2020 HCCA BOARD & AUDIT COMMITTEE COMPLIANCE CONFERENCE

Cyber Security

Barry Mathis
Principal, PYA, P.C.

Roy Wyman
Partner, Nelson Mullins

0

Agenda

- Security Risks
  - Cybercrime
  - Hacking
  - Ransomware
- Privacy—the Concept and Risks
- Best Practices to Be and Remain Compliant

1

IC3 by The Numbers

FBI's Internet Crime Complaint Center **(IC3)** which provides the public with a trustworthy and convenient mechanism for reporting information concerning suspected Internet-facilitated criminal activity.

Cyber Crime Environment

2019 Crime Types *Continued*

By Victim Loss

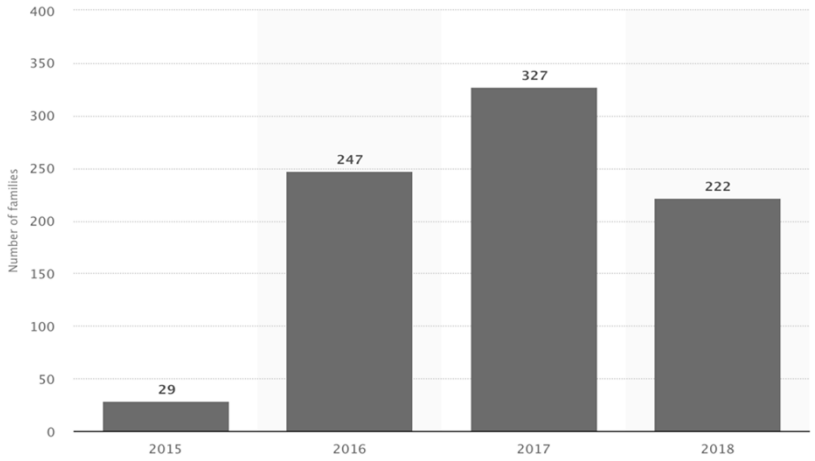
Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,776,549,688	Employment	$42,618,705
Confidence Fraud/Romance	$475,014,032	Civil Matter	$20,242,867
Spoofing	$300,478,433	Harassment/Threats of Violence	$19,866,654
Investment	$222,186,195	Misrepresentation	$12,371,573
Real Estate/Rental	$221,365,911	IPR/Copyright and Counterfeit	$10,293,307
Non-Payment/Non-Delivery	$196,563,497	Ransomware	**$8,965,847
Identity Theft	$160,305,789	Denial of Service/TDoS	$7,598,198
Government Impersonation	$124,292,606	Charity	$2,214,383
Personal Data Breach	$120,102,501	Malware/Scareware/ Virus	$2,009,119
Credit Card Fraud	$111,491,163	Re-shipping	$1,772,692
Extortion	$107,498,956	Gambling	$1,458,118
Advanced Fee	$100,602,297	Health Care Related	$1,128,838
Other	$66,223,160	Crimes Against Children	$975,311
Phishing/Vishing/Smishing/Pharming	$57,836,379	Hacktivist	$129,000
Overpayment	$55,820,212	Terrorism	$49,589
Tech Support	$54,041,053		
Corporate Data Breach	$53,398,278		
Lottery/Sweepstakes/Inheritance	$48,642,332		

*** This number only represents what victims report to the FBI via the IC3 and does not account for victim direct reporting to FBI field offices/agents.**

Source: https://www.ic3.gov

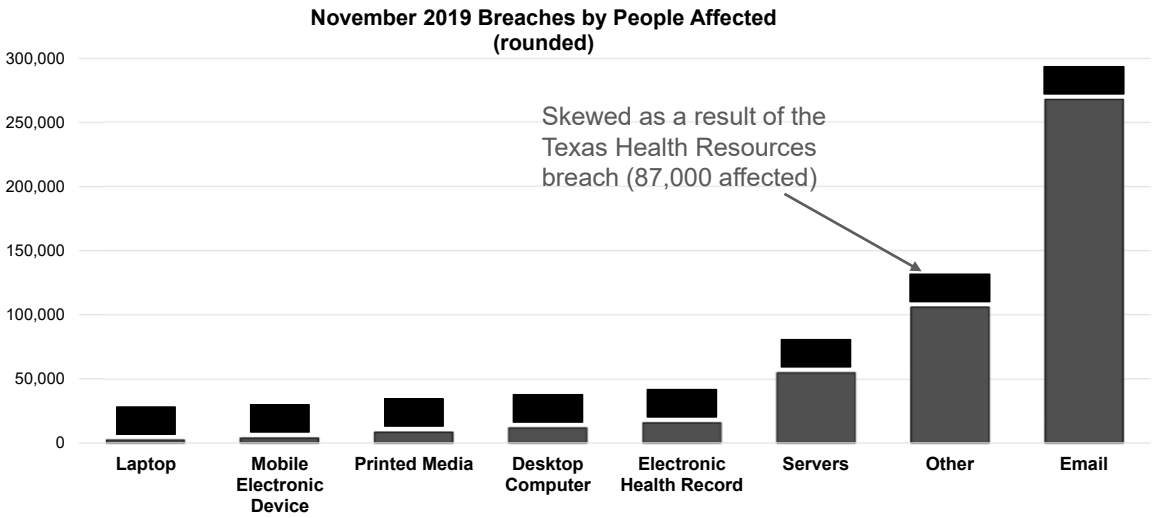
Ransomware Environment

- Number of Newly Discovered Ransomware Families 2015 to 2018



Source: https://www.statista.com/statistics/701029/number-of-newly-added-ransomware-families-worldwide/

2019 Healthcare Breaches



Source Data: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html

Hacking

- **Origin:**
  - In the 1960s at MIT, of the term “hacker”, where extremely skilled individuals practiced hardcore programming in FORTRAN and other older languages.
  - Some may ignorantly dub them “nerds” or “geeks” but these individuals were, by far, the most intelligent, individual, and intellectually advanced people who happen to be the pioneers and forefathers of the talented individuals that are today the true hackers.
- **Ethical Hacking:**
  - An ethical hacker is an individual hired to hack into a system to identify and repair potential vulnerabilities, effectively preventing exploitation by malicious hackers. They are security experts that specialize in the penetration testing (pen-testing) of computer and software systems for the purpose of evaluating, strengthening and improving security.
  - An ethical hacker is also known as a white hat hacker, red team, tiger team or sneaker.

Who Are The Hackers

Black Hat

Extraordinarily skilled at using their abilities and tools for personal gain or disruption. Dedicated to destruction.

White Hat

Experienced in using the same knowledge and tools as Black Hat, but use those skills to assist in education, and prevention for the common good.

Grey Hat

Mercenaries for hire. These hackers use their skills and tools for the highest bidder or to capitalize on an opportunity.

Some Terminology

Ransomware	Bad Actor	Vulnerability	Attack Campaign	Attack Vector
• A type of malicious software designed to block access to a computer system until a sum of money is paid.	• An entity that is partially or wholly responsible for a security incident that impacts an organization's security."	• *A weakness or gap in our protection efforts.*	• Designed to bypass conventional advanced threat prevention controls and are typically executed by well-funded organizations.	• A path or means by which a bad actor can gain access to a computer or network server in order to deliver a payload

Payload	Encryption	Crypto Key	Key Logger	Cryptocurrency
• Malware such as worms or viruses which performs the malicious action; deleting data, sending spam or encrypting data.	• Data that is scrambled using an encryption algorithm and an encryption key.	• A string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa.	• A software program that logs keystrokes	• A digital currency in which encryption techniques are used to regulate the generation currency and verify the transfer of funds

Ransomware Origins

- BC – Before Crypto
  - Earliest known malware classified as "Ransomware"
    - PC Cyborg Trojan – 1989, replaced Autoexec.bat
    - After boot count reached 90, hid & renamed boot directories and files.
    - Ransom: $189
  - Extortionate ransomware became prominent in 2005
    - Limited to .JPG, .PDF, .ZIP and .DOC
    - Compressed and locked files with a password
    - Later variants locked Operating Systems and Master Boot Records
    - Ransom: $300 to get password

Sources: https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf.
https://www.pexels.com/photo/grayscale-photography-of-pedestal-balustrade-161875/.

Ransomware Origins

- AC – After Crypto
  - Ransomware hits mainstream around 2013
    - Typically starts with a social engineering attack
    - Users tricked into launching malware
    - Files are encrypted leaving behind a ransom note
    - Payment is via crypto currency: $500 to $1,000
  - Becomes criminal enterprise between 2015 and 2016
    - Target shifts from individuals to businesses
    - 29 ransomware families discovered in 2015
    - 2016 saw a 752% rise to 247 ransomware families
    - More “lit fuse” strains that increase ransom over time
    - Generates $1 billion in 2016 and 2017

Sources: https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf.
https://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646.

Genealogy of Ransomware

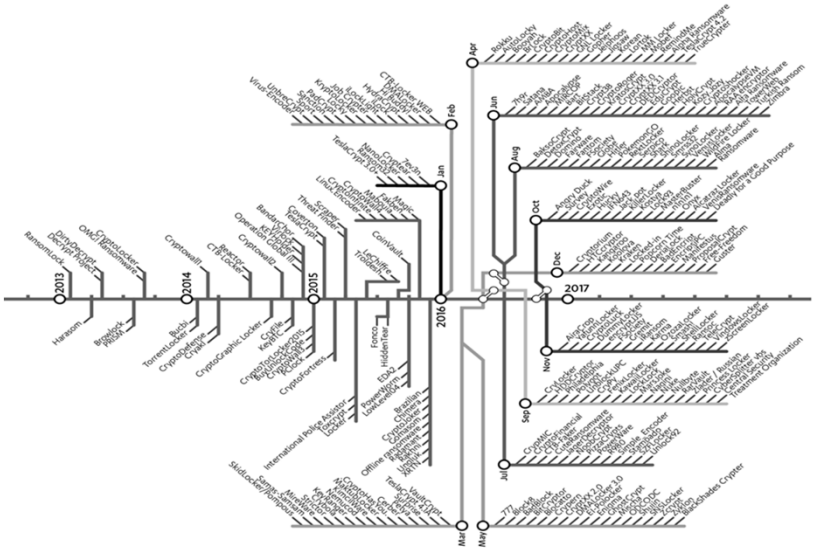


Image Source: https://labsblog.f-secure.com/2017/04/18/ransomware-timeline-2010-2017/

Crypto Ransomware Organized Attack

Campaign	Bad actors use techniques such as social engineering and weaponized tools to identify vulnerabilities for the attack.
Payload Delivery	The most common and effective method for delivering a payload is through email phishing. The most productive payloads are key loggers or weaponized websites.
Attack Coordination	Once the payload has reached its target, the crypto malware "phones home" to the bad actor who generates the crypto key that will be embedded on the target server.
Crawl and Encrypt Files	The crypto software scans servers, shared drives and files for types of files that it will encrypt. Then based on the family of ransomware, files, databases or entire servers are encrypted.
Extortion	The "ransom note" is most often found when technical support is troubleshooting problems caused by the files being encrypted. To get the "key", a ransom must be paid.

Chemistry of Crypto Ransomware

- How Ransomware interacts with the target environment.
- How we respond and interact with Ransomware.

Chemistry of Crypto Ransomware

- How Ransomware interacts with the target environment.
  - The most common injection points of successful Ransomware are through known vulnerabilities and email phishing.
    - Unpatched devices top the list of vulnerabilities
    - Social media and retail sales websites top the list for email phishing
    - The ultimate goal is to gain access to an administrator account or any account with elevated access such as an executive or system admin.

Chemistry of Crypto Ransomware

- How Ransomware interacts with the target environment (continued).
  - Once inside, the crypto malware crawls looking for common database types such as MS SQL,IBM DB2, Oracle, XML, MySQL, CACHE, MUMPS. These are high value targets as encrypting them yields a high likelihood of disruption.
  - Along with database files, the crypto malware will encrypt many common file types to cause maximum disruption.

Chemistry of Crypto Ransomware

- Sample Ransomware Note – SamSam 2017

Time Played: 1 days 20 hours 6 minutes 35 seconds

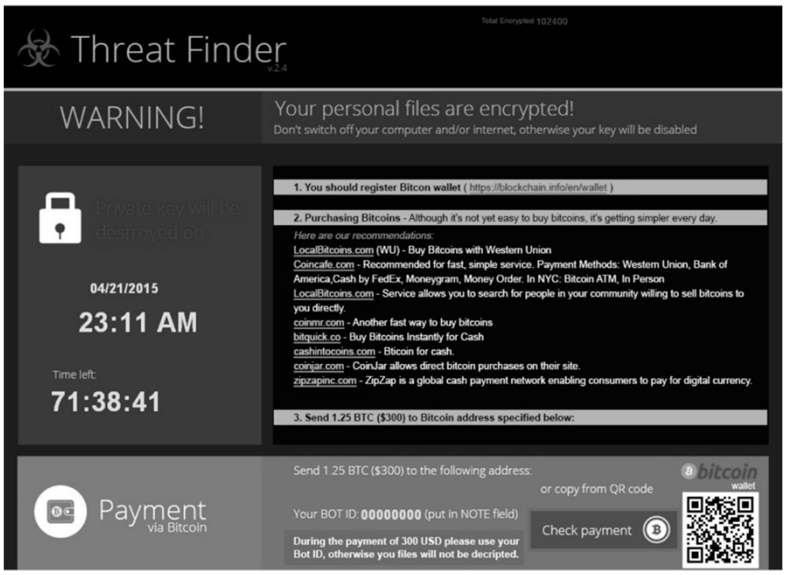
Please wait for decrypt files

Upload File For Decryption

Files Available To Decrypt: 0

Your comments	Our Answer
27.09.2016 08:02 --▼▼▼▼@gmail.com hello there, I am not sure it worked there seem to be some systems it didnt work on can you check if there are any more keys please? thank you	all keys: You can download it from address: http://s000.tinyupload.com/?file_id=[redacted] You can delete file from address: http://s000.tinyupload.com/?del_id=[redacted]
27.09.2016 12:08 --▼▼▼▼@gmail.com an error occured when decoding OAEP padding value cannot be null parameter name: yek is the error we see after the tool has been running some time around 1/4 files are restored, the rest fail with this error thank you for your help	What error did you get? It was all of your keys
27.09.2016 13:26 --▼▼▼▼@gmail.com ok, how do you think we can fix? thank you	Padding Error most occur for files in shared folder because they are used in many computers and some files encrypted with another computer key.
27.09.2016 13:30 --▼▼▼▼@gmail.com ok, how do you think we can fix? thank you	fixing is a little boring, You should find undecrypted file that send you error, copy this file to a new PC, now copy all keys in the next to of unencrypted file, now you should write a batch file that select key one by one and start decrypting.

Chemistry of Crypto Ransomware



Sample Ransomware Note - 2019

Chemistry of Crypto Ransomware

- Response to Ransomware attack.
  - Timing is critical: Report to Law Enforcement (https://www.ic3.gov)
    - Date of Infection
    - Ransomware Variant (identified on the ransom page or by the encrypted file extension)
    - Victim Company Information (industry type, business size, etc.)
    - How the Infection Occurred (link in e-mail, browsing the Internet, etc.)
    - Requested Ransom Amount
    - Actor's Bitcoin Wallet Address (may be listed on the ransom page)
    - Ransom Amount Paid (if any)
    - Overall Losses Associated with a Ransomware Infection (including the ransom amount)
    - Victim Impact Statement

Chemistry of Crypto Ransomware

- Response to Ransomware attack.
  - Consider Behavioral Based End Point Protection
    - Assumes you will be compromised
    - Uses Machine Learning and profile templates to detect and stop abnormal behavior
    - Uses Virtual Patching (security enforcement layer analyzes transactions and intercepts attacks in transit)
    - Monitors all points of environment and not just access points
    - Not based on 3rd party malware definitions
    - More effective on Zero Day attacks.

Chemistry of Crypto Ransomware

- Much more sophisticated and even autonomous.
  - Machine Learning that embeds and makes attack decisions based on analytics gathered.
    - Minor changes to Backup and Recovery resources for months ending in unrecoverable backups.
    - Rifle vs. shotgun approach targeting only the most critical files.
    - Very few human factors in deployment, injection and encryption.

Image Source:https://www.pexels.com/photo/business-businessmen-classroom-communication-267507/

Chemistry of Crypto Ransomware

- Much more than just encrypting files
  - Imagine if Payroll was held hostage or stolen
    - Malware that specifically targets payroll transactions
    - Happening in UK now
  - Trade Secrets
    - Captures, encrypts and allow data owners to bid with others on release of the data
    - Happening in China now

Chemistry of Crypto Ransomware

- Much more than just encrypting files (continued)
  - Reputation Ransom
    - Malware craws for months collecting every letter, photo, email, financial transaction or social media post (public and private) that might be considered unethical, immoral or illegal
    - Demands ransom with countdown before going public
    - Happening in US now (distributed through advertising traffic and targeting Internet Explorer on Windows and Safari on OS X)

Ransomware: Now anyone can do it

- Current environment for ransomware
  - Now there is a third type of ransomware that is gaining ground quickly.
    - **DataKeeper** – Franchised ransomware
      - To become an affiliate and have a hand-on experience with the Datakeeper ransomware, it is necessary to sign up on its website, without any activation fee. The owner of a new Datakeeper-based infection is promised a share of every ransom fee paid by the victim.
      - Franchised clients of the Datakeeper ransomware are provided with a pack of features enabling them to customize their destructive software.
      - A Datakeeper-based threat may also be instructed to attempt running administrative rights such as deleting backups or recovery points.

Privacy

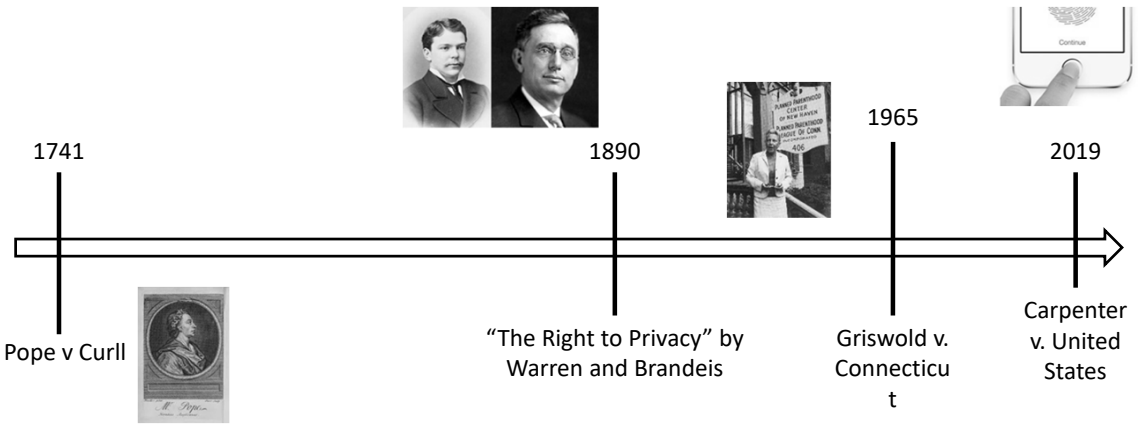
From Tangible to the Intangible

"It is certain every man has a right to keep his own sentiments, if he pleases… the manuscript is, in every sense, his peculiar property; and no man can take it from him, or make any use of it which he has not authorized…"

Millar v. Taylor (1769)

Privacy

A Quick Timeline



The Privacy Syllogism

- We have rights in our own property
- Our thoughts and words are our property

.·.Privacy in thought and word is a property right

Privacy

- The Current Sources of Privacy Guidance and Constraints
  - Common Law
    - *Intrusion of Solitude*: physical or electronic intrusion into one's private quarters
    - *Public Disclosure of Private Facts*: the dissemination of truthful, private information that is objectionable
    - *False Light*: the publication of facts that place a person in a false light, even if not defamatory
    - *Appropriation*: the unauthorized use of a person's name or likeness

Privacy

- The Current Sources of Privacy Guidance and Constraints (continued)
  - Statutory/Regulatory of Interest to Healthcare Entities
    - HIPAA
    - SEC/FTC
    - PCI/DSS
    - GDPR/PIPEDA/Other
    - California Consumer Privacy Act
    - Other State Law

Privacy and Security

Some Common Risks

- The Negligent
  - Everyone Makes Mistakes—Teaching to Slow Down
  - Is There a Breach?
  - Training and Reinforcement

Privacy and Security

Some Common Risks

- The Willful
  - The Maximum is Necessary Standard—Snooping, Spying and Sharing
  - When Culture Breaks Down—HR and Compliance
  - The Need for Monitoring and Logging

Privacy and Security

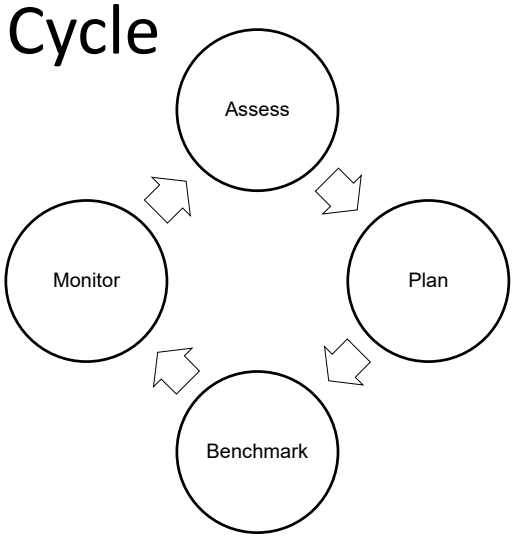
Some Common Risks

- The Criminal
  - Growing Number of “Inside Jobs”—Low Tech Crime
  - State Actors—Highest of High Tech
  - Reporting—Is it Mandatory? Is it a Good Idea?

Following are some slides for consideration under Best Practices

Best Practices

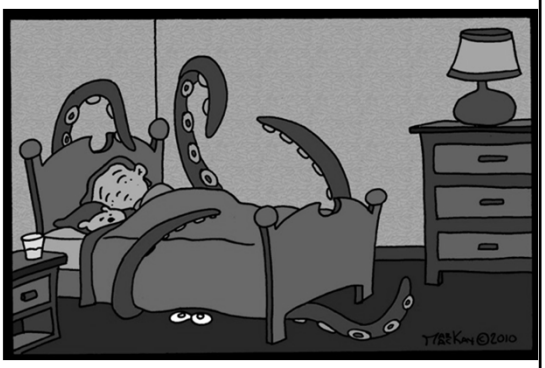
The Compliance Cycle



Risk Assessments:

The Context

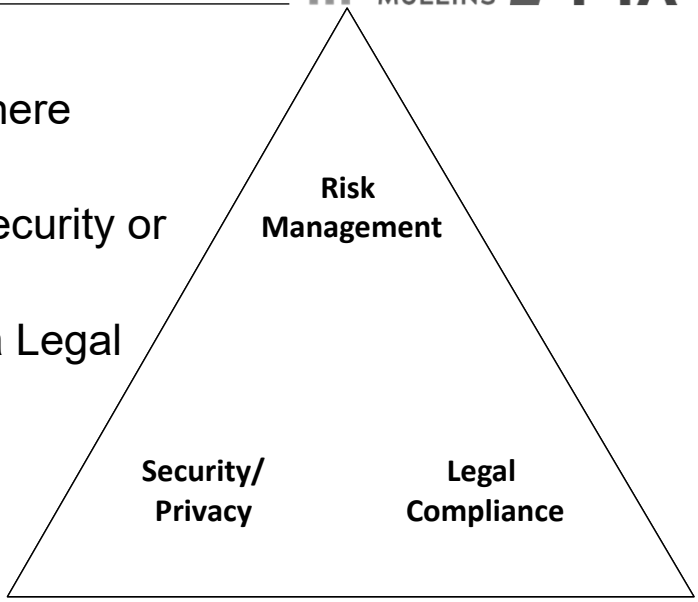
- *C*ompliance as a *D*epartment
- Can you Handle the Answer?
  - Privilege Considerations
  - A Mitigation Strategy
- Picking the Modules
  - Beyond Privacy and Security
  - Which Facilities, Departments and Functions?



Risk Assessments:

The Purpose

- Checking the Box: Where Required by Law
- Legal compliance ≠ security or privacy
- Risk Assessment as a Legal and Security Tool



Risk Assessment

- A Few of the Standards
  - Sentencing Guidelines: "*Periodically assess the risk of misconduct and take appropriate steps to reduce this risk*"
  - HIPAA: "*Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI"*
  - GDPR: "*…the controller shall…carry out an assessment of the impact of the envisaged processing operations on the protection of personal data*"
  - GLBA: *"(1) Identify reasonably foreseeable internal and external threats…(2) assess the likelihood and potential damage…; and (3) assess the sufficiency of policies, procedures, customer information systems and other arrangements…"*

Risk Planning

- Risk Management Plan
- Developing and Using Tools to Promote Compliance
  - Policies
  - Procedures
  - Training
  - Testing
  - Reminders
- Technology
  - Governance, Risk Management and Compliance (GRC) software
  - Security Logs, Tracking, etc.
  - Regulation-Specific Tools (e.g., HIPAA2Z™)

Ransomware: What can you do?

- Ransomware isn't going away
  - Many of the worst manual ransomware attacks started when the attacker discovered that an administrator had opened a hole in the rewall for a Windows computer's remote desktop. Closing these easy loopholes goes a long way to preventing these kinds of attacks. If you need to RDP, put it behind a VPN.
  - Multi-factor authentication is an amazingly effective tool for preventing the abuse of stolen credentials. If you're not using it now, you should be.
  - Administrators who manage networks should limit their use of the Domain Admin credentials to a dedicated machine or machines that are used for no other purpose.

    - Sophos Labs 2019 Threat Report
- Be diligent about what you click in emails. A Business Email Compromise is still one of the most effective ways to deliver a ransomware payload.

Image Source: https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf

Breach Notification

- HIPAA requires notification in the event of a breach of unsecured PHI.
  - Notification must be made to the patient, government, and in some cases the media.
  - **Breach** → acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI.
  - ePHI encrypted by ransomware has been **acquired** (i.e., unauthorized individuals have taken possession or control of the information).
  - That makes the attack a **BREACH** unless:

Low Probability of Compromise

- **Factors you must consider:**
  - Nature and extent of PHI
  - Who used the PHI or to whom the disclosure was made
  - Was PHI acquired/viewed
  - Has risk been mitigated
- **May also want to consider:**
  - Risk of unavailability of data
  - Risk to integrity of data
  - Was PHI exfiltrated
- **Must maintain documentation of the risk assessment**

Breach Incident Response

- Develop a plan before a breach occurs.
  - Create a site profile that includes contacts, legal, finance and public relations.
- The Incident Response Plan should designate:
  - Roles and responsibilities:
    - Notify your regional FBI field agent, PR firms, legal counsel, your cybersecurity insurer (only to the extent required in your policy), etc.; and
    - Identify a data forensics team to determine the source and scope of the breach and ensure vulnerable systems are patched as soon as possible.
  - Timelines
  - A communication plan for all audiences (employees, patients, board members, etc.)
    - Determine reporting obligations under federal and state law requirements.

Managing Cybersecurity Threats

- Recently HHS released a guidance document on Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)
- The purpose of the HICP is to:
  1. Raise awareness of cybersecurity;
  2. Provide vetted cybersecurity practices;
  3. Move organizations towards consistency in mitigating cybersecurity threats to the sector; and
  4. Aid health care and public health organizations to develop meaningful cybersecurity objectives and outcomes.
- HHS identified e-mail phishing, ransomware, loss or theft of equipment or data, insider, accidental, or intentional data loss, and attacks against connected medical devices as the 5 most common threats to patient health information.

Benchmarking

"If you cannot measure it, you cannot improve it."
~William Thomson, 1st Baron Kelvin

"Finding the appropriate measurement is…not a mathematical exercise. It is a risk-taking judgment."
~Peter Drucker

Benchmarking

- Prove It!
  - Places Numbers on the Risk Management Plan
- What is Watched is Transformed
  - Choosing Wisely based on Risk Assessment
- Expect Improvement
- Benchmarks Change each Cycle with the Change in Risks

Auditing and Monitoring

- Auditing:
  - Irregular
  - Can be Pointed
  - Tied to Benchmark or Risk
- Monitoring
  - Regular
  - Can be General
  - Tied to Benchmark

Questions