FORRESTER®

For: Security &
Risk Professionals

Planning For Failure

by John Kindervag, Rick Holland, and Heidi Shey, February 11, 2015

KEY TAKEAWAYS

You Will Suffer A Security Breach; You May Even Have A Breach Right Now

Forrester predicts that in 2015, at least 60% of enterprises will discover a breach of sensitive data. Most breaches are not even discovered by the breached party. Inadequate incident response leads to financial, operational, and reputational losses.

Incident Response Is One Of The Most Overlooked Areas In Information Security

In Forrester's experience, incident response is one of the most overlooked areas of information security. It is impossible to prevent every breach, and when they do occur, S&R pros find themselves inadequately prepared to respond.

You Must Establish An Ongoing Incident Management Program

An incident response plan, like a business continuity or an IT disaster recovery plan, is your immediate response to a specific threat. To be effective, you need to establish an ongoing incident management program that lets you identify the potential risks so that you can create appropriate response plans, test those plans, and keep them current.

Planning For Failure

An Effective Incident Management Program Is Essential To Help You Stay In Business

by John Kindervag, Rick Holland, and Heidi Shey
with Stephanie Balaouras, Kelley Mak, and Josh Blackborow

WHY READ THIS REPORT

S&R pros, it's not a question of if — but when — your organization will experience a serious security breach. Cybercriminals are using more sophisticated and targeted attacks to steal everything from valuable intellectual property to the sensitive personal and financial information of your customers, partners, and employees. Their motivations run the gamut from financial to political to retaliatory. With enough time and money, they can breach the security defenses of even the largest enterprises. 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. A poorly contained breach and botched response have the potential to cost millions in lost business and opportunity, ruin the organization's reputation, and perhaps even drive the company out of business. 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 and vendors across industry sectors.

Related Research Documents

Forrester's Targeted-Attack Hierarchy Of Needs: Assess Your Core Capabilities
January 7, 2015

Lessons Learned From Global Customer Data Breaches And Privacy Incidents Of 2013-14
November 14, 2014

Seven Habits Of Highly Effective Incident Response Teams
April 17, 2013

YOU WILL SUFFER A SECURITY BREACH; YOU MAY HAVE A BREACH RIGHT NOW

Breaches are expensive. A recent Ponemon Institute study concluded that the average cost of a breach is $3.5 million, up 15% from 2013. Ponemon also determined that each record lost cost $136, which was up 9% from 2013.[1]

During the past 12 months, 45% of network security decision-makers at enterprises reported at least one potential compromise or breach of their sensitive information (see Figure 1-1). Among those in North America and Europe, this is a 6% increase from 2013.[2] Forrester predicts that in 2015, at least 60% of enterprises will discover a breach of sensitive data.[3]

It's important to understand that most breaches are not discovered by the breached party, however. According to the 2014 Verizon Data Breach Report, "With all internal discovery methods combined, only 9% of victims discovered data breaches of their own accord."[4] In today's changed threat landscape, cybercriminals are skilled, well-funded, and patient. They target their attacks and do everything in their power to conceal their activity so that they can accomplish their goal, whether it's to steal intellectual property or personally identifiable information.

Inadequate Response Leads To Financial, Operational, And Reputational Losses

Multiple examples can be found that illustrate the importance of having an *effective* incident management program. Whether the damage unfolds in the span of a few days or explodes after one or many years after the initial intrusion, the consequences can be severe. Consider the events at:

- **Nortel Networks.** Alleged Chinese attackers compromised Nortel Networks for almost a decade. "Hackers had almost complete access to the company's systems."[5] It took Nortel nearly four years to detect the initial intrusion, and after detecting the intrusion, Nortel failed to follow a consultant's remediation recommendations. Nearly six years later, in January 2009, Nortel filed for bankruptcy protection.

- **Target.** The massive breach of the Target retail chain in November and December 2014 led to the Target CIO and CEO being fired. According to a US Senate report on the breach, "Target missed information provided by its anti-intrusion software about the attackers' escape plan, allowing attackers to steal as many as 110 million customer records."[6]

  One unexpected result of the Target breach is the new pressure on boards of directors to become involved in data protection and breach response. In an unprecedented step, the influential proxy advisor Institutional Shareholder Services (ISS) recommended that shareholders remove seven of the 10 members of Target's board. In its statement to investors, ISS said, "It appears that failure of the committees to ensure appropriate management of these risks set the stage for the data breach, which has resulted in significant losses to the company and its shareholders."[7]

- **Code Spaces.** Code Spaces closed its doors after a combination AWS EC2 console hack and DDoS extortion attempt.[8] By the time Code Spaces regained control of the console, the hackers had already deleted data, backups, machine configurations, and off-site backups. This all happened within the span of a few days.

- **Sony Pictures Entertainment.** The massive breach at Sony Pictures Entertainment resulted in a shutdown of production on several films, the leak of unreleased films, sensitive employee data, and spools of internal emails, in addition to preventing the release of a film that cost $40 million to produce.[9] Angry former employees are now suing the company for failing to protect their personal data.[10]

INCIDENT RESPONSE IS ONE OF THE MOST OVERLOOKED AREAS IN INFOSEC

In Forrester's experience, incident response is one of the most overlooked areas of information security. Surprisingly, even at those enterprises that have already suffered a breach during the past 12 months, only 24% of network security decision-makers report increased spending on their incident response program as a result (see Figure 1-2). While many increased spending on breach prevention technologies, 5% actually reported that nothing has changed in the past 12 months as a result of security breaches.

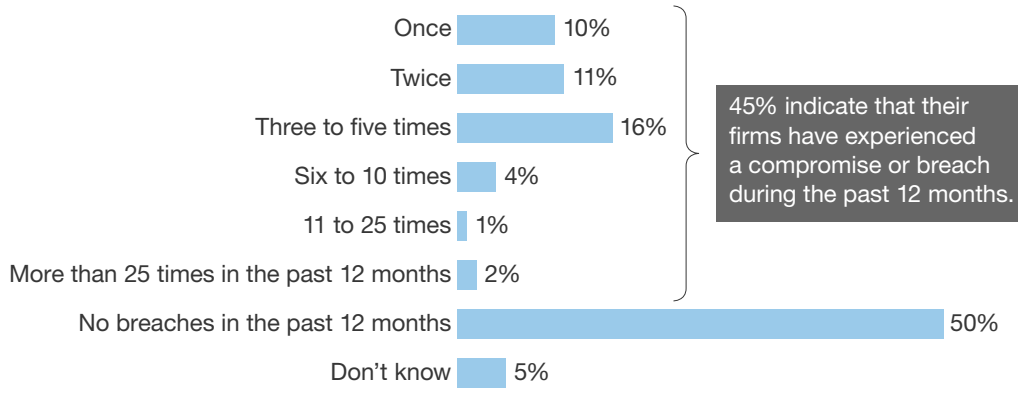
Unfortunately, even enterprises with the most mature security organizations and advanced security controls can't prevent every single breach — especially if your opponent has the time and financial backing to target you. JPMorgan Chase spends $250 million annually on its cybersecurity budget yet was unable to prevent an intrusion that led to the exposure of data of 76 million households.[11]

Every enterprise needs an incident response plan, but enterprises often fail to map out their incident response plan prior to a breach or other security incident. Without a proper plan in place ahead of time, it's extremely difficult to contain or stop the incident once detected and preserve appropriate forensic evidence while you help restore IT services. You must also understand the extent of the incident and what information the attackers compromised so that you can determine if you need to contact law enforcement and send breach notifications to affected parties, such as your customers, partners, and employees.

Figure 1 Frequency And Results Of Data Breaches

1-1 | Frequency of breaches during the past 12 months

"How many times do you estimate that your firm's sensitive data was potentially compromised or breached in the past 12 months?"



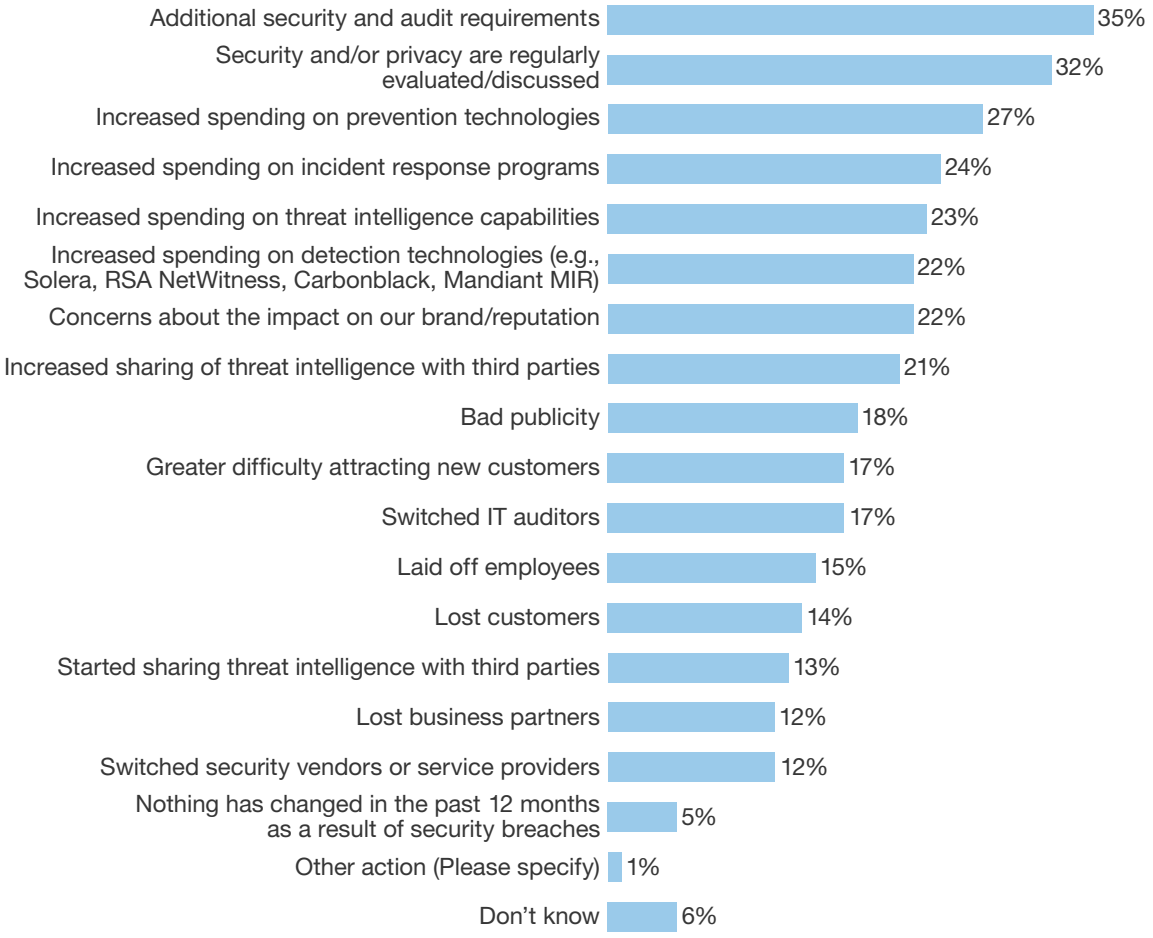
Base: 495 global decision-makers responsible for network security (1,000+ employees)
(percentages may not total 100 because of rounding)

Source: Forrester's Business Technographics® Global Security Survey, 2014

Figure 1 Frequency And Results Of Data Breaches (Cont.)

1-2 Change resulting from a breach

"What has changed at your firm as a result of the breaches occurring in the past 12 months?"



Base: 249 global decision-makers responsible for network security at companies that have had a breach in the past 12 months (1,000+ employees) (multiple responses accepted)

Source: Forrester's Business Technographics® Global Security Survey, 2014

A Patchwork Of Industry And Government Regulations Mandate Incident Response

If you have yet to invest significant time and resources in incident management and response and you fail to respond appropriately to a breach, your organization could find itself facing noncompliance and significant fines. Members of the United States Congress criticized the United States Postal Service over its response and notification of the recent breach that affected more than 800,000 employees. It took over two months for the employees to be notified of the breach.[12] Consider that:

- **Almost every US state requires breach notification.** In the US, 47 states plus the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.[13] Lobbying efforts are currently under way to create a single US national standard on how organizations notify customers of a data breach.[14]

- **The SEC has issued breach notification guidance.** According to CF Disclosure Guidance: Topic No. 2 Cybersecurity: ". . . material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading." This guidance typically applies to all publicly traded companies on US exchanges.[15]

- **Some US federal law requires breach notification.** The US HITECH Act requires healthcare providers and other Health Insurance Portability and Accountability Act (HIPAA) entities to notify when a breach affects more than 500 individuals. Failure to notify individuals of a data breach could result in a HIPAA violation and a fine of up to $50,000 per violation.[16]

- **Significant changes to European data protection are coming.** The European Union is expected to approve sweeping measures that would require "any business that suffers a data breach involving personal information to alert regulators and directly notify individuals." These new breach detection requirements would apply to any company that does business with Europeans.[17]

- **Canadian legislators are reviewing breach notification.** The Digital Privacy Act, also known as Bill S-4, is currently before the Canadian House of Commons. The bill amends the Personal Information Protection and Electronic Documents Act to include specific breach notification requirements.[18]

- **Breach notification requirements are evolving in the Asia Pacific region.** In South Korea and Taiwan, there are legal obligations for breach notification. In Japan and the Philippines, notification is not required unless specific conditions are met. In Australia, notification is strongly recommended, but not required (although a breach notification bill is pending).[19]

- **The PCI Data Security Standard provides very specific guidance on incident response.** Requirement 12.10 states: "Implement an incident response plan. Be prepared to respond immediately to a system breach." Requirement 10.2 requires "automated audit trails for all

system components to reconstruct" seven categories of events. Appendix 1.4 requires an organization to "enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider."[20]

YOU MUST ESTABLISH AN ONGOING INCIDENT MANAGEMENT PROGRAM

An incident response plan, like a business continuity (BC) or an IT disaster recovery (DR) plan, is your organization's immediate response to a specific threat. IT security professionals should talk with their counterparts in BC/DR; the fundamentals of strategy development and response planning are very similar as are the lessons learned. You wouldn't want to learn how to cut over from a failed primary site to a back-up hot site after the outage occurred. You have created a DR plan to handle this scenario. By the same token, you don't want to develop your incident response plan in real time while cybercriminals are pilfering intellectual property. A well-defined incident management program provides a script to follow when incidents occur.

Define The Incident Management Life Cycle

To be effective, you need to establish an ongoing incident management program — one that lets you identify the potential risks and threats to your enterprise so that you can create appropriate response plans, test those plans, and keep those plans current (see Figure 2). Forrester defines the six main areas of the incident management life cycle as:

- **Risk analysis.** Just as with BC/DR planning, before you can plan, you have to understand your business and identify the most probable, high-impact risks that you must mitigate or for which you will develop response plans. Who or what are you trying to protect your assets from?

- **Threat analysis.** Before you deploy a technology or service to improve business and IT resiliency, it helps to understand the organization's IT architecture and infrastructure so that you can identify single points of failure and other weaknesses. In a security context, you want to understand where and how your enterprise stores its most sensitive information and where systems and networks are the most vulnerable to attack. You can conduct a data discovery project to determine where the most sensitive data resides. You can also use a vulnerability management program, including vulnerability scanning and penetration testing to determine weaknesses in the enterprise environment.

- **Security policy mapping.** Over the years, the goal of BC/DR has been to mitigate the most common cause of disruption by building high availability and resiliency into the IT architecture itself. The same is true with security; you want to embed security throughout the environment to mitigate known threats and vulnerabilities as much as possible. Evaluate the results of your risk and threat analyses and compare them against your existing security controls. Implement measures that apply the appropriate level of rigor to your security controls based on the

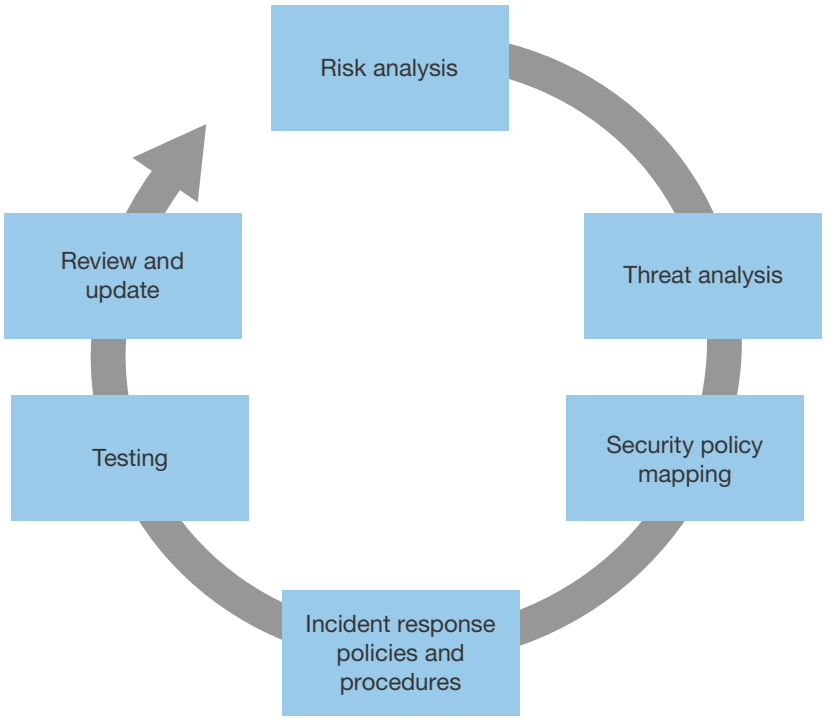
likelihood of a threat occurring and its impact. For example, you may need to purchase a new web application and database firewall to protect a newly launched web application that is core to the business' success.

- **Incident response policies and procedures.** You can't mitigate every risk; at some point you will need to respond quickly to a sudden IT failure or natural disaster such as an earthquake. Likewise, there's no set of security controls that will guarantee you won't suffer a breach. A security breach is inevitable. When it happens, you will need to categorize the incident according to certain criteria, mobilize the response team, contain or stop the incident, gather forensic evidence if applicable, restore the disrupted service, notify individuals if necessary, and continue the forensic investigation to determine what happened and what course of action is necessary to take.

- **Testing.** There's a saying in DR: If you're not finding problems when you test, you're not testing thoroughly enough. It's critical to test your incident response plans before the incident. Testing validates response capabilities, trains the response team in its roles and responsibilities, and uncovers weaknesses or invalid assumptions in the plan. If you're not testing, you're simply not prepared.

- **Review and update.** After each test or incident, you should hold a debriefing, after which you update the plans. You should also update the incident response plans after every major change to the business or the IT environment; ideally, change to the incident response plans is a part of ongoing change and configuration management.

Figure 2 Incident Management Life Cycle



60564 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Set Up A Cross-Functional Incident Response Team

The makeup of the incident response team will vary depending on the company's industry, size, and geographic reach of the enterprise, and the types of incidents to which it will respond. However, your incident response team must include a cross-functional group of both internal and external experts, including (see Figure 3):

- **Information security staff.** These individuals are responsible for handling the detailed investigation of the incident. Depending on the size of the organization, you might have dedicated incident response staff with advanced forensics capabilities. Many organizations hire external consultants to assist with incident response and forensics. Despite this, at a minimum, you still want someone on your staff who can perform basic incident response.

- **IT staff.** You may need these system and network administrators to help with investigations because of their advanced knowledge of the applications and systems they support.

- **Legal representative.** A member of your legal staff should participate in the incident management planning and response to provide guidance on the legality of potential searches and the requirements of evidence collection. He or she can also help you determine if you need to contact law enforcement and other government officials. Many firms will supplement their legal staff with outside counsel from firms like Stroz Friedberg with expertise in breach notification, incident response, and privacy.

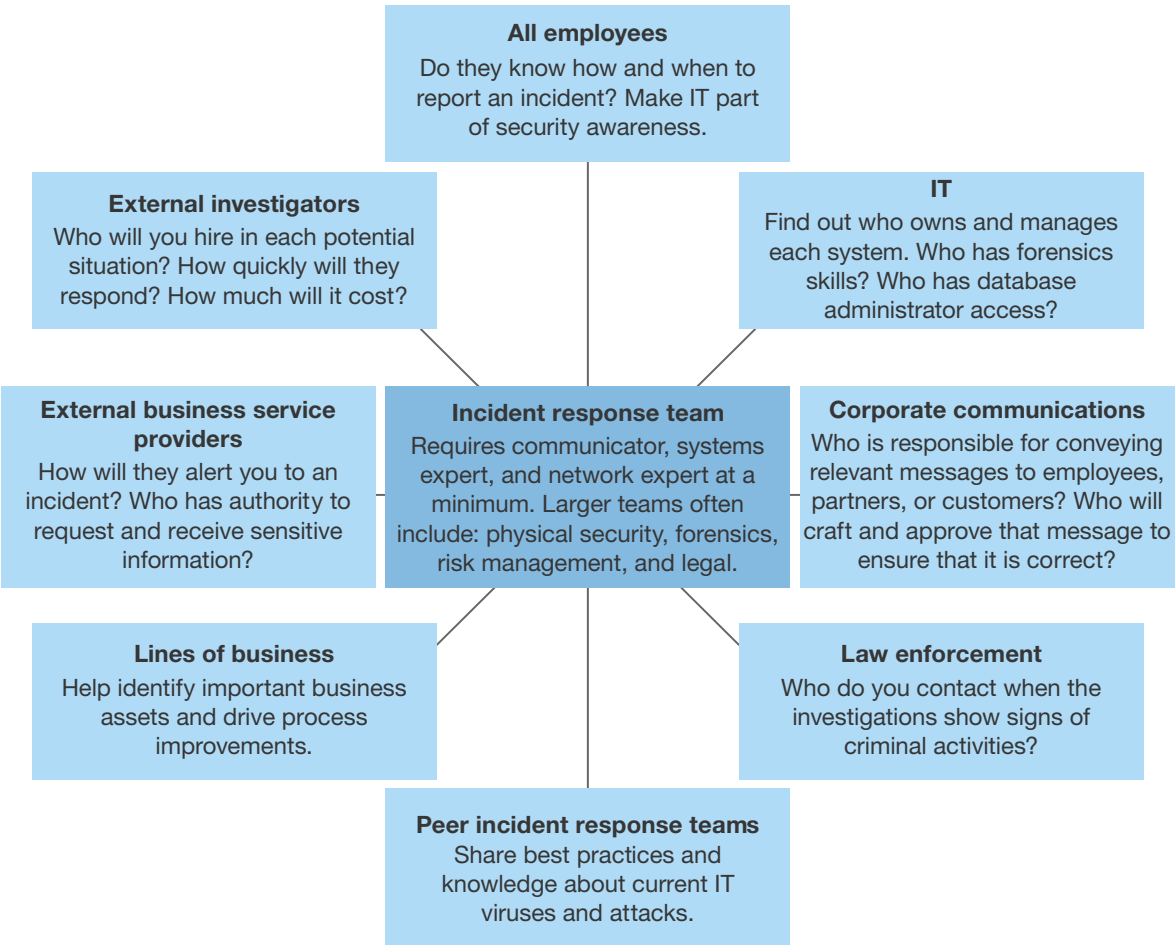
- **Business representative.** The information security team is a custodian of data and will need to partner with the business unit data owners to understand the data and its implications. Ideally, this should be done prior to an incident occurring and not after you've activated the incident response plan. One emerging trend is the rise of the chief data officer (CDO). If a company doesn't have a CDO, Forrester recommends that a "data champion" be appointed to serve this function.[21]

- **Corporate communications representative.** This team member's involvement is critical. The organization must know who is going to speak for the company and what message the company will deliver to customers, investors, and business partners. Poor communication can increase customer frustration and anger and irreparably damage your corporate reputation.

- **External incident responders.** Hire an external investigator when your own team is overwhelmed or lacks the necessary skills to properly respond to the incident. CrowdStrike, Fidelis Cybersecurity Solutions, FireEye/Mandiant, RSA Advanced Cyber Defense, the public accounting firms, and many value-added resellers like Accuvant can assist with incident response. All third-party firms aren't created equal. You should consider the organization's experience, methodology, and consultant availability.

- **External breach notification providers.** In the US, almost every state now has its own breach notification requirements, and although they're generally similar, they're not identical. In the event of a breach for your organization, these laws require a timely response. Service providers such as AllClear ID, Experian, and ID Experts can lend their expertise with the notification process if your organization isn't yet prepared to handle a breach. Identity theft protection organizations such as Equifax often work in concert with the notification providers, and you can hire them to monitor your victims' financial accounts as remuneration. Many will have the option to engage in prebreach planning services, and draw up contracts and arrangements in advance that are activated immediately following a breach event.

Figure 3 Incident Response Team



60564 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Use A Recognized Industry Framework For Incident Handling And Response

When you define incident response policies and procedures, you should make sure that they also follow a life cycle. There are numerous frameworks for this life cycle from industry groups such as the SANS Institute and government groups such as the National Institute of Standards and Technology (NIST). We use the NIST Computer Security Incident Handling Guide (800-61) as our sample reference framework because of its popularity with clients and its simplicity.[22] It consists of the following phases (see Figure 4):[23]

- **Preparation.** This phase includes all the initial planning that we've already described in this report, such as the definition of an ongoing incident management program life cycle and the creation of a cross-functional team. Most of the work is in preparation and ongoing management. NIST provides a "Tools and Resources for Incident Handlers" checklist with very specific guidance on preparing for incidents. Cyberthreat intelligence (CTI) should be incorporated into the preparation phase. From a tactical perspective, CTI can be used to block adversary actions in advance of attacks. From a strategic perspective, CTI can be used to make longer-term decisions that improve detection and response to the adversary.[24]

- **Detection and analysis.** Many S&R pros are not even aware when the enterprise has already suffered a breach. This is commonly caused by underinvestment in network analysis and visibility (NAV) and endpoint visibility and control (EVC) tools that can detect abnormal patterns and user behavior in their networks and IT environment.[25] Adopt Zero Trust principles to better prepare for detecting intrusions.[26]

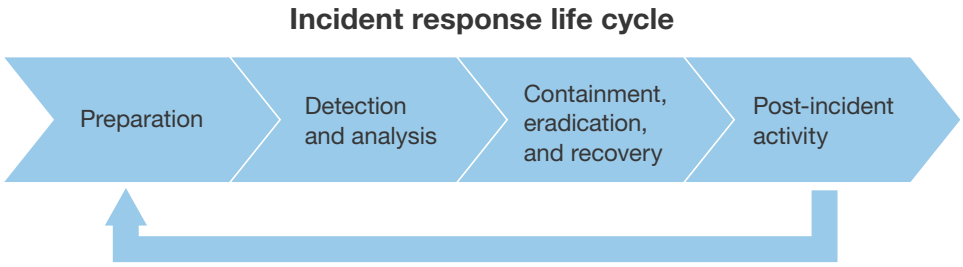
  Once you detect an incident, analysis is also important. In BC/DR, the event or incident must meet certain activation criteria before a designated individual makes the decision to invoke a plan. Similarly, you must provide a clear identification and escalation process for incidents and tightly integrate it with existing incident management processes in the network operations center (NOC) and security operations center (SOC).[27] NIST provides criticality ratings and also includes a sample incident response service-level agreement (SLA) matrix.

- **Containment, eradication, and recovery.** The business has less and less tolerance for downtime, whatever the cause: the weather or a security breach. You will be under tremendous pressure to stop the attack and resume normal operations as soon as possible. You need to be careful, because you want to make sure that: 1) you have truly contained the attack and 2) you don't destroy any forensic evidence in the process of quickly restoring the IT service. It's important that you train employees in forensics and prevent other employees or tools from inadvertently destroying evidence that you might need later in any kind of internal or government investigation. NIST provides helpful criteria for determining the appropriate containment strategy.

  It's critical to ensure that the incident is truly contained or remediated. In the DigiNotar breach, the firm failed to revoke all the malicious certificates. According to Wired.com, "The company insisted that all of the certificates had been revoked — which would have undermined any attempt by someone to use the certificate to impersonate a legitimate site — but somehow missed the Google certificate. DigiNotar finally revoked the Google certificate after the search giant disclosed its existence in the wild."[28]

- **Post-incident activity.** This phase of incident response is critical, and you must not shortchange it. You must incorporate the lessons learned from the incident into future incident response plans. NIST provides a list of questions that you should include in post-incident meetings.[29]

Figure 4 NIST Incident Handling



Source: Karen Scarfone, Tim Grance, and Kelly Masone, "Computer Security Incident Handling Guide," National Institute of Standards and Technology Special Publication 800-61 Revision 1, March 2008

TESTING AND TRAINING ARE CRITICAL TO SUCCESS

We've already discussed testing and training as a key phase in the incident management life cycle, but it's important to call them out separately because they really determine the long-term success of your program and individual response plans.

If You Don't Test, You're Not Prepared

Confucius said, "What I hear, I forget. What I see, I remember. What I do, I understand." To truly understand your incident management capabilities you must periodically test individual incident response plans. You test a BC plan; you should do the same here. Testing helps validate response capabilities and questions assumptions in the plan. In addition, testing helps everyone understand the contents of the plan as well as their roles and responsibilities. Here are some keys to successful testing:

- **Testing needs to include all members of the team.** At least once a year you need to conduct an incident response test that goes beyond the confines of IT or the information security staff. Validate your call tree and ensure that you have correct after-hours contact information for all the team members.

- **Just as in BC, take advantage of multiple test types.** There are multiple types of tests, including plan walk-throughs, tabletop exercises, and simulations. Plan walk-throughs and tabletop exercises help the response team understand the contents of a plan and their roles and responsibilities. For simulations, you should consider hiring a third-party penetration testing company to perform an assessment of your security controls and detection capabilities. Some organizations may elect to inform their staff of the testing, while others choose a blind penetration test. If you want to conduct real-world testing, blind assessments are the route to go.

- **Incorporate test results into incident management planning.** It's absolutely critical that you incorporate the results of the tests into your plans. Your incident management strategy and individual plans should adapt and change based on the successes and failures of the testing scenarios.

You Must Train IT And Non-IT Staff In Incident Response

Companies need to train their staff to understand what an incident is, how to respond appropriately, how to contact responders for services, and how to put incident response into the greater context of information security. This is a necessary next step in order to provide effective response and forensic services. Here are some suggestions to maximize training:

- **Budget for incident response training.** Build incident response training into the annual budget. The threat landscape is constantly changing, and cybercriminals are using new, advanced techniques to breach organizations. Specific training is critical to staying abreast of the latest attack and mitigation techniques. Your staff will also network with other incident handlers, which will result in future collaboration and information-sharing. The SANS Institute and CERT offer widely recognized incident handling courses.[30]

- **Include all employees in incident response training.** Training needs to extend beyond IT staff. End users are on the frontline and need to be aware of the threats and how to respond to them. Conduct end user training that specifically addresses social engineering, spear phishing, and how to respond to suspicious emails, files, and instant messages.[31]

DECIDE IF PROSECUTION IS NEEDED BEFORE REMEDIATION

Things work differently in real life than it does on your favorite crime investigation show. Too often, the executive decision to find and prosecute the perpetrator of the breach occurs after breach cleanup. Unfortunately, at that point, most of the evidence is also cleaned up, and true justice becomes illusory. Electronic crimes and physical crimes are different, so you must:

- **Make an investigation and prosecution decision immediately.** Bringing the bad guy to justice could be problematic. You may need to keep a breached system running in order to preserve evidence. In addition, it could take a significant amount of time before a trained forensic investigator or law enforcement official can respond to your breach.

- **Consider the preservation of evidence and chain of custody.** Remember that to prosecute a cybercrime, you must present breach evidence in court. This means that not only will the details of the crime become part of the public record, but the proper preservation of the evidence may be called into question. There are rules of evidence that must be followed if you want to see justice.

WHAT IT MEANS

MAKE INCIDENT MANAGEMENT A TOP SECURITY PRIORITY

With an avalanche of state, federal, and industry-specific breach notification laws on the horizon, S&R pros have no choice but to implement an incident management program. If you don't have an incident management program and specific incident response procedures in place, it's imperative that you do so immediately. However, don't see incident management as just another regulatory obligation, something that you do half-heartedly to appease internal and external auditors. An effective incident response to a serious security breach can be the difference between your organization's recovery and future success and irreparable damage. Take it seriously, and make it a top priority for your organization. Implement an ongoing program, define your response procedures, test them, and train as many people inside and outside of IT as you can. Set a baseline today, lay out a road map for future improvement, and begin developing relationships with peers and other industry experts to share best practices.

SUPPLEMENTAL MATERIAL

Methodology

Forrester's Business Technographics® Global Security Survey, 2014 was conducted via a mixed methodology phone and online survey fielded in April-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.

We have illustrated only a portion of survey results in this document. For access to the full data results, please contact forrsights@forrester.com.

ENDNOTES

[1] Source: "Ponemon Institute Releases 2014 Cost of Data Breach Study: Global Analysis," Ponemon Institute, May 5, 2014 (http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis).

[2] Source: Forrester's Business Technographics® Global Security Survey, 2014 and Forrester's Forrsights Security Survey, Q2 2013.

[3] Given that more S&R pros will invest in detection and response capabilities, more security teams will be in a better position to detect and respond to breaches. Thus, we feel confident that while at least 60% of enterprises will discover a breach, the actual number of breached entities will be much higher, as high as 80% or more. To learn more, see the November 12, 2014, "Predictions 2015: Security Budgets Will Increase, As Will Breach Costs, Fines, And Lawsuits" report.

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

[5] Source: Ryan Naraine, "Nortel hacking attack went unnoticed for almost 10 years," ZDNet, February 14, 2012 (http://www.zdnet.com/article/nortel-hacking-attack-went-unnoticed-for-almost-10-years/).

[6] Source: "A 'Kill Chain' Analysis of the 2013 Target Data Breach," Committee on Commerce, Science, and Transportation, March 26, 2014 (http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=24d3c229-4f2f-405d-b8db-a3a67f183883%27).

[7] Source: Ed Silverstein, "Inadequate data breach preparation, response should lead to removing 70 percent of directors at Target says ISS," InsideCounsel, May 30, 2014 (http://www.insidecounsel.com/2014/05/30/inadequate-data-breach-preparation-response-should).

[8] Source: Steve Ragan, "Code Spaces forced to close its doors after security incident," CSO, June 18, 2014 (http://www.csoonline.com/article/2365062/disaster-recovery/code-spaces-forced-to-close-its-doors-after-security-incident.html).

[9] SPE scored a data-loss hat trick by failing to secure: personally identifiable information (PII), personal health information (PHI), and intellectual property (IP). The attackers used this stolen information to successfully embarrass and extort the company and prevent the release of the film, *The Interview*. In this report, Forrester will summarize the currently available details and provide recommendations that S&R pros must consider to reinforce their cybersecurity programs and protect their digital business. See the December 18, 2014, "Quick Take: Sony Breach — A Sad Tale Of Epic Failure That Could Have Been Avoided" report.

[10] Source: Kim Zetter, "Former Employees Are Suing Sony Over 'Epic Nightmare' Hack," Wired, December 16, 2014 (http://www.wired.com/2014/12/sony-getting-sued-former-employees-protecting-data/).

[11] Source: Hugh Son and Madeline McMahon, "Dimon Sees Cyber-Security Spending Doubling After Hack," Bloomberg, October 11, 2014 (http://www.bloomberg.com/news/2014-10-10/dimon-sees-jpmorgan-doubling-250-million-cyber-security-budget.html).

[12] Source: Morcos Colon, "USPS draws ire of Congress over data breach response," SC Magazine, November 20, 2014 (http://www.scmagazine.com/congress-criticizes-usps-data-breach-response/article/384520/).

[13] Source: "Security Breach Notification Laws," National Conference of State Legislature, September 3, 2014 (http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx).

[14] Source: Rob Scott, "Retailers push for uniform data breach notification law," Associations Now, November 17, 2014 (http://associationsnow.com/2014/11/retailers-push-uniform-data-breach-notification-law/).

[15] Source: "CF Disclosure Guidance: Topic No. 2 Cybersecurity," Division of Corporation Finance, Securities and Exchange Commission, October 31, 2011 (http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm#_ednref3).

[16] The US HITECH Act requires healthcare providers and other HIPAA entities to notify when a breach affects more than 500 individuals. Failure to notify individuals of a data breach could result in a HIPAA violation resulting in a fine of up to $50,000 per violation. Source: "HHS Issues Rule Requiring Individuals Be Notified of Breaches of Their Health Information," US Department of Health & Human Services press release, August 19, 2009 (http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html) and "Federal Register, Vol. 74, No. 209," US Department of Health & Human Services, October 30, 2009 (http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf).

[17] Source: Matthew J. Schwartz, "EU Prepares Tough Breach Notification Law," Bank Info Security, September 9, 2014 (http://www.bankinfosecurity.eu/interviews/eu-prepares-tough-breach-notification-law-i-2435).

[18] Source: "BILL S-4," Senate of Canada, April 8, 2014 (http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=6524312&File=4).

[19] Source: "Australia Updates Breach Notification Guide; Notice Strongly Recommended, Not Required," Bloomberg BNA, September 2, 2014 (www.bna.com/australia-updates-breach-n17179894312/).

[20] Source: "Payment Card Industry (PCI) Data Security Standard," PCI Security Standards Council, November, 2013 (https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf).

[21] The key here is to ensure that there is an identified business stakeholder who will support and drive data classification efforts as a part of the organization's overall data strategy. A data champion is an individual responsible for the organization's use of data for business purposes, and thus has an incentive to ensure that the data is protected and used appropriately. For more on data classification, see the October 1, 2014, "Rethinking Data Discovery And Data Classification" report.

[22] Source: Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, "Computer Security Incident Handling Guide," National Institute of Standards and Technology Special Publication 800-61 Revision 2, August 2012 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf).

[23] Source: Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, "Computer Security Incident Handling Guide," National Institute of Standards and Technology Special Publication 800-61 Revision 2, August 2012 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf).

[24] See the November 3, 2014, "Know Your Adversary" report.

[25] To provide this type of deep insight into internal and external networks, Forrester has defined a new functional space called network analysis and visibility (NAV). NAV is comprised of a diverse tool set designed to provide situational awareness for networking and information security professionals. See the January 24, 2011, "Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility" report.

[26] See the October 7, 2014, "No More Chewy Centers: The Zero Trust Model Of Information Security" report.

[27] Staffing the traditional security operations center (SOC) is expensive. Forrester anticipates that the SOC will become virtualized in the future, in a next-generation transformation that we call "SOC 2.0." SOC 2.0 will not be a physical place or a projection screen but an enterprisewide, distributed, virtualized information resource that allows security and risk professionals access to the data they need wherever and whenever they need it. See the April 20, 2010, "SOC 2.0: Virtualizing Security Operations" report.

[28] Source: Kim Zetter, "DigiNotar Files for Bankruptcy in Wake of Devastating Hack," Wired, September 20, 2011 (http://www.wired.com/threatlevel/2011/09/diginotar-bankruptcy/).

[29] NIST's list of questions that you should include in post-incident meetings: 1) Exactly what happened, and at what times? 2) How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate? 3) What information was needed sooner? 4) Were any steps or actions taken that might have inhibited the recovery? 5) What would the staff and management do differently the next time a similar incident occurs? 6) How could information sharing with other organizations have been improved? 7) What corrective actions can prevent similar incidents in the future? 8) What precursors or indicators should be watched for in the future to detect similar incidents? 9) What additional tools or resources are needed to detect, analyze, and mitigate future incidents? Source: Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, "Computer Security Incident Handling Guide," National Institute of Standards and Technology Special Publication 800-61 Revision 2, August 2012 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf).

[30] Source: SANS Digital Forensics & Incident Response (http://digital-forensics.sans.org) and CERT (https://www.cert.org/training/).

[31] Forrester's "human firewall" research can assist you with building an effective security awareness program. See the April 24, 2014, "Enforce A Just Culture To Fortify The Human Firewall" 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