Cybersecurity: Managing the Risk in Higher Education

Sean B. Hoar and Randy J. Aliment

The Higher Education Sector: A Continuous Target

The higher education sector is a continuous target of malicious actors due to the multiple revenue streams it offers. Over 70 years ago, when asked why he robbed banks, the infamous bank robber Willie Sutton allegedly responded "I rob banks because that's where the money is." Malicious hackers of today have chosen their roles and targets for the same reason. As participants in numerous multi-billion dollar criminal business models, malicious hackers continuously attempt to monetize unauthorized access to systems and data. Their exploits are constantly evolving, in part due to new technology, but also due to increasingly creative criminal revenue streams derived from extortion and the sale of stolen data. As explained below, the higher education sector must heighten its awareness of these exploits and reallocate resources to better prepare for and respond to them.

Malicious Attackers: Leveraging Providers and Tools

In recent months there has been a spike in the compromise of managed service providers (MSPs). An MSP is a business model that remotely manages client information technology infrastructure and/or end-user systems. MSPs may have hundreds or thousands of business clients, including colleges and universities. They have become targets of malicious hackers because through them the attackers have access to not just the MSP, but to all their clients' information systems. From the attacker's perspective, rather than attack just one college or university, why not target their MSP and successfully affect hundreds or thousands of institutions with the same effort? This cyber-attack trend has shifted the paradigm for both cyber-preparedness and incident response. The sheer size of these attacks are an order of magnitude larger and more complex than previous large scale attacks due to the number of entities simultaneously affected, and the corresponding large-scale efforts that must be undertaken to swiftly and effectively respond and remediate these attacks.

Often as part of the MSP attacks, and as part of a similar attack trend involving the simultaneous victimization of information systems, malicious attackers have compromised the use of professional services automation (PSA) tools, remote monitoring and management (RMM) tools, enterprise resources planning (ERP) applications, and similar means of access to numerous information systems or repositories of data – often simultaneously. Depending upon the exploit used by the attacker, hundreds of systems can be encrypted simultaneously to increase the extortionate value of the attack, and/or much more sensitive data can be exfiltrated from those systems, substantially increasing the resulting profit on the dark web. Preparing for and effectively responding to these attacks requires significant coordination

Malicious Attack Trends

Ransomware continues to ravage systems across the globe and has caused severe disruptions and the loss of critical data within college and university information systems. Certain variants

of malicious computer code comprising ransomware continuously evolve to evade detection by the most sophisticated anti-virus products. The more sophisticated ransomware attacks may be preceded by credential stealing Trojan attacks, allowing the attacker to elevate privileges within the network, providing them access to substantially more digital assets in which to seed the encryption malware. When the ransomware attack is executed, the resulting encryption can be devastating to the network – essentially locking up critical servers containing admissions material, faculty curricula, student records and financial accounts, institutional research and accreditation data and records, alumni records, donor development records, and operational data required for information system functionality. The lack of access to such data may cause serious impairments to, if not the complete loss of, the critical work of college or university personnel.

The expense of responding to a ransomware attack can be substantial. At a minimum, an effective ransomware response typically involves the deployment of robust endpoint monitoring tools to contain the attack. Endpoint monitoring tools are commonly referred to as endpoint detection and response (EDR) tools or advanced threat protection (ATP) tools. Sophisticated endpoint monitoring tools use data analytics in a heuristic manner to identify behaviors that appear to be malicious. They are able to recognize previously undetected malicious computer code due to the algorithmic behaviors of the code. The response to ransomware attacks also typically involve forensics investigations to determine what happened, when it happened and how it happened. The endpoint monitoring and forensics investigation, while necessary, can often result in a substantial five or six figure expense.

Email account compromises present multiple dangers to colleges and universities. One serious risk is to the security of the institutional computer network. Malicious attackers often target email accounts as a means to gain user credentials for access to the computer network. They typically send a sophisticated "phishing" message to the user of the account. The message is often crafted after substantial reconnaissance by the malicious attacker to appear to be from a friend, colleague, or known vendor. Even the most astute and scrutinizing recipient will perceive it as a legitimate message from a known contact. The messages may use multiple means to harvest user credentials – perhaps through malware embedded in an attachment, through a link to an apparent legitimate application that captures log in information, or through basic social engineering requesting certain information. The compromised email accounts often serve as an attack vector to a much larger computer network compromise.

Another serious risk from email account compromises is to the sensitive information contained in the email accounts. Depending upon the target of the attack, malicious attackers may steal personal information from individual students or staff, or obtain much broader access to employee Form W-2 Wage and Tax Statements from human resources personnel. Student email accounts often contain user credentials to the email account and to other online accounts, as well as access credentials for financial accounts. These credentials can be used by the initial attacker for malicious purposes, including sending spam messages to contact lists in order to infect others with a credential harvesting attack, or to steal funds from a bank account. The user credentials can also be sold on the dark web. The employee Form W-2 information can be used to e-file fraudulent tax returns for the purpose of stealing refunds. The bottom line is that an email account can be a treasure trove of sensitive data that a criminal can use for malicious purposes.

A third serious risk from email account compromises is to secondary sources of money that can be obtained through malicious use of the account, or through stolen user credentials to employee portals. Accounting personnel, or financial officers, are commonly targeted in fraudulent wire transfer exploits. Once the attacker compromises the email account, rules are enabled to search for messages and attachments containing terms that pertain to wire transfers, like "invoice," "wire," "transfer," or "ACH." If messages with those terms are received, another rule causes the messages to be deleted from the legitimate account and forwarded to the malicious attacker's account. If the account belongs to an accounts receivable clerk, the malicious attacker typically alters the account number to which the funds are to be transferred and sends that information in a subsequent message from the legitimate account. This often results in the wire transfer or ACH payment being made to the malicious actor's account. Colleges and universities are losing millions of dollars in fraudulent wire transfers to malicious attackers.

Human resources personnel are commonly targeted in W-2 exploits in which malicious attackers attempt to phish Form W-2 information in order to fraudulently e-file tax returns. They are also targeted for employee portal user credentials. Malicious actors use the credentials to access the employee portals and change direct deposit information so that payroll checks are sent to the malicious actor's account. Colleges and universities are losing millions of dollars from payroll accounts to malicious attackers.

The expense of responding to an email account compromise can be substantial. Depending upon the nature of the exploit, a forensics investigation may or may not be necessary. If necessary, it will involve a review of various log files, enabled rules, and data which may have been acquired without authorization. If malicious attackers acquired personal information during the attack, data mining may have to be undertaken. If personal information was acquired, consumer and regulatory notification may be required. Although initial forensics investigations within an email account can be done relatively efficiently and often incur no more than a low five figure expense, the process of data mining can often result in a substantial five or six figure expense. The cost of consumer notification and remediation will depend upon the number to be notified, but it is a necessary expense that victims of the compromise must be prepared to incur.

The dark web is often depicted as having a certain digital location in the long tail of the Internet. It is essentially anywhere on the Internet where malicious actors market or store their services. While some malicious actors work in organized crime syndicates, others work individually, and sell their services on the dark web – the cyber underground. The dark web is a massive collection of criminal online forums that exist for the purchase and sale of criminal products or services. The following are some of these services:

- "Bullet proof" hosting services involving dedicated servers and corrupt domain registration which provides vital infrastructure for hosting infected web sites, malware, botnet command and control stations, VPNs, proxies, and other digital assets necessary to conduct exploits;
- Monetization of data;
- Development and dissemination of spam botnets;
- Coding services to customize the malware, tailor it to specific targets and improve the malware's ability to bypass anti-fraud mechanisms;

- Anti-virus checking services so that, before deployment, malicious code can be checked against numerous anti-virus products to maximize infection rates;
- Exploit kits to identify and exploit vulnerabilities on victim systems;
- Secure communications; and
- Electronic payment systems and virtual currencies.

The regulatory environment is only slightly less frightening than the dark web … This is because entities that incur data security incidents may have consumer and regulatory notification obligations that trigger financial assessments by state, federal and industry regulatory authorities. All 50 states, as well as Washington D.C., Guam, Puerto Rico, and the Virgin Islands, have data breach notification statutes that require relatively immediate notification of consumers if certain unencrypted regulated data – personal information (PI) – is acquired without authorization. The definition of PI is generally defined as first name or initial and last name, combined with one or more of the following data sets (among others):

- A Social Security number (all states);
- A drivers license number or state identification card number (all states);
- A financial account with the means to access the account (all states);
- Medical information (20 states);
- Health insurance information (16 states);
- Online credentials with the means to access the account (16 states);
- Biometric information (14 states).

The notification obligations are determined by the residential location of the affected consumer. This means that if the affected consumers reside in 17 different states, the statutes of those 17 different states will apply to their affected residents. All of the data breach notification statutes regulate PI in electronic form, and the statutes in 10 states also regulate PI in paper form. While most of the statutes require consumer notification as soon as possible ("most expedient time possible," "without unreasonable delay," "as soon as practicable," etc.), several also require it to be made within a certain time frame (two require it within 30 days, 10 require it within 45 days, two require it within 60 days, and one requires it within 90 days).

Many of the statutes require certain content in the consumer notification, and most require some form of regulatory notification. In some states, if one consumer is notified, a regulatory official (typically the state attorney general) must be notified. In other states, if a numerical threshold of consumers is notified, a regulator must be notified. As an example, under the Montana data breach notification statute, if one Montana resident is notified, the Montana Attorney General must also be notified. In Washington state, if more than 500 Washington state residents are notified, the Washington state Attorney General must also be notified. Note that in addition to the state data breach notification statutes, there may also be notification obligations if an institution is subject to the Health Insurance Portability and Accountability Act (HIPAA), or the payment card industry Data Security Standard (PCI DSS). All this indicates that the assessment of and compliance with consumer and regulatory notification obligations can be somewhat complex.

Tips for Prevention and Response

Defending against ransomware attacks should be part of every information security program. In addition to various risk-based information security frameworks that must be employed to protect against general online threats, there are a few specific measures that can be taken to defend against ransomware attacks:

- A system should be deployed for creating backups, checking backups, and restoring backups of all vital applications and data in a separate and secure location. Ideally, backups should be "gapped" to ensure they cannot be accessed or corrupted by a malicious attacker.
- A system should be deployed for creating and maintaining a gapped golden image so that, if necessary, it can be uploaded with backups in the event a system is encrypted.
- Anti-malware tools should be continuously deployed;
- Endpoint monitoring tools, with strong data analytics used in a heuristic manner, should be continuously deployed to detect and quarantine ransomware and other malware;
- A system should be deployed for continuous and timely patch management;
- Ensure the acquisition of appropriate cyber insurance. Risk cannot be completely mitigated with technology. There will always be residual economic risk which should be mitigated by the acquisition of appropriate cyber insurance.

Responses to ransomware attacks should involve the following actions:

- Contact your cyber insurance broker/carrier immediately. Your cyber insurance carrier has critical resources available to you and those resources (forensics, consumer remediation, and legal) can guide you through the entire response process.
- Do not initiate contact with the attacker from your .edu domain. Attackers often do not know the identity of their victims – they may only know their IP addresses. It is important that you not reveal your identity to the attacker as the information may result in higher ransom demands or further damage to your infrastructure.
- Do not disclose information about your network infrastructure. Information pertaining to your infrastructure may result in higher ransom demands. If the incident is not yet fully contained, it may also result in further damage to your network infrastructure.
- Do not pay ransom without exhausting other resources for decryption keys. Decryption keys for some ransomware variants exist in the public domain, are maintained by digital forensics firms, or are maintained by the FBI. Decryption keys should be sought in all available sources before paying ransom for them.
- Do not pay ransom directly to the attacker. Use a vetted third party that has established protocols for compliance with U.S. Treasury regulations pertaining to anti-money laundering and foreign asset laws.
- Engage appropriate forensics resources. It is important to deploy appropriate forensic resources to detect and remove the malware before the system is returned to operational status.

- If ransom is paid for a decryption key, ensure that the key is analyzed by appropriate forensics resources to determine if it properly decrypts, does not contain malware, and is otherwise safe to deploy in your network.
- Do not wipe digital devices without obtaining forensic image. It is important to gather forensics evidence before rebuilding the network. The forensics evidence may help to determine how and when the attack happened, what the malware was designed to do, and whether sensitive evidence was accessed or acquired without authorization.
- Do not enable operations without identifying and securing vulnerabilities – or clearing all end points. It is important that the environment be free of malware before it is returned to operational status to prevent reinfection.
- Do not make unnecessary public statements. It is important to not make unnecessary public statements that may reveal your identity to the attacker. The best course of action is to work with legal counsel to draft internal and external messaging that will comply with your legal obligations while simultaneously protecting your institution's best interests.

Defending against email account compromises should be part of every information security program. In addition to various risk-based information security frameworks that must be employed to protect against general online threats, there are a few specific measures that can be taken to defend against email account compromises:

- Multi-factor authentication is essential to protect email accounts and should be deployed. In addition to requiring a user name and a password to access an email account, multi-factor authentication requires at least one additional piece of information to access the account. This requires authorized individuals to utilize both something they "know," such as a user name and password, with something they "have," such as a unique code sent to the authorized user's smart phone, or something they "are," such as a fingerprint or other biometric measurement, in order to gain access to the account. The concept of multi-factor authentication is to provide a secondary level of protection in order to validate online accounts beyond solely a username and password. Multi-factor authentication tools help prevent malicious actors from hijacking email accounts and using them for malicious purposes.
- Audit logging must be deployed. It is important to note that in some email platforms, audit logging is not enabled by default, so users must actively enable it for added security. Log retention schedules should be extended to at least 90 days, and then archived for up to 12 months, if possible.
- Domain-based Message Authentication, Reporting & Conformance (DMARC) should be deployed on the domain of the organization so that emails attempting to spoof the actual domain are blocked from delivery.
- External message flagging should be deployed, so that users will always have notice that a message is from an external source.
- Use complex passwords of at least 12 characters or more. The longer the password, assuming some complexity, the more difficult it is to compromise.

Responses to email account compromises should involve immediately disabling of any unauthorized connection, immediately changing the user password, the deployment of multi-

factor authentication if it was not previously deployed, and the preservation of evidence in the account.

Responses to fraudulent wire transfers must occur immediately. Although billions of dollars have been lost to criminals in the past few years through fraudulent money transfers, that trend does not have to continue. If colleges and universities are able to detect a fraudulent money transfer within 72 hours of the initial transmission, a process called the Financial Fraud Kill Chain (FFKC) can be initiated in an attempt to stop the transfer. Although the funds are not always recoverable, even if the kill chain is initiated within the 72 hour window, it is far more likely to occur than if an attempt is made outside that window.

The FFKC utilizes a relationship between the FBI, the Financial Crimes Enforcement Network (FinCEN), and the Egmont Group, to help stop the fraudulent international transfer of funds by criminals. The FFKC is intended to be utilized as a means for U.S. financial institutions to obtain the return of victim funds. The FFKC can be used if the fraudulent wire transfer meets all of the following:

- The wire transfer is $50,000 or more;
- The wire transfer is international;
- A SWIFT recall notice has been initiated; and
- The wire transfer occurred within the last 72 hours.

If the wire transfer does not meet the above criteria, **it should still be reported to the FBI as soon as it is detected.** The FBI may be able to aggregate details of the matter with other investigations to recover the funds and/or hold malicious actors accountable.

To initiate the FFKC process, upon detection of a fraudulent money transfer, a complaint with the Internet Crime Complaint Center (IC3) should be filed immediately, which can be done online at https://complaint.ic3.gov/default.aspx. If possible, the following information should be provided in the complaint:

- Victim business name and address;
- Transaction type (i.e. wire transfer), amount and date;
- Victim bank (i.e. originating bank) name and address;
- Victim bank account and routing number;
- Recipient bank (i.e. beneficiary bank) name and address;
- Recipient bank name and address;
- Recipient bank account and routing number;
- Recipient bank SWIFT number; and
- Summary of the incident.

The more information that is provided about the incident, the more effectively the FBI can respond. As soon as the report is filed with IC3, an FBI agent in the geographic jurisdiction of the victim bank should be contacted and provided with the IC3 report and any other relevant details. The FBI can then interact with the victim bank to ensure everything is done to recover the funds.

The criminals do not have to win the cybersecurity battles. With appropriate preparation, colleges and universities can effectively respond to malicious attacks and protect the digital assets required for their critical educational missions.