AN A.S. PRATT PUBLICATION
AUGUST/SEPTEMBER 2015
VOL. 1 • NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 1 **NUMBER 1** **AUGUST/SEPTEMBER 2015**

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) 487-3000
Fax Number .... (518) 487-3584
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 ..... (518) 487-3000

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);
David Kalat, *Day One: The Origin Story of Computer Forensics*, [1] 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

(2015–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

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.

Department of Justice Issues Guidance on Best Practices for Cybersecurity Preparedness

By A.J. Kess, Yafit Cohn, and Linda M. Nyberg*

The authors of this article explain the Department of Justice's first published guidance on cybersecurity, titled "Best Practices for Victim Response and Reporting of Cyber Incidents."

The newly-formed Cybersecurity Unit of the Criminal Division of the Department of Justice ("DOJ") issued guidance on best practices for organizations to protect against and respond to data breaches and other cybersecurity risks.[1] As announced by Assistant Attorney General Leslie R. Caldwell at an inaugural invitation-only industry round-table in Washington, D.C., that day, the publication will be a living document updated over time as part of the DOJ's efforts to "elevate cybersecurity efforts" and "build better channels of communication with law enforcement."[2]

The publication, titled "Best Practices for Victim Response and Reporting of Cyber Incidents," is the DOJ's first published guidance on cybersecurity. While it was drafted with smaller organizations in mind, its lessons apply to companies of all sizes. The bulk of the DOJ's guidance focuses on developing an appropriate incident response plan and executing that plan when a data breach or other cybersecurity incident occurs.[3] The DOJ also gives helpful tips on what *not* to do following a breach and exhorts companies to remain vigilant after an attack to prevent similar occurrences in the future.

---

* A.J. Kess is a partner at Simpson Thacher & Bartlett LLP, where he is head of the Public Company Advisory Practice. Yafit Cohn and Linda M. Nyberg are associates at the firm. The authors may be reached at akess@stblaw.com, yafit.cohn@stblaw.com, and linda.nyberg@stblaw.com, respectively.

[1] *See* Cybersecurity Unit, Computer Crime & Intellectual Property Section, Criminal Division, U.S. Dept. of Justice, *Best Practices for Victim Response and Reporting of Cyber Incidents*, http://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf (April 2015). The Cybersecurity Unit was formed in December 2014 "to serve as a central hub for expert advice and legal guidance regarding how the criminal electronic surveillance and computer fraud and abuse statutes impact cybersecurity." *See* http://www.justice.gov/criminal/cybercrime/about/cybersecurity-unit.html (accessed May 8, 2015).

[2] Office of Public Affairs, U.S. Dept. of Justice, *Assistant Attorney General Leslie R. Caldwell Delivers Remarks at the Criminal Division's Cybersecurity Industry Roundtable*, http://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-criminal-divisions (April 29, 2015).

[3] As explained in the Verizon 2015 Data Breach Investigations Report, a cybersecurity incident is "any event that compromises the confidentiality, integrity, or availability of an information asset," while a "data breach" is "any incident that resulted in confirmed disclosure (not just exposure) to an unauthorized party." *See* http://www.verizonenterprise.com/DBIR/2015/.

WHAT TO DO BEFORE A BREACH OCCURS

The DOJ advises organizations to develop an incident response plan now, *before* a cybersecurity incident occurs. Citing the "excellent guidance" of the Cybersecurity Framework published by the National Institute of Standards and Technology,[4] the DOJ recommends that an organization:

- Identify its "crown jewels"—its data, assets or services that merit the most protection;
- Develop, test, and keep up-to-date an *actionable* incident response plan that describes specific, concrete steps the organization will take in response to a cybersecurity incident or data breach;
- Have in place (or keep readily available) the technology and tools necessary to respond to a cybersecurity incident, including data back-ups, intrusion detection capabilities and data loss prevention and filtering services;
- Monitor systems communications after obtaining users' prior consent, such as through network warnings, workplace policies or other written acknowledgements;
- Ensure it has legal counsel on hand that is well-acquainted with technology and knowledgeable about relevant privacy and cybersecurity laws;
- Maintain proper personnel and information technology ("IT") policies to minimize the risk of "insider threats";
- Establish a point-of-contact at a local federal law enforcement office, such as a Federal Bureau of Investigation ("FBI") field office; and
- Form relationships with applicable cyber information sharing organizations, such as the Information Sharing and Analysis Centers for companies engaged in sectors of critical infrastructure.

HOW TO RESPOND TO A BREACH: PUTTING THE INCIDENT RESPONSE PLAN INTO ACTION

As detailed in the DOJ's publication, an effective incident response plan not only lays out the procedures for managing a breach, but also provides how the organization will continue to operate while responding to such breach. Once an intrusion occurs, the victim organization should:

- Assess the nature of the incident and determine whether it is a malicious act or simply a system glitch;
- Take steps to minimize ongoing damage, such as by rerouting and/or blocking network traffic and isolating some or all of the compromised network;

---

[4] *See* National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (February 12, 2014).

- Collect information and evidence regarding the cybersecurity incident, including making an exact copy (or "forensic image") of the affected hard disk, preserving logs of network activity, recording ongoing malicious activity and keeping detailed records of all response measures taken by the organization; and
- Notify:
  - relevant internal personnel, including senior management, IT personnel, public affairs officers and counsel;
  - law enforcement, including the FBI, Secret Service and/or the Department of Homeland Security, if criminal activity is suspected;
  - customers, in accordance with state data breach notification laws; and
  - other potential victims, such as another company whose data was also stored on the compromised network.

WHAT *NOT* TO DO AFTER A BREACH

The DOJ counsels organizations to avoid using the compromised security network as much as possible. If an organization must use the system, the DOJ suggests that it encrypt its communications. Finally, the victim organization should not respond to a data breach in kind by attempting to access or damage another system it suspects was involved the cyber attack.

STAY VIGILANT AFTER A BREACH

Lastly, the DOJ's guidance urges organizations to continue monitoring their computer systems for anomalous activity even after a cybersecurity incident seems to be under control. In addition, the DOJ recommends that a victim organization conduct a post-incident review of its response to the incident, and address any deficiencies the incident uncovered.

CONCLUSION

As Attorney General Loretta Lynch remarked at the roundtable, the government and private industry have "a mutual and compelling interest in developing comprehensive strategies for confronting this threat [of theft of consumer information and valuable intellectual property,] and it is imperative that our strategies evolve along with those of the hackers searching for new areas of weakness."[5] The DOJ's guidance confirms that one of the first steps in addressing these challenges is developing, maintaining, and

[5] Office of Public Affairs, U.S. Dept. of Justice, *Attorney General Loretta E. Lynch Delivers Remarks at the Criminal Division's Cybersecurity Industry Roundtable*, http://www.justice.gov/opa/speech/attorney-general-loretta-e-lynch-delivers-remarks-criminal-division-cybersecurity (April 29, 2015).

testing an incident response plan that will allow organizations to appropriately respond—and evolve—in line with cybersecurity threats. Moreover, an incident response plan enables an organization to respond to a potential data breach quickly, efficiently, and calmly and could mitigate the impact of a breach on the company's business, including its legal exposure and reputation.