AN A.S. PRATT PUBLICATION
JULY-AUGUST 2019
VOL. 5 • NO. 6

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 NUMBER 6 JULY-AUGUST 2019

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*, [5] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [171] (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

(2019–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, 646.539.8300. 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 and Privacy Risks for Nonprofits: Navigating the Minefield

Matthew D. Dunn and Jeremy S. Steckel [*]

Given the increased threat of cyber-attacks, the ever-expanding privacy laws, the massive amount of personal data that nonprofits collect, and the costs of privacy violations and data breaches, nonprofits must be proactive in order to minimize risks and costs. The authors of this article discuss cyberthreats to nonprofits, security and privacy initiatives, and best practices.

If you thought that cyber-criminals were morally opposed to targeting charities, foundations, and other nonprofits, you would be very wrong. Such criminals do not discriminate. In fact, nonprofits are particularly vulnerable because they tend to collect and store sensitive financial and personal data (*e.g.*, information about donors, members, and program beneficiaries such as children, students, seniors, patients, and grantees), and may lack adequate information security teams and other resources that protect large companies. These vulnerabilities, along with nonprofits' strong online presence and the rise in online donations, make them an ideal target for cyber-attacks.

Yet nonprofits continue to lag behind for-profit entities in their data security efforts and preparations. According to a recent survey of more than 250 nonprofit organizations, approximately 40 percent of those nonprofits did not have policies to guide the handling of cybersecurity risk, technology use, and data privacy, and almost 60 percent provided no cybersecurity training for their personnel.[1]

In addition to cybersecurity, nonprofits also must stay informed about the ever-expanding patchwork of data privacy laws, including the European Union's Global Data Protection Regulation ("GDPR") and U.S. data-breach notification laws.

Make no mistake—cybersecurity and privacy are Board-level concerns. Directors and officers owe fiduciary duties to the nonprofit organizations they manage. This does not mean that every Board member must become a cybersecurity and privacy expert. A Board may manage the corporation's business and affairs directly, or designate a committee or other group to do so under the Board's direction. In general, a member of the Board or committee will be protected in relying in good faith upon information provided by persons with professional or expert competence who are selected with reasonable care.

---

[*] Matthew D. Dunn is a partner at Carter Ledyard & Milburn LLP representing clients in complex litigation matters. Jeremy S. Steckel is an associate at the firm counseling tax-exempt organizations on corporate and compliance matters. The authors may be reached at mdunn@clm.com and steckel@clm.com, respectively.

[1] *See* Robert Hulfshof-Schmidt, STATE OF NONPROFIT CYBERSECURITY, NOVEMBER, 2018, https://www.nten.org/wp-content/uploads/2018/11/Cybersecurityreport2018NTEN.pdf.

Although there is limited case law addressing nonprofit directors' and officers' fiduciary duties in the context of cybersecurity and privacy laws, there are a few guiding principles we can glean from the wealth of case law addressing fiduciary duties in other contexts. As a general rule, Board members should attempt in good faith to ensure that systems and controls are in place to manage cybersecurity risks and comply with privacy laws, and that those systems are adequate. The Board should remain reasonably informed of all material information reasonably available to it at the time of significant decisions about cybersecurity and privacy, and the Board cannot ignore "red flags."

The remainder of this article describes some common cyber threats and provides an overview of privacy and data-breach laws, and the Appendix offers some recommended best practices.

COMMON TYPES OF CYBER THREATS AND RISKS

The following are a few of the more common types of cybersecurity attacks affecting nonprofits:

Malware Attacks

Malware attacks involve the use of malware (malicious software) to infect a victim's computer system in order to disable the system, prevent user access, or steal sensitive or valuable data. It is often concealed in an email attachment, link, pop-up, or webpage. When the link or pop-up is opened, malware can spread. For example, in November 2018, Make-A-Wish Foundation's international website was the subject of a crypto-mining malware attack, which then affected all users that visited the infected webpage and allowed the attackers to generate cryptocurrency from the users. The attackers exploited the charity's website, likely because of the high number of users accessing the site during the holidays. The attack severely compromised the charity's website operations and fundraising.[2]

Ransom Malware

Ransom malware, or ransomware, is a type of malware attack in which the hacker prevents users from accessing their system or data, or threatens disclosure of data, until or unless a ransom payment is made, often in the form of cryptocurrency such as Bitcoin.

- In January 2017, a small cancer-related charity in Indiana was the victim of a malware attack which wiped its servers of information pertaining to operations,

[2] *See* Shaun Nichols, *Scumbags cram Make-A-Wish website with coin-mining malware,* THE REGISTER (Nov. 19, 2018), https://www.theregister.co.uk/2018/11/19/makeawish_coinmining_malware/.

grant documents, donor names and contact information, and some employee social security numbers. The hacker threatened to release the data on the dark web and demanded a ransom of 50 Bitcoins, then valued at about $43,000, later reduced to about $12,000, for the return of the data. The charity refused to pay the ransom, but reportedly spent months rebuilding its data.[3]

- In February 2016, a Los Angeles nonprofit hospital suffered a ransomware attack and reportedly paid a ransom of 40 Bitcoins (then approximately $17,000) in order to access critical medical records that were rendered inaccessible by the attack.[4]
- In May 2017, the global ransomware known as WannaCry struck the UK's National Health Services ("NHS"), shutting down the computer systems and demanding Bitcoin ransom. According to a government report, no ransom was paid but the attack caused more than 19,000 medical appointments to be cancelled and cost the NHS over £90 million to restore data and upgrade its computer systems.[5]

Denial of Service Attacks

Denial of Service ("DoS") attacks disrupt web services by flooding web servers with traffic in order to prevent access to a company's website. A Distributed Denial of Service Attack ("DDoS") is accomplished using multiple computers. These attacks can be easily engineered from nearly any location, and finding those responsible can be extremely difficult. For example, in May 2018, a DDoS attack struck a crowdfunding website operated by an Irish group lobbying for removal of the constitutional ban on abortion, which caused the site to be shut down during a peak time for donations in advance of the national referendum vote.[6]

Password Attacks

Password attacks use software or programs to learn a user's password and then access sensitive or financial data.

---

[3] *See* Sarah Murray, *Charities unprepared for cyber attack risk,* Financial Times (Nov. 8, 2017), https://www.ft.com/content/1c9ad7a0-996c-11e7-8c5c-c8d8fa6961bb.

[4] *See* Michelle Lemming, *Nonprofit Cybersecurity: Hospital Pays Ransom to Hackers,* Nonprofit Quarterly (NPQ) (Feb. 23, 2016), https://nonprofitquarterly.org/2016/02/23/nonprofit-cybersecurity-hospital-pays-ransom-to-hackers/.

[5] *See* Matthew Field, *WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled,* The Telegraph (Oct. 11, 2018), https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/.

[6] *See* Ellen Tannam, *DDoS attack hits Eighth Amendment referendum crowdfunding website,* Silicon Republic (May 10, 2018), https://www.siliconrepublic.com/enterprise/referendum-ddos-attack-ireland.

Phishing Attack

In a phishing attack, a scammer typically obtains personal or financial information through trickery or false pretenses, such as impersonating a supervisor, financial institution, supplier, vendor or other person or entity. The attacker may mimic a charity's brand to dupe donors into clicking a fake link to donate, thereby providing their financial information to criminals.

- In August 2017, after Hurricane Harvey, the U.S. Department of Homeland Security warned of scammers using email to send bogus links that promised to let users help victims; instead, the links led to fake websites soliciting credit card and personal information.[7]
- In April 2019, a Massachusetts nonprofit hospital reported that it was the victim of a phishing incident which resulted in the unauthorized access to email accounts of several employees and exposed information of about 12,000 patients.[8]

Spoofing Attacks

Spoofing attacks similarly involve impersonation of a trusted sender in which the impersonator asks the user to perform a specific action, such as transferring money or providing the impersonator with access credentials.

Many of these attacks, particularly phishing and spoofing attacks, are caused by, or can be linked directly to, human error. Nonprofits should train directors, officers, employees and, where appropriate, volunteers, on the types of prevalent cyber threats, typical red flags, and the organization's cybersecurity policies and procedures.

PRIVACY RISKS AND REGULATIONS

Nonprofits must stay informed about the ever-evolving patchwork of privacy laws. Following the enactment of the GDPR in 2018, and sweeping proposals for similar legislation in several U.S. states, privacy will remain an area of focus for all companies, including nonprofits, for the foreseeable future.

The GDPR, which took effect in May 2018, applies to all entities throughout the world, including nonprofits, which do business with persons who are in the EU, regardless of such persons' nationality or place of residence, or which directly

[7] *See* U.S. Department of Homeland Security, U.S. Computer Emergency Readiness Team (US-CERT), *Potential Hurricane Harvey Phishing Scams* (Aug. 28, 2017), https://www.us-cert.gov/ncas/current-activity/2017/08/28/Potential-Hurricane-Harvey-Phishing-Scams.

[8] *See Hospital says patient info exposed after phishing incident,* BOSTON.COM (Apr. 8, 2019), https://www.boston.com/news/local-news/2019/04/08/hospital-says-patient-info-exposed-after-phishing-incident.

or indirectly possess, collect, or otherwise process personal data of such persons (the GDPR refers to such entities as "data controllers" or "data processors"). "Personal data" is broadly defined to mean any information directly or indirectly relating to an identified or identifiable natural person, such as a name, an ID number, location data, online identifiers (*e.g.*, IP and email addresses and cookie identifiers), or banking information.

Data controllers must minimize data collection and processing to only what is necessary, ensure appropriate security of data, keep accurate records of all processing of applicable data, and provide such records upon request. Lawful processing of personal data requires that organizations obtain consent of the data subject (the EU person) or have another authorized legal basis for processing. Consent must be explicit as opposed to implied, and must be "freely given." In addition, data controllers must disclose to data subjects what data they collect, how it is stored and the purposes for which it is used, as well as the data subjects' right to request access to their data, to withdraw consent, and to lodge a complaint with an EU state's supervisory authority. Data controllers are required to report breach incidents under certain circumstances, and the penalties for GDPR violations can be severe.

U.S. states, as well as the District of Columbia, have statutes requiring private entities, including nonprofits, to report security breaches involving personally identifiable information and notify affected individuals. State breach laws typically contain provisions regarding who must comply with the law, definitions of applicable personal information, what constitutes a breach, notice and reporting requirements, and exemptions.

Though not applicable to nonprofits at this point, the State of California recently passed the California Consumer Privacy Act of 2018 ("CCPA"), an expansive and landmark consumer privacy law which becomes operative on January 1, 2020. The State of Washington recently proposed its own sweeping privacy legislation, which, in its current draft form, would apply to nonprofits that meet certain criteria. Other states are starting to follow suit.

Meanwhile, consumer advocates have been joined by legislators and even technology industry leaders in insisting on some form of unified federal consumer privacy regime and accompanying regulatory framework to streamline compliance.

CONCLUSION

Given the increased threat of cyber-attacks, the ever-expanding privacy laws, the massive amount of personal data that nonprofits collect, and the costs of privacy violations and data breaches (financial, legal, reputational and otherwise), nonprofits must be proactive in order to minimize those risks and costs. Nonprofits are encouraged to consult counsel regarding the best practices listed in the Appendix to this article and other security and privacy initiatives.

APPENDIX

Cybersecurity and Privacy—Recommended Best Practices for Nonprofits

1. *Appoint a CISO.* Appoint a Chief Information Security Officer or the equivalent.
2. *Build Compliance into Governance Structure*. Make sure it is clear whether the Board will manage cybersecurity and privacy compliance itself or will delegate this to a committee under the Board's supervision. If the latter, include a section about cybersecurity and privacy in the committee's charter, and require the committee to update the Board periodically.
3. *Conduct Organizational Risk Assessment*.

    - Identify the types of information maintained by the organization that may be prone to cybersecurity attacks and data breaches, and determine whether such information is protected by the GDPR or other privacy laws. Identify how and where such data is stored, and whether there are adequate security safeguards in place.
    - Conduct a technical vulnerability assessment, identifying weaknesses and risks associated with computer systems and websites.
    - Assess the organization's existing cybersecurity and privacy policies or protections.
    - Conduct a risk assessment of third party vendors or professionals that have access to the organization's data (*e.g.*, fundraising counsel, online fundraising platforms, production/mailing services, caging, list management or brokers), and ask about their cybersecurity and privacy policies and programs.

4. *Understand Legal Obligations.* Evaluate which U.S. and foreign laws apply to the organization, and understand the organization's obligations under such laws. Adopt/update cybersecurity and privacy policies and programs to reflect such requirements.
5. *Understand and Comply with the GDPR, if applicable.*

    - Adopt or update GDPR-compliant privacy or data protection policies.
    - Ensure that privacy policies disclose to data subjects the data collected, how it is stored, and the purposes for which it is used, as well as the data subjects' right to request access to the data, to withdraw consent, and to lodge a complaint with an EU state's supervisory authority.

- Consider posting or providing a link to the privacy policy on the organization's website and, if cookies are used to collect data on users, including a pop-up consent banner.

6. *Improve Data Storage and Security.* Minimize the personal data that is collected and stored and the locations where such data is stored, and ensure that there are adequate physical and online security measures in place. Doors and offices should be locked after hours. Only authorized personnel should have access to computer systems.
7. *Train Personnel, Adopt Incident Response Plan, and Test Organizational Breach Response*.

    - Conduct training to ensure personnel understand cybersecurity and privacy policies and how to identify red flags associated with phishing, spoofing, and other cyber-attacks.
    - Maintain an "Incident Response Plan" detailing steps to take in the event of a breach and allocating responsibilities to certain personnel. Run simulation exercises to practice the incident response plan. Review and update the plan periodically.
    - Conduct penetration testing that simulates certain cyber-attacks and tests the security of IT systems. This is typically done by a consultant or vendor.

8. *Review Diligence of Third Party Vendors*. Ensure that third party vendors and professionals with access to the organization's data have cybersecurity and privacy policies that adequately protect such data. Include corresponding representations, warranties and indemnification provisions in third party contracts to protect the organization.
9. *Improve Network Security and Technology*. Consider implementing technology such as a network firewall, anti-virus and anti-malware software, encryption of data in transit and at rest, unique login and passwords for personnel access to network, complex password protection with passwords required to be changed regularly, and dual factor authentication for remote access to the network, among other similar measures.
10. *Consider Cloud-based Data Management*. For an organization with a small budget, consider moving to a reputable cloud-based data management platform, which effectively allows the organization to outsource certain aspects of data security to the platform provider.
11. *Assess Insurance Coverage*. Review existing insurance plans to determine whether and to what extent they cover cyber-attacks or data breaches.