYBERSECURITY

ARE YOU WILLING TO RISK KILLING YOUR BUSINESS?

BY THOMAS M. STOCKWELL

The era of cybercrime is upon us, and the questions it raises are simple: How much is it hurting us? And can it be stopped?

Across the Cybercrime Spectrum

Cybercrime has evolved with the technologies that enable it, but generally, the term describes any criminal activity that involves the Internet, a computer system or computer technology.

Cybercrime covers a wide range of activities and includes both technological and contextual components. At one end of the spectrum are breaches of personal or corporate privacy, otherwise known as identity theft. At the midway point are transaction-based crimes, such as fraud, digital piracy, money laundering and counterfeiting. These crimes have specific victims, but the criminals often remain anonymous.

At the farthest end are larger attacks that use advanced technology to damage businesses, institutional credibility and/or physical infrastructure. One such example occurred in 2011, when foreign hackers remotely accessed a water station in Springfield, Ill., and destroyed a water pump.

All of these activities represent a misuse or misappropriation of technology to subvert a victim's control of resources. But no matter how the term is defined—either technically or contextually—the cost of cybercrime continues to escalate.

Robert Rodriguez, chairman and managing principal of Security Innovation Network (SINET), a company focused on creating a coalition of builders, buyers, researchers and investors to help fight cybercrime, says it's a significant conflict that should be taken seriously.

"The challenge is real and the time is now to advance innovation, lead change and build trusted global collaboration models between the public and private sectors to defeat cybersecurity threats," he says.

Managing Risks As Cybercrime Targets Widen

In 2011, it's estimated that cybercrime cost individuals and corporations worldwide an astounding $388 billion, according to a Norton study conducted in September 2011. The average cost to U.S. businesses in 2011 by one sample of organizations was an incredible $5.9 million a year, according to the Ponemon Institute.

During 2012, however, that average escalated to $8.9 million per year, an increase of 6% from 2011 and 38% from 2010, according to the 2012 Cost of Cyber Crime Study.

Most telling is the increasing average time it takes for corporations to counter cyberattacks. In 2011, it was 18 days (average cost: $416,000). In 2012, the time rose to 24 days (average cost: $592,000), an increase of 42%, according to that 2012 study.

Of course, the estimates are speculative, and, according to Kelly Bissell, who leads Information & Technology Risk Management and Global Incident Response at Deloitte & Touche LLP, highly suspect.

"It's surprising to me that there is no reliable estimate of the cost of cybercrime," says Bissell. "In 2009, President Obama

noted that cybercrime might cost businesses $1 trillion. There are other estimates of $250 billion, but others say it is $12 billion."

Regardless of the estimated size of the problem, the unfortunate truth is that every individual, company and government entity faces significant risks of becoming a victim of cybercrime. And while the cost in time and money required to address the holes in our cybersecurity continue to stagger the imagination, the question most C-level executives are asking is, "how can they manage this risk?"

Addressing the Risks

Bissell has ample experience in tackling critical aspects of cybercrime risk management. His practice helps organizations devise and implement critical security strategies that measure threats and protect against cybercrime.

"There are at least three elements that we look for in a company's security strategy," he says. "Which security projects do we focus on based on our risk tolerance? How do we achieve operational efficiency by automating manual security efforts? And how do we make security easier for user acceptance?

"If we do these right, we can make sure we are focused on serving the business the best way."

According to Bissell, C-level executives should first become more familiar with how their organizations are exposed to cybercrime. He advises that executives have four awareness thresholds:

1. **Know What You Have:** Many executives have limited awareness of the scope of sensitive information, including intellectual property, contract, customer and employee data, which is contained in their organizations' databases or systems. These are also assets of the company.
2. **Mobile Computing Is Vulnerable:** Computing trends are distributing access of sensitive data to untold numbers as companies embrace mobile technology. This additional distribution creates the opportunity for new cybercrime threats since sensitive data assets can easily end up on unsecured devices.
3. **Third-Party Service Providers May Be Insecure:** As more data services move to the cloud or are outsourced, they become increasingly vulnerable to security schemes that are beyond executives' direct control.
4. **Compliance With Cyber Regulations Is No Remedy:** Organizations should not rely solely on compliance with security regulations as a substitute for proactive security planning. Regulations are nearly always years behind cybercrime's technological threats.

Building a Proactive Cybercrime Management Process

Cybersecurity requires C-level executives to first build a proactive process to measure the risks their organizations will face, and then adapt as both technologies and threats evolve. Bissell offers some suggestions:

- **Key Risk Indicators (KRIs):** Start by building the KRIs that impact the organization's bottom line. With KRIs, executives can begin to estimate the risks that impact their business strategies.
- **Road Maps:** With the "tone from the top," focus on embedding a risk-based security awareness approach—not just annual training—into all aspects of the business. Companies need to drive this strategy across a multi-year road map so they can understand where they are and where they want to be, and how they "snap into" the corporate strategy.
- **Execution With Key Performance Indicators (KPIs):** Monitor the progress of security projects using KPIs, which permit the organization to execute identifiable goals and measurements. By reporting upward through KPIs, C-level executives are empowered to control the resources needed to make progress.
- **Continuous Evaluation:** As cybercrimes occur in response to technological vulnerabilities, plan to continually monitor cybercrime events to determine how they might reveal the organization's own weaknesses.

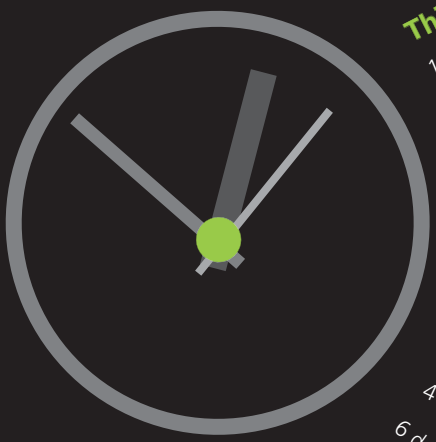
By instituting forward-thinking approaches to the evolving threat of cybercrime, C-level executives can strengthen their organizations' security while more effectively measuring risk for the benefit of the bottom line.

The organizations with the most proactive programs designed to combat threats of cybercrime will ultimately win the loyalty of new customers and stakeholders. Additionally, these organizations will have powerful tools at their disposal for controlling security expenses. This risk-management process is not a short-term fix, but a long-term strategy that adds value to the organization as a whole, delivers a measurable ROI, and enables executives to better control the fates of their strategic business processes.

But, as Bissell adds, collaboration is key.

"If we can create a better mechanism of having more fluid and open communication between companies and law enforcement agencies, we have a good chance of achieving success against cybercrime," he says. ■

www.deloitte.com



This is the moment your business is attacked.

11 minutes later. Your CIO calls during Sunday lunch. Someone's posted thousands of sensitive files online with a threat to release more.

3 hours later. IT wants to shut down the entire system so they can investigate. Reluctantly you give the okay.

4 hours later. The system's still down. Already, your reputation is getting a hammering on social media sites

18 hours later. You arrive at HQ to find the press camped outside. All you can tell them is 'No comment.'

3 days later. Regulators want an update. You'll have to give them something – but what?

4 days later. Your shareholders are demanding an Emergency General Meeting.

6 days later. The chairman calls you in for a chat.

Cybercrime. Be ready.

The second your business is hit by cybercriminals, the clock is ticking. Do you know how you'll respond? As a leader in cybersecurity, Deloitte is ready to help your board and IT team prepare for the threat—and contain the damage, fast.

Stop the clock on cybercrime. Call Kelly Bissell, US Information and Technology Risk Management Leader and Global Incident Response Leader, Principal, Deloitte & Touche LLP at +1 404 220 1187, or Kieran Norton, US Cyber Threat Management Leader, Principal, Deloitte & Touche LLP at +1 415 783 5382.

For more information, please visit us at www.deloitte.com/us/security/forbes

Deloitte.