HUSCH BLACKWELL

March 30, 2015

DATA BREACH RESPONSE READINESS

Is Your Organization Prepared?

Peter Sloan
Pete Enko
Jeff Jensen
Deborah Juhnke

The data security imperatives of Prevention, Detection, and Response do not end with prevention, for good reason. Data breaches have become inevitable, despite best efforts to prevent them. And once an unauthorized disclosure, hack, or other compromise of protected information has been detected, the organization must respond.

Effective response is no small feat. There are ten 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 overlap, interrelate, and must be handled in a synchronized manner if the response will be successful.

Security

An organization's internal security systems may detect thousands of events daily. Through filtering and evaluation significant events are escalated for further review, ultimately to determine whether an incident may be a breach requiring response. Alternatively, other functions within the organization may first notice the intrusion's symptoms, or external parties may first sound the alarm.

After a potential breach is detected, the internal security team will 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. Services of an external security firm may be needed for sophisticated intrusions and whenever the security vulnerability and response may be questioned by regulators or future litigants.

The organization's IT function likely has several important elements already in place for these security activities. Many have a Security Operations Center (SOC) within their IT function, which commonly uses a Security Information and Event Management (SIEM) tool to detect and evaluate network intrusions. Organizations may also have a Computer Security Incident Response Team (CSIRT or CIRT), usually with IT Security leadership, focused on computer security activities for incident response. Though vitally important, these IT security capabilities are typically neither intended nor sufficient to manage the other nine activity channels needed for effective breach response.

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.

Legal

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. Federal, state, and contractual breach response requirements must then be analyzed to determine whether a reportable breach has occurred, and if so, what notifications of individuals, regulators, and others, with what content, must be made within what timeframe. Decisions, notifications, and other actions must be properly documented. If subsequent litigation is anticipated, legal hold decisions to preserve relevant information must also be made.

Forensic

Many types of breaches will require forensic investigation for regulatory, law enforcement, and potential litigation purposes. The collection and preservation of forensic evidence must be done compliantly with evidentiary standards and regulatory and contractual mandates. The forensic services of an external security firm are generally crucial for the necessary expertise, objectivity, and independence.

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, in the right way. After notification, interaction with law enforcement must be coordinated to serve the organization's interests and ensure that the organization speaks with one voice.

Regulators

Through incident investigation and legal analysis, the organization must determine whether, when, and how to notify which regulators. After such notifications, the organization must coordinate with regulators to manage the relationship and repercussions.

Insurance Coverage

Coverage under the organization's existing insurance policies must be evaluated. It is possible, though unlikely, that some coverage may exist under traditional forms of coverage. In addition, the 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. 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, the organization will

need to comply with policy requirements, coordinate with the insurer, and protect its rights under the applicable coverages.

Public Relations

Any breach may have publicity repercussions. Significant breaches can have a dramatic impact upon the organization's reputation and financial performance. The organization will need a plan for external communications about the breach that reconciles its brand and reputational interests with its regulatory requirements and legal exposures. The communications plan must be executed in a way that best positions the organization with customers, employees, the media, and the public, and that also allows flexibility for effective reaction and response.

Stakeholders

Internal stakeholders, including executive management and the Board, must be briefed, 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.

Notification

Once the 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 and 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.

Personnel Management

If employee involvement contributed to the breach, from malicious misconduct to mere mistake, the organization must 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 Ten 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
Plan, Execute, React, Respond
Stakeholders
Brief, Escalate, Update
Notification
Identify, Determine, Deploy
Personnel Management
Determine, Act, Communicate

These ten activity channels are not linear. They must be pursued in parallel, and they have significant, interrelated impacts. 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 pre-notification groundwork in each activity channel must be synchronized, or else the organization will lose control of the response.

Breach Response Readiness

Breach response is 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.

Effective breach response requires breach response readiness.

Also, by delaying preparations until a breach occurs, the 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.

In our experience, effective readiness requires that the organization understand what will be needed in each of the ten activity channels 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, the 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.

1. Coordinate Readiness Efforts through Legal Counsel under Attorney/Client Privilege

The ten activity channels are truly a multi-disciplinary 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.

2. Gather the Information Needed for Readiness Planning

Pertinent information must be gathered to confirm data security and breach notification requirements applicable to the organization under federal and state laws and contractual relationships. Also, the current, internal capabilities for incident detection and breach response must be understood.

3. Identify and Involve your Incident Response Governance Team

The organization must identify its internal individuals 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 Incident Response Governance (IRG) Team responsibilities, so their involvement in readiness planning is essential.

4. 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 the organization to have made these determinations in advance.

5. Prepare Your Breach Response Readiness Plan

Information gathered in the above steps must be distilled into breach response plan documentation, including team responsibilities, response processes for anticipated breach scenarios, and useful resources. No plan can anticipate every contingency. But an effective readiness 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, secure communication channels, and other crucial resources for rapid response.

6. Train Your Team

The point of this effort is not simply to have a "plan," but to be ready for effective response. The IRG Team must be familiar with the plan, and Team members' roles and responsibilities, across the range of anticipated breach scenarios. Training of IRG Team members and other stakeholders on breach response is essential. And tabletop breach exercises are invaluable for making breach response readiness a reality for your organization.

Contacts For Breach Response Readiness

Peter Sloan
Kansas City, MO
peter.sloan@huschblackwell.com
816.983.8150

Pete Enko
Kansas City, MO
peter.enko@huschblackwell.com
816.983.8312

Jeff Jensen
St. Louis, MO
jeff.jensen@huschblackwell.com
314.345.6462

Deborah Juhnke
Kansas City, MO
deborah.juhnke@huschblackwell.com
816.983.8803

About Our Data Security Team

Husch Blackwell's Data Security Team helps clients with security compliance and risk management, data breach response, and risk mitigation, including security risk assessments and breach response readiness planning. The team is part of the firm's Information Governance Group, which provides interdisciplinary expertise in Privacy, Data Security, and Information Management to help clients satisfy information compliance requirements and manage risk while maximizing information value.

About Our Firm

Husch Blackwell is an industry-focused, full-service litigation and business law firm with offices in 15 U.S. cities and in London. We represent national and global leaders in major industries including energy and natural resources; financial services; food and agribusiness; healthcare, life sciences and education; real estate, development and construction; and technology, manufacturing and transportation.