MARSH

HOOK, LINE AND SINKER: HOW TO AVOID BEING CAUGHT IN A PHISHING SCAM

MARCH 05, 2020

MARSH & McLENNAN COMPANIES

Overview

- What is data privacy and security
- What is ransomware and why is it such a problem?
  - Review of college cyber events
- What are social engineering and phishing attacks?
  - Review of education industry cyber events
- What are the risks to my institution?
- What can my institution do to protect ourselves from bad agents?
- Risk Mitigation
- Incident response handling

Data privacy and security

- Data privacy and security are often neglected in normal course of business.
- People may feel it's “too difficult” or “too time-consuming” to take extra steps to ensure information is protected.
- Institutions may weigh costs and benefits without taking into account the full range of risks.
- Today, all institutions need to realize the implications of collecting information from consumers: the types and amounts of information, and the state and federal law associated with collecting, using, and disposing of this information. IT MATTERS!

Data Privacy and Security

Cyber attackers often view colleges and universities as easy targets. The open, collaborative nature of most campuses – lead to security headaches

Higher education networks are plagued by unique security challenges, such as homegrown hackers, network visitors, countless personal devices and decentralized control centers comprised of potentially incompatible products and applications from various vendors.

RANSOMWARE

What is ransomware and why is it such a problem?

- What it is.
  - Ransomware is a type of malicious software that typically encrypts a victim's data or network accessibility to data so that the victim can't use it for their ongoing business and operational functions.
  - To decrypt the data or environment, the bad actor usually makes a ransom demand in the form of a cryptocurrency, such as bitcoin, in exchange for a decryption tool.

- How it works
  - Ransomware attacks are typically carried out through email phishing. Malware is deployed into a victim's computer system through a malicious attachment or embedded link within an email.
  - Once deployed, the ransomware moves quickly throughout the computer system, identifying key system components and data files, including any available backup files on the computer system, and encrypting those files to prevent access and cause business disruption.

“

More than 103 state and municipal governments and agencies, 759 healthcare providers and 86 universities, colleges and school districts nationwide were victims of ransomware in 2019.

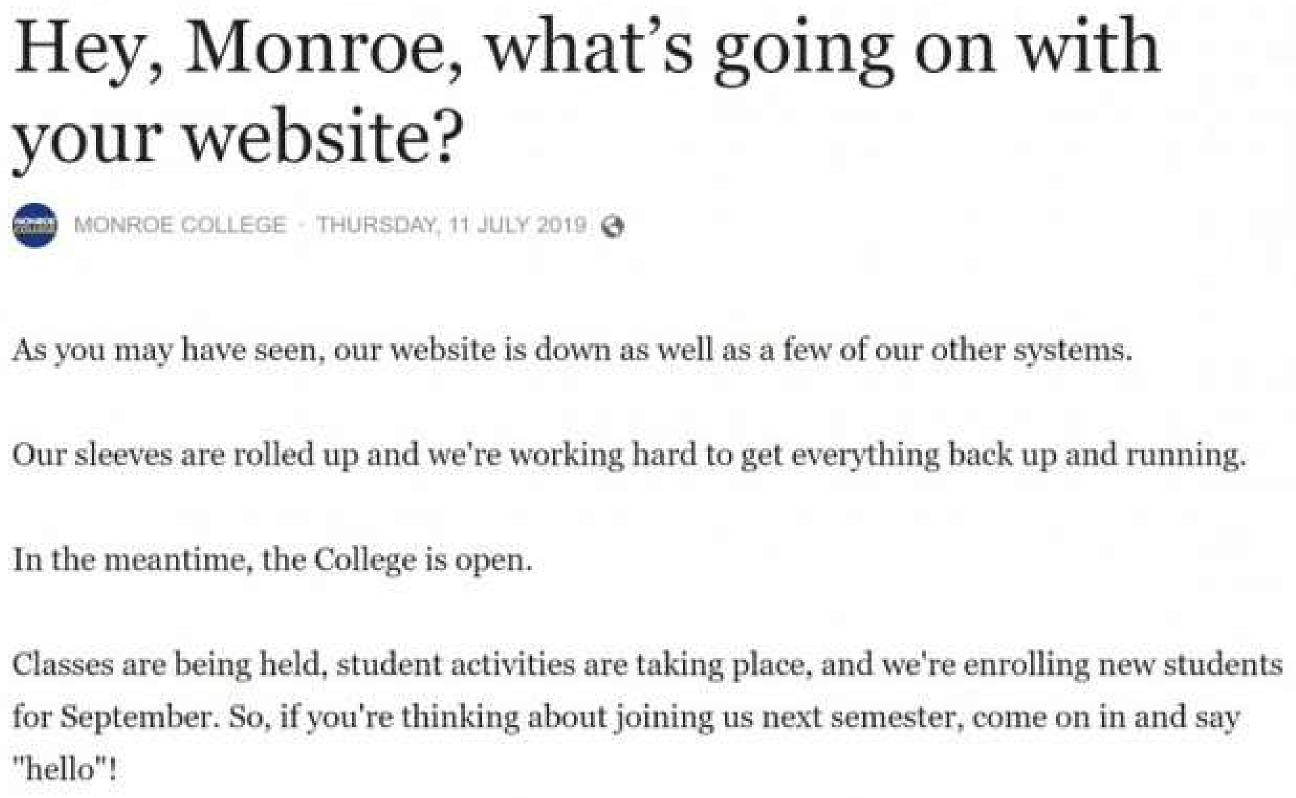
”

#Privacy: Study informs institutions about ransomware strain vulnerabilities

3rd February 2020 by Stephen White in News

Two Florida cities, Lake City and Riviera Beach, acknowledged making a combined $1 million in ransom payments to hackers.

What’s happening to our institutions?



Hey, Monroe, what’s going on with your website?

MONROE COLLEGE · THURSDAY, 11 JULY 2019

As you may have seen, our website is down as well as a few of our other systems.

Our sleeves are rolled up and we're working hard to get everything back up and running.

In the meantime, the College is open.

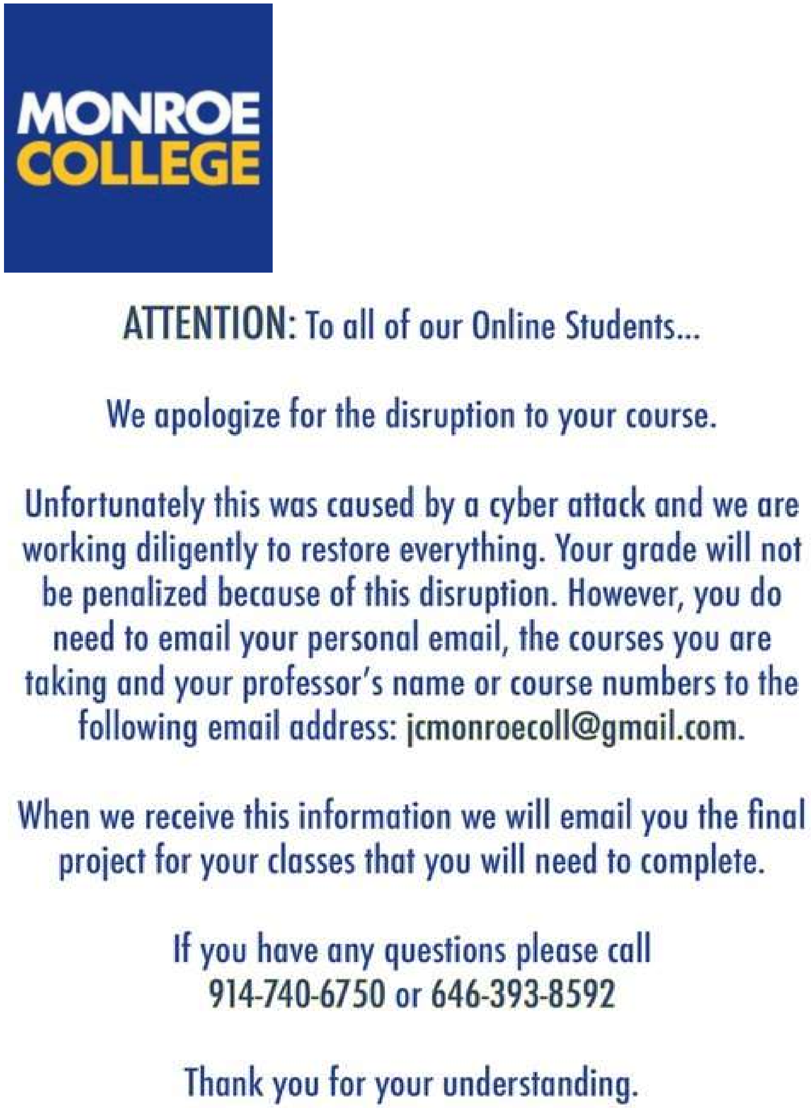
Classes are being held, student activities are taking place, and we're enrolling new students for September. So, if you're thinking about joining us next semester, come on in and say "hello"!

Business Interruption

Hackers Demand $2 Million From Monroe

- College’s IT system was attacked by hackers demanding $2 million in Bitcoin. Experts warn that other institutions are vulnerable to similar attacks.

> *“They scope out the size of the institution and its ability to pay the ransom,” said Phipps. “They’re determining your pain threshold.*



MONROE COLLEGE

ATTENTION: To all of our Online Students...

We apologize for the disruption to your course.

Unfortunately this was caused by a cyber attack and we are working diligently to restore everything. Your grade will not be penalized because of this disruption. However, you do need to email your personal email, the courses you are taking and your professor’s name or course numbers to the following email address: jcmonroecoll@gmail.com.

When we receive this information we will email you the final project for your classes that you will need to complete.

If you have any questions please call
914-740-6750 or 646-393-8592

Thank you for your understanding.

Monroe is notable because of the large ransom the hackers are demanding from the college.

- Michael Corn, chief information security officer at the University of California San Diego, said crippling ransomware attacks like the one Monroe College experienced are the “exception and not the rule.”

higher education institutions should be doing more to prevent and prepare for these kinds of attacks.

Grinnell, Oberlin and Hamilton applicants ransomed over hacked application info – March 8, 2019

- Applicants at three private colleges -- reportedly received ransom notes from hackers claiming to have accessed their application files
- The allegedly hacked data included personal information as well as notes from admissions' officers, their interview reports and acceptance decisions
- The hackers asked for $3,890 in bitcoin payments, but later lowered the amount to $60, according to emails posted on Twitter and Reddit.

On Twitter, Grinnell advised applicants not to respond to the emails. "We have contacted appropriate authorities, including the Federal Bureau of Investigation," it noted.

Niagara University to reopen Friday following **ransomware attack**

Niagara University canceled all classes Thursday, one day after officials discovered the school was the victim of a ransomware attack. Feb. 13, 2020

Niagara University

Two schools, two ransomware attack and two different outcomes.

The Allegheny Intermediate Unit school system

- A regional public education agency that is part of Pennsylvania’s public education system, reported that portions of its network recently were hit with ransomware with the attackers demanding a ransom payment to restore the files.
- The school system refused to pay the unnamed amount.
- AIU hired an outside security firm to lock down and restore the system using back up files.

“The AIU had backup versions of the most critical information and was able to restore access to the vast majority of the impacted files without engaging or paying the intruder…AIU Interim Director

The University of Maastricht

- Unable to recover from a December 24, 2019 attack
- The university hired the security firm Fox-IT which traced the attack to the cybergang TA505 who used a phishing email most likely containing a malicious document to download the malware.
- The school reported that the lost data contained student and scientific work and the overall damage to the institution was very severe.
- The school considered rebuilding its system from scratch, but in the end opted to pay the 30 bitcoin ransom, or about $300,000.

Bad actors are becoming more sophisticated with targeted ransomware strains.

Bitpaymer & Ryuk

- Ryuk accounts for 50% of known variants we have seen in 2019.

- Bitpaymer and Ryuk are two strains of ransomware that have been impacting computer systems since 2018.

- **How they work.**
  - A "banking Trojan" type of malware, like TrickBot or Emotet, infiltrates the victim's system through an open remote desktop protocol (RDP) access point or a phishing email.
  - The malware then allows the bad actor to see sensitive information in the victim's system such as financial statements, which demonstrate the victim's ability to pay the ransom.

Sodinokibi: Evolution in Ransomwar

- **What it is.**
  - Sodinokibi appears to be the evolution of Bitpaymer and Ryuk and emerged in April/May 2019.
  - Like the earlier variants of ransomware, Sodinokibi specifically targets its victims and demands larger-than average ransoms

- **How it works.**

- Sodinokibi is unique in that it targets Managed Service Providers (MSPs), which provide IT services to various other organizations.

- This type of ransomware infects its victims through mass phishing campaigns with malicious links or attachments, open remote desktop protocols, as well as using compromised system credentials.

- Once inside the MSP's system, the bad actor drops the malware into the victim's network infrastructure, infecting its customers' systems as well.

“

The combined impact of human error and targeted phishing campaigns mean that many more institutions have been affected, even as awareness of cyber risks increases.

”

Advisen - Quarterly Cyber Risk Trends:
Global Fraud is Still on the Rise

“WE STILL SEE THOSE INSTITUTIONS THAT SAY

‘I NEVER THOUGHT IT WOULD HAPPEN TO ME,”

Dom Paci, director of global breach at CyberScout

500+ Schools Have Been Affected by Ransomware in 2019

- A new report found in the past two weeks, 15 school districts made up of over 100 K-12 schools have been hit by ransomware attacks. Universities are also being targeted…*Campus Safety, October 04, 2019*

RANSOMWARE ATTACK
You only have 3 days to submit the payment, or your files will be lost.
Time Left

Cybersecurity firm Armor found and tracked ransomware infections at 54 educational institutions, including school districts and universities

Over a two week period in 2019

- 15 school districts comprised of over 100 K-12 schools have been hit
- Of the 15 incidents, five were caused by the Ryuk ransomware, one of the most active ransomware strains today.

Where is it happening?

- Overall, Connecticut was the most compromised state in 2019 with ransomware hitting seven school districts
- Crowder College in Neosho, Mo., is believed to have received the highest ransomware demanding $1.6 million to provide the district with means to decrypt its systems.

Districts affected over the two week period

- Ava R-I School District – Ava, Mo.
- Wallenpaupack Area School District – Hawley, Penn.
- Mad River Local Schools – Riverside, Ohio
- Papillion-La Vista Comm. Schools – Papillion, Neb.
- Rockford Public Schools – Rockford, Ill.
- Souderton Area School District – Lansdale, Penn.
- Wakulla County School District – Crawfordville, Fla.
- Jackson County School District – Marianna, Fla.
- Wyoming Area School District – Exeter, Penn.
- Mobile County School District – Mobile, Ala.
- Houston County Board of Education – Perry, Ga.
- Guthrie Public Schools – Guthrie, Okla.
- Smyth County Public Schools – Saint Marion, Va.
- Northshore School District – Bothell, Wash

The report also provides some trends it has seen develop in 2019, including:

- Attacks through managed service providers (MSPs) are on the rise
- Cyber insurance is becoming more popular, making insured entities more likely to pay demands which result in ransomware being more profitable
- Ransom demands are getting bigger, partly attributed to the increase in cyber insurance
- Email and attachments continue to be the attack vectors of choic

Username
Password
Phishing

What are social engineering and phishing attacks?

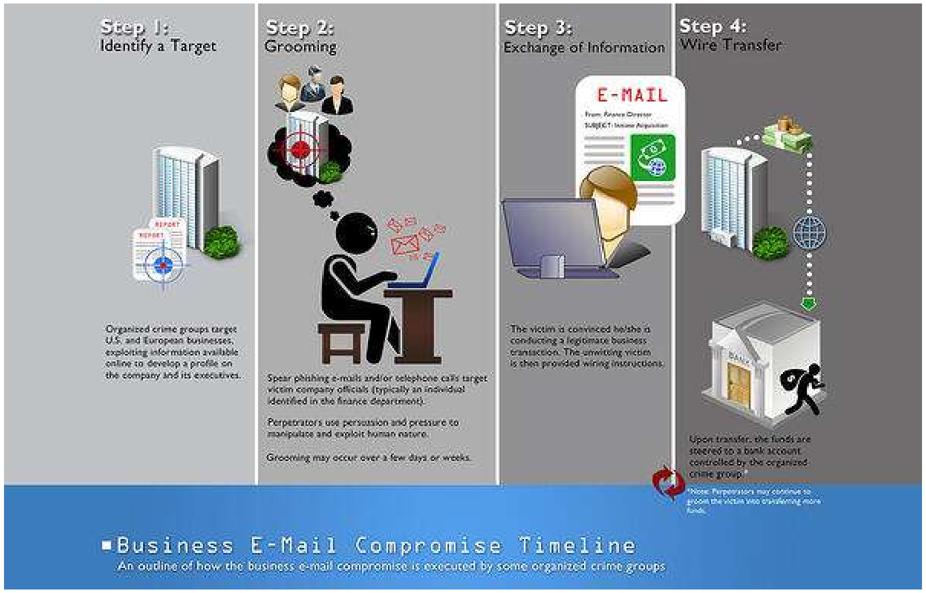
- Social Engineering
  - This type of attack often comes in the form of a phone call or physical conversation where a person is manipulating the conversation to extract certain information that they are looking for.
- Phishing
  - Phishing is a type of social engineering tactic that tricks a person into doing something in order for an attacker to gain knowledge or access to leverage information or an account.

Business email compromise attacks (BEC)

- A form of cyber crime which use email fraud to attack commercial, Government and non-profit organizations to achieve a specific outcome which negatively impacts the target organization.

- Examples of common BEC attacks include invoice scams and spear phishing spoof attacks which are designed to gather data for other criminal activities.

- Often consumer privacy breaches occur as a results of a BEC attack.



Step 1: Identify a Target

Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

Step 2: Grooming

Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).

Perpetrators use persuasion and pressure to manipulate and exploit human nature.

Grooming may occur over a few days or weeks.

Step 3: Exchange of Information

The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4: Wire Transfer

Upon transfer, the funds are steered to a bank account controlled by the organized crime group.*

*Note: Perpetrators may continue to groom the victim into transferring more funds.

▪Business E-Mail Compromise Timeline

An outline of how the business e-mail compromise is executed by some organized crime groups

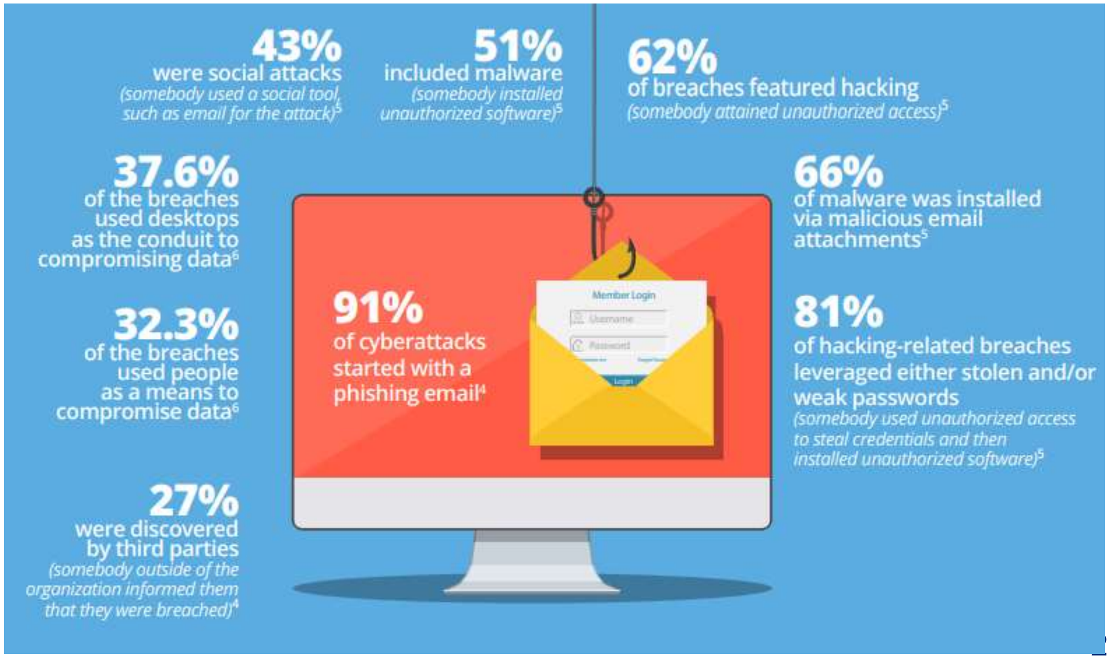
Texas School District Loses $2.3 Million to Phishing Scam, BEC

- Manor Independent School District (MISD) in Texas is investigating an email phishing attack after a series of seemingly normal school-vendor transactions resulted in the loss of an estimated US$2.3 million.
- According to the statement posted on Twitter, the district is cooperating with the Manor Police Department and the Federal Bureau of Investigation (FBI), and encouraged the community to share any information related to the incident.

- The attack was done across three separate transactions, with the cybercriminals contacting multiple individuals in the district from November to December.
- Failing to recognize that the bank information was changed, one email recipient responded and followed through with the transactions before recognizing that it was a fraudulent bank account.

Other headlines…..

- US$1.7 Million Stolen From North Carolina County After BEC Scammers Posed as Contractor, August 1, 2019
  - Cabarrus County, North Carolina, announced that it lost US$1.7 million to a BEC scam after a series of email exchanges that began in November 2018.
  - US$2.5 million was initially deposited to the scammers' bank account, but the county was able to recover US$770,000 weeks later after it sought help from its bank.



43% were social attacks (somebody used a social tool, such as email for the attack)[5]

51% included malware (somebody installed unauthorized software)[5]

62% of breaches featured hacking (somebody attained unauthorized access)[5]

37.6% of the breaches used desktops as the conduit to compromising data[6]

66% of malware was installed via malicious email attachments[5]

32.3% of the breaches used people as a means to compromise data[6]

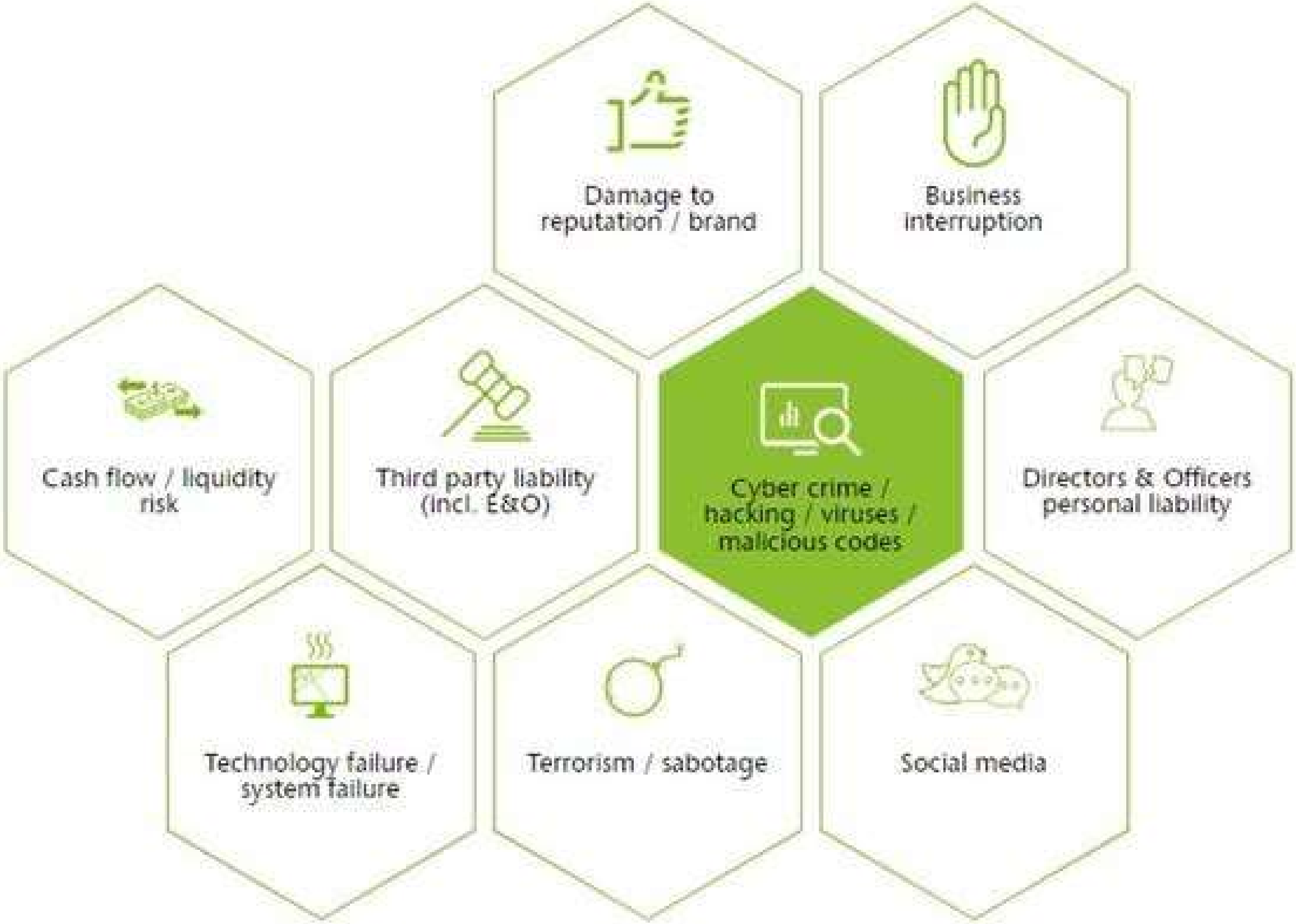
91% of cyberattacks started with a phishing email[4]

81% of hacking-related breaches leveraged either stolen and/or weak passwords (somebody used unauthorized access to steal credentials and then installed unauthorized software)[5]

27% were discovered by third parties (somebody outside of the organization informed them that they were breached)[4]

BACK TO SCHOOL
WELCOME

What are the risks to my institution?



Damage to reputation / brand

Business interruption

Cash flow / liquidity risk

Third party liability (incl. E&O)

Cyber crime / hacking / viruses / malicious codes

Directors & Officers personal liability

Technology failure / system failure

Terrorism / sabotage

Social media

The University’s Role

- Financial Security
  - W-2 forms
  - Credit card transactions
- Ethics and Integrity
  - Cheating and grade modification scandals cause damage to a university’s reputation. To protect an institution’s integrity, IT specialists must keep servers secure from student hackers.
- Regulation Policies
  - Many colleges are home to major research facilities, and many of the studies conducted there are government-funded, and therefore subject to myriad regulatory requirements. Many of these facilities include university hospitals, requiring administrators to follow Health Insurance Portability and Accountability Act guidelines that protect patients and students’ health information.

Faculty and Students’ Responsibility

- **Smart Practices** –
  - Universities must educate faculty and students on how to identify and steer clear of corrupted links – such as phishing scams – and create passwords that are difficult to decode.
- **Personal Devices Care**
  - With the average student bringing seven different devices to campus, colleges have countless unmanaged personal devices to secure. Staff members and students can reduce cyberattack risks by being mindful when signing into public Wi-Fi and avoiding suspicious links.

What can my institution do to protect ourselves from bad agents?

- Almost every analysis of a business-damaging ransomware attack points out the criminals exploited well-known vulnerabilities or failures of basic security hygiene
- Institutions that have been successful in avoiding or mitigating ransomware impact have the same staffing difficulties as everyone else but have focused on enhancing staff skills for effective security operations and the integration of security tools to act as ‘force multipliers’ to increase efficiency
- Damage from ransomware and data theft attacks can be minimized by making sure vulnerability and risk status is accurate and current, critical patches are applied as a priority and that critical functions like backup and restore are available and tested.

Cyber Risk Mitigation

We all rely on being connected at all times

- Special considerations for portable devices and media
  - Encrypt anything electronic
    - Whole disk encryption (laptops/workstations)
    - Thumb drive/USB devices – restrict read/write or encrypt automatically
- Special considerations for the mobile world
  - Mobile devices / handhelds
    - Mobile device management (MDM) tools and software policy restrictions
- Special considerations for cloud computing
  - Third-party contracts
    - Cyber-insurance – Does your cloud provider have it?
    - Who is responsible for loss of your data?

Data protection

- Careful collection and use
  - Ask yourself why you are asking for the information? Is it required? Do you really need the full Social Security number, for example? Could you still collect information and not ask for personal information?
- Storage and retention
  - How many months or years are you required to save? Is there a business need to store or save the data? What procedures exist to destroy the data?
  - Consider proper disposal methods like file shredding and disk destruction
- Access Control
  - This is how your institution controls access to e-mail, applications, company resources like data centers, or even something as simple as file cabinets.
    Access control is also referred to as identity management (IM) or identity and access management (IAM). Know your policy and follow it, for instance, by changing passwords as requested.

What do you need to do?

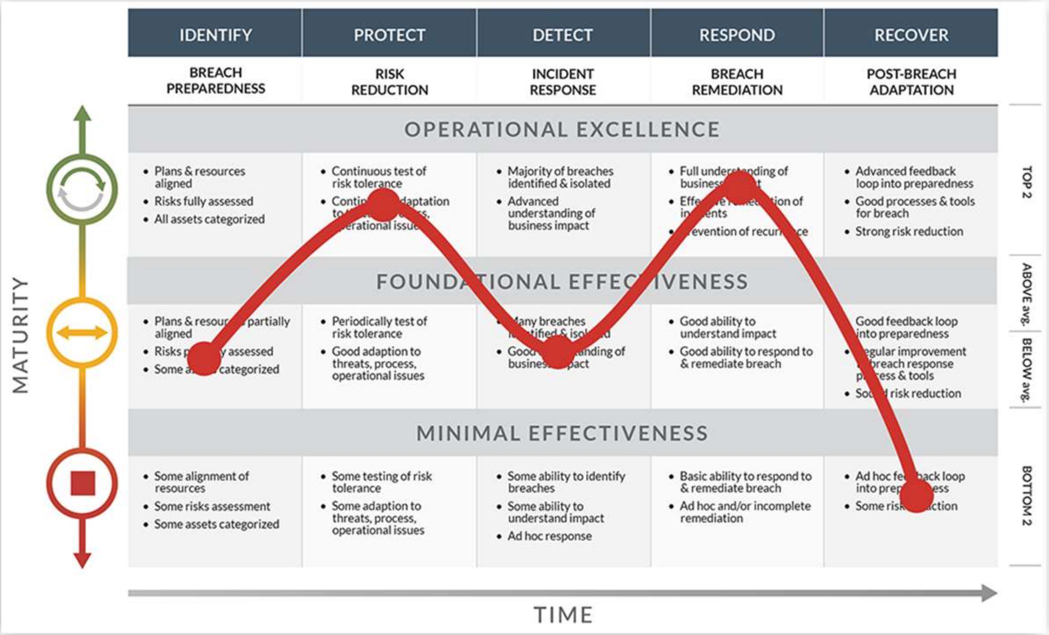
- Understand policies
- Understand the foundations of information access control
- Practice strong password security
- Defend against basic attacks

Your role

- **YOU** are the holder of the keys, which is your password
- Take necessary precautions to ***protect your password***.
  - Never write it down on paper
  - Try to make it hard to guess but something that you will remember
  - Words are vulnerable to dictionary attacks; names of children, pets, spouses can be guessed easily
  - Consider using a small phrase that you can remember with upper and lower case letters, and use special characters or numbers, e.g.,
    - *"I just met you*, *and t*his *is* *craz*y, *b*ut *h*ere's *m*y *number"* could become IjmU&ticbhm#
  - When required to change, don't make it the same as your last password
  - Try not to have the same password for all of your personal and work accounts
- Always ***lock your screen*** when leaving your computer or terminal unattended, it only takes one second!!

Security recommendations

- According to a report by the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN), the amount BEC attackers attempted to steal reached an average of US$301 million per month since 2016.



	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER	
	BREACH PREPAREDNESS	RISK REDUCTION	INCIDENT RESPONSE	BREACH REMEDIATION	POST-BREACH ADAPTATION	
OPERATIONAL EXCELLENCE						
	• Plans & resources aligned • Risks fully assessed • All assets categorized	• Continuous test of risk tolerance • Continuous adaptation to threats, process, operational issues	• Majority of breaches identified & isolated • Advanced understanding of business impact	• Full understanding of business impact • Effective remediation of incidents • Prevention of recurrence	• Advanced feedback loop into preparedness • Good processes & tools for breach • Strong risk reduction	TOP 2
FOUNDATIONAL EFFECTIVENESS						
	• Plans & resources partially aligned • Risks partially assessed • Some assets categorized	• Periodically test of risk tolerance • Good adaption to threats, process, operational issues	• Many breaches identified & isolated • Good understanding of business impact	• Good ability to understand impact • Good ability to respond to & remediate breach	• Good feedback loop into preparedness • Regular improvement of breach response process & tools • Sound risk reduction	ABOVE avg. BELOW avg.
MINIMAL EFFECTIVENESS						
	• Some alignment of resources • Some risks assessment • Some assets categorized	• Some testing of risk tolerance • Some adaption to threats, process, operational issues	• Some ability to identify breaches • Some ability to understand impact • Ad hoc response	• Basic ability to respond to & remediate breach • Ad hoc and/or incomplete remediation	• Ad hoc feedback loop into preparedness • Some risk reduction	BOTTOM 2

- To stay one step ahead of BEC attackers, here are some best practices to follow:
  - Employees should always verify fund transfer and account update requests.
  - Emails should always be checked for any red flags. While many BEC attackers try to make their messages appear legitimate, there are many ways to tell if an email is impersonated.
  - institutions should encourage their staff to use two-factor authentication (2FA) to provide an additional layer of security

Detecting phishing emails

- Institutions should implement multiple layers of preventative measures to mitigate the potential of future incidents and have a business continuity plan in place in the event the organization is affected by a ransomware attack

- Keep your backup process consistent and up-to-date
  - A majority of ransomware attacks can be traced back to email phishing where login credentials are compromised or a malicious link is clicked. Therefore, it is vital that employees are trained on how to detect phishing emails and why it’s so important to never click on a link or attachment they do not recognize.

Useful detection tools

- Make sure there is a consistent backup process in place across all systems, that all backups are properly labeled (segregate labels to avoid encryption), and that no matter what form of backup is used, it is segregated from the main system to avoid deletion or encryption by the bad actor.
- Because bad actors are becoming more sophisticated and able to bypass traditional antivirus software, next-generation antivirus (NGAV) protection, which includes endpoint detection and response, can be a useful tool to detect credential-stealing banking Trojans, which are often a precursor to Ryuk and BitPaymer ransomware.

Higher education institutions can take a few key steps to further bolster their defense against hackers:

- **Establish Flexible and Adaptive Security Architectures**
  - Keep costs low and establish a centralized network control center. IT teams should work together with administrators to evaluate which devices do not meet network requirements, map a plan to replace these tools over time and create a timeline to purchase new products that are compatible with other campus devices.

- **Manage Risk and Mitigate Impact**
  - Breaches will happen; it is inevitable. Institutions should concentrate on minimizing the potential harm of cyberattacks before they occur. Instead of the “build higher walls” mentality, focus on developing security controls on the other side of the network wall to reduce the access hackers have to servers once they infiltrate the network. IT teams should establish back-end protection and develop processes that will shorten the amount of time it takes to identify and report an attack.

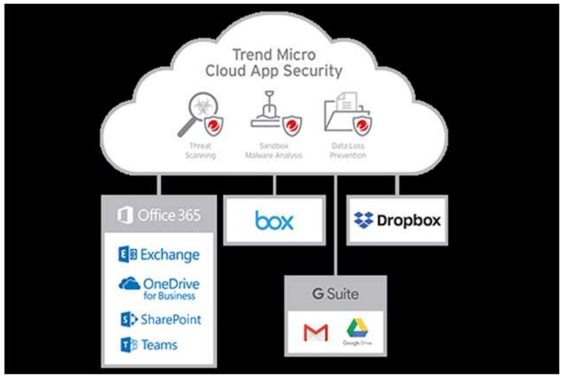
- **Provide Services Securely to Unmanaged Devices**
  - Inform faculty and students about safety guidelines for proper network use on personal devices. IT service departments may also require new students and staff to complete online cybersecurity training, or offer free security/ad-blocking software for personal devices.

Resources

- Earlier this week, Alphabet (Google) launched an interactive phishing quiz website aimed at educating users on the effectiveness of phishing and the specific dangerous elements within an email. Over the past couple of years, companies have looked to mitigate phishing attacks with a number of approaches including hardware-based authentication (e.g. Yubico) and a renewed approach security-oriented training and awareness.
- https://phishingquiz.withgoogle.com/

Advanced technologies to keep fraudsters from stealing money from e-mail based attacks

- Trend Micro™ Cloud App Security
  - Advanced threat and data protection for Office 365, Gmail, and cloud file-sharing services
  - Uncovers ransomware, Business Email Compromise (BEC) and other malicious attacks.

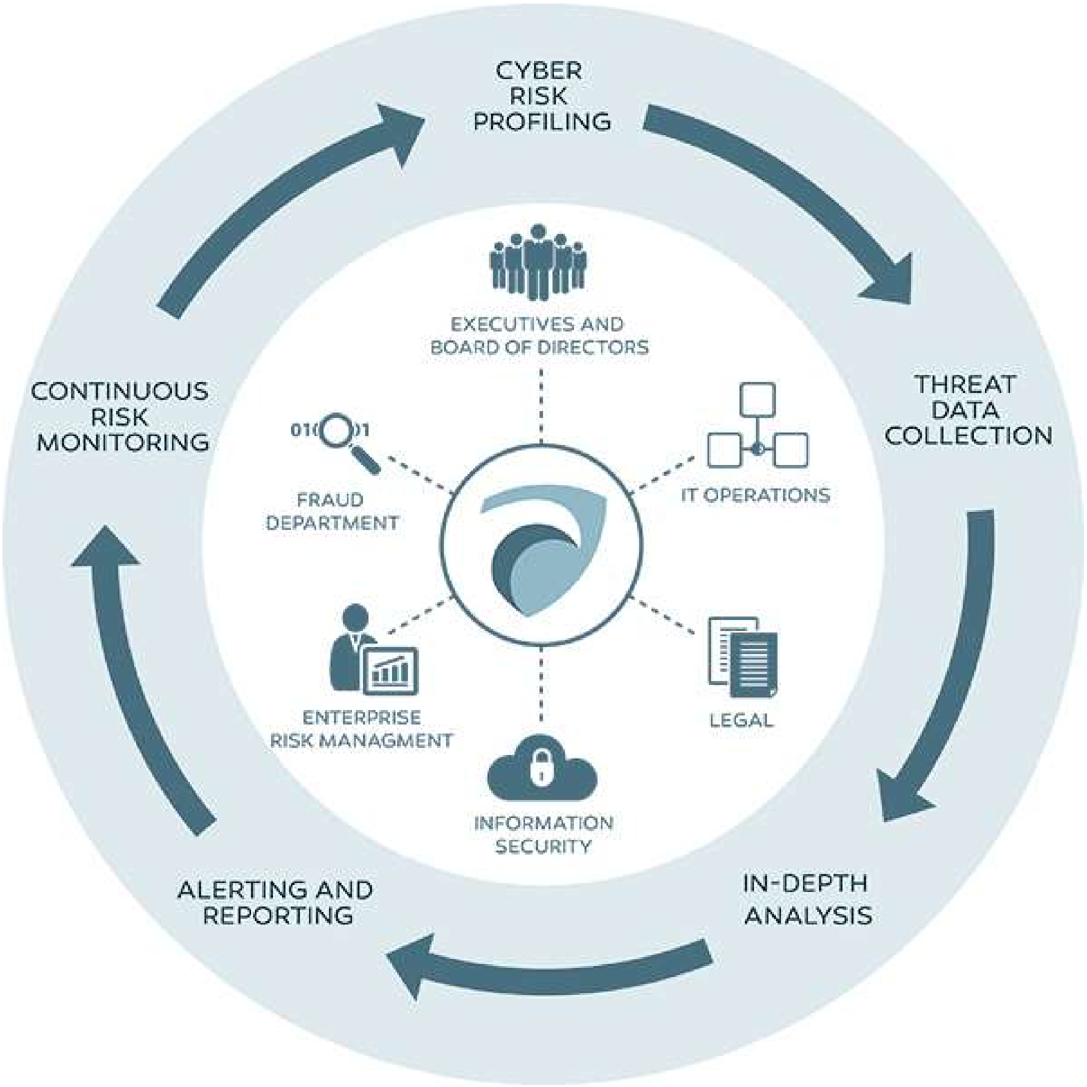


- https://www.trendmicro.com/en_ph/business/products/user-protection/sps/email-and-collaboration/cloud-app-security.html

- ScanMail™ Suite for Microsoft® Exchange™ s
  - tops highly targeted email attacks and spear phishing by using document exploit detection, enhanced web reputation, and sandboxing as part of a custom APT defense—protection you don’t get with other solutions. In addition, only ScanMail blocks traditional malware with email, file, and web reputation technology and correlated global threat intelligence from Trend Micro™ Smart Protection Network™ cloud-based security.
    - https://www.trendmicro.com/en_ph/business/products/user-protection/sps/email-and-collaboration/scanmail-for-exchange.html

Cyber Threat

Risk Mitigation



Incident response handling

- Ideally, your institution already has an incident response plan that covers reporting of and responding to security or privacy incidents.

Every institution is different, but get to know what procedures exist already, what you need to do, and how and when to escalate.

- Report suspected data security or privacy incidents early and often
- All institutions have some form of legal obligation to protect and report security and/or privacy breaches. Often the size and complexity of the breaches can be reduced drastically by more efficient and effective incident response handling.
- Report account lockouts and repeated failed login attempts immediately

- Report suspected information snooping and information disclosures about customers, patients, internal employees, etc.
- Report when sensitive information or IT resources are left unattended
- Report when you get a suspicious e-mail, phone call, or package
- Report when something just doesn't seem right.
  If it doesn't seem right, it probably isn't.

“ To stop the frequency in ransomware, it is recommend institutions implement improved coordination and communication channels between the private sector and law enforcement agencies to ensure impacted entities are aware of the availability of potential solutions and workarounds which may minimize recovery cos ”

Campus Safety, October 4, 2019

```
Ooops, your important files are encrypted.

If you see this text, but d[illegible]e the "Wana Decrypt0r" window,
then your antivirus removed [illegible]crypt software or you deleted
it from your computer.

If you need your files you hav[illegible]to run the decrypt software.

Please find an application fi[illegible]amed "@WanaDecryptor@.exe" in
any folder or restore from[illegible] an[illegible]irus quarantine.

Run and follow the instructions!
```

Risk Mitigation

ESSENTIALS OF RISK MANAGEMENT:
1. DON'T DO ANYTHING WRONG TODAY.
2. DON'T DO ANYTHING WRONG TOMORROW.
3. REPEAT.
ComplexDiscovery
GLASBERGEN
© Randy Glasbergen / glasbergen.com

MARSH