EDITOR'S NOTE: CHILLING SUMMER READING
Victoria Prussen Spears

PAY UP ... OR ELSE? RANSOMWARE IS A GROWING THREAT TO HIGHER EDUCATION – PART I
Kimberly C. Metzger and Stephen E. Reynolds

A GUIDE TO CORPORATE INTERNAL INVESTIGATIONS – PART I
Jennifer L. Chunias and Jennifer B. Luz

ABA ISSUES NEW GUIDANCE ON CONFIDENTIALITY AND THE USE OF TECHNOLOGY
Shari Claire Lewis and Avigael C. Fyman

NIST RELEASES UPDATED CYBERSECURITY FRAMEWORK AND GUIDE FOR CYBERSECURITY EVENT RECOVERY
Rajesh De, Marcus A. Christian, David A. Simon, Stephen Lilley, Kendall C. Burman, and Joshua M. Silverstein

CHINESE GOVERNMENT RELEASES DRAFT RULES TO IMPLEMENT CYBER SECURITY LAW
Jay Si and Ron Cai
Editor’s Note: Chilling Summer Reading
Victoria Prussen Spears 195

Pay Up . . . or Else? Ransomware is a Growing Threat to Higher Education – Part I
Kimberly C. Metzger and Stephen E. Reynolds 197

A Guide to Corporate Internal Investigations – Part I
Jennifer L. Chunias and Jennifer B. Luz 206

ABA Issues New Guidance on Confidentiality and the Use of Technology
Shari Claire Lewis and Avigael C. Fyman 216

NIST Releases Updated Cybersecurity Framework and Guide for Cybersecurity Event Recovery
Rajesh De, Marcus A. Christian, David A. Simon, Stephen Lilley, Kendall C. Burman, and Joshua M. Silverstein 220

Chinese Government Releases Draft Rules to Implement Cyber Security Law
Jay Si and Ron Cai 227
Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF
STEVEN A. MEYEROWITZ
President, Meyerowitz Communications Inc.

EDITOR
VICTORIA PRUSSEN SPEARS
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

EMILIO W. CIVIDANES
Partner, Venable LLP

RICHARD COHEN
Special Counsel, Kelley Drye & Warren LLP

CHRISTOPHER G. CWALINA
Partner, Holland & Knight LLP

RICHARD D. HARRIS
Partner, Day Pitney LLP

DAVID C. LASHWAY
Partner, Baker & McKenzie LLP

CRAIG A. NEWMAN
Partner, Patterson Belknap Webb & Tyler LLP

ALAN CHARLES RAUL
Partner, Sidley Austin LLP

AARON P. SIMPSON
Partner, Hunton & Williams LLP

RANDI SINGER
Partner, Weil, Gotshal & Manges LLP

JOHN P. TOMASZEWSKI
Senior Counsel, Seyfarth Shaw LLP

TODD G. VARE
Partner, Barnes & Thornburg LLP

THOMAS F. ZYCH
Partner, Thompson Hine
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 ransomware as “one of the most serious online threats facing businesses.” 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?

---

1 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.


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.”

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 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. The typical ransomware payment ranges from $500-$1,000, though criminals have demanded as much as $30,000. Apart from any ransom paid, infected businesses incur additional costs such as network mitigation, network

---

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.\textsuperscript{7}

Former FTC Chair Edith Ramirez recently described ransomware as “the most profitable malware scam in history.”\textsuperscript{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…”\textsuperscript{9}

Ransomware attacks can be crippling. Los Angeles Valley College reported\textsuperscript{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\textsuperscript{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”\textsuperscript{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.”


\textsuperscript{8} Ramirez Remarks.

\textsuperscript{9} Kadzik Letter.

\textsuperscript{10} http://www.lavc.edu/presidentsoffice/From-the-Desk-of-the-President.aspx.

\textsuperscript{11} https://services.laccd.edu/districtsite/docs/LAVC_cybersecurity_event_FAQ_from_president_endrijonas.

\textsuperscript{12} http://www.natlawreview.com/article/increasing-ransomware-attacks-higher-education/mkt_tok=eyJpIjoiWkRNMF1uaGlOYVMxT1R0bSI2InQiOjvdI1AwVU9CWHVHFaFT2xMDliWTQ5dDRkUG80eDhiUjc0ZDlaWDhwQ1pEZkNhOGpTXC9KUlnmQ1NuWW1MOFRZGVyaVRENUpXeW5rereGRYMjZmN6NERUVWZNYUYvQ1pVYXICZUJ5TG5zYWFQdjYxSmNOXC9MeUViWTJseYwblNuIn0%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. 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.”

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).

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. 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 “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 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 nyamain (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 Nyaim, “although typically associated with ransomware, is actually a Trojan that can be used to install a variety of malware.” Id.
16 Id. p. 3.
### 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.
<table>
<thead>
<tr>
<th>The Threat</th>
<th>The Issue</th>
<th>The Remedy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poor configuration management</td>
<td>Failure to control modifications to hardware, software, and firmware leaves information systems vulnerable to attack.</td>
<td>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.</td>
</tr>
<tr>
<td>Unencrypted mobile devices</td>
<td>Lost or stolen unencrypted mobile devices are a frequent cause of data breaches.</td>
<td>Encrypt data on mobile devices that store sensitive information. Implement a strict mobile device policy, and monitor the network for malicious activity.</td>
</tr>
<tr>
<td>Cloud computing</td>
<td>Delegating data protection to a third party shifts enterprise security architecture.</td>
<td>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.</td>
</tr>
<tr>
<td>Portable media</td>
<td>Flash drives, CDs, DVDs, and other portable media are efficient paths for malware to migrate between networks and hosts.</td>
<td>Disable “auto run” feature of operating system on organization’s machines. Train workforce to scan for viruses before opening files.</td>
</tr>
<tr>
<td>Botnets&lt;sup&gt;20&lt;/sup&gt;</td>
<td>Infection of organization’s network compromises all resident data.</td>
<td>Create a strong security architecture.</td>
</tr>
</tbody>
</table>

<sup>20</sup> A botnet is a network of compromised computers used for malicious purposes.
## The Threat

<table>
<thead>
<tr>
<th>The Threat</th>
<th>The Issue</th>
<th>The Remedy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poor authentication</td>
<td>Failure to verify the identity or other claimed attributes of a user, process, or device leaves information systems vulnerable to intrusion.</td>
<td>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.</td>
</tr>
<tr>
<td>Over-reliance on a firewall</td>
<td>Failure to use an array of complementary defensive tools leaves your applications, networks, and perimeters open to intrusion.</td>
<td>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.</td>
</tr>
<tr>
<td>Failure to scan</td>
<td>Failure to scan your own system for vulnerabilities leaves hackers one step ahead.</td>
<td>Regular automated vulnerability scanning minimizes the time the network is exposed to known vulnerabilities.</td>
</tr>
<tr>
<td>Too many access points</td>
<td>Unapproved or unnecessary ports, protocols, and services are additional avenues to exploit your information systems.</td>
<td>System security configuration should include shutting down unnecessary services and ports, and continuously monitoring for unapproved ports, protocols, and services.</td>
</tr>
<tr>
<td>Poor transmission policies</td>
<td>Emailing unencrypted sensitive information makes you one autofill or misdirect away from a breach.</td>
<td>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.</td>
</tr>
<tr>
<td>Zero-day attacks</td>
<td>Exploit software vulnerabilities before vendor and security community is aware.</td>
<td>Keep abreast of latest patches and deploy fixes as soon as developer distributes.</td>
</tr>
</tbody>
</table>

## Non-Technical Threats

<table>
<thead>
<tr>
<th>Non-Technical Threats</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Right hand/left hand issues</td>
<td>Absent or ad hoc data security policy and governance can mean uncoordinated, inconsistent approaches to data security and responses to security incidents.</td>
</tr>
<tr>
<td></td>
<td>Develop a comprehensive data governance plan describing organization-wide policies and standards for data security and privacy. Identify workforce responsibilities and empower actors.</td>
</tr>
<tr>
<td>The Threat</td>
<td>The Issue</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Poor workforce security</td>
<td>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.</td>
</tr>
<tr>
<td>Compromised physical security</td>
<td>Ineffective or absent physical security for hardware, software, firmware, and information systems jeopardizes data confidentiality, integrity, and availability.</td>
</tr>
<tr>
<td>Un-inventoried assets</td>
<td>Unknown hardware, software, and firmware may not be properly secured, and therefore vulnerable to intrusion.</td>
</tr>
<tr>
<td>Insufficient backup and recovery</td>
<td>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.</td>
</tr>
<tr>
<td>Social media</td>
<td>Frequent targeting of social media sites by malware.</td>
</tr>
</tbody>
</table>
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.