THE NEW PARADIGM IN CYBER SECURITY

KEVIN R. BROCK AND DAVID X. MARTIN

The term "Cyber Security" is starting to sound like an oxymoron. The amped up rhetoric around growth of threats and vulnerabilities makes it feel like this may be a problem without a solution. At a recent cybercrime conference sponsored by the FBI and Fordham University, the mood seemed almost apocalyptic. Senior executives from law enforcement, from the military, and even the White House proclaimed that, despite all defensive efforts, the cyber threat was becoming "existential" and "more worrisome" than the terrorism threat. Not feeling panicky yet? It also represents the "greatest potential transfer of wealth in history." Whew. Now what do we do?

Time to Think Differently

Part of the answer lies in reorienting our thinking, particularly in the private sector, about how we can improve corporate cyber behaviors and information security in a network-connected world. There has long been a focus on technical solutions and hardening the perimeter of company networks. That's not cutting it anymore; threat actors are increasingly sophisticated, developing imaginative work-arounds and effective attacks on perimeter defenses. The fact that several of the nation's top cyber security companies have been hacked and embarrassed recently is revealing. If the best security firms are vulnerable, new strategies and approaches are in order. Companies are beginning to realize that their greatest vulnerability may not be faulty technology but faulty human behavior.

Increasing Sophistication of the Threat

Two key factors are setting the tone: first, the number of capable bad actors is increasing dramatically; second, the exposure of available targets (the "attack surface" as government cyber warriors would say) is likewise rapidly expanding. The FBI has detected and anticipates continued growth in the professionalization of cyber intruders, with the most skilled operating on behalf of state sponsored intelligence services, transnational organized crime enterprises, or ideological movements such as Anonymous and Lulzsec. These attackers plan and execute sophisticated, well-resourced exploits designed to steal, manipulate or destroy your data, or to use your data to expose and embarrass your company or others.

Boiled down, an intruder needs a way to get into a network and tools to achieve objectives once inside. Internet security company McAfee estimates that nearly two million pieces of new malware were written *each month* in 2011. Bad actors seek and design increasingly sophisticated ways to gain entry to a company's network that often leverage careless behavior among network users. New and improved phishing (sounds like "fishing") and spear-phishing (more sophisticated and targeted) techniques trick employees of targeted entities into injecting sophisticated malware on otherwise well-protected networks.

A recent event illustrates just how creative the bad guys can be. During the holiday season, intruders placed a box of thumb drives at the main entrance of a targeted company's headquarters. The box had the company logo prominently displayed and employees, thinking the thumb drives were holiday gifts, eagerly helped themselves to the drives and plugged them into company computers. The malware contained in the drives was injected and the intruders, at least, had a wonderful holiday season!

The widespread use of social networks like Facebook and LinkedIn provides intruders the opportunity to research company employees by name, biographical information, current and past positions, and other background details that seem innocuous (important dates, pet names, etc.) but which provide information that helps intruders guess passwords. This helps make spear-phishing much more effective. At the same time, the proliferation of mobile computing devices such as smartphones and tablets provide additional pathways into company networks. Live communications are increasingly targeted as well. Malware specifically designed to take over the camera and voice functions of a computing device can provide real-time access to conference calls and private conversations at almost any level. Consider the value of being able to trade in front of a large order from a major asset manager.

The financial sector is particularly vulnerable to attacks that manipulate data because of its dependence on trusted sources of real-time information. A recent Cyber Risk and Data Breach conference in New York highlighted a successful intrusion of a weather forecasting website. By manipulating the site's forecast to predict a hard frost over three consecutive nights, long enough to kill crops in a key citrus producing region, the market responded in a way that was advantageous to the crooks. Although not yet a commonplace risk, the attack illustrates the broad and imaginative thinking of today's attackers.

Different Thinking Leads to Different Strategies

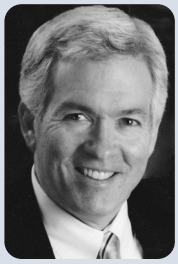
In light of today's rapidly evolving cyber threat landscape, smart companies are moving toward broader, integrated risk management strategies that address human behaviors as well as technology. Their strategy focuses on making their total environment difficult for intruders. Most intruders are not persistent and will move quickly to focus on the many easier targets that are available. 64% of small and mid-sized companies do not believe they are targets, and nearly half provide no cyber security training to their employees. There's your primary victim pool.

Nor should companies rely on the Intelligence and Law Enforcement communities to deter the problem, which is too big and moving too fast. Companies must take full ownership of this risk issue. We recommend the following:

- A company-wide strategy for managing cyber security risks must be integrated into the enterprise risk management portfolio with a C level executive assigned primary responsibility. All functions must be involved including technology, operations, compliance, internal audit and risk, as well as representatives of major lines of business. The appointment of a Chief Information Officer is a plus.
- Senior management should regularly report to the Board of Directors on the firm's cyber security risk profile as well as the relevant governance and adequacy of resources to address these risks.
- Mandatory, ongoing training and counter-threat awareness programs improve employee behaviors and practices, which is the first defense against cyber threats. Command and control efforts do not work. Every employee is a risk manager.
- Management should evaluate their "insider threat" risks and develop plans to mitigate any damage from intentional or inadvertent mishandling of sensitive data. Firms need to understand who has what access to their sensitive information, how those individuals are vetted and trained to handle such information, and what protections are in place should they separate from the company.
- Public companies must understand which cyber security risks they may be compelled to communicate as risk disclosures in formal filings, such as SEC form 10K. Required disclosures may include reporting of cyber security events that have occurred, a statement as to the health of the company's cyber security posture and an indication of resources expended to reasonably ensure cyber security.

Former CIA Director George Tenet is quoted as having said, "We have built our future on a capability that we have not learned how to protect." In one sense he's absolutely right. There will never be absolute security in cyber space. But that does not mean the future is hostage to risks. Risk can be managed. Forward-thinking businesses that develop prudent, comprehensive strategies to improve their cyber security posture will survive. Meanwhile, failing to adapt to the new reality can be lethal: as W. Edward Deming famously noted, "It is not necessary to change. Survival is not mandatory." Senior management and the corporate directors have a duty to ensure that organizations adapt effectively.

ABOUT THE AUTHORS



Kevin R. Brock is a retired FBI Agent who served as Assistant Director over the FBI's Directorate of Intelligence as well as Principal Deputy Director of the National Counterterrorism Center. He currently consults on law enforcement, intelligence, and cyber security matters in Northern Virginia.

David X. Martin is a risk management expert who has worked at major buy and sell side firms at the senior executive levels. He is the founding chair of the Investment Company Institute's Risk Committee, author of Risk and the Smart Investor (McGraw-Hill, September 2010) and an Adjunct Professor at New York University Graduate School of Business.