AN A.S. PRATT PUBLICATION
JULY/AUGUST 2017
VOL. 3 • NO. 6

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 NUMBER 6 JULY/AUGUST 2017

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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [197] (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

(2017–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.

Pay Up . . . or Else? Ransomware is a Growing Threat to Higher Education – Part I

By Kimberly C. Metzger and Stephen E. Reynolds*

Ransomware attacks are becoming more frequent in higher education, and have serious implications regardless of the institution's size, scope, or geographic diversity. The authors of this two-part article address the questions: what exactly is ransomware, why is it targeting higher education, and how can your institution protect itself? This first part of the article explains what ransomware is, the rise and effect of ransomware, and how ransomware is impacting higher education. The second part of the article, which will appear in an upcoming issue of Pratt's Privacy & Cybersecurity Law Report, *discusses responding to a ransomware incident, preventing a ransomware attack, and information-sharing for better security.*

What do Los Angeles Valley College and the University of Calgary have in common with Hollywood Presbyterian Medical Center and the state prosecutor's office in Allegheny County, Pennsylvania? It should come as no surprise that each serves a diverse constituency and generates, stores, and transmits a vast array of sensitive personally-identifying data. However, these disparate entities share another common fact, this one unexpected: each paid hackers to restore encrypted data after being attacked by a form of malicious software (malware) known as "ransomware."

Virtually unknown to the general public even a few years ago, ransomware is currently making headlines in the popular press and causing untold headaches across industries. The Federal Trade Commission ("FTC") describes[1] ransomware as "one of the most serious online threats facing businesses."[2] This particularly vicious type of malware disrupts operations, threatens the confidentiality, integrity, and availability of business-critical information, and can be incredibly expensive to remediate.

Ransomware attacks are becoming more frequent in higher education, and have serious implications regardless of your size, scope, or geographic diversity. What exactly *is* ransomware, why is it targeting higher education, and how can your institution protect itself?

---

* Kimberly C. Metzger is a partner in the Litigation and Intellectual Property Group at Ice Miller LLP. She focuses her practice on data security and privacy, and drug and device litigation. Ms. Metzger, who may be contacted at kimberly.metzger@icemiller.com, is a Certified Information Privacy Professional (CIPP/US), Certified Information Privacy Manager (CIPM), and Fellow of Information Privacy through the IAPP. Stephen E. Reynolds is a partner in the firm's Litigation Group, and co-chair of the Data Security and Privacy Practice, with a practice that focuses on commercial litigation and data security and privacy law. He may be contacted at stephen.reynolds@icemiller.com.

[1] https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look.

[2] Federal Trade Commission, Ransomware – A closer look (November 16, 2016). Accessed February 2, 2017.

WHAT IS RANSOMWARE?

Ransomware is a type of malware that targets critical data or information systems for purposes of extortion. It works by encrypting data with a key known only to the hacker. The encrypted data is then inaccessible to authorized users until the user pays a ransom in exchange for the decryption key.

A ransomware attack typically begins when a computer or system user receives an email asking the user to click on a legitimate-looking link, or open an "innocuous" attachment that purports to be an invoice, resume, or the like. The link, however, directs the user to a website that infects the computer with malware ("drive-by downloading"), or the attachment contains malicious code. Opening the link or attachment infects the user's computer with malware that begins *encrypting* (locking) files and folders on local drives, attached and backup drives, and perhaps even other computers on the same network. The criminal then demands a ransom – usually, Bitcoin or another anonymous form of cryptocurrency – in exchange for the key to *decrypt* (unlock) the data.

Ransomware "targets both human and technical weaknesses in organizations and individual networks in an effort to deny the availability of critical data and systems."[3] At its most effective, ransomware exploits *social engineering* techniques to encourage the recipient to cooperate. The U.S. Department of Homeland Security ("DHS") defines social engineering[4] as using "human interaction (social skills) to obtain or compromise information about an organization's computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity." For example, an email containing an infected link or attachment may appear to come from a superior and demand an immediate response that only the recipient can provide, or may look like an email from a legitimate job-seeker directed to human resources personnel.

THE RISE AND EFFECT OF RANSOMWARE

Ransomware is escalating alarmingly across industries. The FTC estimates that the number of ransomware attacks has quadrupled in the past year alone, now averaging 4,000 incidents per day.[5] The typical ransomware payment ranges from $500-$1,000, though criminals have demanded as much as $30,000.[6] Apart from any ransom paid, infected businesses incur additional costs such as network mitigation, network

[3] U.S. Department of Justice, Federal Bureau of Investigation ("FBI"). *Ransomware*. Accessed August 18, 2016.

[4] https://www.us-cert.gov/ncas/tips/st04-014.

[5] Former FTC Chair Edith Ramirez, remarks at FTC *Fall Technology Series: Ransomware* (September 2016) ("Ramirez Remarks").

[6] *Id*.

countermeasures, loss of productivity, legal fees, IT services, and/or remediation efforts such as the purchase of credit monitoring services for customers.[7]

Former FTC Chair Edith Ramirez recently described ransomware as "the most profitable malware scam in history."[8] This level of profitability means we will not see the end of ransomware anytime soon. It also means that cybercriminals can afford to hire experts to help them develop sophisticated malware based on scientific social-engineering techniques, and teams to help them deploy it in new ways at an astounding rate. The DOJ states that "the most sophisticated ransomware variants are practically impossible to defeat without obtaining the actor's own private decryption keys. . .."[9]

Ransomware attacks can be crippling. Los Angeles Valley College reported[10] that its ransomware attack impacted "key servers" such as the email system, website, voicemail, financial aid, master calendar, shared department files, and bookstore, "to name a few." LAVC President Erika A. Endrijonas confirmed[11] that the Los Angeles Community College District paid the ransom (via a cybersecurity insurance policy) after an outside security expert determined that "making a payment would offer an extremely high probability of restoring access to the affected systems, while failure to pay would virtually guarantee that data would be lost." Dr. Endrijonas noted that the hackers provided a decryption key, which so far had worked on every attempt. Likewise, in May 2016, the University of Calgary in Canada experienced a ransomware attack that encrypted its email servers. The National Law Review reported that while there was no indication that any personal or university data were released to the public, the university nevertheless paid $20,000 CDN in order to "maintain all options"[12] to address resulting systems issues.

As their targets become smarter about ransomware, cybercriminals keep pace. The Department of Justice's Federal Bureau of Investigation ("FBI") recently reported that ransomware attacks "are not only proliferating, they're becoming more sophisticated."

---

[7] Letter from Peter J. Kadzik, Assistant Attorney General (U.S. Department of Justice, Office of Legislative Affairs) to Senator Thomas R. Carper (D-Del.), March 4, 2016 ("Kadzik Letter"). The Kadzik Letter responds to December 2015 correspondence (https://www.hsgac.senate.gov/media/minority-media/senators-carper-johnson-seek-information-on-threat-of-ransomware-to-our-nations-cyber-defenses-and-to-the-american-public) by Senator Carper - Homeland Security and Governmental Affairs Committee Ranking Member – and Committee Chair Ron Johnson (R-Wis.) to U.S. Attorney General Loretta Lynch and DHS Secretary Jeh Johnson with a request: help us understand the nature and extent of the ransomware epidemic, and what the federal government is doing to fight back.

[8] Ramirez Remarks.

[9] Kadzik Letter.

[10] http://www.lavc.edu/presidentsoffice/From-the-Desk-of-the-President.aspx.

[11] https://services.laccd.edu/districtsite/docs/LAVC_cybersecurity_event_FAQ_from_president_endrijonas.

[12] http://www.natlawreview.com/article/increasing-ransomware-attacks-higher-education?mkt_tok=eyJpIjoiWkRNMFlUaGlOVGMxT1RObSIsInQiOiJvd1AwVU9CWHVHaFJFT2xzMDlhWTQ5dDRkUG80eDhiUjc0ZDlaWDhwQ1pEZkNhOGpTXC9KUnlmQ1NuWW1MOFRRZGVyaVRENUpXeW5reGRYMjZnMzN6NERUVWZNYUVpQ1pVYXlCZUJ5TG5zYWFQdjYxSmNOXC9MeUViWTJxejYwbjNuIn0%3D.

While ransomware was once delivered almost exclusively by spam email, criminals had to change direction when spam filters became better at catching the detritus. Undeterred, their next wave of attack involved targeted "spear phishing" email attacks against carefully selected and researched individuals. The FTC reports that 93 percent of phishing emails contain some form of malicious code.[13] The FBI now emphasizes that criminals may not need to use email at all. Instead, they can "bypass the need for an individual to click on a link by seeding legitimate websites with malicious code, taking advantage of unpatched software on end-user computers." For example, the FTC reports that the ransomware variant SamSam exploits a webserver application found on almost 3.2 million machines used in schools, local governments, and aviation companies. Wrongdoers may also engage in "malvertising" – planting malicious code on trusted websites, or fake sites made to look like trusted websites.

Clearly, ransomware has moved beyond "hackers in the basement."[14]

RANSOMWARE IN HIGHER EDUCATION

Ransomware attacks are also on the rise in education, perhaps even more so than in other business sectors. Security ratings provider BitSight Technologies ("BitSight") recently reported that of the six industries it examined (Education, Government, Health Care, Energy/Utilities, Retail, and Finance), Education had the highest rate of ransomware: 13 percent of the 2,100 educational institutions surveyed experienced ransomware on their network. This was more than three times the rate found in Health Care (3.5 percent; n=3,800), and more than 10 times the rate found in Finance (1.5 percent; n=7.639).[15]

Why is higher education a target? BitSight speculates that "smaller IT teams, budgetary constraints, and a high rate of file sharing activities on their networks" may contribute to low security ratings found in academic institutions.[16] By extension, these factors likely contribute to the education sector's vulnerability to ransomware attacks. The U.S. Department of Education ("DOE") has also weighed in. DOE's Privacy Technical Assistance Center ("PTAC") emphasizes that "[i]nadequate IT security may compromise confidentiality, integrity, and availability of data due to unauthorized access." PTAC recently described[17] "critical" technical and non-technical threats to educational data and information systems, many of which increase the likelihood of successful ransomware attacks. PTAC also suggests security fixes[18] to safeguard data confidentiality, integrity, and availability:

---

[13] Ramirez Remarks.

[14] Craig Williams, Security Outreach Manager, Cisco, remarks at FTC Fall Technology Series: Ransomware (September 2016).

[15] BitSight Insights Report, *The Rising Face of Cyber Crime: Ransomware*. BitSight Technologies, Cambridge, MA. Common ransomware strains include nymaim (11 percent of Education institutions), and Locky (nearly four percent). Matsnu, DirCrypt, and CryptoWall invested around one percent or fewer Education institutions (p. 5). BitSight reports that Nymaim, "although typically associated with ransomware, is actually a Trojan that can be used to install a variety of malware." *Id.*

[16] *Id.* p. 3.

[17] http://ptac.ed.gov/sites/default/files/Issue Brief Data Security Top Threats to Data Protection.pdf.

[18] http://ptac.ed.gov/sites/default/files/Data Security Checklist.pdf.

The Threat	The Issue	The Remedy
Technical Threats		
Non-existent security architecture[19]	Unstructured, non-integrated networks are vulnerable to exploitation – including by ransomware. For example, ad hoc networks may be connected directly to the internet, or connected using off-the-shelf appliances with only default configurations.	Even when IT resources are scarce, implement "minimal user, network and perimeter security protection mechanisms (such as anti-virus)" – and ensure they are properly configured.
Inattention to access controls	Failure to affirmatively grant or deny specific requests to obtain and use information or information systems, or enter physical facilities, jeopardizes data confidentiality, integrity, and availability.	Employ access controls such as strong passwords, multi-factor authentication, role-based access, limited length of access (e.g., locking access after session timeout), limited administrative access, and segregated sensitive information.
Unpatched software and applications	Older versions of software may contain vulnerabilities that malicious actors can exploit.	Implement a robust "patch management program" to identify and regularly update vulnerable software.
Phishing and spear phishing	Emails containing or directing the recipient to malicious code.	Install professional, enterprise-level security software to check both incoming and outgoing emails. Provide regular internet security training to all workforce members.
Compromised internet websites	Malicious code transferred simply by visiting compromised or unsecure websites.	Employ firewalls and antivirus software to identify and block problem sites.

[19] An enterprise's security architecture is its entire set of information systems: how they are configured and integrated, how they interface with the external environment, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture. When the enterprise lacks qualified IT staff or sufficient resources, information systems are more likely to be ad hoc rather than structured.

The Threat	The Issue	The Remedy
Poor configuration management	Failure to control modifications to hardware, software, and firmware leaves information systems vulnerable to attack.	Implement policies governing what hardware (computers, printers, networking devices) can connect to the network and how they must be configured. Include a network access control solution to prevent noncompliant hardware from connecting. Implement a change management program to ensure that hardware and software is not connected to the network until it has been securely scanned and optimally configured. Continuous compliance scanning will enhance data protection.
Unencrypted mobile devices	Lost or stolen unencrypted mobile devices are a frequent cause of data breaches.	Encrypt data on mobile devices that store sensitive information. Implement a strict mobile device policy, and monitor the network for malicious activity.
Cloud computing	Delegating data protection to a third party shifts enterprise security architecture.	Weigh cloud benefits (efficiency, cost) against security risks. Ensure that cloud solutions comport with the organization's information system security requirements. Carefully review contracts with cloud service providers regarding such issues as data ownership and security. Institute a cloud usage policy and discourage ad hoc cloud solutions.
Portable media	Flash drives, CDs, DVDs, and other portable media are efficient paths for malware to migrate between networks and hosts.	Disable "auto run" feature of operating system on organization's machines. Train workforce to scan for viruses before opening files.
Botnets[20]	Infection of organization's network compromises all resident data.	Create a strong security architecture.

[20] A botnet is a network of compromised computers used for malicious purposes.

The Threat	The Issue	The Remedy
Poor authentication	Failure to verify the identity or other claimed attributes of a user, process, or device leaves information systems vulnerable to intrusion.	Multi-factor authentication verifies some combination of what you know, what you have, or who you are. It may be more costly, but provides added security.
Over-reliance on a firewall	Failure to use an array of complementary defensive tools leaves your applications, networks, and perimeters open to intrusion.	A firewall alone is inadequate to protect information systems. Employ a Defense-in-Depth system architecture with specific security controls suited to applications, networks, and the perimeter.
Failure to scan	Failure to scan your own system for vulnerabilities leaves hackers one step ahead.	Regular automated vulnerability scanning minimizes the time the network is exposed to known vulnerabilities.
Too many access points	Unapproved or unnecessary ports, protocols, and services are additional avenues to exploit your information systems.	System security configuration should include shutting down unnecessary services and ports, and continuously monitoring for unapproved ports, protocols, and services.
Poor transmission policies	Emailing unencrypted sensitive information makes you one autofill or misdirect away from a breach.	Consider data sensitivity when selecting a transmission process. Implement policies and procedures for secure transmission: use secure carriers for paper, desensitize whenever possible, and apply technical solutions such as encryption for electronic transfers.
Zero-day attacks	Exploit software vulnerabilities before vendor and security community is aware.	Keep abreast of latest patches and deploy fixes as soon as developer distributes.
Non-Technical Threats		
Right hand/left hand issues	Absent or ad hoc data security policy and governance can mean uncoordinated, inconsistent approaches to data security and responses to security incidents.	Develop a comprehensive data governance plan describing organization-wide policies and standards for data security and privacy. Identify workforce responsibilities and empower actors.

The Threat	The Issue	The Remedy
Poor workforce security	Inappropriate use of information systems compromises data confidentiality, integrity, and availability. Lack of published policies and data-security aspects of job descriptions leaves the workforce in the dark. Inadequate training leads to unintentional data protection errors; ineffective vetting allows malicious insider access.	Create and disseminate an Acceptable Use Policy outlining appropriate use of internet, intranet, and extranet systems. Incorporate data security elements into job descriptions. Regularly train workforce members to ensure understanding of terms and conditions of employment. Use robust security screenings, training, and confidentiality agreements to lessen insider threat.
Compromised physical security	Ineffective or absent physical security for hardware, software, firmware, and information systems jeopardizes data confidentiality, integrity, and availability.	Secure access to areas where sensitive data are stored and processed (e.g., server rooms). Monitor access to prevent intrusion attempts.
Un-inventoried assets	Unknown hardware, software, and firmware may not be properly secured, and therefore vulnerable to intrusion.	Inventory both authorized and unauthorized hardware, software, and firmware.
Insufficient backup and recovery	Lack of routine backup and secure storage put data integrity and availability at risk, and will limit the organization's options after a ransomware attack.	Develop and enforce organization-wide policy and procedures for data backup, storage, and retrieval.
Social media	Frequent targeting of social media sites by malware.	Implement and enforce a strong social media access policy, which may include forbidding access to certain sites, and deploying a strong anti-virus and spam filtering solution.

The Threat	The Issue	The Remedy
Social engineering	Malicious actors can gain access to sensitive information (passwords, access codes, IP addresses, router and server names) by manipulating legitimate users after gaining their trust.	Workforce training and education.

***

The second part of this article, which will appear in an upcoming issue of *Pratt's Privacy & Cybersecurity Law Report*, discusses responding to a ransomware incident, preventing a ransomware attack, and information-sharing for better security.