

“Big data” takes on the cybercrook of tomorrow

Today’s antifraud, anti-money laundering, and general anti-online bad guy measures are pretty good compared with a few years ago—but so what? Today’s digital thieves and malcontents already can run rings around such measures and are gearing up for mischief that is orders of magnitude more sophisticated.

You can get a good feel for this just by reading the list of training courses planned for the upcoming Black Hat USA Technical Security conference, to be held July 21-24 in Las Vegas. Included are: “Advanced malware analysis”; “Cyber network defense”; “Hacking by numbers [from boot camp to combat level].” And this conference is intended for the good guys.

Meanwhile, there’s no doubt that cyber attacks are on the rise. Trustwave—endorsed by ABA’s Corporation for American Banking—reported performing 42% more data breach investigations in 2011 than in the previous year, which it attributed to an increase in targeted, sophisticated attacks.

Who are the attackers? Not the stereotypical digit heads camped out in their parents’ basements slathered in Cheez Doodle dust. Rather, they are organized crime members, state-sponsored agencies, and social action activists, all highly sophisticated and fervently motivated, either by greed, policy, or beliefs.

Here’s an interesting quote:

“The day-to-day use of cyber risk intelligence is no longer just for government agencies—it’s a required competency for corporate survival,” says Art Coviello, executive chairman of RSA. “The tempo and serious nature of recent attacks calls for urgent and bold countermeasures that position organizations not only to detect advanced threats, but also to predict how attacks may occur so they can take steps to help mitigate risk and impact. Combating advanced threats requires a new security mindset and vastly improved practices for gathering, sharing, and acting on cyber risk intelligence.”

A few observations about the above quote. RSA is the security division of EMC, which is all about providing big data services. For example, it just announced it is opening a “big data” center in Russia. Coviello calls not only for detecting what he calls “advanced threats,” but for predicting when and where they will happen. He also calls for a new security mindset and vastly improved practices—meaning, it’s not too much of a leap to say, automating the analysis of data in order to increase security.

An unnamed spokesman in an RSA video on YouTube explains it pretty clearly. First he talks about accessing, in near-real time, various sources of information, such as those used by vendors, the government, and other open sources. “Let’s take all of these different data sources, let’s take this universe of valuable data that’s out there, and make it machine readable. Make it so that it comes in an automated fashion so that security teams can act on it in an operational manner.”

A recent RSA research report puts a name on this: intelligence-driven information security. “This collaborative, big data approach,” it says, includes:

- The consistent collection of reliable and actionable cyber-risk data from a range of government, industry, commercial, and internal sources to gain a more complete understanding of risks and potential exposures.
- Ongoing research on prospective cyber adversaries to develop knowledge of attack motivations, favored techniques, and known activities.
- The growth of new skills within the information security team focused on the production of intelligence.
- A process for efficient analysis, fusion, and management of cyber-risk data from multiple sources to develop actionable intelligence.
- Full visibility into actual conditions within IT environments, including insight that can identify normal versus abnormal system and end user behavior.
- Informed risk decisions and defensive strategies based on comprehensive knowledge of the threats and the organization’s own security posture.
- Best practices to share useful threat information such as attack indicators with other organizations.

That’s a plateful and more, no doubt. Trustwave offers a check list that can start to get a handle on all this:

Education of employees—The best intrusion detection systems are neither security experts nor expensive technology, but employees. Security awareness education for employees is the first line of defense.

Identification of users—Focus on achieving a state where every user-initiated action in your environment is identifiable and tagged to a specific person.

Homogenization of hardware and software—Fragmentation of an enterprise's computing platforms is an enemy to security. Reducing fragmentation through standardization of hardware and software, and decommissioning old systems, will create a more homogenous environment that is easier to manage, maintain, and secure.

Registration of assets—A complete inventory or registry of valid assets can provide the insight needed to identify malware or a malicious attack.

Unification of activity logs—Combining the physical world with the digital affords organizations with new ways to combine activities and logs to identify security events.

Even this is quite a job. (If nothing else, comb your organization for people who use weak passwords. Trustwave found that the most common password is "Password1" which satisfies the default Microsoft Active Directory complexity setting but hardly challenges the rankest hacker bootcamper.)

But help is available. Here's a fairly random sample, since the following were announced very recently:

- MasterCard will partner with Silver Tail Systems to enable merchants to differentiate fraudsters from legitimate consumers in real-time during the online shopping experience. It's an attempt to accommodate ecommerce merchants who increasingly not only transact with their customers, but interact with them through smartphones, social networks, and online apps.

- ThreatMetrix partnered with TransUnion to provide two fraud prevention platforms. One, called TrustDefender, provides "enhanced real-time online contact verification." The other, called Device Verification Service—identifies potential cybercriminals trying to mask their identity through cookie manipulation, hidden proxies, or invalid IP addresses.

- Jack Henry & Associates, through its ProfitStars division, now offers web-based security awareness training specifically designed to meet FFIEC guidance requiring financial institutions to educate commercial customers on evolving fraud risks and best practices. It addresses internal and external threats unique to commercial banking customers' online financial transactions, educates them on identity protection, and details the highest security practices.

Of course, consult CAB's endorsement of Trustwave, particularly its new Data Loss Prevention services.

And good luck.

Sources used for this report include:

Black Hat USA 2012, July, Las Vegas, training courses

New SBIC research: Getting Ahead of Advanced Threats: Achieving Intelligence-driven Security

Information Security, Compliance Management and Data Loss Prevention Solutions Trustwave

Leading Chief Security Officers Outline Roadmap to Combat Advanced Threats

ProfitStars Introduces eCommercial Security Awareness Training

MasterCard Establishes Relationship with Silver Tail Systems to Combat Online Fraud

Trustwave Report Reveals Global Data Breach and Security Trends

About the Author

John Ginovsky is contributing editor of ABA Banking Journal and editor of the publication's TechTopics e-newsletter. For more than two decades he has written about the commercial banking industry. In particular, he's specialized in the technological side of banking and how it relates to the actual business of banking. He previously was senior editor for Community Banker magazine (which merged with ABA Banking Journal) and was a staff writer for ABA's Bankers News.