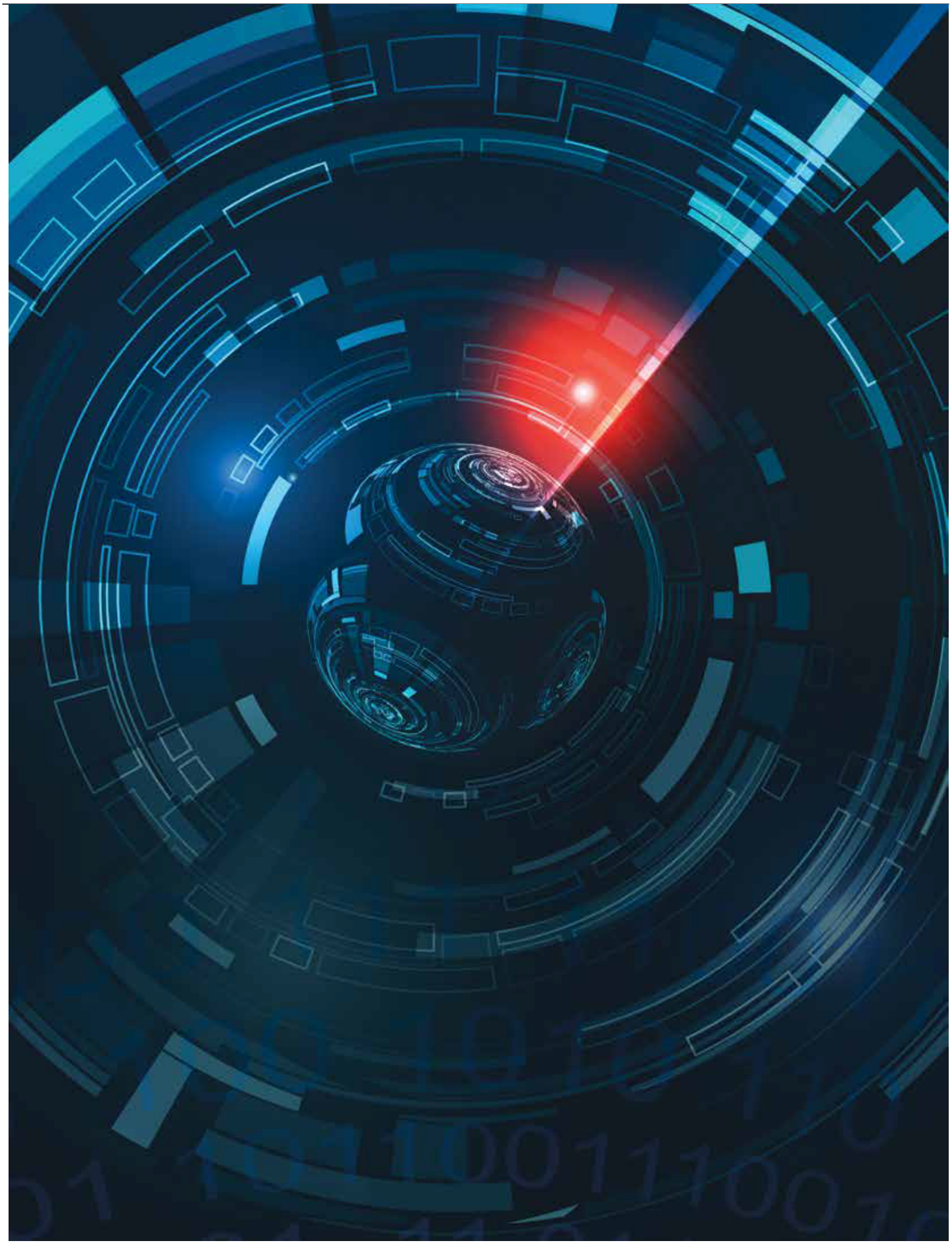
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Once More Unto the Breach: Why and How to Be Ready For a Data Breach

Technology, Privacy, and eCommerce



CHEAT SHEET

- ***When, not if.*** Data breaches have exploded over the last year. The magnitude and severity of recent high-profile breaches mean that effective breach response should be a priority.
- ***A stitch in time.*** IBM's benchmark cites the average compromised record as costing $217. Save on payouts by proactively training an incident response team.
- ***Uncertain reputational damage.*** While consumers are wary of breaches and find them stressful, 'breach fatigue' and the effort of switching companies might insulate affected organizations from the ill effects of the breach.
- ***Have a plan.*** A thorough breach response requires simultaneously interfacing with 10 parties, including legal, forensic and law enforcement teams, regulators, insurance, PR, stakeholders and personnel management.

"You're going to be hacked. Have a plan." These blunt words from Joseph Demarest, assistant director of the FBI's Cyber Division, capture the reality of our cyber threat environment. Data security breaches have become ubiquitous across industries, and high profile breaches at Target, eBay, Home Depot, JP Morgan Chase, Sony, Anthem and the federal Office of Personnel Management have saturated the news. The New York Times ran more than 700 data breach articles in 2014, a fivefold increase from the prior year.

Many organizations have reacted by throwing more resources into IT security controls and prevention. Global spending on IT information security for 2015 is forecasted at $77 billion, with annual growth at eight percent. But in a "when, not if " world of data breaches, organizations must also position themselves for effective breach response.

Effective breach response readiness cannot be achieved by your organization's IT security team alone. Eighty percent of data breaches are first discovered by law enforcement, financial institutions or other third parties, rather than by the organization itself. And response to an actual breach requires synchronized coordination of multidisciplinary activities beyond the ambit of IT security: legal, forensic, law enforcement, regulatory, insurance, public relations, stakeholders, notifications and personnel management.

Your organization's legal and compliance function has a central role in data breach response, handling substantive legal repercussions of the breach and also ensuring coordination of the overall response. As recent guidance from the Department of Justice's Cybersecurity Unit indicates, "[a] cyber incident is not the time to be creating emergency procedures or considering for the first time how best to respond." So, to paraphrase Demarest: In-house counsel, you're going to be notified that your organization has a data breach. Be prepared — have a plan.

Why be prepared?

Picture yourself meeting with the CEO or the audit committee chair, who asks you the following questions:

“I’ve seen a lot about data breaches lately — what are we really up against?”

Answer: Lots of threats, from multiple directions. Verizon’s Data Breach Investigations Report (“DBIR”) is an annual, global overview of security incidents and breaches with confirmed data loss. The 2015 DBIR analyzes nearly 80,000 incidents and more than 2,000 actual breaches that occurred during calendar year 2014. The results are sobering. While frequent targets are in healthcare, financial services and retail, essentially every industry is at risk. The means of attack are far more varied than the retailer point-of-sale intrusions so commonly mentioned in media reports, including such other patterns as crime-ware, cyber-espionage, insider misuse, web app attacks, miscellaneous errors, physical theft or loss, and denial of service attacks. And the threat environment is dynamic and volatile, not static. Incident patterns vary significantly between different industries, and they also change year to year.

In addition, the notion of “too small to be a target” is illusory. The 2014 NetDiligence study of cyber insurance claims found that more than 60 percent of data breaches resulting in cyber insurance payouts during 2013 involved organizations with less than $300 million in annual revenue, and a third were for organizations with revenue of less than $50 million. The two largest insurance payouts in the study, $13.7 million and $11.7 million respectively, were for a healthcare provider and a retailer that each had annual revenue under $300 million. And a smaller-sized entity may not be the ultimate objective. Speaking of “target,” a cyber-infiltration of HVAC service provider Fazio Mechanical is widely believed to have enabled the hackers’ entry, through a supplier portal, into the retailer Target’s network.

“We have significant spend on IT/network security. Why doesn’t that get the job done?”

Answer: Perimeter security defenses are essential, but clearly not sufficient to protect against data breaches. AT&T’s Chief Security Officer Ed Amaroso, at the January 2015 International Conference on Cybersecurity, described relying solely on perimeter security as “ridiculous” (best not to use that adjective in your conversation with management). Amaroso’s observation was that the system perimeter is porous by design, to allow external communication and data transmission (e.g., external email) and remote connectivity (e.g., access over the Internet from external servers and devices). While Amaroso’s ultimate point is valid — that internal system architecture should be reengineered for better segmentation and access control — the fact remains that data security is more than merely an IT problem with an IT solution.

For most organizations, the greatest security vulnerability is … us, the individuals. Verizon’s 2015 DBIR indicates that three of the four most common patterns for security incidents are miscellaneous errors, insider misuse and physical theft or loss, which each turn upon human behavior. And the fourth, crime-ware, is most commonly injected through phishing attacks or other social engineering that result in a person opening an attachment or clicking on a link laden with malware.

“How much would a data breach cost us?”

Answer: Odds are, a lot. The most commonly cited statistic is an average of $217 per compromised record for US breaches, based upon the most recent annual benchmarking study conducted by the Ponemon Institute and sponsored by IBM. Ponemon’s 2015 Cost of Data Breach Study offers a wealth of detail gleaned from 350 companies globally, including 62 US companies, that suffered breaches of up to 100,000 records. For example, the average US cost of a “malicious or criminal

breach" is $230 per compromised record, $210 per record for a breach resulting from a "system glitch," and $198 per record for breaches due to "human error." The US breaches in the study averaged at just over 28,000 compromised records, with a total average cost of more than $6.5 million, comprised of detection and escalation costs (9 percent), notification costs (9 percent), post-breach expenses (25 percent) and lost business (57 percent). Different industries yielded different average breach costs, ranging from healthcare at $398 per compromised record down to public sector at $73. The most significant factor reducing breach costs was found to be having an incident response team.

But one must be wary about forecasting data breach expense by rote cost per record arithmetic. The reality is that breaches involving only a few compromised records can be highly expensive, and those with large record volumes less so, at least per record. The NetDiligence 2014 Cyber Claims Study of 111 data breaches with insurance payouts during 2013 found a minimum cost per record of $0, a maximum cost per record of $33,000, and an average cost of $956 and a median cost of $20, respectively. And Target, for example, has already incurred $252 million in expenses through fiscal year 2014 for its data breach, only partially offset by $90 million in cyber insurance.

In its 2015 DBIR, Verizon offers a new, different approach to estimating expected data breach response costs, based upon an analysis of NetDiligence cyber claim data, and not including reputational damage. The result is continuums of probable hard costs, ranging for a 10,000-record breach from approximately $143,000 to $223,000, and from roughly $892,000 to $1,775,000 for a million-record breach.

Verizon's 2015 DBIR Model for Data Breach Hard Costs					
RECORDS	PREDICTION (Lower)	AVERAGE (Lower)	EXPECTED	AVERAGE (Upper)	PREDICTION (Upper)
100	$1,170	$18,120	$25,450	$35,730	$555,660
1,000	$3,100	$52,260	$67,480	$87,140	$1,461,730
10,000	$8,280	$143,360	$178,960	$223,400	$3,866,400
100,000	$21,900	$366,500	$474,600	$614,600	$10,283,200
1,000,000	$57,600	$892,400	$1,258,670	$1,775,350	$27,500,090
10,000,000	$150,700	$2,125,900	$3,338,020	$5,241,300	$73,943,950
100,000,000	$392,000	$5,016,200	$8,852,540	$15,622,700	$199,895,100

As is often the case with forecasting, the hard cost of an actual data breach depends on lots of variables — but it's undoubtedly expensive. And also consider the intangible costs for tying up your executives' time for months while data breach repercussions unfold, and the delay of planned upgrades and other organizational "improvements" put on hold while you determine impact and validate network integrity after a data breach. Though quantifying these types of indirect costs is almost impossible, there is a real impact on your business, employees and customers.

"OK, I get the hard cost exposure. But what about reputational damage?"

Answer: Here things get murky. Breaches intuitively should result in a loss of trust and goodwill with the affected individuals and other constituencies, such as unaffected customers, business partners and investors. And there are forecasts and analyses that attempt to quantify breach reputational damage. More than half of Ponemon's per record cost of a US data breach is the "opportunity cost" from abnormal turnover of existing customers and the decrease in new customer acquisition.

According to Ponemon, these opportunity costs vary per industry: Retailers have relatively low post-breach customer loss (2 percent) compared to organizations in other industries, such as financial (7.1 percent), healthcare (6 percent), technology (5.4 percent) and pharmaceutical (5.1 percent).

But actual numbers on reputational damage, separating the hype from the actual harm, are hard to come by. For example, stock prices of publicly traded companies suffering mega breaches do not reflect the reputational "hit" one might expect. Target closed at $61.65 per share the day before its December 18, 2013 breach announcement, at $62.15 the day after, and at $60.24 a month later. Likewise, Home Depot closed at $93.50 per share the Friday before its September 2, 2014 breach disclosure, $89 the day after, and $92.24 a month afterward. The day before its breach became public on February 13, 2015, Anthem closed at $142 per share, only to close the next trading day at $141.76, and a month later at $150.01.

A recent study of consumer sentiment about data breaches illuminates the contradictions at play. Three quarters of consumers whose information was compromised in a breach described the experience as "stressful," and 45 percent were very or extremely concerned about suffering identity theft. Yet 81 percent had no out of pocket expenses from the breach, and those who did averaged just $38. Fifty-five percent reported doing nothing independently, post-breach, to protect themselves from ensuing identity theft. Seventy-one percent continued their relationship with the company, most commonly responding with some combination of "It is too difficult to find another company with comparable products and services," "Data breaches affect most companies and I think it's unavoidable," and "The company resolved the data breach to my satisfaction."

On the one hand, we may be seeing "data breach fatigue," a new normal in which affected individuals simply accept breaches as an unfortunate fact of life. On the other hand, such a new normal will likely bring elevated expectations for how well organizations respond to a breach. Notably, the consumer sentiment study discussed above found that approximately half of the customers who did sever their business relationship post-breach reported that the company could have kept them as customers by providing some combination of a sincere, personal apology; free identity theft protection and credit monitoring; a responsive call center; and product or service discounts. Governmental and regulatory expectations for breach response will likely continue to increase as well, along with the level of scrutiny and penalties.

Some pundits have opined that, as expensive as data breaches may be, they are not yet expensive enough to compel truly effective security, resulting in a systemic "moral hazard." But let's leave such musings to the blogosphere, focusing instead on the more immediate, occupational hazard of data breaches — what must in-house counsel do to manage an effective response?

How to respond

Managing effective breach response is no small feat. There are 10 different channels of response activity for an organization that has suffered a data security breach. Most of these activity channels are involved in every data breach, and all must be attended to in significant breach scenarios. These activity channels are not sequential — they must be orchestrated in a synchronized manner in order for the response to be successful.

1. **Security.** Your organization's internal security team and systems may detect thousands of incidents daily, and through filtering and evaluation, significant incidents are escalated for further review, ultimately to determine whether the incident may be a breach requiring response. Alternatively, other functions within your organization may first notice the symptoms

of an intrusion, and financial institutions or other external parties may first sound the alarm. Once a potential breach is detected, third-party security firm expertise may be needed by internal security personnel to determine the nature and scope of the intrusion. Vulnerabilities must be neutralized, and intrusions contained and eradicated, with confirmation of effectiveness. And compromised systems must be restored to meet operational needs.

2. **Legal.** The attorney/client privilege should be invoked at the outset and be maintained for the overall response effort, including the engagement of any response service providers for security consulting, forensics, crisis communications, and notification management. Fact-finding must be done to identify the nature, scope and means of the data compromise, along with the type of protected information involved and the status and residency of affected employees, customers and others. For example, the definition of “protected information” under state PII breach notification satutes varies between different jurisdictions, with such laws triggered by the residency of the affected individuals. The applicability of federal, state and contractual breach response requirements must then be analyzed to determine whether a reportable breach has occurred, and if so, what notification of individuals, regulators and others, with what content, must be made within what timeframe. Decisions, notifications and other actions must be properly documented, and if subsequent litigation is anticipated, legal hold decisions to preserve relevant information must also be made.
3. **Forensic.** Many types of breaches will require forensic investigation, for regulatory, law enforcement and potential litigation purposes. Payment card data breaches will trigger merchant processor and card brand contractual requirements for an independent forensic investigation by an approved PCI firm, and forensic collection of evidence will also be important whenever civil litigation or regulator involvement is anticipated. The collection and preservation of forensic evidence must be done compliantly with evidentiary standards and regulatory and contractual mandates. The services of an external forensics firm are generally crucial for the necessary expertise, objectivity and independence.
4. **Law enforcement.** Based on the circumstances established through investigation, the organization must determine whether and when to notify law enforcement. Care must be taken to make first contact with the right agency, best done through pre-existing relationships with contacts in law enforcement. After notification, interaction with law enforcement must be coordinated in a way that serves the organization’s interests and ensures that the organization speaks with one voice through a designated contact, preferably its legal counsel.
5. **Regulators.** Through incident investigation and legal analysis, your organization must determine whether, when and how to notify which regulators. For example, HIPAA notifications are made to the federal Health and Human Services Department’s Office of Civil Rights, and the PII breach notification statutes of the respective 47 states, the District of Columbia, Guam, Puerto Rico, and the US Virgin Islands dictate which state agencies or credit bureaus must be notified, when, and in what manner, based upon the applicable jurisdictions’ regulatory reporting thresholds. After such notifications, the organization must coordinate with regulators to manage the relationship and repercussions.
6. **Insurance coverage.** The availability of coverage under your organization’s existing policies must be evaluated. It is possible, though unlikely, that some coverage may exist under traditional forms of coverage. In addition, your organization may have a cyber-insurance policy, usually with claims-made, named-peril coverages providing reimbursement for certain first-party expenses or losses, and defense and indemnity for certain third-party liabilities. Some cyber insurers require the use of panel providers for breach response, while others retain approval rights for the various service providers whose assistance will be needed. Cyber-insurance policies have a complicated web of conditions, exclusions and sub-limits for different coverage elements, which must be understood. After determining whether and when to notify its insurer, your organization will want to comply with policy requirements, coordinate

with the insurer, and protect its rights under the applicable coverages.

7. **Public relations/communications.** Any breach may have publicity repercussions, and significant breaches can have a dramatic impact upon the organization's financial performance. Your organization will need a plan for external communications about the breach that reconciles your brand image and reputational interests with regulatory requirements and legal exposures. The communications plan must be executed in a way that best positions your organization with customers, employees, the media and the public, and that also allows flexibility for effective reaction and response. And as with the law enforcement coordination, a single consistent message is key for external communications.
8. **Stakeholders.** Internal stakeholders, including customer-facing employees, executive management and the board, must be briefed on an escalating basis with timely updates, to avoid surprise and provide appropriate assurance. And business partners, employee unions and other stakeholders may need or expect appropriate information regarding the breach and response status.
9. **Notification.** Once your organization determines it is legally required or otherwise prudent to notify affected individuals, they must be notified in a timely, compliant manner under the applicable federal, state and contractual breach notification requirements. When large groups of individuals must be notified, the services of a notification management provider may be needed to accomplish the notifications, staff a call center and provide credit monitoring and fraud resolution services.
10. **Personnel management.** If employee conduct contributed to the breach, from malicious misconduct to mere mistake, your organization will need to determine what personnel action is warranted, ranging from counseling, to discipline, to termination for egregious conduct. Regardless, every breach is a teachable moment for the entire workforce on data security, including what to do and what to avoid.

The 10 Activity Channels for Breach Response

SECURITY

Detect, escalate, determine, contain, eradicate, confirm, restore

LEGAL

Fact-find, analyze, determine, document, preserve

FORENSIC

Investigate, collect, document, preserve

LAW ENFORCEMENT

Determine, notify, coordinate

REGULATORS

Determine, notify, coordinate

INSURANCE COVERAGE

Evaluate, determine, notify, coordinate

PUBLIC RELATIONS/COMMUNICATIONS

Plan, execute, react, respond

STAKEHOLDERS

Brief, escalate, update

NOTIFICATION

Identify, determine, deploy

PERSONNEL MANAGEMENT

Determine, act, communicate

In managing an effective breach response, these 10 activity channels are not linear. They overlap and interrelate. The analysis of legal responsibilities informs the security and forensic efforts, and vice versa. Results of the forensic and fact-finding investigations drive the planning for stakeholder briefings, crisis communications and notifications to law enforcement, regulators, insurers and affected individuals. Tensions may arise between the reputational interest of early communication and the compliance interest of an exhaustive investigation before any disclosures are made. And since disclosure to any involved constituency may accelerate awareness by others, the prenotification groundwork in each activity channel must be synchronized or else the organization will lose control of the response.

Breach response activities are most often executed in full crisis mode. Deciding how to handle all of these interwoven activities in the midst of an unfolding, high-stakes breach, with no advance planning, is a guarantee for failure. Also, by delaying preparations until a breach occurs, your organization surrenders its bargaining power when engaging the various breach response service providers it may need, including security and forensic investigation firms, breach notification management providers, and crisis communications consultants. Simply put, effective breach response requires breach response readiness.

Data Breach Acronyms for Lawyers

IT data security is an alphabet soup of acronyms. Here are some useful ones to know when discussing breach detection and response with your organization's InfoSec team:

- *CIRC:* Computer Incident Response Capability
- *CIRT:* Computer Incident Response Team
- *CSIRC:* Computer Security Incident Response Capability
- *CSIRT:* Computer Security Incident Response Team
- *DoS:* Denial of Service Attack
- *DDoS:* Distributed Denial of Service Attack
- *ISAC:* Information Sharing and Analysis Center
- *NIST:* National Institute of Standards and Technology
- *SIEM:* Security Information and Event Management
- *SLA:* Service Level Agreement
- *US-CERT:* United States Computer Emergency Readiness Team

How to prepare

Effective breach response readiness requires that your organization understand what will be needed in each of the ten activity channels as applicable for its anticipated breach scenarios, and also how these activities will be managed simultaneously, to avoid unnecessary risk, delay and cost. Through breach response readiness, your organization lays the groundwork in advance for these activity channels, so that structure, direction, and resources for dealing with an actual breach will be readily available. Here are key steps to take:

Coordinate readiness efforts through legal counsel under attorney/client privilege

The 10 activity channels are truly a multidisciplinary effort, and legal activity is only one of many functions involved. But there is no effective substitute for using legal counsel to coordinate the overall readiness effort, because of the significance of the underlying legal requirements and exposures, and the value of conducting the readiness work under the attorney/client privilege.

Gather the information needed for readiness planning

Pertinent information must be gathered to confirm data security and breach notification requirements applicable to your organization under federal and state laws and contractual relationships, and also to understand the current, internal capabilities for matters pertinent to breach response, including the management of protected information, IT system data security programs and controls, security incident detection and escalation, computer security incident forensics, cyber insurance coverage, media and crisis communications, FBI and other law enforcement liaisons, and business continuity capabilities.

Identify and involve your Incident Response Governance Team

Your organization should identify its internal individuals in roles and with responsibilities for managing security incident detection, investigation, and response; system restoration and business continuity;

breach determinations and notifications; cyber insurance coverage and coordination; law enforcement notification and involvement; and media and crisis communications. Through interviews and coordinated preparations these individuals will collaborate in the readiness effort. In the resulting readiness plan, many of these individuals will have Response Governance Team responsibilities, so their involvement in readiness planning is essential.

Establish your breach response service provider relationships

The organization should identify its preferred service providers for such matters as IT system data security services; security incident forensics; breach notification, credit monitoring and fraud resolution services; and media and crisis communications assistance. Whether such providers are simply identified, or service level agreements are put in place, it is invaluable for your organization to have worked through these determinations in advance.

Prepare your response plan

Information gathered in the above steps must be distilled into a documented response plan, including team roles and responsibilities, response processes for anticipated breach scenarios, and useful resources. Though no plan can anticipate every contingency, an effective response plan establishes internal roles and responsibilities; provides clear protocols for who does what, when and how, with which inputs; clarifies which service providers may be brought into the response, when and for what purposes; and contains contact information and other crucial resources for rapid response.

Train your team

The point of this effort is not simply to have a “plan,” but to be ready for effective response.

Your organization’s response team must be familiar with the plan, and with team members’ roles and responsibilities, across the range of anticipated breach scenarios. Training of response team members on breach response is essential, and tabletop breach exercises are invaluable for making breach response readiness a reality for your organization.

Conclusion

In a highly uncertain data security environment, two things are clear — breaches will happen, and organizations must respond. How well your organization handles the 10 activities necessary for effective breach response will turn upon how well you have prepared. Have a plan.

Further Reading

Verizon, 2015 Data Breach Investigations Report (Verizon 2015 DBIR) at 1.

Verizon 2014 Data Breach Investigations Report at 12, Fig. 14.

Verizon 2015 DBIR at 1.

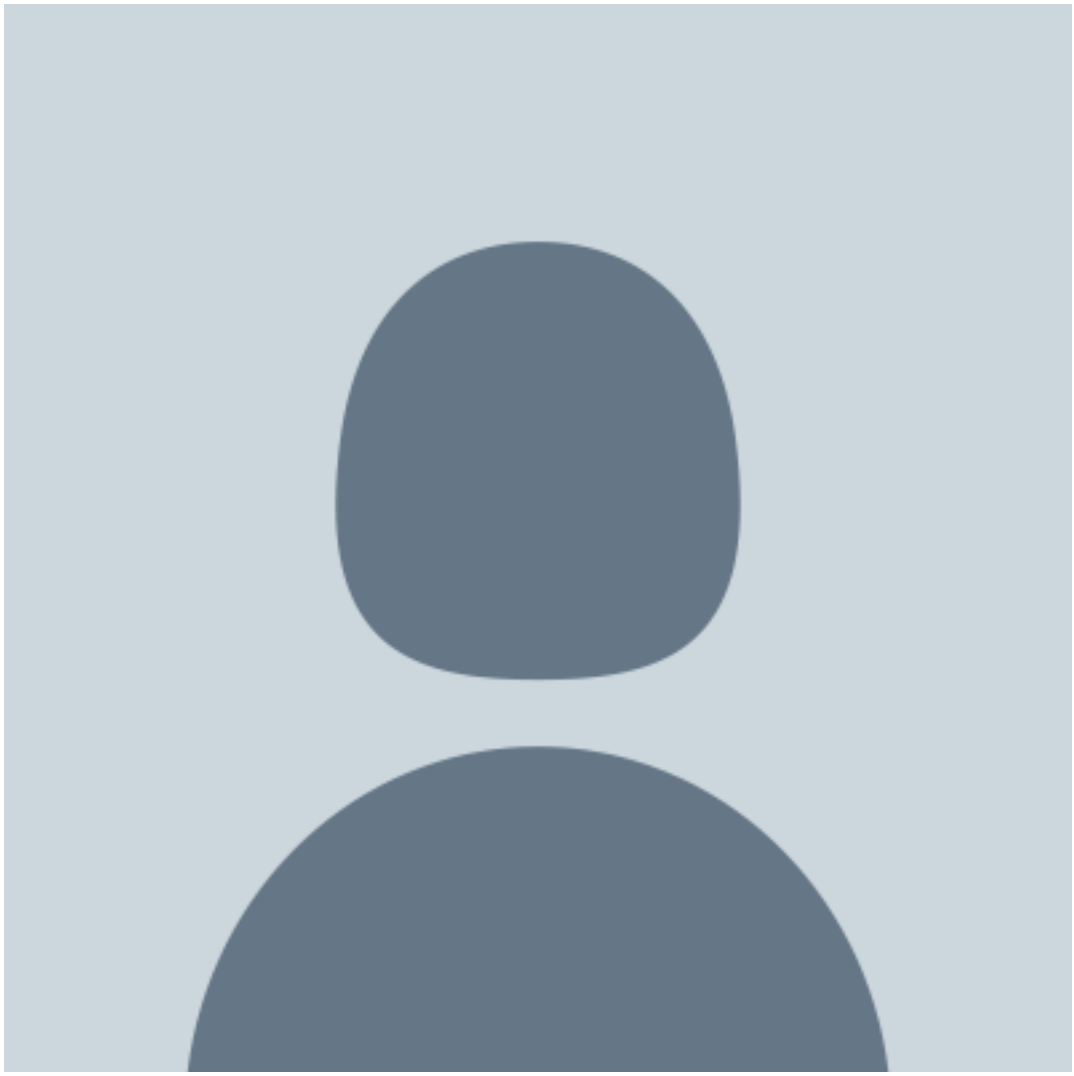
NetDiligence, 2014 Cyber Claims Study at 26-27.

Ponemon Institute, 2014 Cost of Data Breach Study: Global Analysis at 1. and 13

NetDiligence, 2014 Cyber Claims Study at 8.

Ponemon, The Aftermath of a Mega Data Breach: Consumer Sentiment (April 2014).

Robert Jett III

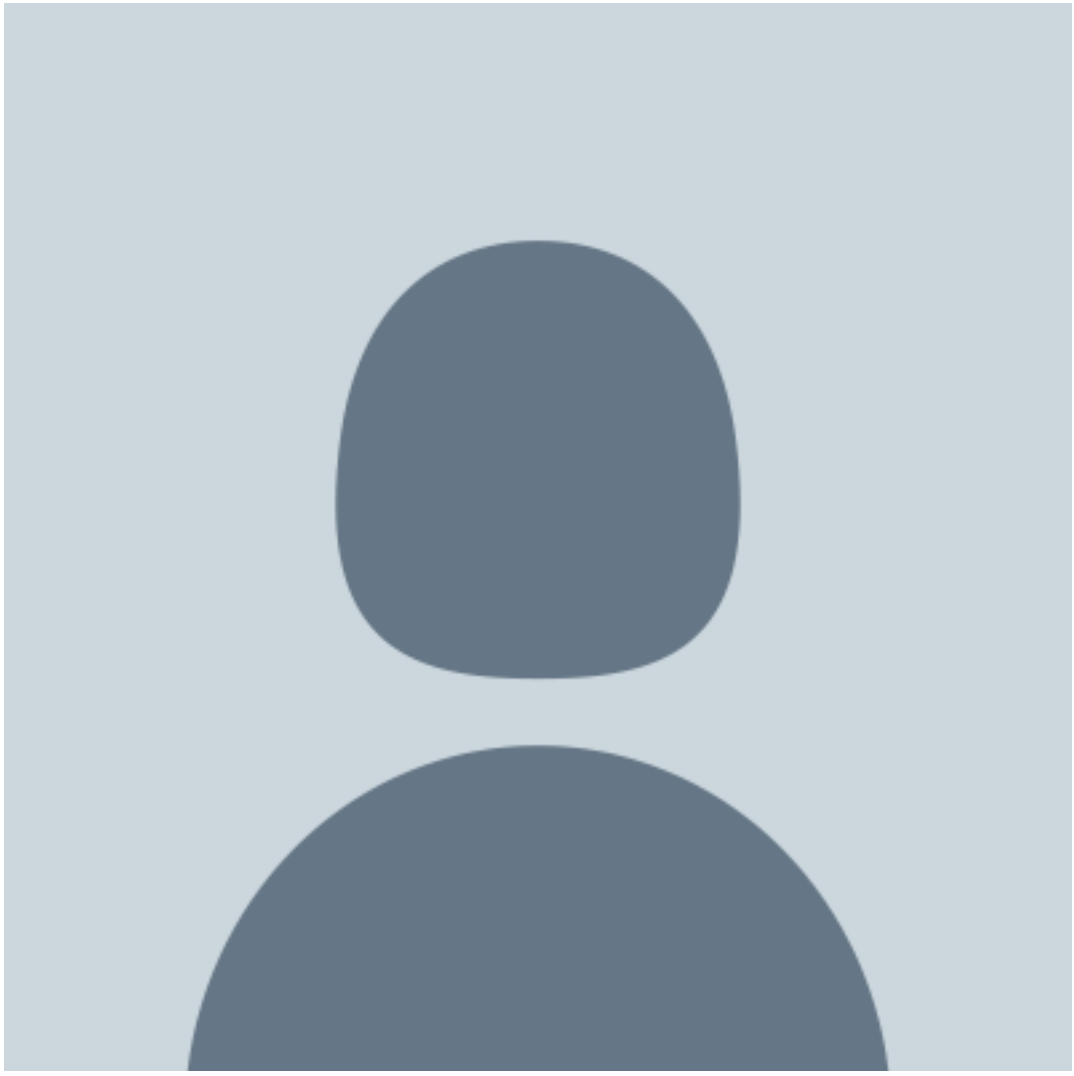


Global Compliance Counsel and Data Privacy Officer

RGA Reinsurance

He manages RGA’s global compliance and ethics program, and data privacy initiatives and policies in support of both.

Peter Sloan



Partner

Husch Blackwell LLP

Peter Sloan is founding member of the firm’s information governance group, advises clients on data security, breach incident response and breach response readiness.