FORRESTER®

For: Security & Risk Professionals

Understand The Business Impact And Cost Of A Breach

by John Kindervag, Heidi Shey, and Kelley Mak, January 12, 2015

KEY TAKEAWAYS

The Threat Landscape Is Rapidly Mutating

The security gap between new attack methods and traditional controls continues to grow in favor of the attackers. Hackers today are highly organized, well-funded crime syndicates, or in some cases, state-sponsored agents. There are eight fundamental changes occurring, with attacks overall becoming more targeted, sophisticated, and resourceful.

Breach Costs Vary Widely And Hit Many Areas Of The Business

Understand the different costs of breaches, and estimate damages to elevate security conversations with management. Consider response and notification, lost productivity, staff departures, legal action, regulatory fines, additional security and audit requirements, loss of customers, and other liabilities like downgraded credit risk ratings.

Prepare Counterarguments To Management Cop-Out Statements

Upper management can no longer ignore the business implications of today's threat landscape. Use breach costs to help build your business case, and fortify your argument by countering three common statements: 1) "We're not very visible"; 2) "But we've never had a breach"; and 3) "The probability of this happening is so low, I'll take my chances."

Understand The Business Impact And Cost Of A Breach

Business Case: The Security Architecture And Operations Playbook

by John Kindervag, Heidi Shey, and Kelley Mak
with Christopher McClean, Stephanie Balaouras, and Josh Blackborow

WHY READ THIS REPORT

We are in the midst of a golden age of hacking. The information security threat landscape is changing rapidly, and security organizations are struggling to keep up with the changing nature, complexity, and scale of attacks. This dynamic landscape will not stabilize. As security managers struggle to keep up with this changing landscape and develop capabilities for handling new threats, the attacks of 2014 taught us that the threat landscape is rapidly mutating as attackers find ever more devious ways of bypassing security controls. This report will help security and risk (S&R) leaders educate business executives about these threats and build the business case for investments in security architecture and operations necessary to defend against them. This is an update of a previously published report; Forrester reviews and updates it periodically for continued relevance and accuracy.

Table Of Contents

Notes & Resources

In developing this report, Forrester drew from a wealth of analyst experience, insight, and research through advisory and inquiry discussions with end users across industry sectors. This report also includes data from CyberFactors and Forrester Business Technographics® surveys on security and IT budgets.

Related Research Documents

Maintain Your Security Edge
December 4, 2014

No More Chewy Centers: The Zero Trust Model Of Information Security
October 7, 2014

The Cybercriminal's Prize: Your Customer Data And Competitive Advantage
August 6, 2014

TODAY'S THREAT LANDSCAPE IS REAL AND DISTURBING

The gap between new attack methods and traditional security controls has widened in favor of the attackers. Cyberattacks have become multidimensional in their complexity and sophistication, continuously adapting and altering techniques to evade security defenses. The defenses S&R pros have built only last so long before attackers find a way around them. It's a matter of when you'll be breached, not if.

The Nature, Complexity, And Methods Of Attack Are Changing In Eight Significant Ways

In the past, we dealt with highly talented hackers primarily motivated by ego. Hackers typically worked as individuals or as small teams; they had limited resources and looked for any weakness they could find in any system and then went after it. Their attacks were audacious and inflicted a great deal of damage, but were mere blips in the overall operations of large enterprises.

Today, adversaries also include highly organized, well-funded crime syndicates and state-sponsored agents. The ubiquity of attacks and number of records compromised in 2014 made it an alarming year for the security world (see Figure 1). Attacks today are much more targeted, sophisticated, and resourceful. The eight fundamental changes are not static; cybercriminals are always mutating their attacks to adjust to controls and real-time security response (see Figure 2):

- **Motivation: from fame to financial gain *plus* hacktivism.** Gone are the days when hackers simply bragged about their latest exploits openly in underground newsgroups to gain fame and notoriety. Those were much simpler times. Today, organized criminals are looking for notoriety *and* huge sums of money. Going after a few records or credit card numbers is not considered lucrative anymore; the attackers target systems that store millions of records or intellectual property that could bring in the big bucks.[1] According to a report from Intel Security in conjunction with the Center for Strategic and International Studies, the estimated global loss from cybercrime is $575 billion annually.[2]

  Along with financially incentivized cybercrime, hacktivism has increased in frequency through the rise of groups like Anonymous and LulzSec, which perpetrate distributed denial of service (DDoS) attacks and deface websites as methods of protest or to spread political ideology. For example, Anonymous protested perceived social injustices related to the 2014 World Cup in Brazil by taking down and defacing websites related to the tournament.[3] In a more prolonged attack, the Izz ad-Din al-Qassam Cyber Fighters claimed to have launched crowdsourced attacks in 2012 and early 2013 against Wells Fargo, US Bank, and Bank of America.[4] While hacktivists' aims aren't geared toward stealing information for financial gain, extended outages or website defacement can cost companies millions while also damaging the brand and causing customers to go to competitors.[5]

- **Method: from audacious to low and slow *plus* blended.** "Low and slow" is a phrase used in the industry to describe the act of collecting valuable information from an environment over long periods of time — weeks, months, or even years. This is a very systematic and precise attack in which the attackers go after the network, then the applications, and then the data, covering all traces of their presence as they penetrate the different parts of the environment. Attackers are constantly discovering new vulnerabilities and exploiting multiple vectors to ultimately compromise the system with whatever means necessary, which means attacks are now often blended, using a mixture of different tactics. These typically are nearly invisible hacks that aren't discovered until it's too late — after the criminals have made off with valuable data or inflicted other serious financial damage.

  The Target and Home Depot breaches in 2013 and 2014 are good examples of slow, blended attacks. In both cases, hackers infiltrated the network using stolen credentials from trusted third parties. From there, the attackers were able to siphon out millions of credit card and debit card numbers as well as customer email addresses over the course of several weeks for Target and several months for Home Depot.[6]

- **Focus: from indiscriminate to targeted *plus* surgical.** In the past, attackers continuously scanned IT environments to find vulnerabilities; as soon as they found one, they unleashed the hounds, trying to exploit that same hole in as many systems as possible. While broad attacks still occur often, attackers are increasingly using more-targeted techniques.[7] These more-sophisticated attacks seek out specific information assets within financial institutions, business competitors, political groups, and countries of political or economic interest to other nation-states. Common targeted attack methods are phishing and watering holes. Attackers can also now harvest information from social networking sites to gather information about their victims that will make spear phishing attacks more likely to succeed.

  In Mandiant's February 2013 APT1 report, researchers exposed the identities of a Chinese cyberespionage army unit that attacked American organizations and government agencies with the intent of economic gain.[8] In October 2014, Mandiant researchers uncovered a Russian-backed cyberespionage group, labeled APT28, which used malware to harvest information and intelligence related to governments, militaries, and security organizations.[9] Kaspersky's threat researchers uncovered The Mask, an APT campaign primarily targeting government agencies, embassies, diplomatic offices, and energy companies in Spanish-speaking countries.[10] In these and similar attacks, cybercriminals targeted their victims' assets with surgical precision.

- **Tools: from manual to automated *plus* cooperative.** It's amazing to see the amount of information and context a machine can use to extract information from unsuspecting users. French researchers have developed an automated social engineering tool that uses a man-in-the-middle attack to strike up online conversations with potential victims. It lets an attacker glean personal and other valuable information from victims via these chats or lure them into clicking on malicious links. The researchers had plenty of success in their tests: They enticed users to click on malicious links sent via their chat messages 76% of the time.[11] Add to this the ability of machines to crawl the web and glean publicly available information about any individual, and we see astonishingly precise attacks penetrating personal defenses. In fact, many of the requests people get from potential Facebook "friends" link to unscrupulous websites working in conjunction with information-harvesting and automated information-gathering technologies.

- **Result: from disruptive to disastrous *plus* devastating.** A security breach in the past meant that you had to respond quickly, keep law enforcement involved, deal with your affected customers, and ask their forgiveness. Today, a breach could mean a combination of compounding challenges: millions of dollars in fines and remediation costs, widespread public scrutiny, a plethora of lawsuits, the firing of executives and board members, or the loss of an innovative engineering design into the hands of your competitor.

  Devastating impacts are becoming more commonplace. The breach at Target rocked the company: the CIO was fired, the CEO resigned, and the high financial toll is still racking up. Target suffered a 46% decline in its Q4 2013 earnings and reported in August 2014 that the breach cost the company $148 million in the second quarter alone.[12] The December 2014 breach at Sony has so far led to online leaks of sensitive employee data, but stolen data also includes full copies of movies that have yet to be released in theaters.[13] In 2013 and 2014, we also saw government agencies handing out hefty fines for breaches and other consumer protection violations.[14]

- **Type: from unique malware to variant toolkits *plus* the entire toolbox.** Crimeware kits that allow people to customize a piece of malicious code designed to steal are freely available to novices. Botnets, for example, can be bought or rented and used to gain control of unwitting users' machines for malicious purposes such as stealing banking information or implementing click fraud. The range of tools and services available for purchase at low costs today shows the maturity of this underground market.[15] In the Brazilian underground, a fake phishing page for a bank can be purchased for R$100 (US$39), while a banking Trojan goes for R$1,000 (US$386).[16] In the Chinese underground, a one-month DDoS toolkit rental costs US$81, while a *lifetime* rental costs anywhere from a mere US$452 to US$484.[17]

- **Target: from infrastructure to applications *plus* strategic assets.** According to Verizon's latest Data Breach Investigations Report, web applications were the top attack target in 2013, representing 35% of breaches globally, followed by cyberespionage, which represented 22%.[18] But a majority of spending in security is on infrastructure components. Network security commanded the largest portion of the security technology budget, at 17%, in 2014.[19] This is mostly because many companies lack expertise in application security and therefore may not understand the magnitude of the problem. Companies that want to focus on web application attacks struggle to find people with the right skills — let alone technologies — to manage this area of risk.

- **Agent: from insider to third parties *plus* organized groups.** The most common source of breach is from internal incidents within their organization.[20] Internal threats are often discussed in the security industry, but third-party threats are often overlooked as potential sources of "insider" attacks. Third parties often enjoy the same liberties as employees, depending on trust and access levels, which can spell disaster for businesses. Many companies that have relied on their business partners and service providers to protect their information are finding that these third parties do not have the appropriate security controls.

  For example, personal information of current and former Lowe's employees was exposed when a third-party vendor wrongly backed up employee data to an unsecure server.[21] Attackers gained access to Home Depot's network by compromising the credentials of a third-party vendor.[22] Goodwill was breached when its payment processing vendor's systems were compromised.[23] The list goes on. Along with the growing threat from third parties, organized groups, including state-sponsored actors and hacktivists, have companies on the defensive against adversaries with more manpower, more resources, and advanced expertise.

Figure 1 2013 To 2014 Notable Hacks

	Date made public	Industry	Record count	Data
eBay	May 21, 2014	Technology	145 million	Contact information, encrypted passwords, usernames
Home Depot	September 2, 2014	Retail	109 million	Email addresses, payment card data
Korea Credit Bureau	January 19, 2014	Financial services	105 million	Contact information, payment card data
JPMorgan Chase	August 27, 2014	Financial services	83 million	Contact information
Benesse Holdings	June 14, 2014	Media	48.6 million	Customer information
Naver	March 26, 2014	Technology	25 million	Contact, passwords, user names
P.F. Chang's China Bistro	June 12, 2014	Hospitality	7 million	Payment card data
Community Health Systems	August 17, 2014	Healthcare	4.5 million	Patient information, including names, addresses, birthdates, social security numbers
Michaels Stores	January 25, 2014	Retail	2.6 million	Payment card data
TripAdvisor .com	September 19, 2014	Technology	1.4 million	Contact information, passwords, payment card data
Orange	May 7, 2014	Comm./ISP	1.3 million	Email addresses, phone numbers, dates of birth
Montana Dept. of Public Health and Human Services	May 29, 2014	Government	1.3 million	Customer information, social security numbers
Think W3 Limited	July 21, 2014	Services	1.2 million	Payment card data

Note: Information as of November 20, 2014

Source: CyberFactors, a wholly owned subsidiary of CyberRiskPartners and sister company of CloudInsure.com

60563 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Figure 2 A Mutating Threat Landscape

Motivation	Fame	→	Financial gain	+	Hacktivism
Method	Audacious	→	Low and slow	+	Blended
Focus	Indiscriminate	→	Targeted	+	Surgical
Tools	Manual	→	Automated	+	Cooperative
Result	Disruptive	→	Disastrous	+	Devastating
Type	Unique malware	→	Variant tool kits	+	The toolbox
Target	Infrastructure	→	Applications	+	Strategic assets
Agent	Inside	→	Third parties	+	Organized groups

60563 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

BE PREPARED FOR THE COST OF A BREACH

Many executives and S&R pros have a hard time estimating their organization's exposure to data breaches; as a result they are hesitant to invest in security technologies and processes. However, developing an estimate of possible damages and cost considerations will elevate the conversation to management and help align security to seven key categories of critical business metrics.[24] Estimating breach costs can also help S&R pros better assess the impact of a breach to the business and how to adequately prepare for such an event. Breaches are no longer a matter of "if" but "when," so you must plan for failure.[25]

To get a better understanding of what to expect post-breach, consider the costs incurred from:

- **Notification and other response costs.** These costs typically include breach notification for affected individuals as well as government and regulatory bodies that require notification by law. Relevant costs after the initial notification include increased call center costs, additional marketing and PR support costs, and discounted consumer product offers and services like credit or identity theft monitoring. Costs here will vary widely based on the size and complexity of the breach notification.

  Most companies are better off here with professional help, engaging with a breach notification services provider to guide the enterprise through customer-facing response. Speed and quality of customer-facing breach response is critical for diffusing a situation under public scrutiny and mitigating damage.[26] Response costs can also include incident response services, forensics, and other post-breach advisory services, some of which may be priced hourly or on a retainer fee.

- **Lost employee productivity and staff departures.** Companies incur additional expenses and lost productivity from normal duties when employees' attention is diverted to help respond to the data breach. This does not just affect employees with technology, security, or risk-related responsibilities. For example, account executives who may otherwise be growing the business are now working to reassure existing clients, the CEO is now spending time preparing to speak to the board and shareholders rather than meeting with company executives about expansion into a new market, and marketing has put its next campaign on hold to help PR with damage control. In some cases, there will also be staff departures — of both the voluntary and involuntary variety. For example, following the Korea Credit Bureau breach in 2014, 37 bank executives offered their resignations.[27] The time that it takes to recruit new personnel is an added cost, especially in the case of a high-profile breach that is covered widely in the media.

- **Lawsuits and settlements.** If you experience a large-scale breach of customer data, expect to see the lawsuits roll in. Most occur in the first year or two following the breach, although litigation can occur later or also drag on for years to create a long tail of costs.[28] Even if cases are dismissed, enterprises still must spend time and money responding to legal disputes. In addition, while consumer class action lawsuits are a cost concern, enterprises cannot ignore the costs that can arise from business partner and shareholder claims, too. Business partners may claim a breach of contract, while shareholders may claim that the company's board of directors breached its fiduciary duties (by not protecting customer data). Shareholders may also hold your organization accountable for damages relating to the loss of share value and perceived waste of company assets (for example, the breach costs associated with legal fees and government investigations).[29]

- **Regulatory fines.** In highly regulated industries or for organizations that experience a breach of regulated data (mainly payment information, healthcare data, or personally identifiable information), regulatory fines can start to add up as details of the breach unfold from resulting investigations. Given the prevalence of major data breaches today, the circumstances that surround the breaches, and heightened public concerns regarding privacy and personal data handling, regulators are looking at events with greater scrutiny. The largest HIPAA settlement to date — $4.8 million — was issued in 2014.[30] State and country breach notification and privacy laws worldwide also typically have fines for noncompliance, and many are pushing for even larger fines.[31] In some countries, fines can be in the form of a percentage of a company's annual revenue (e.g., 3% of annual revenue in South Korea).[32]

- **Additional security and audit requirements.** This includes the cost of fixing infrastructure or onboarding new technology and equipment to remediate the initial cause of breach. It also includes any mandated security and audit requirements resulting from a legal settlement or regulatory settlement. For example, conditions of a class action settlement against health insurance provider AvMed after a breach included upgrading all corporate laptops with additional security mechanisms including GPS tracking and full disk encryption, as well as physical security upgrades for company facilities.[33] FTC settlements stemming from breaches over the years against companies like Ceridian, ChoicePoint, GMR Transcription, Lookout Services, and T.J.Maxx have all resulted in an agreement to undergo 20 years' worth of audits. GMR will have to have its information security program "evaluated both initially and every two years by a certified third party."[34]

- **Brand recovery costs.** After a breach, there will be many costs associated with winning back customers and rebuilding customer loyalty, all of which can vary widely depending on your business and industry. Typically, banks and hospitals are affected the least here, since consumers are averse to the hassle of changing from one bank or hospital to another. Retailers, restaurants, and hotels may see greater fluctuations as consumers can more easily take their business elsewhere. B2B companies can face brand costs in the form of delayed contract agreements and lost business as well. Most organizations have a good idea of how much it costs, on average, to acquire a new customer as well as average spending per customer and can thus extrapolate the total recovery costs and lost revenue.

- **Other liabilities.** Costs and consequences can cascade and compound in various ways. For example, not only did Target see a drop in earnings following its data breach in late 2013, the S&P downgraded Target's credit rating a few months later as a result.[35] Lower ratings mean higher interest rates for borrowing money. The Home Depot breach in September 2014 has already cost credit unions close to $60 million in card replacement costs.[36] In the past, banks have sued breached organizations for card replacement costs, and sometimes breached organizations proactively pay up in an attempt to avoid such lawsuits — both expensive propositions.[37] Consumer expectations in different countries can also add to your costs. In Japan, for example, breached companies often voluntarily compensate much higher sums to their affected customers than required by law to maintain customer loyalty, making legal penalties appear small in comparison.[38]

WHAT IT MEANS

BE PREPARED TO RESPOND TO COP-OUT STATEMENTS

Ideally, you should make investment decisions based on rational, objective risk assessments and build your security program based on a risk-centered approach. Unfortunately, the reality remains grim for many security professionals, because while management may realize the severity of the problem, other priorities and funding challenges get in the way. The first step to combat this problem? Be brutally honest with management and be prepared to counter these likely statements and arguments:

- **"We're not very visible."** This is a "why would anyone want to target us?" mentality that needs to stop. It doesn't matter if your company has a widely known public brand or not. If you have a shady competitor, a corrupt business associate, or an unhappy employee, they could be potential conduits or even facilitators of a security breach. Headline security breaches are more often occupied by high-profile organizations. Yet, most security breaches today are at "not visible" organizations. Your organization — whether you are a law firm, accounting firm, an HVAC company, or a community health center — is a means to target your customers. Also, it is widely believed that the attacker community has mapped the entire publicly accessible Internet and knows where vulnerable assets reside. It is impossible to remain invisible if you are connected to the Internet.

- **"But we've never had a breach."** Don't confuse luck with competence. If you haven't had a security breach so far, there is a good probability that it's because of luck. It's also possible that you've had a breach and just don't know it; many companies have no way of knowing if they are in a breach state.[39] As previously noted, low-and-slow attacks often go on for months and months before companies discover them. Similar to the fine print in financial statements, past performance does not have any bearing on future results. Companies that have not been breached are still very much at risk if they're not paying enough attention.

- **"The probability of this happening is so low that I'll take my chances."** First, it's unlikely that anyone in the organization knows the probability of certain security incidents happening. This is because there's no reliable data source that can be used to predict such occurrences, as companies generally don't share this information externally. Second, even with a low probability, the potential impact of a breach is so high that it's often a clear decision to invest in the preventive controls from a financial standpoint.

- **"We're a small organization."** Size is also not a significant factor when determining the likelihood of attack or the potential damage that would result. A much bigger factor today is whether you have information that is valuable to attackers now or will be valuable in the future. Being a small company is actually a lot tougher these days because you have to maintain a certain threshold of security just to be as good as some of the larger companies. In fact, larger companies are more likely to have reserves or other assets on hand to weather the storm after they've been breached.

- **"We have insurance."** A typical business insurance policy won't cover costs associated with a breach, and even a cyberinsurance policy will only help to offset a fraction of the cost of a major breach. Read the fine print to ensure you know exactly what will be covered by your insurance policy, and remember: Cyberinsurance is not a get out of jail free card.

SUPPLEMENTAL MATERIAL

Methodology

Forrester collaborated with CyberFactors to obtain the breach timeline data in this report. The data may contain publicly available information and/or proprietary data collected by CyberFactors. The analysis of the data is exclusively Forrester's. More information about CyberFactors is available at www.cyberfactors.com.

Forrester's Business Technographics Global Security Survey, 2014 was conducted via a mixed methodology phone and online survey fielded in April 2014 to May 2014 of 3,305 business and technology decision-makers located in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Each calendar year, Forrester's Business Technographics fields business-to-business technology studies in 10 countries spanning North America, Latin America, Europe, and Asia Pacific. For quality control, we carefully screen respondents according to job title and function. Forrester's Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Additionally, we set quotas for company size (number of employees) and industry as a means of controlling the data distribution and establishing alignment with IT spend calculated by Forrester analysts. Business Technographics uses only superior data sources and advanced data-cleaning techniques to ensure the highest data quality.

ENDNOTES

[1] Protecting customer data such as credit card information, log-in credentials, and personally identifiable information is an important part of enterprise IT security. Such data fuels a large and lucrative underground market economy. However, as the threat landscape continues to evolve, CISOs must adjust their risk management strategies accordingly to counter the next frontier: intellectual property theft. As costly as the breach of customer data may be, the breach of intellectual property can be far worse. See the August 6, 2014, "The Cybercriminal's Prize: Your Customer Data And Competitive Advantage" report.

[2] Source: "Net Losses: Estimating the Global Cost of Cybercrime — Economic impact of cybercrime II," Intel Security — Center for Strategic and International Studies, June 2014 (http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf).

[3] Source: Kate Vinton, "Hacktivist Group Anonymous Targets World Cup," Forbes, June 18, 2014 (http://www.forbes.com/sites/katevinton/2014/06/18/hacktivist-group-anonymous-targets-world-cup/).

[4] Source: Mathew J. Schwartz, "PNC Bank Hit By Crowdsourced Hacktivist Attacks," InformationWeek Dark Reading, September 28, 2012 (http://www.informationweek.com/security/attacks/pnc-bank-hit-by-crowdsourced-hacktivist/240008128) and Sean Gallagher, "'Funded hacktivism' or cyber-terrorists, AmEx attackers have big bankroll," Ars Technica, March 30, 2013 (http://arstechnica.com/security/2013/03/funded-hacktivism-or-cyber-terrorists-amex-attackers-have-big-bankroll).

[5] For more information on protecting against DDoS attacks, see the June 19, 2014, "Develop A Two-Phased DDoS Mitigation Strategy" report.

[6] Source: Brian Krebs, "In Home Depot Breach, Investigation Focuses on Self-Checkout Lanes," Krebs on Security, September 18, 2014 (http://krebsonsecurity.com/2014/09/in-home-depot-breach-investigation-focuses-on-self-checkout-lanes/).

[7] For more information on targeted attacks, see the January 7, 2015, "Forrester's Targeted-Attack Hierarchy Of Needs: Assess Your Core Capabilities" report.

[8] Source: "APT1: Exposing One of China's Cyber Espionage Units," Mandiant (http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf).

[9] Source: "APT28: A Window Into Russia's Cyber Espionage Operations?" Mandiant (http://www.fireeye.com/resources/pdfs/apt28.pdf).

[10] Source: Dennis Fisher, "New 'Mask' Apt Campaign Called Most Sophisticated Yet," Threatpost, February 10, 2014 (http://threatpost.com/new-mask-apt-campaign-called-most-sophisticated-yet/104148).

[11] Source: Kelly Jackson Higgins, "Tool Automates Social Engineering In Man-In-The-Middle Attack," InformationWeek Dark Reading, June 10, 2010 (http://www.darkreading.com/insiderthreat/security/privacy/showArticle.jhtml?articleID=225600304).

[12] Source: Rachel Abrams, "Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop," The New York Times, August 5, 2014 (http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html?_r=0).

[13] Source: Kim Zetter, "Sony Got Hacked hard: What We Know and Don't Know So Far," Wired, December 3, 2014 (http://www.wired.com/2014/12/sony-hack-what-we-know/).

[14] For more information on lessons learned from customer breaches and privacy incidents, see the November 14, 2014, "Lessons Learned From Global Customer Data Breaches And Privacy Incidents Of 2013-14" report.

[15] Source: Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, "Markets for Cybercrime Tools and Stolen Data — Hackers' Bazaar," the RAND Corporation, March 2014 (http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf).

[16] Source: Fernando Merces, "The Brazilian Underground Market — The Market for Cybercriminal Wannabes?" Trend Micro, 2014 (http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-brazilian-underground-market.pdf).

[17] Source: Lion Gu, "The Chinese Underground in 2013," Trend Micro, 2013 (http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-chinese-underground-in-2013.pdf).

[18] Source: "2014 Data Breach Investigations Report," Verizon, 2014 (http://www.verizonenterprise.com/DBIR/2014/).

[19] Source: Forrester's Business Technographics Global Security Survey, 2014 (base: 924 North American and European security decision-makers at companies with 20 or more employees).

[20] We've built strong perimeters, but well-organized cybercriminals have recruited insiders and developed new attack methods that easily bypass our current security protections. For more information on making security ubiquitous throughout the network, see the October 7, 2014, "No More Chewy Centers: The Zero Trust Model Of Information Security" report.

[21] Source: Adam Greenberg, "Lowe's employee info accessible online for about 10 months," SC Magazine, May 20, 2014 (http://www.scmagazine.com/lowes-employee-info-accessible-online-for-about-10-months/article/347676/).

[22] Source: Seth Rosenblatt, "Home Depot says 53 million emails stolen," CNet, November 6, 2014 (http://www.cnet.com/news/53-million-emails-stolen-in-home-depot-breach/).

[23] Source: Eduard Kovacs, "Goodwill Blames Credit Card Breach on Third-Party Vendor," SecurityWeek, September 3, 2014 (http://www.securityweek.com/goodwill-blames-credit-card-breach-third-party-vendor).

[24] Forrester proposes seven key categories of metrics as part of information security reporting to move the CISO toward a common language for business: 1) strategic alignment to corporate goals; 2) functional alignment to performance objectives; 3) support for regulatory compliance; 4) dedication to efficiency and effectiveness; 5) commitment to process excellence; 6) enthusiasm to service and quality; and 7) a drive for innovation. See the July 18, 2011, "Don't Bore Your Executives — Speak To Them In A Language That They Understand" report.

[25] You can't stop every cyberattack. However, your key stakeholders, clients, and other observers do expect you to take reasonable measures to prevent breaches in the first place, and when that fails, to respond quickly and appropriately. An effective incident response management program is essential. See the November 9, 2011, "Planning For Failure" report.

[26] There are long-term lessons we can glean from breaches that will help all S&R pros improve their enterprise's overall security posture, their specific breach response capabilities, and their understanding and appreciation for privacy law and changing consumer sentiment on privacy. To do this, each year we will select five notable incidents from the past 12 months that represent different industries and different types of incidents, summarize the details, and provide critical lessons learned for S&R pros. See the November 14, 2014, "Lessons Learned From Global Customer Data Breaches And Privacy Incidents Of 2013-14" report.

[27] Source: Brian Patrick Eha, "37 South Korean Bank Execs Offer to Resign Over Breach. Should Target Execs Follow Suit?" Entrepreneur Media, January 20, 2014 (http://www.entrepreneur.com/article/230980).

[28] Looking at a sample of publicly reported security incidents that occurred from 2000 to 2014 that resulted in both litigation and legal costs (judgments lost, settlements, and legal defense fees), the majority of legal costs are typically incurred within the first two years of the event. See the June 19, 2014, "Brief: Legal Costs In A Customer Data Breach Now Pack A Bigger Punch" report.

[29] Source: Robert E. Sumner IV and E. Brandon Gaskins, "The consumer may not be your worst enemy in the case of a data breach," InsideCounsel, November 3, 2014 (http://www.insidecounsel.com/2014/11/03/the-consumer-may-not-be-your-worst-enemy-in-the-ca?ref=hp).

[30] Source: Joseph Conn, "New York-Presbyterian, Columbia to pay largest HIPAA settlement: $4.8 million," Modern Healthcare, May 7, 2014 (http://www.modernhealthcare.com/article/20140507/NEWS/305079946).

[31] To help security and risk professionals navigate the complex landscape of privacy laws around the world, Forrester created a data privacy heat map that highlights the data protection guidelines and practices for 54 different countries. Due to the dynamic nature of data protection legislation, information within the interactive tool is kept up-to-date with an annual update cycle. See the August 6, 2014, "Forrester's 2014 Data Privacy Heat Map" report.

[32] Source: James Lim, "South Korea Increases Data Breach Fines, Lowers Liability Threshold," Bloomberg BNA, May 19, 2014 (http://www.bna.com/south-korea-increases-n17179890601/).

[33] Source: "In The United States District Court For The Southern District Of Florida: Case No. 10-cv-24513-JLK," The Garden City Group (http://www.databreachsettlement.com/docs/sa.pdf).

[34] Source: "FTC Approves Final Order in Case Against GMR Transcription Services," Federal Trade Commission, August 21, 2014 (http://www.ftc.gov/news-events/press-releases/2014/08/ftc-approves-final-order-case-against-gmr-transcription-services).

[35] Source Ashley Carman, "S&P lowers Target's credit rating following breach," SC Magazine, March 31, 2014 (http://www.scmagazine.com/sp-lowers-targets-credit-rating-following-breach/article/340510).

[36] Source: "Home Depot Data Breach Cost Credit Unions Nearly $60 Million," Credit Union National Association press release, October 30, 2014 (http://cuna.org/Stay-Informed/Press-Room/Press-Releases/2014-Press-Releases/Home-Depot-Data-Breach-Cost-Credit-Unions-Nearly-$60-Million).

[37] Source: Ryan Tracy, "In a Cyber Breach, Who Pays, Banks or Retailers?" The Wall Street Journal, January 12, 2014 (http://online.wsj.com/articles/SB10001424052702303819704579316861842957106).

[38] Across Asia, data privacy laws are fragmented, and the regulatory environment is different for each jurisdiction. Significant penalties mean that compliance is not optional and specific focus is required to remain within the legal boundaries. This study highlights key data privacy regulations from across the Asia Pacific region and presents best practices for staying on top of these evolving requirements. See the May 15, 2013, "What You Must Know About Data Privacy Regulations In Asia Pacific" report.

[39] Our experience leads us to believe that most networking or information security professionals have no insight regarding the behavior of internal traffic and the potential threats incumbent with that traffic. Evidence suggests that most breached entities or organizations do not discover their own breaches. A Verizon report indicates that third parties discover 61% of data breaches. For more, see the January 24, 2011, "Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility" report.

FORRESTER®

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals

Forrester Research (Nasdaq: FORR) is a global research and advisory firm serving professionals in 13 key roles across three distinct client segments. Our clients face progressively complex business and technology decisions every day. To help them understand, strategize, and act upon opportunities brought by change, Forrester provides proprietary research, consumer and business data, custom consulting, events and online communities, and peer-to-peer executive programs. We guide leaders in business technology, marketing and strategy, and the technology industry through independent fact-based insight, ensuring their business success today and tomorrow.