ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy ADVISORY ■

FEBRUARY 9, 2021

Managing a Cyber Crisis: 7 Practical Tips to Recover with Strength

by Kim Peretti and Kate Hanniford

Due in part to the COVID-19 disruption and fast-tracked adoption of digital solutions associated with a remote workforce, the continued proliferation of targeted ransomware attacks, and an unprecedented supply chain attack of a widely used IT performance management software, 2020 witnessed extraordinary activity in the cybersecurity arena. As companies confront the ever-evolving cyber threat landscape anew in 2021, Alston & Bird has outlined seven practical tips for incident response in 2021.

1. Act Swiftly and Be Nimble

Companies are expected to respond swiftly to cybersecurity incidents – they are often crisis events. A company subject to a cyber-attack should be ready to assemble its team and stand up its incident response structure immediately so that the response team can quickly begin executing its investigation, containment, and remediation strategies. Team participants—including third-party forensics, outside counsel, and communications—should be identified and known to key internal incident response participants in advance. All team members should understand and be prepared to respond within the expected timeframes.

Because "everyone has a plan until they get punched in the face," it is important to bear in mind that cybersecurity incidents can evolve until the threat is contained. Cybersecurity incidents require a company's incident response team and outside experts to be nimble and ready to adjust and retrench quickly, including the need to retain forensic assistance with varying specialties to mitigate evolving threats and investigate new developments.

2. Maximize the Privilege

Engage forensics, communications, and notifications providers under privilege. Although recent court decisions have cast doubt on a company's ability to withhold forensic reports as protected by attorney-client privilege and attorney work product doctrine under certain circumstances, much of the incident response process can still be protected from disclosure if particular steps are taken to establish and maintain applicable privileges and protections. For example: Once the privileged relationships have been established, carefully limit the scope, purpose, and audience of privileged reports and parse ordinary-course, business-related

security information related to the incident from investigative information necessary for legal analysis and conclusions so that technical security teams have the information necessary to fulfill their mandate without jeopardizing privileged information.

3. Enhance Security as You Go

Don't wait for the regulators (or plaintiffs). By implementing additional security measures tailored to the threat involved in an incident, a company can demonstrate it continually enhances security as appropriate to the evolving threat landscape.

Because data security incidents are a matter of "when" and not "if," companies are judged by the quality of their incident response. One measure of this is the relative speed that a company can remediate the current incident and then withstand "second wave" threats. The ability to defend against attempted cybersecurity attacks that may result from an initial incident can be bolstered when a company accelerates security enhancements already in progress and implements additional measures designed to specifically address the threat vectors exploited in the incident. This proactive improvement of current state security will also better position the company to withstand any collateral regulatory scrutiny.

4. Control the Narrative

Share information with key external stakeholders only once you have a high degree of confidence in its accuracy and completeness. By timing disclosures until the company is ready to provide accurate and largely complete information, the company may build credibility and avoid setting expectations for continuous updates or, even worse, corrective statements. In addition, an increasing number of external partners (regulators, auditors, business partners, cloud vendors, affected customers) expect and may need information related your company's data security incident, so anticipating external communications, and ensuring they are consistent, is a key part of managing incident response in today's environment.

Depending on the regulatory risks involved, among other factors, consider whether and when to approach law enforcement and regulators, as appropriate, before the formal notifications process.

5. Coordinate with Your Business Partners

Rare is the data security incident that does not involve a business partner's data or network. Incident response typically requires interaction with business partners—either as a practical matter or by virtue of contractual agreement. Increased coordination of response efforts to investigate, remediate, and fulfill regulatory and individual notification obligations typically contributes to a more efficient resolution of the incident.

6. Know Your Obligations and Reserve Your Rights

Understand the company's material agreements, both in terms of what obligations it may have to others and what obligations others may owe to it. Preserve any contractual rights for redress, such as indemnification, with impacted business partners as you coordinate efforts to respond to the incident. Once the incident has been contained and remediated, and any obligations to notify regulators and individuals have been completed, your focus can shift to contractual liability.

7. Test Your Plan Ahead of Time

Confirm your incident response team is prepared and ready to respond by testing your incident response plan. This includes training all employees to recognize and report suspicious activity immediately so that it can be promptly investigated and appropriately escalated according to the company's stated incident response plan.

Given the prevalence of ransomware and unique timing considerations involved in responding to and recovering from this type of incident, consider including a standalone playbook to guide the response to ransomware events. Know your position on ransomware payment, and the outside experts whose assistance you may need, depending on the circumstances.

As cross-border incidents become more common, consider whether your incident response plan accounts for the differing reporting timelines and other considerations (e.g., legal thresholds) that may apply to the data at risk in the incident.

We understand the unprecedented challenges faced by many companies, including the need to defend against increasingly sophisticated and aggressive cybersecurity threats. Although each incident is unique, we have found that this approach minimizes risks to the company and maximizes its opportunities for a favorable outcome among its various stakeholders while still complying with applicable law.

You can subscribe to future ***Privacy, Cyber & Data Strategy*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Katherine Doty Hanniford
202.239.3725
kate.hanniford@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: 3700 Hulen Street ■ Building 3 ■ Suite 150 ■ Fort Worth, Texas, USA, 76107 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 5th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333