AN A.S. PRATT PUBLICATION
MAY 2024
VOL. 10 NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 10 **NUMBER 4** **May 2024**

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
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
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) 487-3385

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*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (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

(2024–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, 631.291.5541. 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.

Cybersecurity Insurance: Practical Steps Businesses Can Take to Become More Insurable

By Kathryn T. Allen, Kelsey L. Brandes and Scott M. Tobin*

In this article, the authors discuss steps that companies can take to make themselves more attractive to cyber insurers and to improve their security posture.

With the global average cost of a data breach now $4.45 million, a 15% increase over the past three years,[1] it is not a surprise that businesses have shown an increased interest in cybersecurity insurance amid frequent news of computer hacking, network intrusions, data theft and high-profile ransomware attacks.

At the same time, there is a range of insurance policies that may cover aspects of cybersecurity incidents and crime, like stand-alone cyber policies, errors and omissions policies, commercial general liability, directors and officers / management liability, commercial crime coverage, media liability, network security and privacy policies, and other blended products.

However, insurers have started writing exclusions for cyber and privacy liabilities into "non-cyber" policies and directing policyholders to buy cyber insurance specifically for those risks. Thus, it is more important than ever for businesses to have a clear understanding of whether their current policies cover cyber incidents and, if so, to what extent. And if not, what can your organization can do as a company to make it more attractive to insurers?

PRACTICAL INTERNAL STEPS

Security Awareness Training

We have all heard that employees are your company's greatest risk point. But with regular, documented training sessions, you can reduce this risk by educating and empowering your employees to prevent and detect common cyber threats. This also promotes a "security-aware mindset" that can have ancillary benefits. Many insurers partner with cyber-training firms and may offer them to your company at no cost. The key to success with these trainings is to be frequent and consistent.

---

* The authors, attorneys with Polsinelli PC, may be contacted at kallen@polsinelli.com, kbrandes@polsinelli.com and scott.tobin@polsinelli.com, respectively.

[1] https://www.ibm.com/reports/data-breach.

Conduct Full Data Backups

You will not have to pay money to a cybercriminal if you have another copy of the data it is holding for ransom. The goal of regular data backups is to allow businesses to continue operating even if data is compromised. Regularly backing up all of your business data, whether it is on-premises or in the cloud, is the ultimate safety net.

Automate Passwords/Use MFA

Because most cybercriminals depend on stolen user credentials to access a private network, automated passwords and use of multifactor authentication (MFA) could disrupt a majority of network compromise attempts. Microsoft has even gone so far as to say it would prevent 99.9% of them![2] MFA is the process of using at least two pieces of evidence to confirm a user is who she is supposed to be (usually a password plus a one-time password or code sent to the user's phone or email).

Additionally, employ a password manager to help keep track of multiple passwords and generate new passwords at random. This cuts down on employees using the same passwords for multiple platforms or writing those passwords down.

Establish a Vendor Management Process

The greatest data privacy threat companies actually faced in 2023 was their upstream and downstream vendors, with 63% of all data breaches being tied to or directly caused by vendors. Many companies rely on their procurement department to gather information and negotiate with vendors. This may be fine outside of the cyber context, but when it comes to information technology (IT), software and other vendors that have cloud-based or "connected" solutions, additional vetting and contracting processes must be employed to properly assess and mitigate the risks your vendors pose to you.

PRACTICAL EXTERNAL STEPS

Conduct Penetration Testing and System Audits

It is important to test your company's systems, network and technical infrastructure so you find the vulnerabilities before a cybercriminal does. Often, companies that can show regular system scans and audits done by a reputable third party enjoy a break in their cyber premiums. Penetration testing is an authorized, simulated attack on your IT systems. It should be designed to mimic the techniques a cybercriminal would use to determine the efficacy of your company's security controls.

Consult a Managed Service Provider

Utilizing a third-party security professional, or managed service provider (MSP), to help your company better plan, monitor and secure its digital environment is an

[2] https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/.

excellent way to bolster your protections. MSPs can offer 24/7 system monitoring and proactive threat detection as well as compliance management. An MSP may identify a blind spot your company did not have on its radar. And as there is a crowded market for these services, they can often be the same price or less expensive than having a captive team of employees doing all of these tasks.

Draft an Incident Response Plan

No Incident Response Plan (IRP) can guarantee the prevention of a data breach, but a well-drafted and well-rehearsed IRP can significantly minimize the impact a cyber incident has on your company. IRPs outline company procedures to follow and individual roles to engage in the event of an incident. Organizations with comprehensive IRPs had approximately $2.66 million less in damages and costs than those that did not have an IRP in place.[3] Companies that have an IRP should review it annually. Tabletop cyber exercises bring all of the key players into the same room and have them act out what their roles and responsibilities would be if an incident were to take place. Some insurers will offer their clients a facilitator who can guide the company through this exercise. Other professional organizations should be present as well, including any MSP you have engaged and your trusted law firm partner.

With cyber insurance premiums going up and policy limits going down, as well as a consolidation of cyber insurance providers in the market, insurers want to see that their clients are engaging in industry-standard preventive measures.

CONCLUSION

Taking advantage of these practical steps will not only make companies more attractive to insurers but also improve the security posture of the company in the process, which lowers the company's need to ever claim on that policy in the first place.

[3] https://www.ibm.com/reports/data-breach.