



CYBER RISK



READINESS



RESPONSE

# NetDiligence<sup>®</sup>

## Incident Response Planning

Insights and Best Practices for Cyber Risk Managers

Sponsored by



# Incident Response Planning

## Insights and Best Practices for Cyber Risk Managers

The number and severity of cyberattacks continue to increase. According to a report<sup>1</sup> from security intelligence vendor Risk Based Security (RBS), over 6,500 incidents that resulted in compromised data have been publicly disclosed for 2018, two-thirds of them originating in the business sector. The government sector accounted for 13.9 percent, the medical sector for 13.4 percent and education for 6.5 percent.

The incidents were both large and widespread. A breach of the reservations system for a global hotel chain exposed the personal information of 500 million customers. A borough in Alaska hit with a ransomware attack had to resort to typewriters and handwritten notes in order to conduct routine business. That borough was identified as victim number 210 in a series of attacks on municipalities that included the city of Atlanta. And, according to Health IT Security<sup>2</sup>, email, targeted phishing attacks, and database misconfigurations were behind the year's largest breaches of patient data, with one attack lasting more than a year.

These attacks demonstrate the importance of having an actionable, tested incident response plan for all organizations, regardless of sector or size.

The purpose of this whitepaper is to help your organization develop an effective, actionable data breach response plan by sharing our insights, best practices and lessons learned from more than 15 years of experience supporting the cyber insurance incident response community.

### Planning is Compliance

Developing an Incident Response Plan (IRP) has long been recognized as a critical component of risk management, crucial to minimizing the fallout from a catastrophic breach event. Moving quickly can minimize lost profits, mitigate liability exposure, and reduce expenses associated with a drawn-out or delayed response. What's more, many leading cyber insurers and business partners now require companies to demonstrate readiness for an incident by having a written response plan in place.

In addition, IRPs are no longer just a best practice, they're becoming a regulatory requirement. The New York State Cybersecurity Regulation (23 NYCRR 500)—here referred to as "NY DFS"—is a new set of rules issued in 2017 by the New York Department of Financial Services. As of February 2018, covered entities—state-chartered banks, licensed lenders, private bankers, foreign banks licensed to operate in New York, mortgage companies, insurance companies and service providers—are required to comply with these rules. That includes having written security policy documents, one of which should be an IRP to demonstrate a good-faith effort to respond to a data breach in a responsible manner. This precedent-setting regulation is likely to be emulated by other states and business sectors, and potentially included in national requirements.

<sup>1</sup> <https://pages.riskbasedsecurity.com/2018-ye-breach-quickview-report>

<sup>2</sup> <https://healthitsecurity.com/news/the-10-biggest-u.s.-healthcare-data-breaches-of-2018>

In the European Union, the General Data Protection Regulation (GDPR), which went into effect in May 2018, stipulates that any company operating within the EU and holding data on EU citizens must notify regulatory authorities of a data breach within the challenging time frame of 72 hours. While there is no stated requirement for an IRP, having one is a baseline measure to ensure that proper remedial measures are taken, regulatory authorities contacted, and notification provided within the required timeline. This same principle applies for U.S. state-level data protection laws (not to mention District of Columbia, Guam, Puerto Rico and the Virgin Islands, which have their own laws).

Steven Peikin, Co-Director with the Securities and Exchange Commission's (SEC) enforcement division noted that "the greatest threat to our markets right now is the cyber threat."<sup>3</sup>

As the SEC's focus shifts more to cybersecurity enforcement, it would not be surprising to see the agency examine disclosures relating to data breaches, and the timing of those disclosures, more closely. Now, more than ever, companies may be held accountable if they fail to invest in data security or adequately prepare to respond to cyber incidents.

## Aligning with Regulation

Regulators now want to see that your company has an **actionable** cyber IRP and, in the case of an event, they will want to confirm that it has been followed to the letter. While there are many regulations that will require your organization to have an incident response plan, we've elected to use NY DFS as an example. The text of NY DFS provides useful detail for building an effective and compliant program and is a good indication of the types of questions regulators will ask. Section 500.16 contains the Incident Response Plan portion of the regulation. We've broken out the major required elements within this section and, in the "Our read" segments, extrapolated what we believe regulators will be looking for in a formal response plan.

### 1. The internal processes for responding to a Cybersecurity Event;

**Our read:** Each type of cyber event requires specific response processes. Consider, for example, if an employee opens an email, and then clicks on a URL that launches a ransomware attack that encrypts local PC files, LAN share files, and applications:

- How and to whom should the incident be reported?
- Is there a formal IRP, accessible to management at a moment's notice, that fully outlines responsible action steps?
- Who will remediate the damage and limit further data loss?

### 2. The goals of the incident response plan;

**Our read:** The IRP should be more than a response blueprint—it should also mitigate liability exposure and promote regulatory compliance.

- Does the plan detail an efficient method for quickly assessing the incident's root causes and damage to information systems?

<sup>3</sup> SEC Increases Focus on Cyber Incident Response, Technology Law Dispatch, Reed Smith, August 6, 2017, <https://www.technologylawdispatch.com/2017/08/privacy-data-protection/sec-increases-focus-on-cyber-incident-response/>

- Does it prioritize recovery tasks to minimize business disruption?
  - Does it account for the stipulations of laws and regulations and minimize legal liability?
3. The definition of clear roles, responsibilities and levels of decision-making authority;
- Our read:** The IRP should be unambiguous in its assignments to staff, management, vendors and other personnel so that it can be launched into action at a moment's notice, even in off-hours.
- Is there a Breach Coach® lawyer in place to assist (see "Assign external leadership" below)?
  - Who will lead the response internally and what vendors or experts outside the company will be involved?
4. External and internal communications and information sharing;
- Our read:** All communications must be optimized to support the response and ensure that internal and external stakeholders (including customers and regulators) receive timely updates.
- Who will helm communications and how will they keep everyone in the loop? Who needs to know what and when?
  - How will people with specialized tasks/skills necessary for identification, investigation, remediation, and reporting stay in continuous contact and provide timely input and updated status on the response effort?
5. Identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;
- Our read:** Once the cause of the cyber incident has been identified with confidence, responsible IT team members must demonstrate that remediation measures have been taken.
- What is the protocol for proposing, seeking approval for, implementing, and confirming successful deployment of the technical/procedural fixes necessary to resolve weaknesses (and prevent them from reoccurring)?
6. Documentation and reporting regarding Cybersecurity Events and related incident response activities;
- Our read:** It's not enough to respond. Regulators, auditors and stakeholders will want to see documentation of the response and assurance that it was effective.
- How should the tasks arising from requirements (1)-(5) above be documented so that an otherwise uninvolved party, such as a federal/state regulator, can quickly and thoroughly understand the entire life cycle of a given cybersecurity incident?

7. The evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

**Our read:** The IRP is a living document that must be regularly updated—no less than annually—to account for the evolving threat, liability and regulatory landscape, as well as organizational changes.

- Has the IRP program and associated documentation been structured to ensure that important changes within the organization and the cyber threat/remediation landscape are promptly identified and associated updates applied to the IRP on a regular basis?

## Best Practices for Creating a Plan

**Build a team.** In practical terms, creating an IRP begins with building an internal incident response team that may include representatives from the following departments or areas:

- executive management
- compliance
- legal
- privacy and insurance risk management
- finance and auditing
- human resources and customer service
- information technology and information security
- marketing and public relations



Depending on the breach scenario, it should also include an external 'tiger team' of experts in the following areas:

- legal guidance
- computer forensics
- victim notification
- credit/ID monitoring services
- public relations

**Assign internal leadership.** Choose an internal Incident Response Manager to direct and manage the internal response team, and to act as liaison to senior management. Other members of the team have specific responsibilities to protect your company and customers, but all should report directly to the Incident Response Manager during an incident response.

**Assign external leadership.** At NetDiligence®, we've coined the term Breach Coach® for the cybersecurity legal counsel who typically acts as a first responder. The regulatory framework and growth in cyber insurance has driven the need for businesses of all sizes to engage experienced outside counsel to help drive and coordinate the increasingly complicated process of responding to a breach.

**Outline actionable steps.** A good IRP needs to be actionable and very granular, going step by step through the data breach response process in order of priority, to ensure that the response is compliant with state, federal and international laws.

**Keep it accessible.** To facilitate urgent action, the plan should include an abbreviated checklist of action steps and contact information for all internal and external team members. The document itself should be concise and accessible 24/7. A 100-page plan that sits on a shelf will be difficult to use, especially if the breach occurs on a Saturday night.

**Review and revise.** Before putting a plan into place, it must be reviewed by a Breach Coach lawyer or other first responder, to ensure that it actually meets the requirements of relevant state and federal laws and regulations. Since the Breach Coach will be there to coordinate the response with external partners and the insurance carrier's claims department, his/her input is crucial for success.

**Test and update.** Once the plan is created, it must be tested. Tabletop exercises are an important component of cyber risk planning and security training. They allow your organization to walk through a data breach event before it happens. Typically, the exercise is facilitated annually by an outside vendor such as a Breach Coach or forensics expert, who leads the internal Incident Response Team through IRP procedures in real time. This exercise makes sure your staff is fully apprised of the data breach response process. Plans should be reviewed and updated frequently.

## An IRP Tool to Count On

Our Breach Plan Connect® portal, developed in close concert with Breach Coach lawyers, helps organizations build and securely store their IRPs. A "Build Your Plan" tool guides users as they easily create tailored plans for their organizations. The tool walks them through the process step by step, helping them identify their teams, engage experts, and establish protocols and procedures for incident response. For ease of use during a live event, key response procedures are presented in a user-friendly checklist format.

The time and effort normally required to build an IRP can be reduced from months to days. Our mobile-friendly platform with secure hosting means that your IRP can be accessed from any device, anywhere in the world, at any time. For more information, please visit us at [BreachPlanConnect.com](https://BreachPlanConnect.com).

## About NetDiligence®

NetDiligence® specializes in Cyber Risk Readiness & Response services. With more than 15 years of experience in cyber, NetDiligence is an award-winning provider of innovative cyber risk management software and services to the insurance industry, including [QuietAudit®](#), [Cyber Risk Assessments](#), the [eRiskHub®](#) cyber risk management portal, and [Breach Plan Connect®](#) software-as-a-service (SaaS) that helps companies develop an effective data breach response plan. NetDiligence publishes an annual [Cyber Claims Study](#) and hosts annual [Cyber Conferences](#) in Philadelphia, Santa Monica, Toronto, London and Bermuda. For more information, visit [NetDiligence.com](#).

## About Experian

Experian Data Breach Resolution, powered by the nation's largest credit reporting agency, is a leader in helping businesses plan for and mitigate consumer risk following data breach incidents. With more than a decade of experience, Experian Data Breach Resolution has successfully serviced some of the largest and highest-profile breaches in history. The group offers swift and effective incident management, notification, call center support, and reporting services while serving millions of affected consumers with proven credit and identity protection products. For more information, visit [experian.com/databreach](#) or call 866.751.1323.

