Minimizing Risks and Protection of IT systems and Personal Data

Presented by Stephen J. Cerro, MS, CPSI, ARM
Risk Control Coordinator
Wright Specialty Insurance

Objectives of Cyber-Security

- **Ensure** the confidentiality, integrity, and availability of information.
- **Protect against** any anticipated threat or hazard.
- **Protect against** unauthorized access to a user of information.
- **Ensures** the appropriate management of information throughout the lifecycle.

The Internet & New Technology

- We use it to
  - Make financial decisions
  - Process transactions
  - Keep records
  - For reporting to State and Federal Agencies
  - For academic studies
  - Research

The Internet & New Technology

- This technology is so convenient and wonderful!

- Treasure Trove of Information:

- **But** the technology **increases exposure** to **digital data, personal information, client data, vendor data, student information, social security numbers, financial information, research – and so on…**

Cyber Criminals

- Selling software specifically designed to break into colleges, banks, retailers, law firms, etc., now

- Routinely offer 24-hour help desks and technical support for the unskilled cyber criminal.
  - Breeding ground for all kinds of new and sophisticated cyber attacks.

Malicious Cyber Activity

- Cost: $109,000,000,000!!
  - 2016

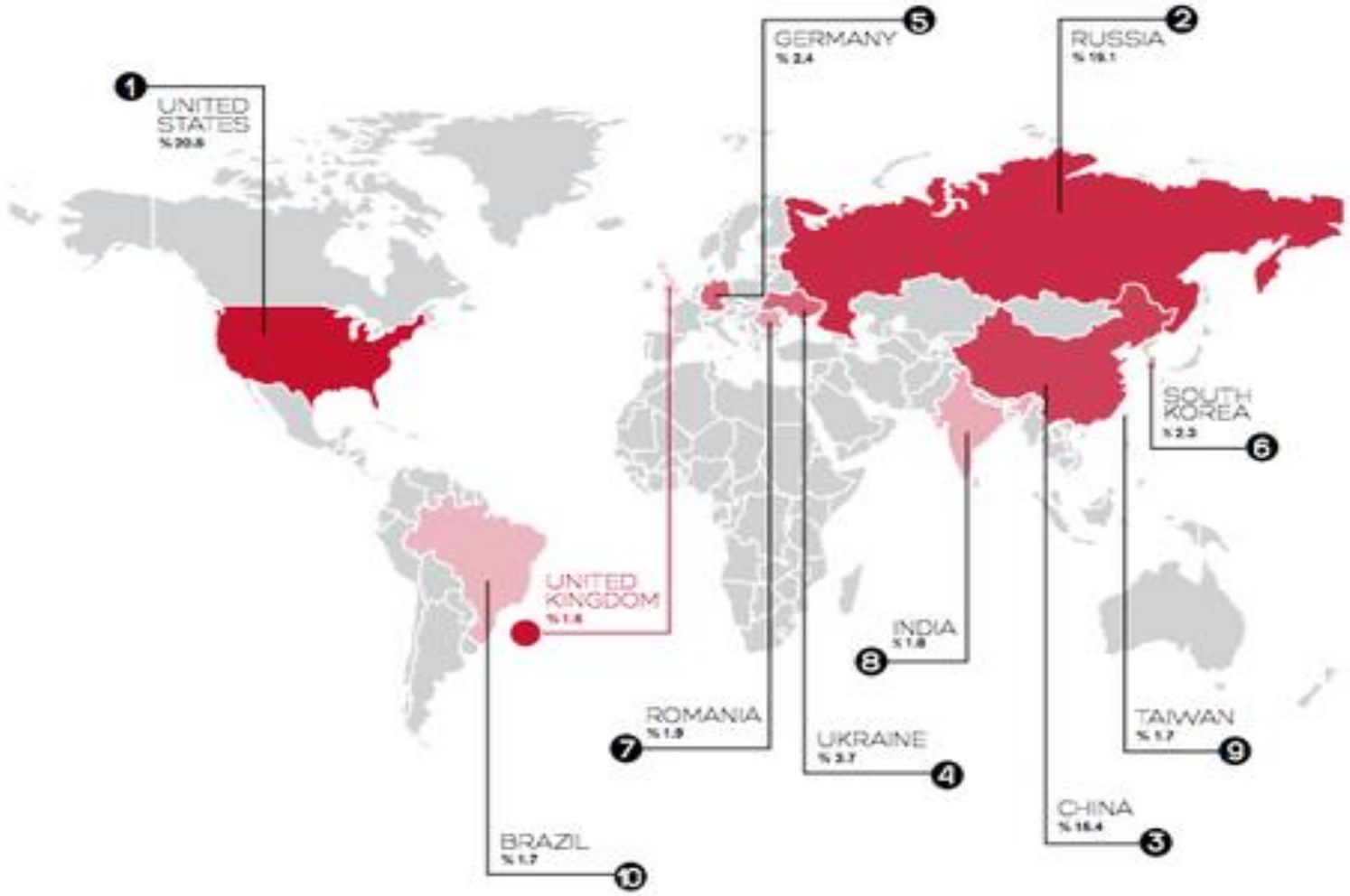
Who leads the World in Generating Hacking Attacks?

- **U.S.A.**
- Russia
- China

Q3 Top 10 Countries

% by country of origin

nccgroup
freedom from doubt



Definition - Data Breach

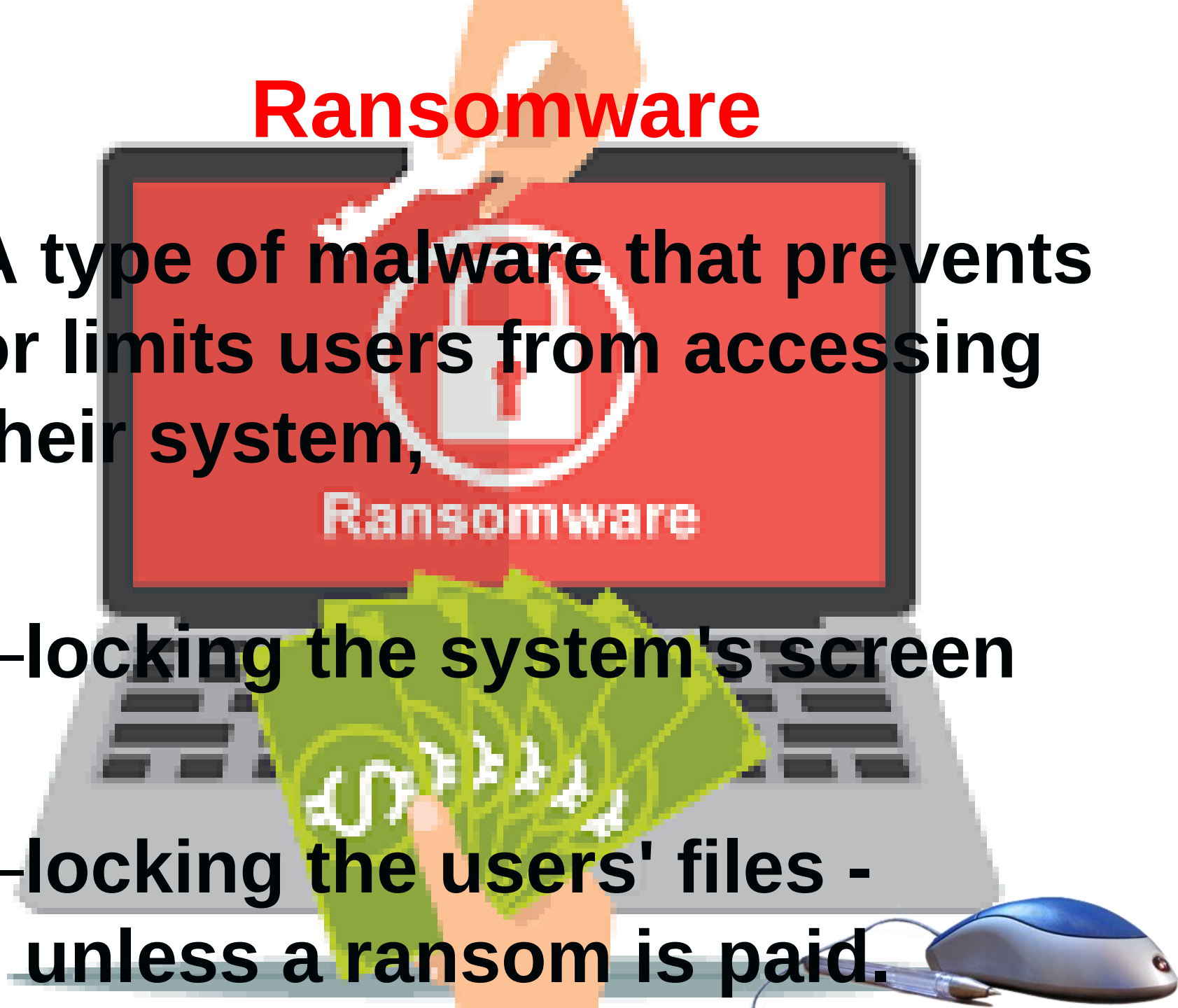
- A **breach** usually involves
  - an individual's name and
  - a medical record and/or
  - a financial record or
  - debit card that is potentially put at risk
  - Can be either in electronic or paper format.

Malware

- Malicious software - an umbrella term used to refer to a variety of forms of hostile or intrusive software
  - computer viruses,
  - worms,
  - Trojan horses,
  - scareware,
  - spyware,
  - adware,
  - Logic bombs
  - Trap Doors
  - ransomware and other malicious programs.
- It can take the form of executable code, scripts, active content, and other software

Ransomware

- A type of malware that prevents or limits users from accessing their system,
  - locking the system's screen
  - locking the users' files - unless a ransom is paid.

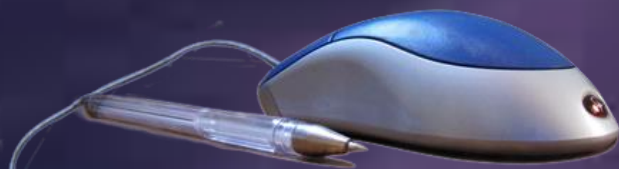


Ransomware

- Crypto-Ransomware, aka: Crypto-Jacking
  - encrypt certain file types on infected systems
  - forces users to pay the ransom through certain online payment methods to get a decrypt key.
  - Bitcoins.
  - iTunes
  - Amazon gift cards.

Ransomware

- SATURN ransomware,
- Software so powerful it can be used to encrypt and completely seal off an organization’s entire database!
- Ransomware-as-a-Service (RaaS),



“Watering Hole” Attacks

- Exploiting weaknesses in the defenses of third parties such as
  - suppliers,
  - sub-contractors,
  - partners, and clients.
- Sit within a compromised IT system, carrying out repeated fraud, siphoning off cash and conducting cyber-espionage.

Dark Patterns

- Tricks used in websites and apps
- Make you buy or sign up for things that you didn't mean to:
  - Bait & Switch
  - Confirmshaming
  - Disguised Ads
  - Forced Continuity
  - Friend Spam
  - Hidden Costs
  - Trick Questions
  - Misdirection
  - Price Comparison Prevention
  - Privacy Zuckering
  - Roach Motel
  - Sneak into Basket

The **Dark Web**

- “Credential Stuffing”

- Hackers throw thousands of email and password combinations at a given site or service until they succeed in breaking in.

- Tesco Bank – “cash milking cow”

Phishing

Phishing

Fraudulent practice of sending emails

Pretending to be from reputable companies or your own company

Induce you to reveal personal information, such as:

- passwords
- credit card numbers

Vulnerabilities

- Cyberattacks - more sophisticated and targeted.

Phishing emails are more difficult to detect.

- Increasingly clicking on phishing links and ignoring warnings.


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
Klossner

Phishing Works Best

- Is simple and effective.
- Often goes undetected.

- Most common - messages designed to trick a user into providing Office 365 account credentials.*

- *Phishing was the attack vector in 37% of the more than 750 incidents that Cleveland-based Baker & Hostetler LLP helped manage in 2018, according to its fifth annual Data Security Incident Response Report 4-5-19

Phishing

A **phone call** or message/an **email** that is designed to convince you to:

- hand over your personal information under false pretenses.
- install malicious software.
- convince you to download something off of a website.

What Does a Phishing E-Mail Look Like?

Hello!

As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Spelling

Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link bellow to fill the Copyright Law form:

http://www.facebook.com/application_form Links in email

Note: If you dont fill the application your account will be permanently blocked. Threats

Regards,

Facebook Copyrights Department. Popular company

Carefully Check It Out

- **If you see a link in a suspicious email message, don't click on it.**

- **Rest your mouse over (but don't click) on the link to see if the address matches the link that was typed in the message.**

https://www.woodgrovebank.com/loginscript/user2.jsp

http://192.168.255.205/wood/index.htm

Phishing Example

- “You have a payment of $500 waiting in your PayPal account! All you have to do is click Here!”

CAMDEN • NEWARK • NEW BRUNSWICK/PISCATAWAY

OFFICE OF INFORMATION TECHNOLOGY

96 Davidson Rd
Piscataway, NJ 08854

Web Mail

Dear Staff, Faculty & Student,

Your recent request to de-activate your mailbox will be processed in the next few hours, this is a confirmation mail, if you believe this was an error or a mistake, kindly see below;

CANCEL REQUEST NOW

Best regards

Additional Sources of Web Mail at UTK.EDU

HIGHER ED

- **54% of attacks to Higher Education!**

Business Email Compromise (BEC)

- Attacker impersonates a high-level executive and attempts to trick an employee or customer into transferring money or sensitive data.

- Contains no malware and goes undetected by traditional security measures.

- “It’s really hard to stop; you can’t stop it with anti-virus or any kind of software, it’s really kind of a human problem.” - Adam Meyers, CrowdStrike

Just This Week

- ***"Team Resources needs your updated bank account and routing information for payroll direct deposit."***
- False origins: payroll leaders and CFO or CEO.
- If you mistakenly take action and respond to these requests, the scammer now has access to your banking information.

Prevention of this type of Phishing Attack

- **Two-factor authentication for external access to all applications,**
- **Educating and training employees about phishing, and**
- **Enforcing strong password/passphrase policies**

Addressing Cyber-Security

Cyber-Security is not just an IT issue

– It is a risk to the Whole Organization, and

– Tackling it is more about

- **People**
- **Behavior**
- **Culture**
  - than it is about technology.

Addressing Risk

Need to treat cyber risk as a

- **Strategic Business Risk**
- **Operational Risk**

- Without change, your vulnerability will only increase ↑

Protecting Data

- We have to take measures to protect it.

- **Cyber-Liability Insurance** will eventually be a core coverage category for everybody

Surprising Fact

- Over half of all data breaches (malicious and accidental) are carried out by

  insiders!

December 2017

Morrison's Supermarkets (UK)

- Found to be vicariously liable for the actions of a rogue employee who,
- driven by a grudge against the supermarket chain,
- took payroll data relating to 100,000 employees and
- published it online!

Who's On The Inside?

People within your own system

- Who are trusted
- Has some level of security clearance
- And – they are **not** a target of these malicious attacks

- Vendors and Contractors

Bring Your Own Device

- BYOD

Pros & Cons of BYOD

- Smartphones, laptops, tablets are part of everyday life and are ingrained in the workforce …

- Pros
  - More productive for employees
  - Saves money when ee use phones check e-mail, synch calendars and make calls.
  - Could save you money.

Pros & Cons of BYOD

- Pros
  - Employees can upgrade when they want.
  - They can work while away from the office.
  - They are happier, more comfortable and more productive.

Pros & Cons of BYOD

- Cons
  - Data ownership
  - Employee relationships w/vendors, contractors, other clients
  - Device liability
  - Legal liability
  - IT support
  - Multiple OS/Plans

Pros & Cons of BYOD

- Cons
  - BYOD is an IT nightmare
    - Cyber breaches need to be defended against
    - Employee training?
  - Hardware/Software compatibility
  - Not updated (installation of updates not done)

What Data Are We Talking About That is Being Compromised?

- PII – Personally Identifiable Information
  - Driver's License
  - Name
  - DOB
  - Social Security Number
  - Address
  - Academic Performance
  - Discipline Records
- Credit Card Numbers
- Financial Account Numbers
- Marketing Plans
- Investment Plans
- Re-routing of direct-deposits into unauthorized accounts
- PHI – Personal Health Information
- Student records

How do we Lose Data?

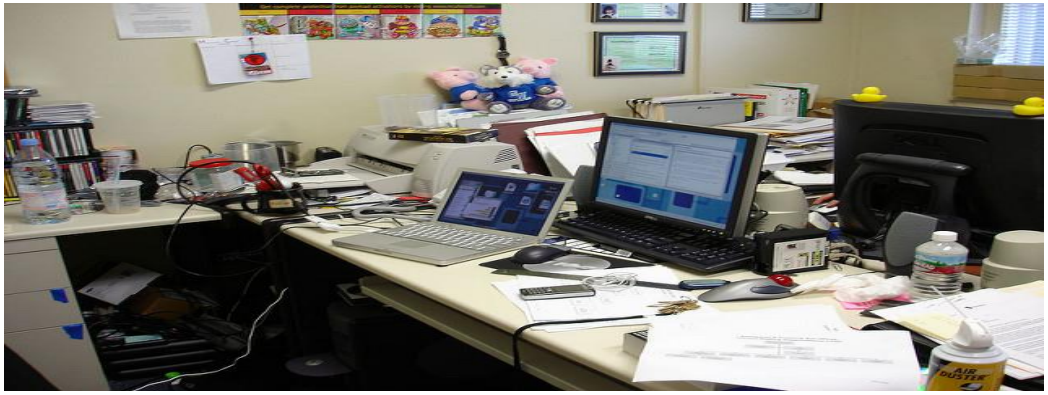
- Can result from a simple mistake
  - **Lost tablet or laptop**
  - Lost cellphone
  - Lost flashdrive
  - Lost other mobile device
  - Inadvertent or Administrative Error
  - Clicking on ….
  - Misconfiguration of Permissions on Shared File Server(s)

How do we Lose Data?

- Can result from improper disposal
  - Hardcopy in the dumpster
  - Paper
  - Backup tapes or discs

How do we Lose Data?

- Can result from sloppy housekeeping
- Messy desks



- Leaving flashdrives on your desk

Leaving files, photos and paper documents next to copy machine

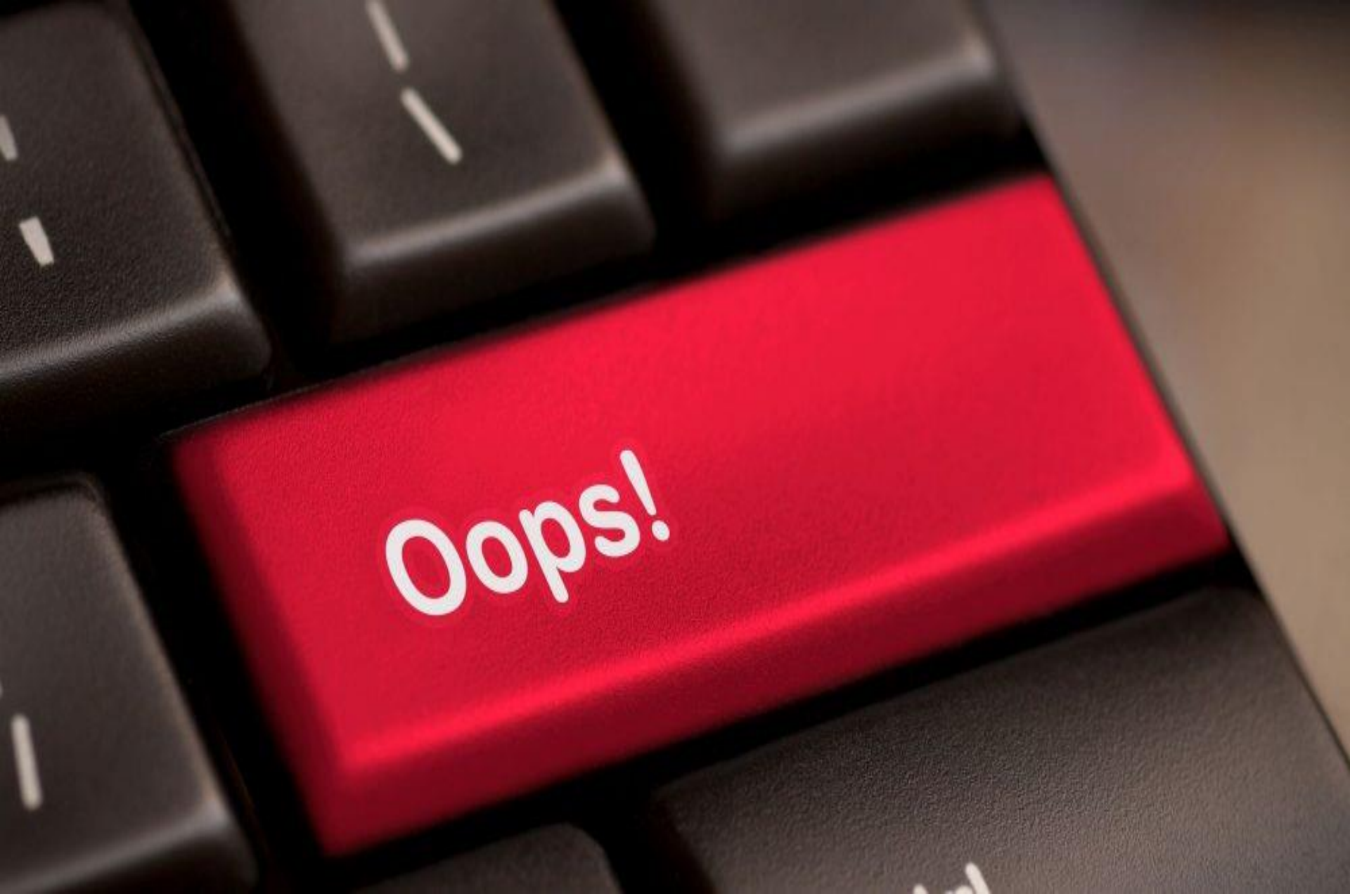
"Thought I'd run off a couple of resumés while the boss is out."

How do we Lose Data?

- What about storage on printers and copiers?
  - Must also be wiped clean before disposal
- Computer hard drives
  - Clean up
  - Wipe out/Erase them

How do we Lose Data?

- Leaving your computer open
- Leaving your door unlocked
- Leaving your computer behind


Oops!

How do we Lose Data?

- **The Accidental E-mail**

- Regular mail

Easy to Remember = Easy to Hack

"Hackers have great success using

- celebrity names,
- pop culture terms,
- sports, and
- simple keyboard patterns to break into accounts online because they know so many people are using those easy-to-remember combinations."

– Splashdata CEO Morgan Slain

Worst PasswOrds of 2018

- 1. 123456
- 2. password
- 3. 123456789
- 4. 12345678
- 5. 12345
- 6**. 111111**
- 7. 1234567
- 8. **sunshine**
- 9. qwerty
- 10. iloveyou
- 11**. princess**
- 12. admin
- 13. welcome
- 14**. 666666**
- 15. abc123
- 16. football
- 17. 123123
- 18. monkey
- 19**. 654321**
- 20**. !@#$%^&***

How Widespread is the Risk?

- Number of sensitive personal records compromised from Jan. 2005 – Oct. 2012 → About 563,656,459
- 2016 – More than 4.2 billion (4,200,000,000) worldwide!
- 2018 – More than 4.5 billion (4,500,000,000) worldwide!

In the first 6 months!

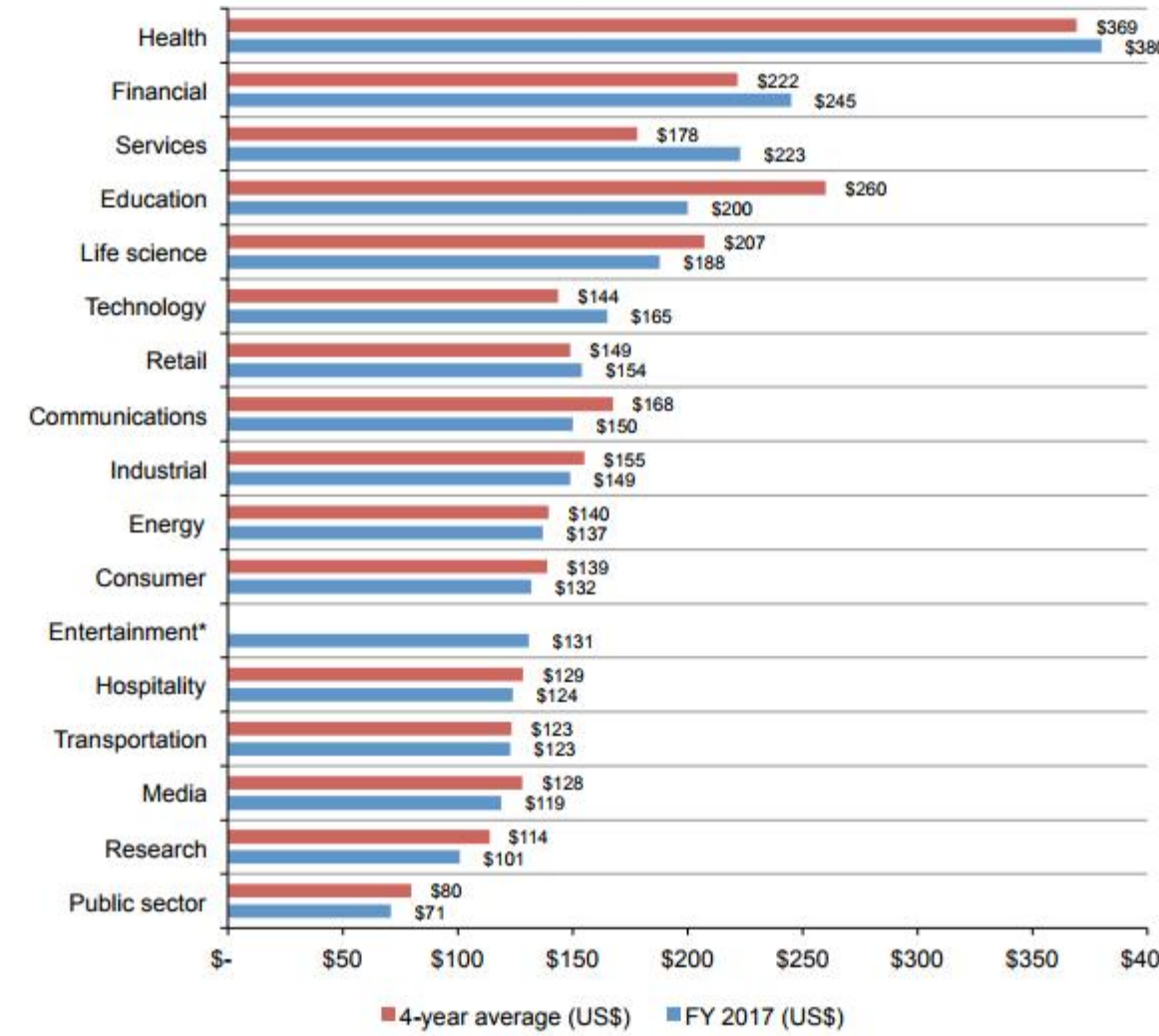
How Much Does Data Breach Cost?

- $3.86 million/data breach
- $148 per lost or stolen record
- 27.7% chance of the data breach recurring over the next two years

Figure 5. Per capita cost by industry classification

*Historical data are not available for all years

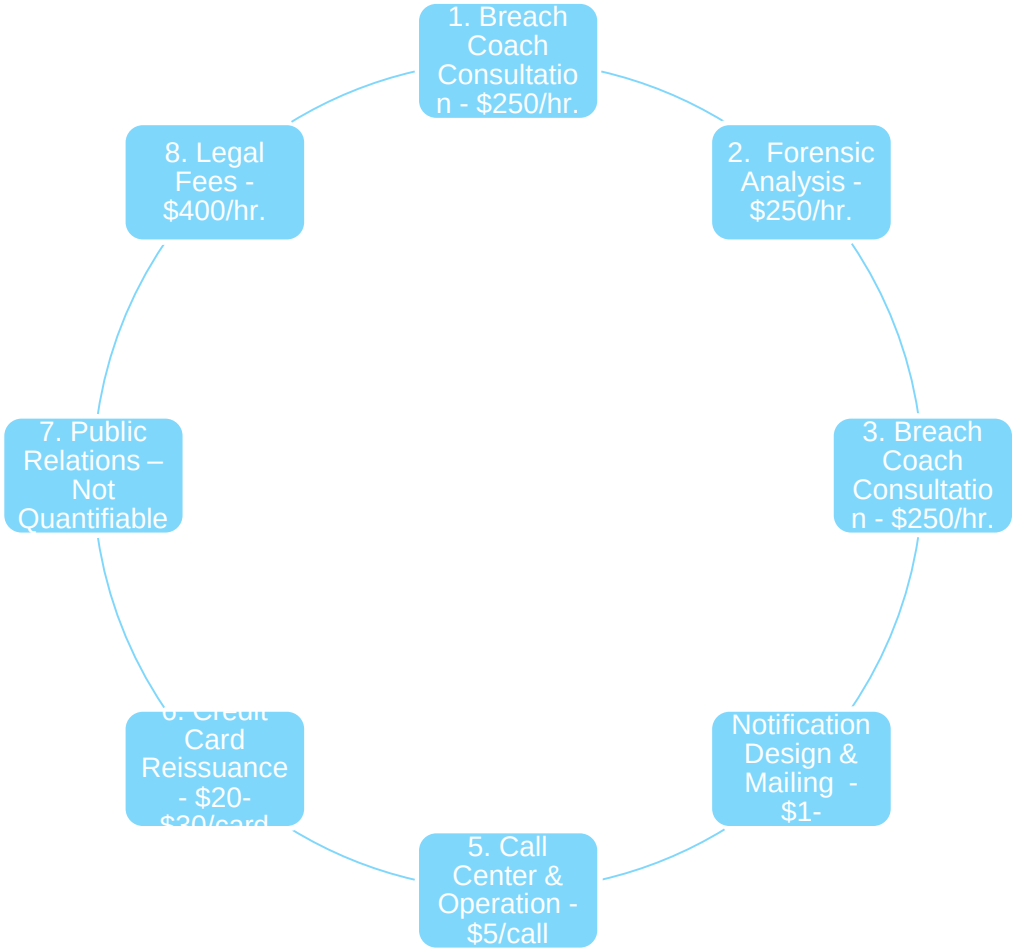
Measured in US$



Cascading Damage

1. Hacker Attacks an Unprotected Network
2. Network Outage-Loss of Data-Theft of Employee &/or Student Info.
3. Loss of Revenue
4. Legal Liability & Lawsuit: Loss of Trust
5. Loss of Funds

The Data Breach Cost Response Cycle



Additional Costs

- Public Relations
- Technology Changes
- Staff Retraining
- Reward Expense
- Extortion Demands
- Replacing Stolen Funds or Securities

Solutions

- **Clear understanding** of how the threats can affect every part of your organization's business – not just IT technology infrastructure.

- Keep your Anti-Virus **up-to-date**.
- **Think before you act**.
- **Review** your privacy settings – websites

Solutions

- Keep your personal information, private.

- Only **unsubscribe** from e-mails and websites that you have or are doing business with.
  - Let the others go to junk mail or trash.

Solutions

- Never save any passwords in your browser or cache, and

- Take advantage of any and all software and firmware updates.

Solutions

- **Never plug** in an **unknown** flash drive.
- **Scan** removable media for viruses **before opening files.**
- **Lock** or power down your computer when your away from it.
- **Never click** on a link **unless you know** the source or e-mail to be valid.

Solutions

- The IT Dept. will **never ask for a password via e-mail.**
- You should **never provide a password** via e-mail.
- When you receive an unusual request or one for funds transfer, **call** the individual or create a new e-mail to verify.
- **Hover your mouse** over the web address – if the address looks odd, don't click on it.

Mobile Phones

- **Use a password PIN # or biometric like a fingerprint or face reader.**
- **Set blue-tooth enabled devices to Non-discoverable.**
- **Perform a factory reset before discarding a device.**

Malware **Solutions**

- **Maintain personal vigilance**.
- Don’t install shared or non-approved software.
- Never download content from unknown sources.

More Safe-Browsing **Solutions**

- Don’t **reveal personal or financial** information in an email or on social media.
- Check **websites for variations** in URL’s, different domains (.net, .com, .edu, etc.) or misspellings.
- Keep all software **up-to-date** on your devices.

Misconfiguration of Permissions on Shared File Server(s)

- **Solutions**
  - **Review access permissions and delete old files**
  - Add an automated periodic permission and file content scanning capability
  - **Do manual reviews by content owners (*who have completed an awareness and training program*)**

Conduct a Risk Assessment

- Identify and Analyze the Risk – how vulnerable are you?
- Assessment of IT
- Assessment of Financial Exposures

Conduct a Risk Assessment

- What are your (internal & external) vulnerabilities?
  - What information might get exposed?
  - Who might expose it?
  - How and Where could it be exposed?
  - What applications use it?

Communication

- Next, **communicate the results** to the leadership so they <u>understand the risks</u> involved and will be <u>more likely to support</u> proposed solutions.

Solutions

- Make improvements to secure the computer system ASAP
  - Internal safety procedures
  - Purchase of new or additional hardware
  - Purchase of new software to safeguard the system and the integrity of information

Acquire Cyber-Liability Insurance – to Mitigate Your Risk

- If you don't have it, what can happen?
  - Exposure to a variety of claims
  - Lawsuits seeking damages for:
    - Invasion of privacy
    - Negligence
    - Violation of Federal statutes governing the handling of
      - Employee or student health information
    - Misappropriation of information
    - Investigations by governmental authorities
  - Business Interruption Expense
  - Notification costs, etc.

Solutions – Before & After

- Most cyber risk policies include coverage for business interruption or loss of income and extra expenses associated with a breach, which typically can make-up some of the more significant costs.

- Quality **documentation** and forensic **analysis** is the cornerstone to effectuate a positive result on a cyber claim.

Actions Needed

- Responsibility of the **Risk Manager** or **Policyholder** to lead the development and presentation of losses caused by the event.

- Immediately after a loss, **significant attention, leadership and data analysis are required** to fully document a claim.

Action Needed

- it is essential to **quickly establish a claim validation and presentation process** to capture and document all loss-related costs.

Next Steps

- Categorize the data
- Determine who has access
- Manage your faculty and staff
- Control the Administrative rights
- Take a multi-layer approach
- Encrypt information
- Track portable devices
- Monitor inoperative assets
- Maintain physical access control
- Dispose of records properly
- Implement policies
- Manage your vendors

Governing Board Responsibilities

- Establish policies/procedures that include a disaster recovery plan to:
  - prevent the **loss of computerized data** and
  - to help school personnel **resume operations**.
  - Develop breach **notification procedures**
  - P/P to address **acceptable** internet and computer **use**
  - **Passwords**
  - **Back-up procedures**
  - **Patch management**
  - **Mobile device encryption**
  - **Physical security of IT components**

If you don’t have policies in place…

- The lack of policies **significantly** increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use.

If you don't have them in place…

- You cannot ensure that your employees are aware of their responsibilities, and
- Then there are no consistent standards for which these users can be held accountable.
- Which increases the risk of inappropriate computer use (intentional or accidental)…

User Access

- You want **restrictions for users' access** to only those applications, resources and data that are necessary for their day-to-day duties and responsibilities.
- Is required to **maintain unique passwords**
  - Complex
  - Updated periodically
- User accounts should be **deactivated when an employee leaves**

User Access

- Application administrative rights for your financial software should be **assigned to someone independent of any Accounting Office functions.**

IT Inventory

- **A reliable inventory** is necessary to protect resources – such as software and hardware assets from theft, loss or misuse
- **Resources** cannot be properly tracked and protected if you don't know **what you have and where they are**
- You also need this to do **effective patch management and software licensing compliance**

Monitoring Use

- Formal procedures should be established for periodically monitoring computer equipment for:
  - **Excessive personal use**
  - **Improper use**
  - Use of unauthorized programs

Such inspections should be documented and appropriate action taken when necessary.

Prevention

- IT – Protocols need to be in place
- IT - Security measures and understanding these measures for cellphones, laptops, and tablets
- IT – Best Practices

Risk Control – What Actions to Take?

- 1. What does your organization need to do to achieve its goals, your information, your data, your risk in the age of technology?

- 2. What tools, resources and systems do you depend on?

- 3. What financial or reputational cost could your organization face in light of a data breach or unavailability of IT systems?

Risk Control – What Actions to Take?

Implement a **Designed Security Policy**.

- Security should be built into the systems from the ground up

- Adopt a **corporate culture of security**
  - Employees and students need to be aware of threats
  - Employees and students need to know how to deal with them

Reasonable Defenses

- Firewall
- Anti-Virus software
- Filters
- E-mail encryption
- Security patches
- Limited network connectivity
- Monitoring servers for hacking attempts

Reasonable Defenses

- We recommend:
  - Both the **proactive implementation of security measures**, and
  - **Meticulous documentation** of these steps

- This is critical in avoiding potential legal liability.

5 Strategies to Thwart Cyberattacks

- First, Ensure you have an internal communications group within IT.

- This could be one person or a small team of individuals who understand technology.

- Their task is to take the **complex and make it easy to understand**. Clarity, brevity and engaging narratives are essential.

5 Strategies to Thwart Cyberattacks

Second: Utilize **analytical tools to track the success** of your strategically timed messages and

- to ensure your end users are reading them.
- Consider using an email marketing service.
  - Provides more sophisticated graphics and formatting options, but more importantly, analytical research tools to track your messages.
  - You can monitor the number of message opens, the time when they are opened and how often.
  - Gleaning analytical data from your audience messages can provide important insights into your communication effectiveness both domestically (and abroad).

5 Strategies to Thwart Cyberattacks

Third: **Click Maps** - track what your users are clicking on within your email.

- Allows you to fine-tune and optimize your messages, and

- provides insight into how well your messages penetrate their intended population,

- all of this creates a road map for the best time to send a well-designed email, with enhanced readability.

5 Strategies to Thwart Cyberattacks

Fourth: Utilize print communications and targeted face-to-face training and presentations.

- Investing effort into targeted groups, where the problem is the greatest, will have the greatest impact.
  - For example, the prime time for hackers to send phishing emails to educational institutions is at the **start of the fall semester**.
  - It's natural for freshmen to click on these links if they have not yet been indoctrinated into your anti-phishing IT messaging.
  - However if your sophomore class is also clicking on phishing links, then you should prioritize your communications toward both groups.

5 Strategies to Thwart Cyberattacks

A culture that fosters collective awareness and understanding of cybersecurity

- **Depends** on the active engagement of students, staff and administration.
- A successful cyber-awareness campaign **requires active engagement** from all groups.
- **Communications** from college administrators can **stress the importance** of data security from the top down.
- **Uniformity in engaging faculty** helps to **spread the message** to their peers.
- Communicating with college support staff helps reinforce the responsibilities of faculty and the awareness of staff themselves in being **vigilant** in protecting colleagues from cyberattacks.

5 Strategies to Thwart Cyberattacks

- **Communicating cybersecurity risks to students** helps them realize the potential of being quarantined from access to technology resources, as well as their personal risks.

- **Engaging each sector of your campus** helps increase your collective defensive shield against cyberattacks and provides a defense against phishing and spamming.

5 Strategies to Thwart Cyberattacks

Fifth: Understanding and **knowing <u>when</u> <u>to target communications</u> is an essential strategy**.

- On Facebook, Thursday at 1 p.m. is the best time to post.
- On Twitter, Thursday at noon is the optimal time, and
- on Instagram, Monday is the best day.

There are some exceptions based on day and time, but understanding the trends in optimal posting can be helpful.

ADA Compliance

- WCAG 2.0 AA*:
- Ref.: https://www.w3.org/TR/WCAG20/
  - 12 Guidelines with 4 success criteria used to measure the **usability of a website**.

  - *Web Content Accessibility Guidelines

IOT

- **Don’t bring interconnected toys to your workplace.** IoT

- **Watch out for your camera and headphones.** IoT

GDPR May 25th, 2018

It may apply to you, if you:

- Participate in EU study abroad programs
- Recruit and/or accept applications from individuals located in the EU
- Offer distance learning to individuals located in the EU
- Possess a campus in any of the 28 EU countries
- Hold personal data on students, alumni, professors or donors who live in the EU
- Receive information from and distribute information to students, alumni, professors or donors who live in the EU (*e.g.* online donations, e-newsletters, emails)

Conclusions

- Information security is **more of a people and process issue** than a technology issue.
- **Awareness of the risks and implications of an individual's actions** are the things that need to be driven home to your people.
- Getting top administrators and the Board **involved and committed** to promoting more robust cyber-security is critical.

Conclusions

- Cyber-Security is **not** a “fix it and forget it” type of problem.
- Cyber-Security is an “insurance policy”
- New cyber weapons
- External access – contractors, vendors
- Repair of breaches, diagnosing them and protecting against future attacks are not sufficient when not done **consistently**.

Conclusions

- **Update your inventory** of digital assets

- Any new inventory must have the same **robust security** features embedded

Conclusions

- This is just the beginning.
- Cyber threats can be defended against
- Start with the **understanding of how the threats can affec**t every part of your operation, not just the technology infrastructure

Conclusions

- **Educate** your IT Dept., Faculty, Staff and Students.

Questions??????????????????

References

- 2017 Hiscox Cyber Readiness Report, conducted by Cambridge, Massachusetts-based Forrester Research Inc.,- Hiscox Ltd
- Office Space movie trailer
- Inforesilientsystems.com
- Web Content Accessibility Guidelines, w3.org