Deloitte University Press

SIGNALS for strategists

Cyber crime fighting

As personal, commercial, and government activities continue to migrate to the digital realm, so do criminals. Large-scale cyber attacks are becoming more frequent and more costly for businesses in the United States. Attackers are better funded, more sophisticated, and better organized than in the past, often representing criminal networks or states. Dozens of US banks have suffered cyber attacks over the last year at the hands of foreign attackers. Cyber crooks stole 3.6 million social security numbers and nearly 400,000 credit card numbers and tax data from South Carolina Department of Revenue computers, saddling the state with $20 million in cleanup costs so far.[1] Better security is not going to come cheap. According to Bloomberg, financial services firms will have to boost annual average cyber security spending 13-fold to nearly $300 million each to fend off 95 percent of cyber attacks.[2]

As enterprises and government agencies increasingly adopt cloud, mobile, and social computing, information technology (IT) environments are becoming more difficult to defend. Increasingly, organizations need to accept that security breaches are inevitable. Security strategies need to go beyond defense

to include detection, response, and recovery. All this gives rise to a need for new skills and approaches and specialized tools and services, including continuous monitoring and threat forensics powered by analytics.

Cyber security is increasingly becoming a concern among corporate leadership, including boards of directors. A biennial study of enterprise security governance practices by the Carnegie Mellon University CyLab found a sharp rise in board-level attention to the topic. Among companies surveyed in 2012, 48 percent have a board-level risk committee responsible for privacy and security, up from just 8 percent in 2008.[3]

The rising number and sophistication of cyber attacks is expanding the market for cyber security services. North American spending on managed security services (IT outsourcing focused on security services) will increase at a compound annual growth rate of 17% during 2013–2017, according to Gartner.[4] The growing market and evolving threat landscape are, in turn, motivating many mergers and acquisitions. The last several years saw many large-scale acquisitions, including over 30 acquisitions of young, US-based cyber security vendors in the last 12 months alone.[5]

Two important trends can help organizations stay ahead of cyber threats.

Collective intelligence

The distributed and evolving nature of cyber threats calls for a collaborative and networked defense. In the context of cyber security, collective intelligence refers to the sharing of information about vulnerabilities, threats, and remedies between enterprises and government and between enterprises and security vendors. Collective intelligence can improve risk management by quickly spreading knowledge of vulnerabilities and threats. It can direct security audits and cyber forensics to areas of known or suspected weakness. And it can reveal trends and suggest areas where investment in additional security measures is warranted. A number of vendors are developing shared-intelligence features such as injecting data feeds of anonymized and aggregated data about IP addresses, file names, email addresses, query and search strings, and the like into security monitoring dashboards to improve security for all of their customers. Promoting the sharing of cyber threat and vulnerability information between the public and private sectors was a key aim of the federal Cyber Security Act of 2012.[6]

Technology and professional services

With cloud, mobile, and social computing creating new security vulnerabilities, traditional cyber security products such as firewalls and antivirus scanners cannot thwart every threat. Tools such as network security analyzers can be difficult for some enterprises to effectively employ without outside help, and specialized cyber security talent is, predictably, in short supply. Professional services firms are responding by introducing security offerings that marry the automation and analytical capabilities of IT platforms with human intelligence to help clients cope. Such technological offerings can help organizations monitor, collect, and analyze large data sets and identify patterns that indicate breaches or attempted breaches. This allows organizations to respond to threats with more agility, and it supports more thorough auditing of cyber security risks at a time when firms—especially public companies—face rising expectations to disclose their security risks and incidents.

Organizations can no longer rely on passive defenses against cyber attacks. Tapping into collective intelligence and joining automation and analytics to human judgment can help organizations reduce the risk of a cyber attack and lower the costs of mitigating attacks that do occur.

Endnotes

1. Andrew Shain, "SC hacking solution could cost $15 million next year," ***The State***, May 8, 2013, http://www.thestate.com/2013/05/08/2761786/sc-hacking-solution-could-cost.html.
2. Eric Engleman and Chris Strohm, "Cybersecurity disaster seen in US survey citing spending gaps," *Bloomberg*, January 31, 2012, http://www.bloomberg.com/news/2012-01-31/cybersecurity-disaster-seen-in-u-s-survey-citing-spending-gaps.html.
3. Jody R. Westby, *Governance of enterprise security: CyLab 2012 report—How boards and senior executives are managing cyber risks,* May 16, 2012, http://www.rsa.com/innovation/docs/CMU-GOVERNANCE-RPT-2012-FINAL.pdf.
4. Gartner, "Forecast: Information Security, Worldwide, 1Q13 Update," May 10, 2013.
5. Deloitte analysis of data from CB Insights.
6. Cybersecurity Act of 2012, S. 2105, 112th Congress (2012), http://www.govtrack.us/congress/bills/112/s2105/text.

Contacts

Kelly Bissell
+1 404 220 1187
kbissell@deloitte.com

Kelly Bissell is a principal with Deloitte & Touche LLP. He is the global lead for cyber security and leads the US IT Risk Management practice.

Vikram Mahidhar
+1 617 437 2928
vmahidhar@deloitte.com

Vikram Mahidhar is a director in Deloitte LLP's innovation group. He focuses on identifying emerging business ideas and driving development and commercialization of emerging products and services.

David Schatsky
+1 646 582 5209
dschatsky@deloitte.com

David Schatsky is a senior manager with Deloitte LLP. His focus is analyzing emerging business and technology trends.

 Follow @DU_Press

Sign up for Deloitte University Press updates at DUPress.com.

About Deloitte University Press
Deloitte University Press publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte University Press is an imprint of Deloitte Development LLC.