What do Los Angeles Valley College and 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.” [1] 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?

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.”[2] 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. [3] The typical ransomware payment ranges from $500-$1,000, though criminals have demanded as much as $30,000. [4] Apart from any ransom paid, infected businesses incur additional costs such as network mitigation, network countermeasures, loss of productivity, legal fees, IT services, and/or remediation efforts such as the purchase of credit monitoring services for customers. [5]

Former FTC Chair Edith Ramirez recently described ransomware as “the most profitable malware scam in history.”[6] 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 ....[7]

Ransomware attacks can be crippling. Los Angeles Valley College reported 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 reported 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 reported 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. 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” 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.” 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% of phishing emails contain some form of malicious code.[8] 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."[9]

**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% 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%; n=3,800), and more than ten times the rate found in Finance (1.5%; n=7,639).[10]

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.[11] 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 “inadequate 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:

<table>
<thead>
<tr>
<th>The Threat</th>
<th>The Issue</th>
<th>The Remedy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Threats</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-existent security architecture[12]</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Inattention to access controls</td>
<td>Failure to affirmatively grant or deny specific requests to obtain and use information or information systems, or</td>
<td>Employ access controls such as strong passwords, multi-factor authentication, role-based access,</td>
</tr>
<tr>
<td>Issue</td>
<td>Description</td>
<td>Recommendation</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Unpatched software and applications</td>
<td>Older versions of software may contain vulnerabilities that malicious actors can exploit.</td>
<td>Implement a robust “patch management program” to identify and regularly update vulnerable software.</td>
</tr>
<tr>
<td>Phishing and spear phishing</td>
<td>Emails containing or directing the recipient to malicious code.</td>
<td>Install professional, enterprise-level security software to check both incoming and outgoing emails. Provide regular internet security training to all workforce members.</td>
</tr>
<tr>
<td>Compromised internet websites</td>
<td>Malicious code transferred simply by visiting compromised or unsecure websites.</td>
<td>Employ firewalls and antivirus software to identify and block problem sites.</td>
</tr>
<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 are secure.</td>
</tr>
</tbody>
</table>
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[13] | Infection of organization’s network compromises all resident data. | Create a strong security architecture. |
| 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 auto-fill or misdirect away from a breach. | Consider data sensitivity when selecting a transmission process. Implement policies and procedures for secure |
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.

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

Develop and enforce organization-wide policy and procedures for data backup, storage, and retrieval.
Responding to a Ransomware Incident

An organization cannot begin to respond and recover until it knows it has been attacked. Unless the entity’s security management processes have detected and stopped the ransomware, the first indication of an attack is often the “pop-up” ransom demand itself. Workforce training and diligence can, however, make a difference by increasing the likelihood that early indicators will be detected and reported in time to limit propagation. According to the U.S. Department of Health and Human Services, Office for Civil Rights (OCR), first signs of a malware attack may include: [14]

- An information system user suspecting he or she clicked on a link, opened an attachment, or visited a website of a malicious nature
- Increased activity in a computer's central processing unit (CPU), or disk activity without apparent reason – which may indicate that ransomware is searching for, encrypting, and removing data
- The inability to access certain data or files – a signal that ransomware may be encrypting, deleting, renaming, or relocating data
- Suspicious network communications between the ransomware and the attackers’ command and control servers, detected by IT personnel via an intrusion detection solution

The FTC also describes general warning signs of a malware attack: [15]

- Your computer:
  - Slows down, crashes, or displays repeat error messages
  - Will not shut down or restart
  - Displays repeated popups
  - Displays inappropriate ads, or ads that interfere with page content
  - Will not let you uninstall unwanted software
  - Injects ads in atypical places, such as government websites
  - Shows webpages you did not intend to visit, or emails you did not write
New or unexpected toolbars or icons
Unexpected browser changes, such as a new default search engine
Sudden change in internet homepage
Unusually fast battery drainage

If the organization believes a ransomware attack is underway, it should immediately implement its incident response plan (IRP). A robust IRP will allow the entity to nimbly and effectively respond to the attack and report it as necessary. Generally, an IRP should include processes and procedures to:

- Detect ransomware attacks
- Take immediate steps to limit propagation
- Conduct an initial analysis, including
  - Scope: what networks, systems, and/or applications are affected
  - Origination: who, what, where, and when
  - Continuation: is the incident finished, or is it ongoing and/or propagating
  - Manner and method: tools, attack methods, ransomware variants
- Contain the event and prevent continuation and propagation
- Eradicate the malware from all information systems and data repositories
- Identify and remediate administrative, physical, and technical vulnerabilities that allowed the malware to attack and propagate
- Mitigate harmful effects to individuals and the organization
- Recover from the attack by restoring data and resuming normal operations
- Conduct post-incident activities, including root-cause analysis, regulatory reporting, fulfilling contractual obligations, and identifying and communicating lessons learned

A critical immediate response step is to prevent the attack from propagating by isolating affected hardware and information systems. The organization should immediately remove infected systems from the network to prevent spread to the network or share drives. It should also isolate or power-off affected devices that have not been completely corrupted. This may give more time to clean and recover data, contain damage, and keep the situation from worsening. Additional first steps include:[16]

- Immediately securing backup data and systems by taking them offline (if they are not already) and ensuring backups are free of malware.
- Determining whether to report the incident to local law enforcement and/or the local FBI or United States Secret Service field office. The DOJ “strongly encourage[s]” immediate reporting. Contact counsel to discuss this.
- Change all online account and network passwords after removing the affected system from the network. Change all system passwords after the malware is removed.
- Delete registry values and files to stop the program from loading.

Note, however, that simply “wiping your system” will destroy valuable forensic data. To prevent panicked decisions from backfiring, it is best to think through the organization’s immediate, mid-range, and long term response before there is a problem, in consultation with technical specialists and counsel. If the organization has done its pre-work, memorialized it in an incident-handling procedure, and trained applicable workforce members, it will be able to take the best steps to
mitigate harm while allowing it to conduct necessary forensic analysis when the immediate crisis has passed.

An entity’s first question is typically: “Should I pay the ransom?” Criminals know that the data they encrypt are important to the victim and its constituents – in fact, they often target what they know to be mission-critical information and systems. To boost the chance for a payout, many attackers set the ransom at an amount the victim can easily afford. With critical operations having ground to a halt, the beleaguered business may think paying the ransom is the clear – albeit infuriating – choice.

However, acquiescing to the ransom demand is not without risk. The attackers may demand more money, disappear after payment without providing the decryption key, or publicize you to other criminals as a vulnerable target known to pay. For these reasons, the FBI generally discourages paying:

*The FBI does not support paying a ransom to the adversary. Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom. Paying a ransom emboldens the adversary to target other organizations for profit, and provides a lucrative environment for other criminals to become involved.*

The FBI apparently recognizes, however, victims cannot always simply refuse to pay. Rather, “there is an understanding that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers.” [17]

Whether to pay is ultimately a business decision. Ice Miller LLP partner and former computer programmer and IT analyst Stephen Reynolds states: “While the decision of whether or not to pay a ransom is a decision that each organization must evaluate on a case-by-case basis considering the totality of the circumstances, paying the ransom comes with the risk that the organization will be targeted again—especially given that cyber-criminals have been known to identify their victims to other hackers.”

Implementing and routinely following a thoughtful *data backup policy* will give the organization options in the event of a ransomware attack. Certain regulated entities, such as those covered by the HIPAA Security Rule, may be *required* to implement a data backup plan.[18] Whether or not required, data backup is good business in light of the ransomware scourge. Maintaining frequent backups, *and ensuring the ability to recover data from the backups*, is critical to recovering from an attack. Because some ransomware variants remove or otherwise disrupt online backups, OCR recommends maintaining business-critical backups and backups of personally-identifying information offline, unavailable to entity networks. OCR also suggests conducting periodic test restorations to verify the organization’s restoration capabilities.

A *contingency or business continuity plan* will also optimize a college’s or university’s response and recovery. Data backup is one element; others include disaster recovery planning, emergency operations planning, analyzing the criticality of applications and data to ensure all are accounted for, and periodic contingency testing. Once activated, the contingency plan will allow the organization to operate while responding to and recovering from the ransomware attack. This, in turn, will inspire constituents’ and the public’s confidence.
Preventing a Ransomware Attack

Effective response and recovery are good for your institution – preventing a ransomware attack in the first place is better. US-CERT recommends the following preventive measures:

- Use application whitelisting to help prevent malicious software and unapproved programs from running. Application whitelisting is an effective security strategy because it allows only specified programs to run, while blocking all others, including malicious software.
- Keep your operating system and software up-to-date with the latest patches. Vulnerable applications and operating systems are the target of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.
- Maintain up-to-date anti-virus software, and scan all software downloaded from the internet before executing.
- Restrict users’ ability (permissions) to install and run unwanted software applications, and apply the principle of “Least Privilege” to all systems and services. Restricting these privileges may prevent malware from running, or limit its capability to spread through the network.
- Avoid enabling macros from email attachments. If a user opens the attachment and enables macros, embedded code will execute the malware on the machine. US-CERT emphasizes it may be best to block email messages with attachments from suspicious sources.
- Do not follow unsolicited Web links in emails.

In addition, your organization should implement administrative, technical, and physical safeguards to protect data confidentiality, integrity, and availability. These include:

Administrative Safeguards

1. Implement a **security management process** – policies and procedures to prevent, detect, contain, and correct security violations.
2. Perform an information security **risk analysis** – an assessment of potential risks and vulnerabilities to confidentiality, integrity, and availability.
3. Institute a **risk management plan** – security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
4. Implement procedures to regularly **review records of information system activity**, such as audit logs, access reports, and security incident tracking reports.
5. Institute and enforce appropriate **sanctions** against workforce members who do not comply with the organization’s security policies and procedures.
6. Implement **access control** policies and procedures to ensure authorized workforce members have access to data, and unauthorized workforce members do not. These may include policies and procedures for:
   a. Authorizing and supervising workforce members who work with sensitive data, or the locations where such data may be accessed
   b. Determining appropriate levels of data and system access and privileges
   c. Terminating system access when employment ends
   d. Modifying system access when job responsibilities change
7. Implement a **security awareness and training program** for all workforce members – including management – that may include:
   a. Periodic security reminders and updates
   b. Procedures for guarding against, detecting, and reporting malware
   c. Procedures for monitoring login attempts and reporting discrepancies
   d. Procedures for creating, changing, and safeguarding passwords
e. Policies and procedures to address security incidents

8. Developing and implementing a contingency plan (policies and procedures for responding to data-security incidents and emergencies), including a data backup and recovery plan

9. Performing a periodic technical and nontechnical evaluation of policies and procedures in response to environmental or operational changes affecting data security

10. Vetting and contracting with vendors who receive, create, maintain, or transmit sensitive information on your behalf – including all cloud service providers – to ensure they will adequately safeguard your data

Physical Safeguards

1. Implement policies and procedures to limit physical access to information systems and the facilities in which they are housed

2. Implement policies and procedures for workstation use, including functions to be performed, manner in which they are to be performed, and physical attributes of the surroundings

3. Implement device and media controls – policies and procedures governing the receipt and removal of hardware and other electronic media containing sensitive information into, out of, and within the organization. These may include:
   a. Policies and procedures to address the final disposition of sensitive information, and the hardware and electronic media on which it is stored
   b. Procedures for removing sensitive information from electronic media before making the media available for reuse
   c. Maintaining a record of the location of hardware and electronic media containing sensitive information

Technical Safeguards

1. Implement access controls – technical policies and procedures for information systems allowing access only to persons or programs that have been granted access rights. These may include:
   a. Assigning a unique name and/or number to identify and track user identity
   b. Establishing procedures for obtaining access to sensitive data in an emergency
   c. Implementing electronic procedures that terminate an electronic session after a set period of inactivity
   d. Implementing a mechanism to encrypt sensitive information at rest and in motion

2. Implement audit controls – hardware, software, and/or procedural mechanisms to record and examine activity in information systems containing sensitive information

3. Implement data integrity controls – policies and procedures to protect sensitive information from improper alteration and destruction.

4. Conduct person or entity authentication – policies and procedures to verify that a person or entity seeking access to sensitive information is the one claimed

5. Attend to transmission security – implement technical security measures to guard against unauthorized access to sensitive information being transmitted over an electronic communications network. These may include both integrity controls and encryption.

When developing and implementing information security safeguards, keep in mind that in most cases you can tailor security measures to your organization’s size, complexity, and capabilities; its technical infrastructure, hardware, and software security capabilities; cost; and the probability and criticality of risks and threats to sensitive information.
These safeguards will not make you bullet-proof against ransomware – with the rapidly-changing threat environment, there can be no guarantees. However, implementing reasonable and appropriate administrative, physical, and technical safeguards will allow your institution to identify threats and vulnerabilities to data confidentiality, integrity, and availability – including ransomware – and manage those risks and vulnerabilities to a reasonable and appropriate level.

**Information-Sharing for Better Security**

Colleges and universities should consider the benefits of information-sharing to combat ransomware and other data security threats. The Research and Education Information Sharing and Analysis Center (REN-ISAC) is a membership coalition of research and higher education institutions that collects, analyzes, and disseminates information on security-related events. The organization establishes information-sharing relationships with other ISACs, DHS/The United States Computer Readiness Team (US-CERT)[19], private network security collaborations, network and security engineers, and REN-ISAC members.

REN-ISAC is part of a network of industry-specific ISACs established by Presidential Decision Directive[20] to serve as the mechanism for (1) gathering information on vulnerabilities, threats, intrusions, and anomalies from participating institutions, (2) analyzing and developing recommendations, (3) and disseminating information to help members better defend and secure their technology environment. REN-ISAC also staffs a 24/7 Computer Security Incident Response Team (CSIRT) to receive and disseminate timely information about cybersecurity in higher education.

Membership in REN-ISAC is open to colleges and universities, teaching hospitals, research and education network providers, and government-funded research organizations.

**Conclusion**

Ransomware is a growing scourge for businesses of all types, and has recently begun targeting higher education. While ransomware can harm both operations and constituents, colleges and universities can do much to protect themselves. Proper preparation – including risk analysis, risk management, and workforce training – can help your organization avoid a ransomware attack. If you do fall victim, an incident response plan, supported by robust backup of critical data, can give you options apart from the risky proposition of paying the ransom. It can also guide your immediate first steps to halt propagation and contain damage.

For more information on protecting yourself from ransomware attacks, contact Kim Metzger, Stephen Reynolds or a member of our Data Security and Privacy team.

*This publication is intended for general information purposes only and does not and is not intended to constitute legal advice. The reader should consult with legal counsel to determine how laws or decisions discussed herein apply to the reader's specific circumstances.*

[4] Id.
[5] 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 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.

[9] Craig Williams, Security Outreach Manager, Cisco, remarks at FTC Fall Technology Series: Ransomware (September 2016).
[10] BitSight Insights Report, The Rising Face of Cyber Crime: Ransomware. BitSight Technologies, Cambridge, MA. Common ransomware strains include nymaim (11% of Education institutions), and Locky (nearly 4%). Matsnu, DirCrypt, and CryptoWall invested around 1% 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.
[12] 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.
[13] A botnet is a network of compromised computers used for malicious purposes.
[16] U.S. Department of Justice, How to Protect Your Networks from Ransomware. This is a U.S. Government interagency technical document.
[17] Id.
[18] A higher education institution may offer a group health plan that is a HIPAA “covered entity” with Security Rule compliance obligations. A college or university that offers health care services through a program or component may also be fully-or partially-covered by the Security Rule.
[19] US-CERT is the U.S. Computer Emergency Readiness Team. In early 2000, Federal Government networks began experiencing an alarming number of cyber breaches. In response, Congress created the Federal Computer Incident Response Center (FedCIRC) at the General Services Administration as a centralized hub of coordination and information sharing between federal organizations. With the creation of the DHS in 2002, Congress transferred these responsibilities to the new Department. In 2003, FedCIRC was renamed “US-CERT,” and its mission was expanded to include providing boundary protection for the federal civilian executive domain and cybersecurity leadership.