AN A.S. PRATT PUBLICATION
FEBRUARY-MARCH 2018
VOL. 4 • NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis®

Pratt's Privacy & Cybersecurity Law Report

VOLUME 4 | NUMBER 2 | FEBRUARY-MARCH 2018

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number .... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [37] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [4] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2018–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Preparation and Practice: Keys to Responding to a Cybersecurity Incident

By Caleb Skeath*

Despite constant advances in available cybersecurity measures, there is no such thing as perfect security, and companies must be prepared to respond to a significant cybersecurity incident at a moment's notice. This article describes some key steps companies can take to respond to a cybersecurity incident in a swift, efficient, and effective manner.

In the immediate aftermath of discovering a cybersecurity incident, companies often face many questions and few answers amidst a frenzy of activity. What happened? What should we do now? What legal risks does the company face, and how should it protect against them? In this fast-paced environment, it can be difficult to coordinate the activity across an incident response. Well-intentioned actions by incident responders can easily expose the company to liability, regulator scrutiny, or a waiver of applicable legal privileges.

Instead of waiting to make critical incident response decisions in the "fog of war" that often occurs during the fast-paced events following the detection of a cybersecurity incident, organizations should think about how to respond before a cybersecurity incident actually occurs. Responding to a cyberattack can involve a wide variety of different stakeholders such as IT and information security personnel, forensic analysts and investigators, legal counsel, communications advisors, and others. Advance planning, including the development and execution of an incident response plan, allows a company to coordinate activities across a diverse array of different incident response work streams, and test that coordination. This article describes some key steps companies can take to respond to a cybersecurity incident in a swift, efficient, and effective manner.

FOLLOW A PLAN

Implementing a cybersecurity incident response plan is a key foundational element of an efficient and effective incident response. Instead of figuring things out as you go into the frenetic aftermath of a cybersecurity incident, an incident response plan will identify individuals to respond to the incident, these individuals' roles and responsibilities, and a framework to coordinate and guide the overall incident response effort. Consider consulting best practices and standards for incident response, such as the

* Caleb Skeath is an associate at Covington & Burling LLP advising clients on a range of cybersecurity and privacy issues, including cybersecurity incident response, cybersecurity and privacy compliance obligations, internal investigations, regulatory inquiries, and defending against class-action litigation. He may be reached at cskeath@cov.com.

NIST Computer Security Incident Handling Guide,[1] in developing an incident response plan. Large organizations should also consider developing an enterprise-wide incident response plan with narrower, more detailed playbooks for different divisions or business lines within the organization to describe each division's incident response processes in greater detail.

Periodic trainings and simulations can also enhance incident response team members' familiarity with the plan and identify weaknesses in the plan that can be addressed before an incident occurs. When an incident occurs, prior training allows incident responders to execute based on their training without spending time to understand the incident response plan and the necessary steps to respond.

ASSESS THE INCIDENT

In the immediate aftermath of the incident, focus on immediately assessing the incident and its impact on the company based on available information. To improve the speed and efficiency of response, take time prior to the incident to consider what questions may need to be answered in the immediate aftermath of the incident. These questions might include what parts of the business have been impacted by the incident, whether the incident is ongoing, and whether the incident impacted regulated data, regulated systems, or a company's "crown jewels" such as trade secrets or intellectual property.

After identifying the questions that should be answered, consider developing a playbook for the Security Operations Center or other cybersecurity first responders to identify questions to answer or data to gather in the immediate aftermath of a cybersecurity incident. This playbook could include a standardized incident form to collect necessary information and provide it to decision-makers in the immediate aftermath of the incident, as well as defined escalation paths to report a cybersecurity incident and kick off the incident response process.

CONTAIN THE INCIDENT

After detecting an incident and assessing what has occurred, consider whether to take immediate steps to contain a cybersecurity incident and prevent its spread within the environment. These steps may include isolating certain sensitive systems or data as well as rolling out security measures to detect and prevent additional incident-related activity. For example, in responding to a ransomware incident, a company may need to shut down or isolate parts of its network to prevent the malware from spreading. Consider, document, and rehearse what steps may be required to implement rapid

[1] NIST SP 800-61.

containment measures in the immediate aftermath of common cybersecurity incidents, such as phishing, DDoS, or ransomware attacks.

However, taking immediate action to contain an incident may not be appropriate in all circumstances. If the assessment of the incident determines that an adversary is active within your network environment, consider whether containment actions could alert the adversary to the fact that you have discovered the incident. Once discovered, a sophisticated adversary may take additional malicious actions in response, including removing data from your network, destroying systems, or changing his or her tactics, techniques, or procedures to avoid further detection.

Consider consulting with forensic investigation and incident response experts to assess whether to take immediate containment actions or develop a more comprehensive containment and eradication plan that, once executed, will expel the adversary from your network and prevent the adversary from maintaining or re-establishing any presence within it.

Additionally, ensure that these containment steps are weighed against other potential impact (e.g., critical system outages or functionality) and do not destroy relevant information or evidence that the company could utilize to investigate the incident or is under a legal duty to preserve. If log data automatically rolls off after a certain time period, consider pausing or suspending the deletion of key data sources the company might need for future investigations or legal proceedings.

PROTECT THE PRIVILEGE

Cybersecurity incidents can not only create legal risk, but can also create documentation that companies should protect under applicable legal privileges. Consider planning how to handle internal and external communications in order to maximize available protections under the attorney-client communication and attorney work product privileges. As an initial step, plan to consult with legal counsel in the immediate aftermath of the incident to protect incident response and investigation efforts under privilege. Legal counsel should ensure that documents are properly labelled and counsel is involved in meetings and communications in order to protect the privilege.

In addition, ensure that all incident responders are aware of the privileged nature of the response and investigation and receive training on how to protect the privilege. To reduce the risk that privilege concerns may slow down incident response efforts, consider training incident response personnel on privilege considerations in advance so protecting the privilege becomes a reflexive part of the incident response process. Also, consider how to protect applicable privileges when engaging with external third parties, such as forensic vendors, law enforcement authorities, or regulators. Such measures may include funneling all communications through legal counsel or another point of contact to ensure consistent, factually accurate communications that do not waive the privilege.

BRING IN HELP

Many companies may not have the in-house bandwidth or expertise to respond to and investigate a major cybersecurity incident. To close this gap, companies often choose to bring in external assistance from forensic investigators, cybersecurity vendors, or communications consultants, as well as other third parties. In doing so, however, companies must take appropriate steps to protect the privileged nature of the incident response and investigation. Include appropriate privilege language in the contract with the vendor to document that the company's legal counsel has retained the vendor on behalf of the company to assist in providing legal advice regarding the cybersecurity incident. In addition, consider establishing a pre-existing relationship with a vendor, including execution of privileged contractual documentation, in advance of a cybersecurity incident in order to get the vendor "on the ground" faster once an incident occurs. A pre-established relationship can also allow a vendor to familiarize itself with the company's IT environment and increase the speed and efficiency of its assistance in the event of an incident.

COORDINATE AND COMMUNICATE

A large cybersecurity incident will impact numerous stakeholders both inside and outside of the company. In addition to the need to engage IT and information security personnel to recover from the incident and forensic personnel to investigate it, the company may have to involve its executive leadership, legal counsel, communications personnel, and other stakeholders in the course of its incident response efforts. Without coordination and communication between different work streams, different stakeholders may duplicate efforts and spread inaccurate information. For example, following an incident, executive leadership may need certain information to make key business decisions, while other parts of the company need different types of information to communicate with employees or customers, respond to regulators, or pursue insurance claims under cybersecurity insurance policies. By establishing and rehearsing an incident response plan, a company can define clear lines of communication and coordination between different work streams across the enterprise that allow stakeholders to receive accurate and useful information when they need it.

Despite constant advances in available cybersecurity measures, there is no such thing as perfect security, and companies must be prepared to respond to a significant cybersecurity incident at a moment's notice. To enhance the speed and efficiency of its response after a cybersecurity incident, a company should consider beforehand how it wants to respond. Relatively small investments in planning, preparation, and training can pay off significantly in the immediate aftermath of a cybersecurity incident.