Cybersecurity Risks & Requirements For Physicians

Presented by: Cathy Bryant

November 4, 2018

TMLT
Texas Medical Liability Trust

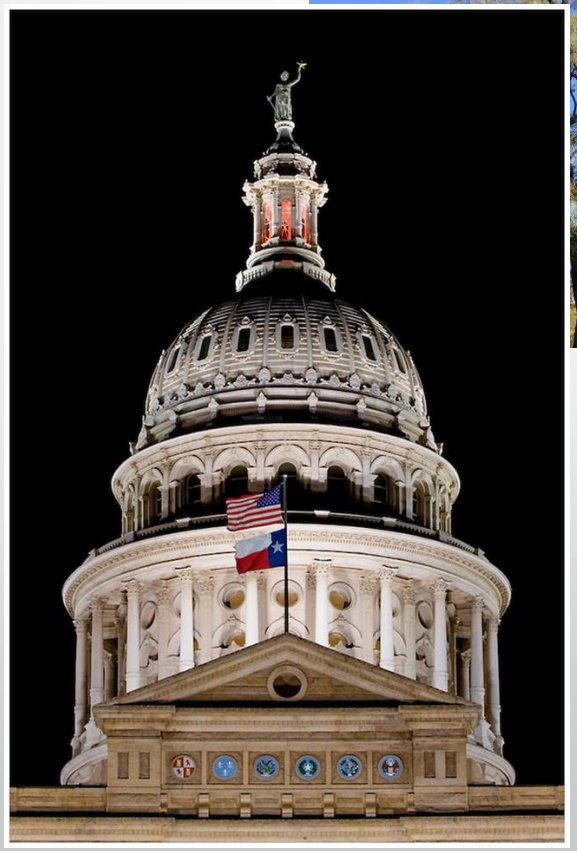
MAKE CYBERSECURITY A PRIORITY EVERY MINUTE OF EVERY DAY

RISKS

- The Laws, Rules and Regulations
- Violations
  - Privacy incidents
  - Security Incidents
  - Loss of your data
  - Social Engineering
  - Ransom demands from cyber criminals
  - Breach Notification federal and states

REQUIREMENTS

- The Laws, Rules and Regulations
  - Federal
  - Texas
  - Other States



HIPAA PRIVACY RULE

BASIC REQUIREMENTS FOR CE – UNDER HIPAA PRIVACY RULE

NOTICE OF PRIVACY PRACTICE

Notify patients of their rights and how their PHI/ePHI will be used Adopt and implement Privacy & Security Polices and Procedures

PRIVACY OFFICER - Designate individuals to be responsible for compliance

USE & DISCLOSURE OF PHI

ADMINISTRATIVE

- Written Policies and Procedures
- *Secure* PHI/ePHI so it is not *accessible* to those who don't "need to know"
- Patient Rights
- Provide a way for complaints to be made
- Train workforce
- Sanctions Policy

TMLT
Texas Medical Liability Trust

HIPAA SECURITY RULE- 2005

- establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity
- requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of *electronic protected health information.*

BASIC REQUIREMENTS FOR CE – UNDER HIPAA SECURITY RULE

ADMINISTRATIVE SAFEGUARDS

- Risk Analysis
- Risk Management
- Security Officer
- Information System Activity Review

PHYSICAL SAFEGUARDS

- Facilities management plan
- Workstation Use
- Device Management

TECHNICAL SAFEGUARDS

- Access Control
- Encryption/Decryption
- Audit Controls
- Integrity
- Authentication
- Transmission Integrity

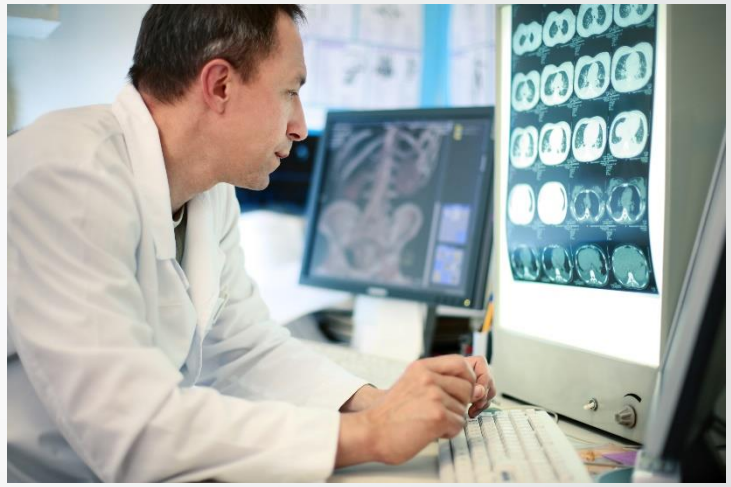
ORGANIZATIONAL REQUIREMENTS

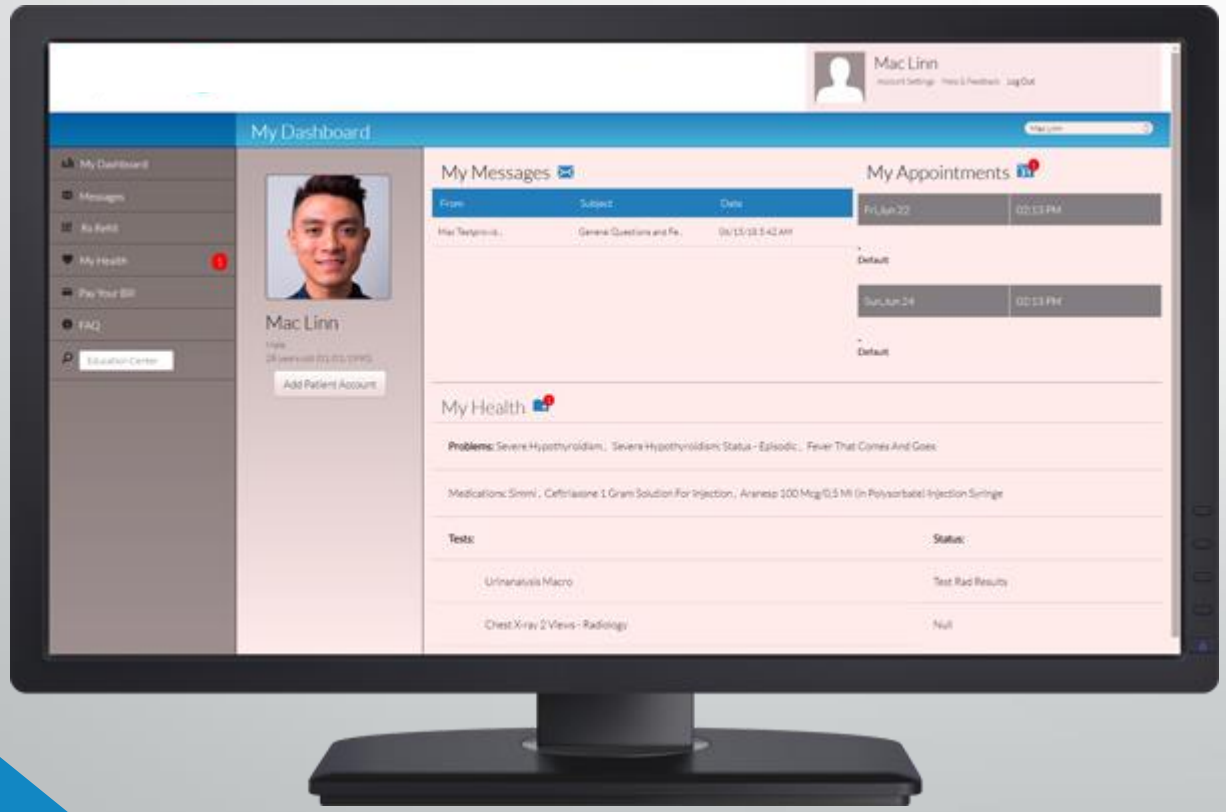
- Business Associate

POLICIES AND PROCEDURES

TMLT Texas Medical Liability Trust

SECURITY RULE





HIPAA OMNIBUS RULE - 2013

- Requires HIPAA covered entities and their business associates to provide notification following a breach of **unsecured** protected health information
- Required
  - **Revision of Notice of Privacy Practices**
  - **Revision of Business Associate Agreements**

HIPAA BREACH

Do Not Use the

Word “Breach”

Unless you have to …
“ALL BREACHES OF UNSECURED PHI ARE REPORTABLE.”

A breach is, generally,
an **impermissible use or disclosure under the Privacy Rule** that **compromises** the security or privacy of the protected health information.

An impermissible use or disclosure of protected health information **is presumed to be a breach** unless the covered entity or business associate, demonstrates that there is a **low probability** that the protected health information has been compromised **based on a risk assessment**.

BASIC REQUIREMENTS FOR CE – UNDER HIPAA BREACH

Breach Notification Rule requires:

- Individual(s) involved to be notified within 60 days
- Breaches involving >500 records
- Notify OCR within 60 days
- Notify local media
- Post on your Web site
- Smaller breaches must be reported to OCR within 60 days of the end of that calendar year

THE RULES

Texas Statute	PHI/Information Type
Texas Government Code, Chapter 420, Subchapter D	Sexual assault
Texas Health and Safety Code, Chapter 81, Section 81.103; see also Texas Administrative Code Section 8.288	HIV/AIDS test results
Texas Health and Safety Code, Chapter 81, Section 81.046	Communicable diseases
Texas Health and Safety Code, Chapter 611	Mental health records/ substance abuse
Chapter 546, Subchapter C, Insurance Code.; Texas Labor Code Section 21.403-04; Texas Occupations Code, Chapter 58	Genetic information
Texas Civ. Prac. & Rem. Code §129.001; Texas Fam. Code §32.003	Disclosures regarding treatment of a minor
Texas Bus. & Com. Code §521 (Texas Identity Theft Enforcement & Protection Act)	SPI
Texas Health & Safety Code §181	All PHI
Texas Bus. & Com. Code §522.002	PHI and other information

RISKS

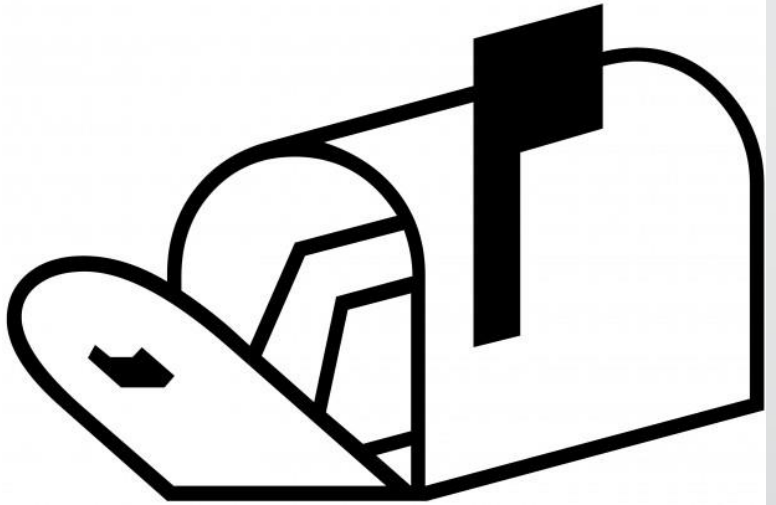
- ✓ The Laws, Rules and Regulations
- Violations
  - Privacy Incidents
  - Security Incidents
  - Loss of your data
  - Social Engineering
  - Ransom demands from cyber criminals
  - Breach Notification federal and states

PRIVACY INCIDENT

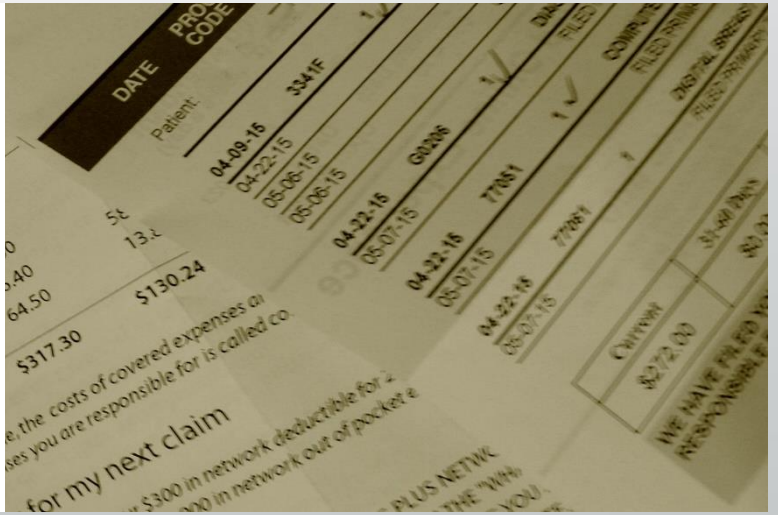
“unauthorized use or disclosure of PHI”

PRIVACY INCIDENT?

- Your office mails Susie Jones her lab results
- A few days later they get a call from Suzie Jones asking why she received someone else's lab results



- Your office hands papers to Cathy as she checks out following an office visit
- She glances at it and says I don't think this is mine it has Susie's name on it



SECURITY INCIDENT

"the **attempted** or **successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations** in an information system."

A covered entity must implement Policies and Procedures to address security incidents:

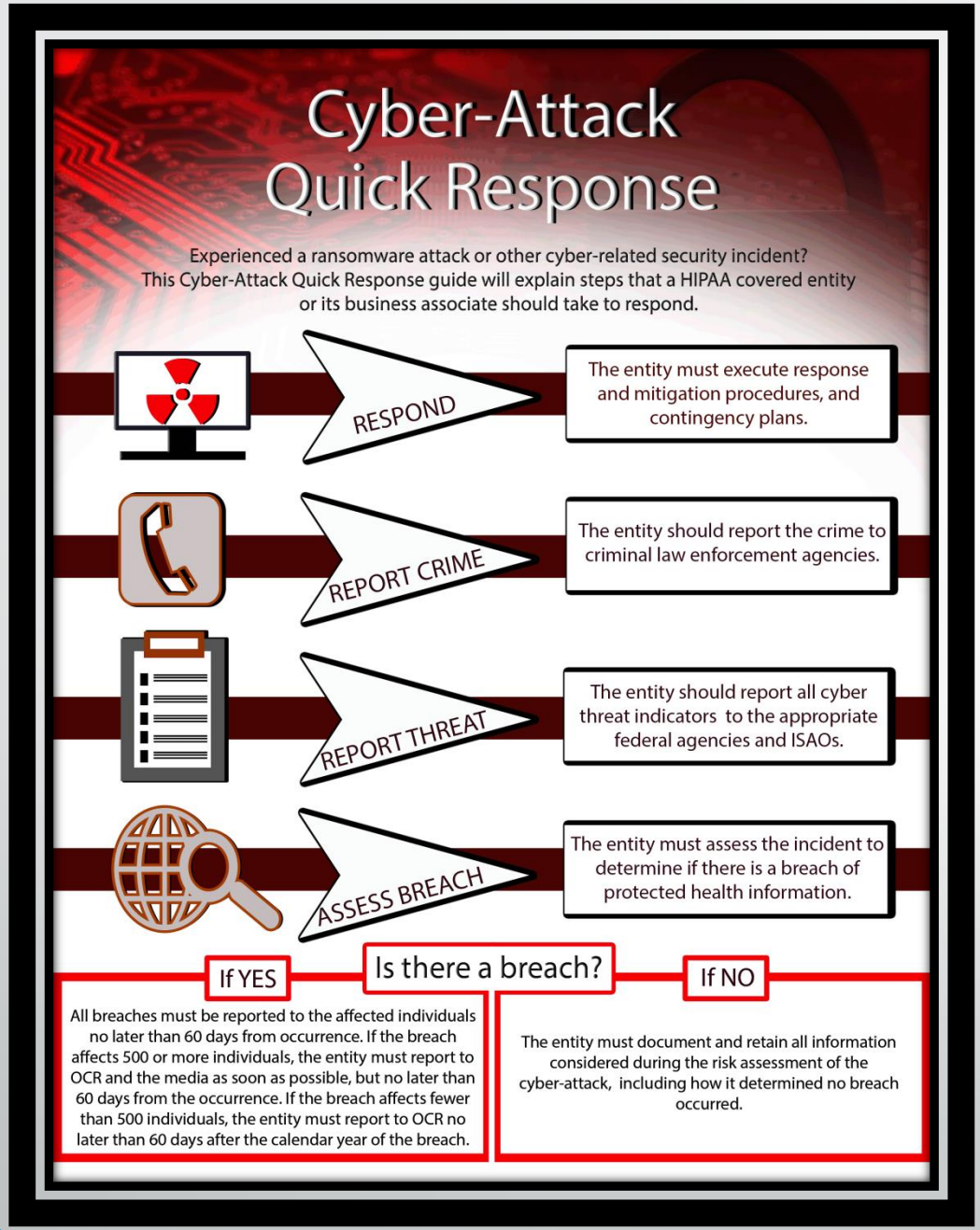
- Procedures must address how to identify security incidents and provide that the incident be reported to the appropriate person.
- How workforce members respond, i.e. preserving evidence.
- Respond to suspected or known security incidents.
- Mitigate harmful effects
- Document the security incident.

SECURITY INCIDENT?

- Your receptionist cannot log into the network when she arrives at work
- Is this a security incident?

- Your office manager routinely takes a backup of your EHR offsite each night
- Her car window is smashed and her bag containing the tape is stolen
- Is this a security incident?
- Is it a reportable breach?

HHS CYBER-ATTACK QUICK RESPONSE



Source: Health and Human Service – Office for Civil Rights

DO YOU PRACTICE DOWNTIME PROCEDURES?

- Develop a computer “crash cart”
- Copies of forms you would need to operate in the event you could not access your EHR
- Practice how your clinic would function, communicate orders and document care

LOSS OF DATA


WEB SERVICES
DATA THEFT
SOCIAL NETWORKS
ONLINE BANKING
CYBER CRIME
INTERNET OF THINGS
INFECTION
COMPUTERS
SMART DEVICES
SYSTEM & NETWORK ADMINISTRATOR
HACKERS
MALWARE & VIRUSES
SECURE CODING
CYBER
SECURITY
PROTECTION
ATTACK
ANALYSIS
BACKDOORS
DENIAL-OF-SERVICE
SPOOFING
PHISHING
HIJACKING
SOCIAL ENGINEERING
ENCRYPTION
SOLUTIONS
E-MAIL
ANTIVIRUS
SECURE APPS
SYSTEM UPDATES
SECURITY BY DESIGN

LOSS OF DATA

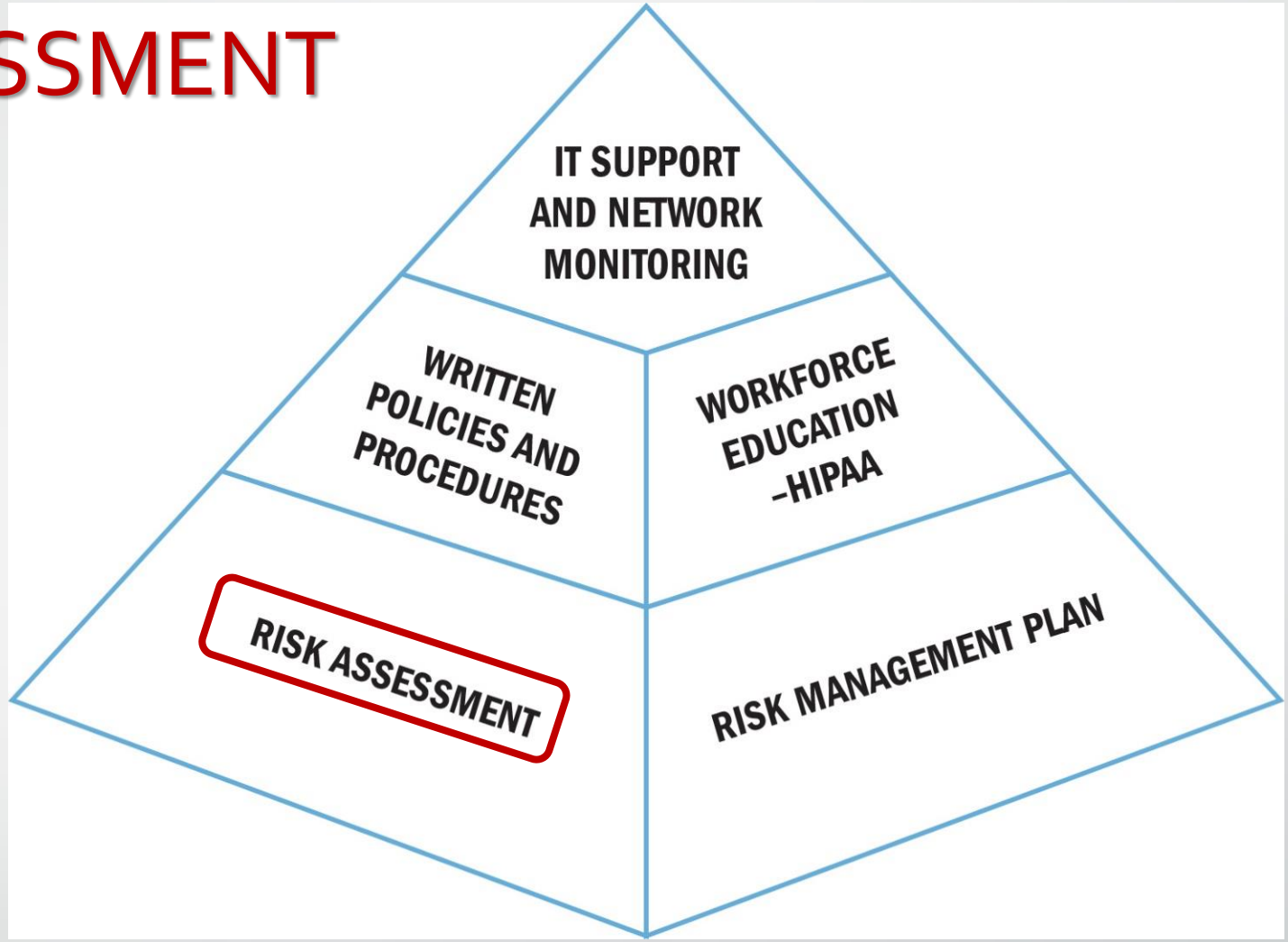
PRACTICES FAIL TO MEET THE BASIC HIPAA SECURITY REQUIREMENTS

- Risk Analysis
- Risk Management Plan
- Written Policies and Procedures
  - Administrative
  - Physical
  - Technical
- Educate workforce members
- Adequate cybersecurity and IT support

WHAT MEDICAL PRACTICES ARE DOING IS NOT WORKING

RISK ASSESSMENT

- Is the Cornerstone of Cyber Risk Management and HIPAA Compliance
- Need a P&P regarding Risk Assessment
- When a practice has an incident they need evidence of a Risk Assessment do one
- OCR will ask for all Risk Assessments for the last 6 years
- Documentation of periodic review of the Risk Assessment by person(s) responsible for it

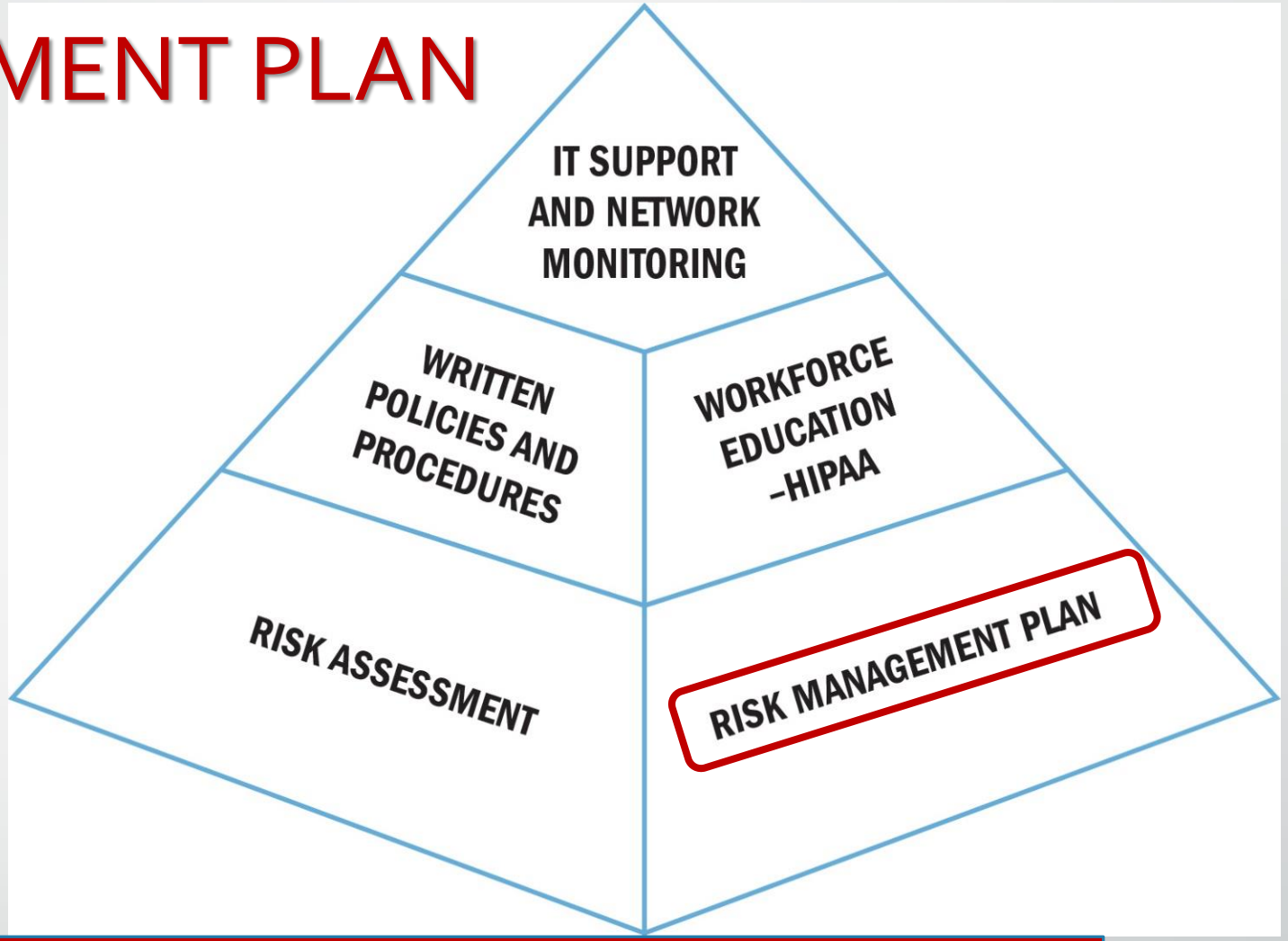


Risk Assessment 2016 Desk Audits

- None of the 63 covered entities were in full compliance
- 13 of the 63 failed to provide evidence of serious attempt to comply with the HIPAA rule

RISK MANAGEMENT PLAN

- Following a Risk Assessment you must do a Risk Management Plan
- How are you going to mitigate risk and vulnerabilities

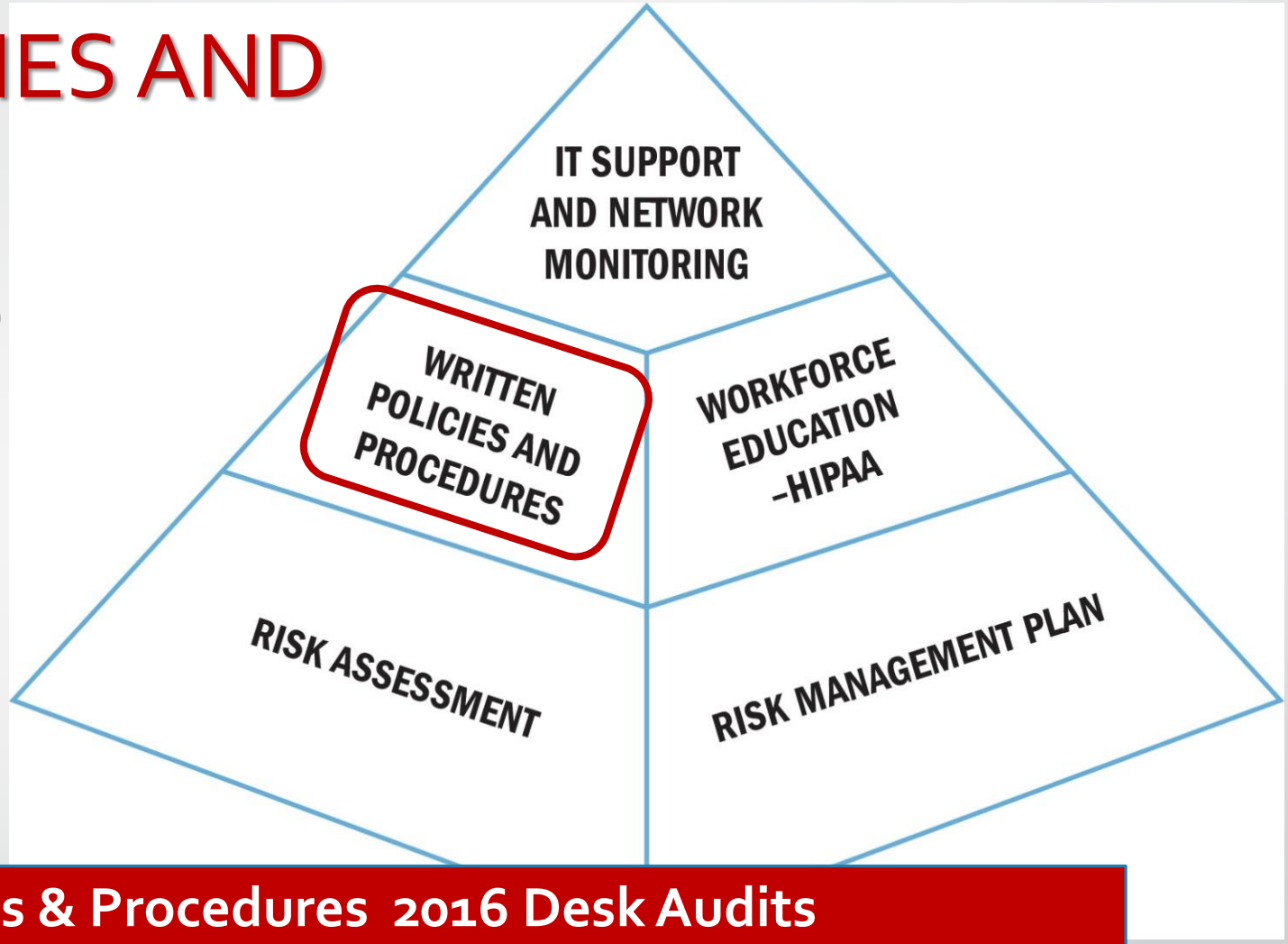


Risk Management Plan 2016 Desk Audits

- 1 of the 63 covered entities were in full compliance
- 17 of the 63 failed to provide evidence of serious attempt to comply

WRITTEN POLICIES AND PROCEDURES

- 2016 Audit Protocol states over 100 times REQUEST WRITTEN POLICY AND PROCEDURE ON …
- If your policies are dated 2003 or 2005 they are not compliant
- The OCR is expecting detailed P&P; how it is done in your organization
- Buying templates and putting them on the shelf will not work

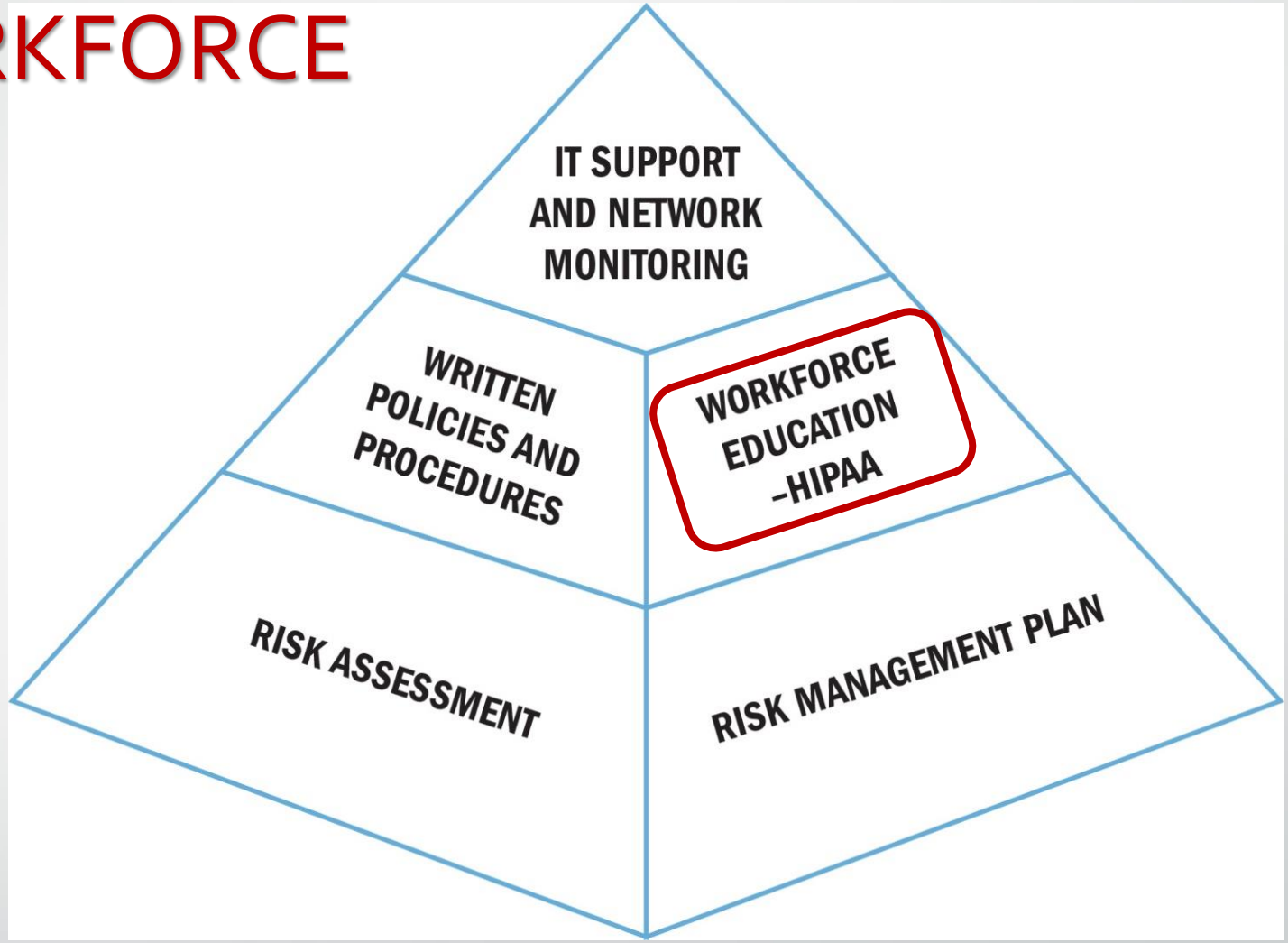


Policies & Procedures 2016 Desk Audits

- Audit focused on one policy: Right to Access Records.
- 1 of the 103 covered entities were in full compliance
- 11 of the 103 failed to provide evidence of serious attempt to comply

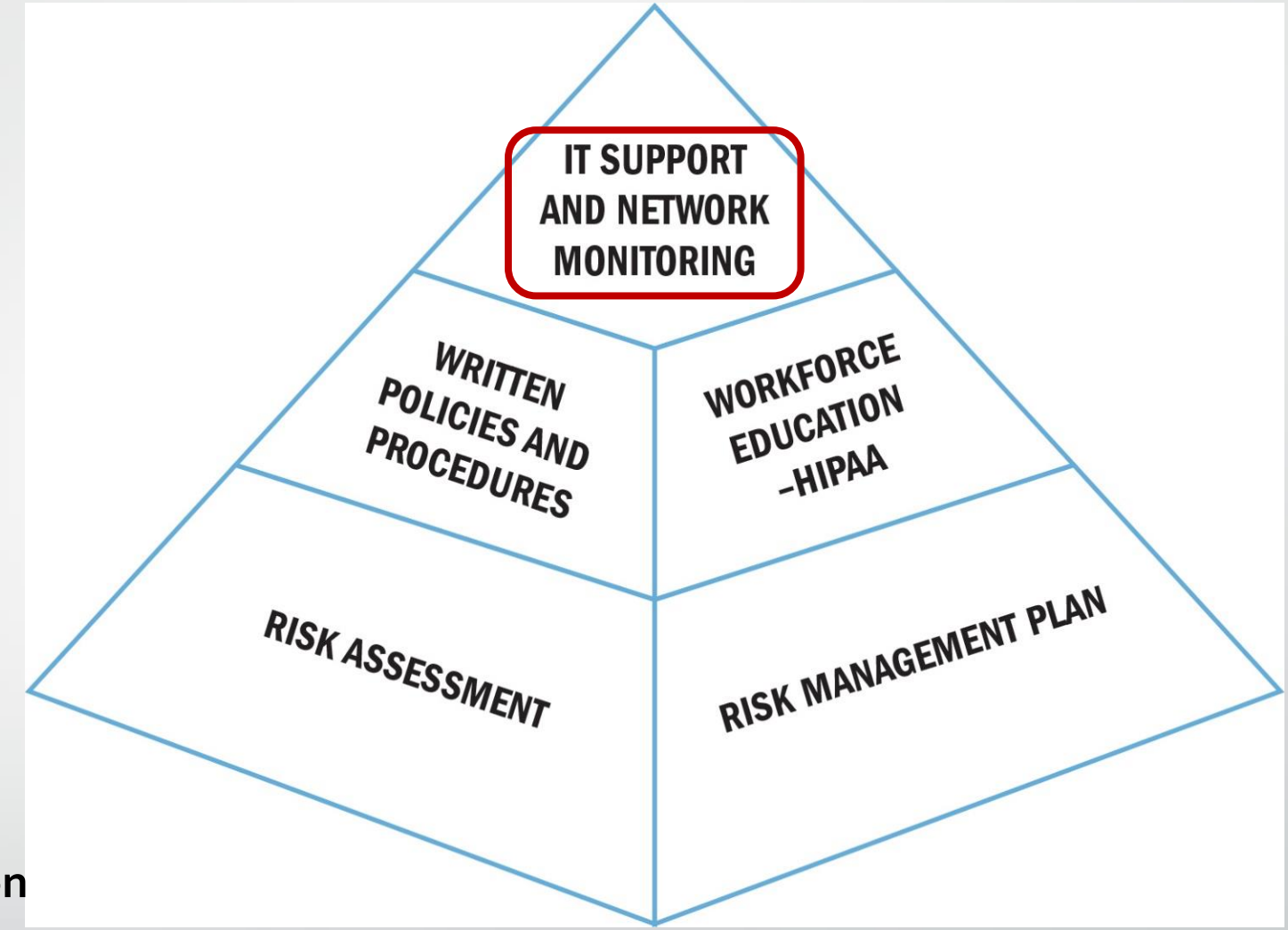
EDUCATED WORKFORCE

- All workforce members must be educated on HIPAA within the first 90 days of employment (*Texas Medical Privacy Act*)
- Video from 2003 is not current
- Education needs to address current threat environment (i.e. Phishing…)
- Evidence will always be asked for during an investigation



IT & NETWORK MONITORING

- IT support is very inconsistent
- IT do not always specialize in HIPAA and Cybersecurity
- HIPAA is the baseline for cybersecurity
- Cyber threats today cannot be managed with the same technology used even two or three years ago
- MSP
- Outsourced Endpoint Protection
- Outsourced Managed Detection and Response



Do they have a written job description?

FAIL TO MEET THE BASICS OF CYBERSECURITY

- Passwords are weak and are never changed
- Login and passwords are shared
- Software is unpatched
- AV/AM protection is out of date
- Administrative access is granted when not needed
- Encryption
  - Mobile devices
  - Email
- WiFi access is uncontrolled

HEALTHCARE ORGANIZATIONS NEED TO BE PREPARED

"You're going to be hacked.

Have a plan."

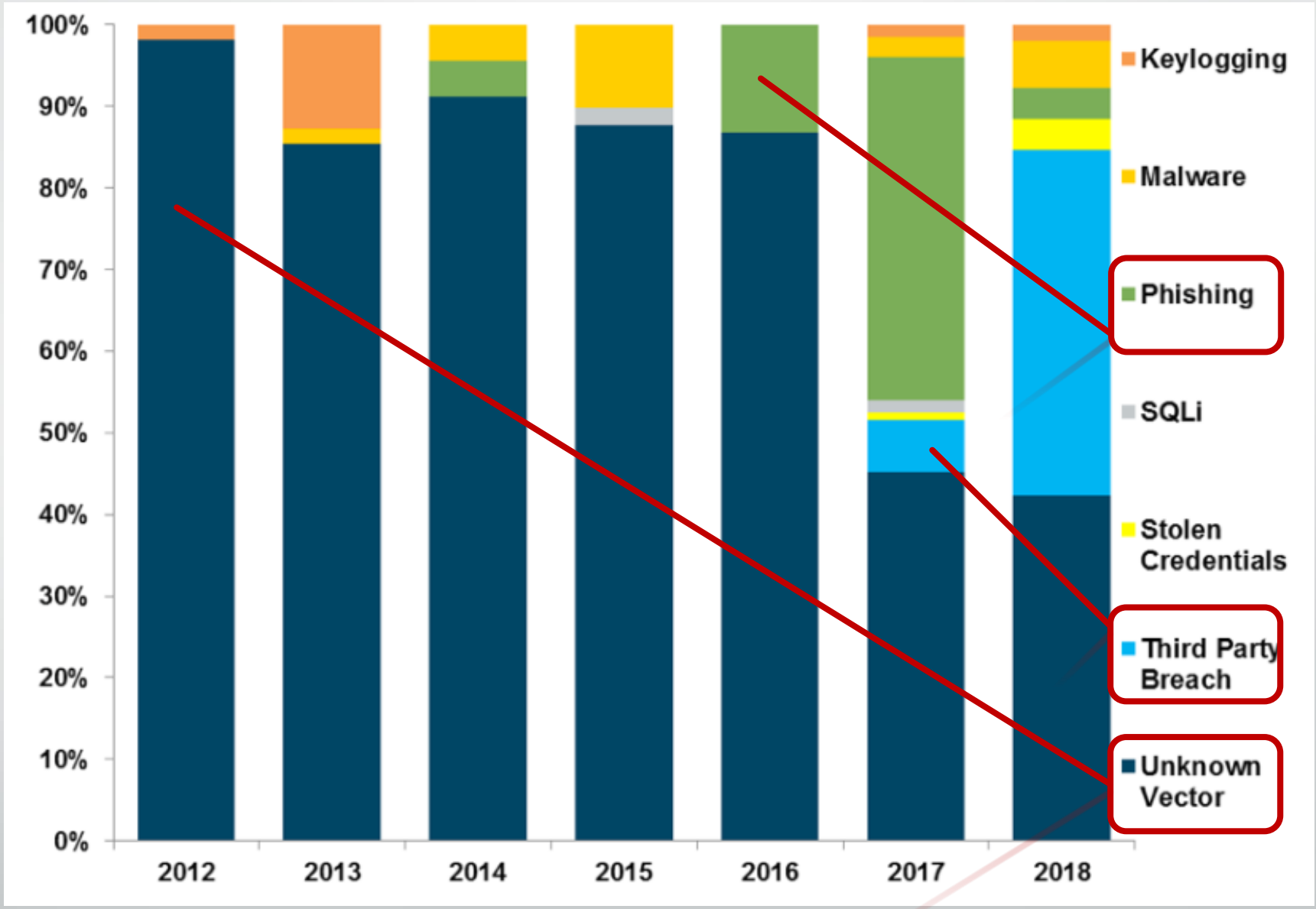
Joseph Demarest, Assistant Director, FBI Cyber Division

CYBERCRIMINALS

SHIFT IN BAD ACTORS

- Previously: cyber criminals wanted complete medical files to resell on the black market
- Shift: from medical ID theft to other tactics, like ransomware, for immediate payoff

DATA BREACH ATTACK VECTOR



WHAT IS YOUR CYBERSECURITY POSTURE?

CYBERSECURITY POSTURE

- The cybersecurity posture of an organization refers to its overall cybersecurity strength.
- It expresses the relative security of your IT network, particularly as it relates to the internet and its vulnerability to outside threats.
- Hardware and software management through policies, procedures or controls, are part of cybersecurity.
- Cybersecurity needs to be in the boardroom, executive committee or any other management meeting
- Cybersecurity is a mainstream business risk
- Building a strong Cybersecurity posture is a priority
- All staff are part of your Cybersecurity posture
  - ✓ Leadership
  - ✓ Administration
  - ✓ Clinical staff
  - ✓ Non-clinical staff
  - ✓ IT

TMLT
Texas Medical Liability Trust

WHAT IS YOUR CYBERSECURITY POSTURE? SOFTWARE UP-TO-DATE?

Do you know how is your software patched?

1. You need to know how this is being done
2. If you outsource it, you need to get regular reports showing all software on all PCs are up to date
3. If you have auto update, do you verify someone has not changed it.

WHAT IS YOUR CYBERSECURITY POSTURE? EMAIL – PHISHING

How are you stopping phishing attempts?

1 in 100 emails has malicious intent

1. Email – professional not personal
2. Email filtering:
3. Training to recognize
4. Do you allow workforce members to access personal email from work PCS or own device logged onto you WiFi?

WHAT IS YOUR CYBERSECURITY POSTURE? ACCESS MANAGEMENT?

How do you manage access or privileges?

1. Everyone does not need access to everything
2. Elevated or administrative privileges need to be given with caution
3. HIPAA requirement for minimal necessary

WHAT IS YOUR CYBERSECURITY POSTURE? BUSINESS ASSOCIATES

Are our Business Associates secure?

1. Do you know who you who your Business Associates are?
2. Do you get a signed Business Associate Agreement prior to exchanging data?
3. What does your BAA require of your BA?
4. How do you obtain assurance that they are secure?

Business Associates

- A Business Associate is someone you share your PHI with
- Know who your Business Associates are
- You are required to have insurance for your Business Associates that have current
- 2016 OCR
  - First with
  - Several with Covered ties regarding BA

April 20, 2017
No Business Associate Agreement?
$31K Mistake

Center for Children's Digestive Health

WHAT CAN YOU DO?

1. Identify who you are sharing PHI with (BA).
2. Obtain a Business Associate Agreement (BAA).
3. Obtain satisfactory assurance from your BA that they will adequately protect your PHI.
4. Consider requiring your BA to carry cyber liability insurance, if technology partner, make sure they have technology errors and omissions.
5. Indemnification language matters – who pays for their breach?

COMMON RISKS, VULNERABILITIES & MISCONCEPTIONS SEEN IN MEDICAL PRACTICES

SECURING AND DISPOSING PHI

INDIVIDUAL RIGHT TO ACCESS RECORDS

Patients have a right to review or access their medical records? [T or F]

Patients have a right to name a Personal Representative to act for them ? [T or F]

You can require a patient to come into your office to sign a release form? [T or F]

You can charge TMB rates to a patient for copies of their medical records? [T or F]

https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/access/

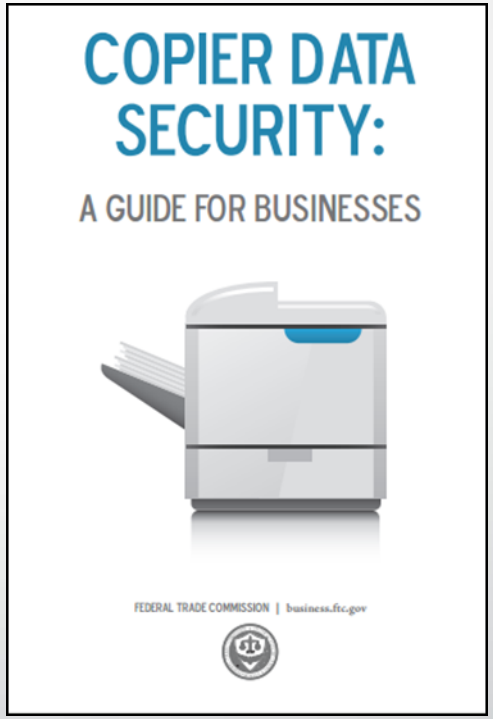
PHOTO COPIERS – HARD DRIVES

CBS News: Digital Photocopiers Loaded With Secrets

April 19, 2010

Affinity Health Plans

- Reported Breach to HHS April, 2010
- Settlement Agreement August, 2013
  - Affinity impermissibly disclosed the protected health information of up to **344,579 individuals**
  - **Fine: $1,215,780**



MEDICAL EQUIPMENT – HARD DRIVES

MEDICAL EQUIPMENT WITH HARD DRIVES

LAPTOPS IN TREATMENT OR TESTING ROOMS

EMAILING PHI

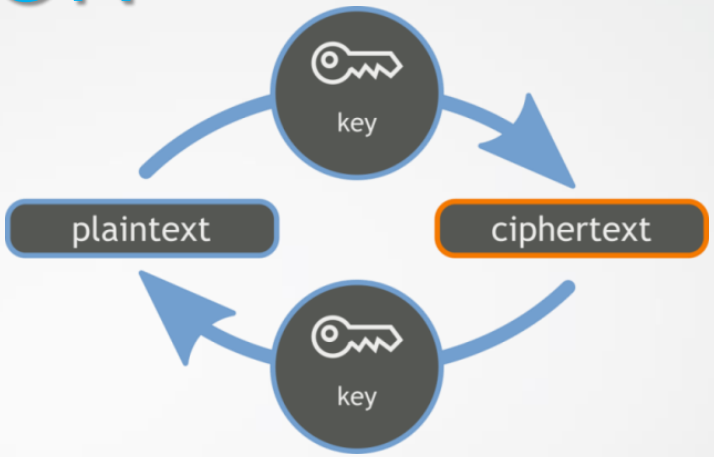
- Is PHI sent encrypted or through a secure file sharing technology?
- Transmitting encrypted data can be accomplished efficiently and without appreciably slowing down the system.

EMAIL OPTIONS

- Encryption
- Portal
- Emailing in an unsecure manner if the patient insists
  - *Omnibus Rule (2013) you may email PHI in unsecure manner **after** explaining the risks to the patient and they agree to have you send it in an unsecure manner*

ENCRYPTION

✓ "*NOT REQUIRED*" by HIPAA. True; but if you don't encrypt you must show what you did to protect PHI equal to encryption



- Encryption is not a password or passcode!
- Encryption is the process of translating words or text into "code" which conceals the text.

THE PROBLEM: UNENCRYPTED DEVICES

August 2015 OCR Settlement with Cancer Care Group

- ✓ Laptop and backup media (unencrypted) was stolen from employee's vehicle
- ✓ 55,000 records
- ✓ Cancer Care was "in **widespread non-compliance** with the HIPAA Security Rule."
  - ❑ Had not conducted an enterprise wide **risk analysis**
  - ❑ Did not have written **P&P** specific to removal of hardware and electronic media
  - ❑ Did not **encrypt**

$750,000

Encryption is a basic cyber risk management tool.

WI-FI

Unsecured Wi-Fi

- Wireless networks that can be freely accessed without a password where you can access the Internet in unsecured locations, such as hospital's guest Wi-Fi and various coffee shops.

- Separate guest WiFi
- Current standard: **WPA2**

MOBILE DEVICE PROTECTION

Delete all stored health information before discarding or reusing the mobile device

Use a password or other user authentication

Install and enable encryption

Use adequate security to send or receive health information over public Wi-Fi networks

Install and activate remote wiping and/or remote disabling

Maintain physical control

Disable and do not install or use file sharing applications

Research mobile aps before downloading

Install and enable a firewall

Keep your security software up to date

Install and enable security software

DO YOU USE SOCIAL MEDIA?

“Employees have Facebook, Instagram, Snapchat and Twitter accounts.
They text.
How many times do you think employees text and post to social media every day?”

"An EMS worker gave CPR to a man who suffered a heart attack in his chicken coop. The EMS worker later posted on Facebook: "Well, we had a first… We worked a code in a chicken coop. Knee deep in chicken droppings."

HANDLING ONLINE PATIENT COMPLAINTS

- The best practice is to avoid responding.
- If you do respond, **don't violate HIPAA**. Confirming that someone is a patient may violate HIPAA.
- Most online patient reviews are positive and provide useful feedback. An analysis of Yelp reviews shows that reviewers are more likely to leave positive reviews for health care professionals.

HANDLING ONLINE PATIENT COMPLAINTS

- A patient complaint is an opportunity to understand your patient's experience. Consider using the information to improve your practice.
- Keep in mind that if one of your patients has a complaint, **there may be others experiencing the same issues who have not come forward.**
- On the flip side, if your satisfied patients see a negative review, they may rebut a negative review or correct misinformation.
- Complain to the website about fake reviews. **If you have credible evidence that a review is fake, report it to the site and ask them to investigate.**

TMLT Texas Medical Liability Trust

APPROPRIATE RESPONSES

"At our medical practice, we strive to provide the highest levels of patient satisfaction. However, we cannot discuss specific situations due to patient privacy regulations. If you are a patient and have questions or concerns, please contact us directly at [phone number]."

"In order to protect our patients' privacy, all patient concerns and complaints are resolved directly by our practice and not through social media. If you are a patient, please contact us at [phone number]."

"We welcome all of our patients and their families to address any concerns or requests for information about their care with us directly at [phone number]."

Source: TMLT Slideshare
Responding to Online Patient Complaints

SAFE IN THE CLOUD

- A cloud provider is a business associate
- BA should be able to offer evidence of compliance with HIPAA security and privacy rules.
- Have a Business Associate Agreement, **before** sharing data.
- Compliance expectations are defined in contracts/service agreements.
- Require proof of Cyber Insurance with Technology Errors and Omissions and ask to be named as an additional insured on a non-contributory basis.

SECURITY AWARENESS TRAINING

- Educate your workforce
- Staff could be the target of Scams (phishing/vishing)
- Take credit for the education as security awareness training (required by HIPAA Security Rule)


Ransomware
malware
piracy
illegal
cyber
spam
hacking
attack
trojan
virus
hacker
bitcoin
privacy
payments
passcode
stealing
alert
network
technology
encryption
block
data
digital spy
software
safety
website
market
www
private
programming
anonymous
thief
code
identity
crime
intruder
protection
spyware
darknet
binary
online
fraud
hack
information
terrorism
password
phishing
danger
security
addiction
organization
internet
web

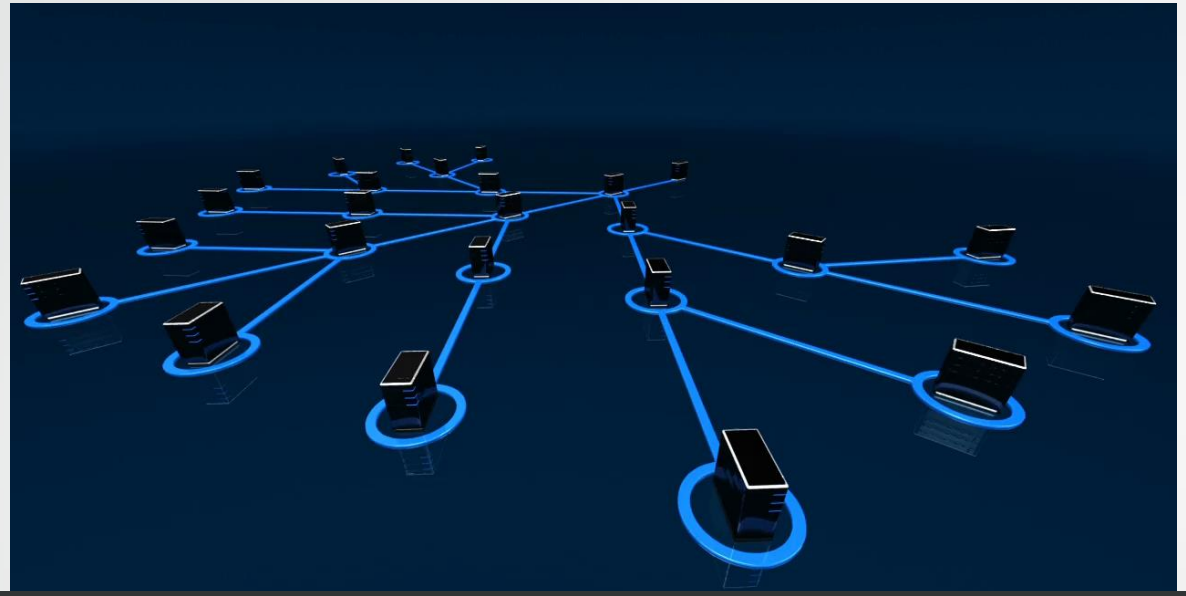
RANSOMWARE: AN INCREASING THREAT

Threat to Medical Practices

- ❑ Some hackers aren't interested in stolen data
- ❑ These hackers just want to make a fast buck (e.g., a Bitcoin payment)
- ❑ All they need is for one employee to engage with their malware
- ❑ Your files are then encrypted/locked!

TMLT
Texas Medical Liability Trust

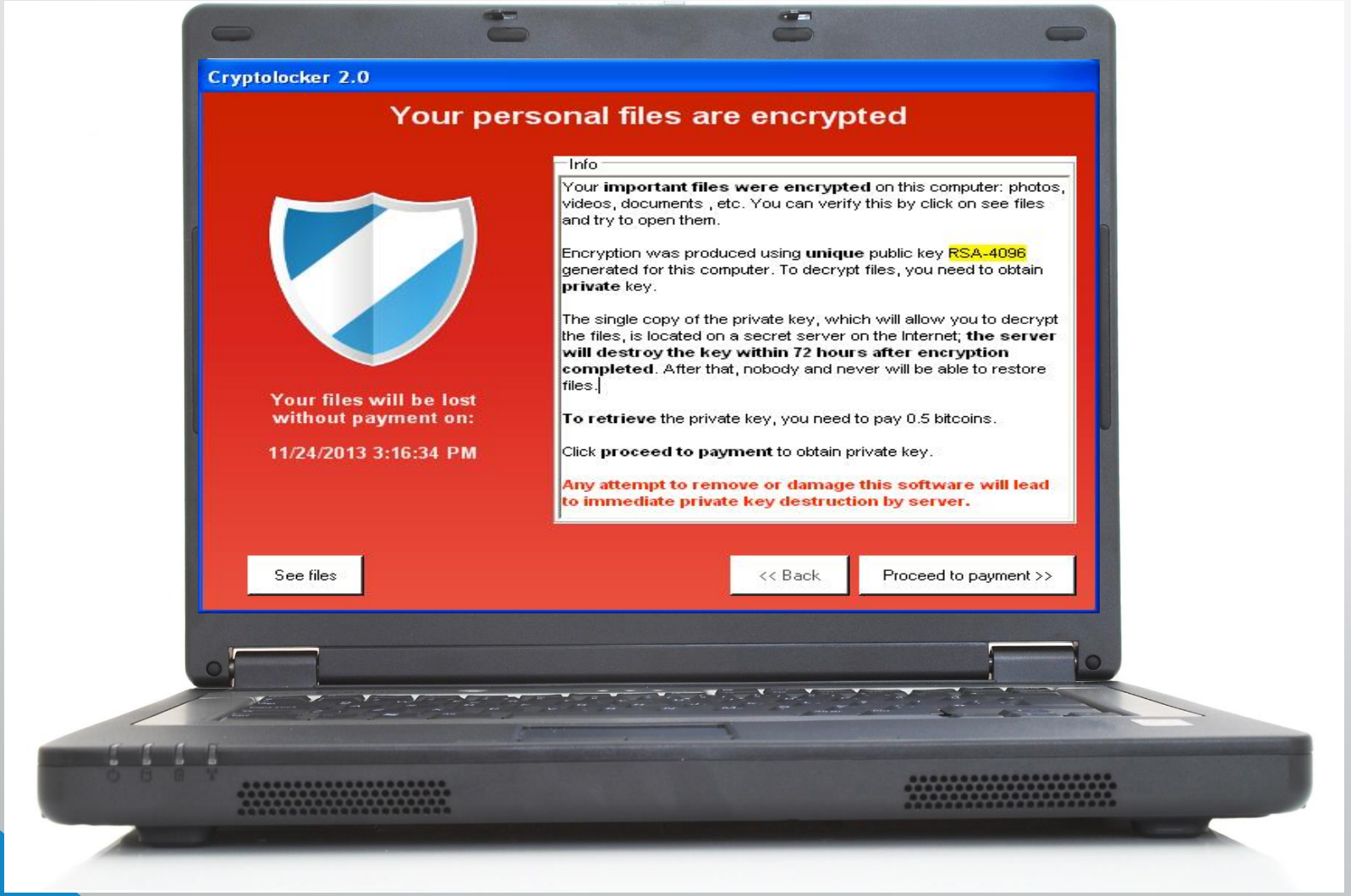
RANSOMWARE



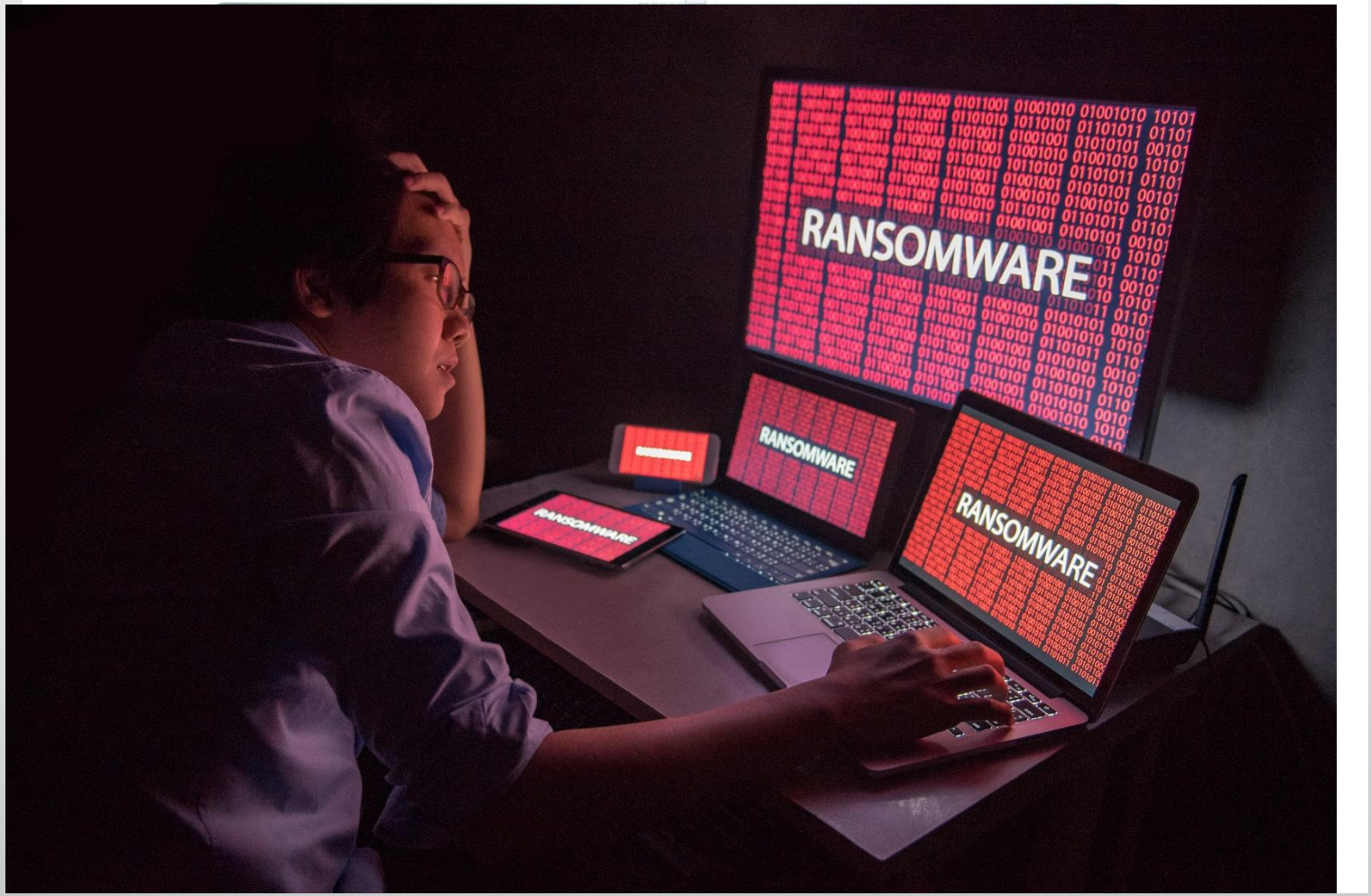
- Ransomware is a form of malware that accesses your electronic data files, passes them through an encryption function, and then stores the resulting encrypted copies in their place.
- The PHI and other sensitive data in your computer are now under the control of a cyber criminal who wants a ransom in exchange for giving access.
- Ransomware itself is mutating and becoming more sophisticated, as more advanced threats will occur.

RANSOM ATTACKS OFTEN END WELL FOR THE CYBERCRIMINALS

YOU ARE JUST DOING WHAT YOU DO EVERYDAY ON YOUR COMPUTER WHEN …



RANSOMWARE EFFECT ON PRACTICES

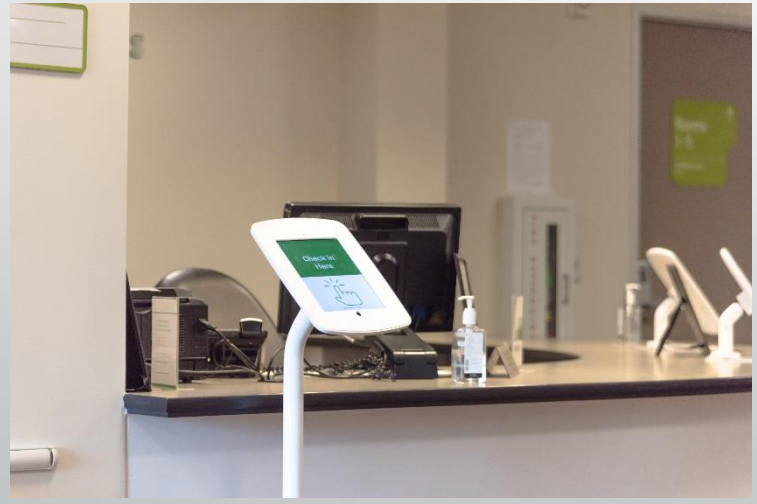


RAPID RISE OF **RANSOMWARE**

- Ransomware is extremely lucrative to cybercriminals
- Average attack yields $1,077 (266% increase since 2015)
- 70% of businesses paid to get their data back in 2016
- 2015 – 2016 there was a 300% increase in ransom attacks (US Dept. of Justice)
- 2016 – 2017 Healthcare saw an 89% increase in ransom attacks (Cryptonite)
- 1 ransom attack every 2 minutes in Q1 2018

WHY IS HEALTH CARE A PRIME TARGET FOR RANSOMWARE ATTACKS?

- April 2014 — FBI warned health care providers their cybersecurity systems were lax compared with other industries.



RANSOMED


Infections can be devastating to an individual or organization.
RANSOMWARE
Recovery can be a difficult process that may require the services of a reputable data recovery specialist

WHAT TO DO IF YOU GET HIT WITH RANSOMWARE

1. Disconnect the computer from the network
2. Alert IT
3. Disable shared drives
4. Alert other users on your network
5. Update and run your security software
6. Notify law enforcement and the FBI
7. Attempt a restore from backup
8. Notify your cyber liability insurance carrier
9. Investigate and do risk assessment to determine if a breach has occurred

FACT SHEET: RANSOMWARE AND HIPAA

FACT SHEET: Ransomware and HIPAA

A recent U.S. Government interagency report indicates that, on average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015).[1] Ransomware exploits human and technical weaknesses to gain access to an organization's technical infrastructure in order to deny the organization access to its own data by encrypting that data. However, there are measures known to be effective to prevent the introduction of ransomware and to recover from a ransomware attack. This document describes ransomware attack prevention and recovery from a healthcare sector perspective, including the role the Health Insurance Portability and Accountability Act (HIPAA) has in assisting HIPAA covered entities and business associates to prevent and recover from ransomware attacks, and how HIPAA breach notification processes should be managed in response to a ransomware attack.

1. What is ransomware?

Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key. However, hackers may deploy

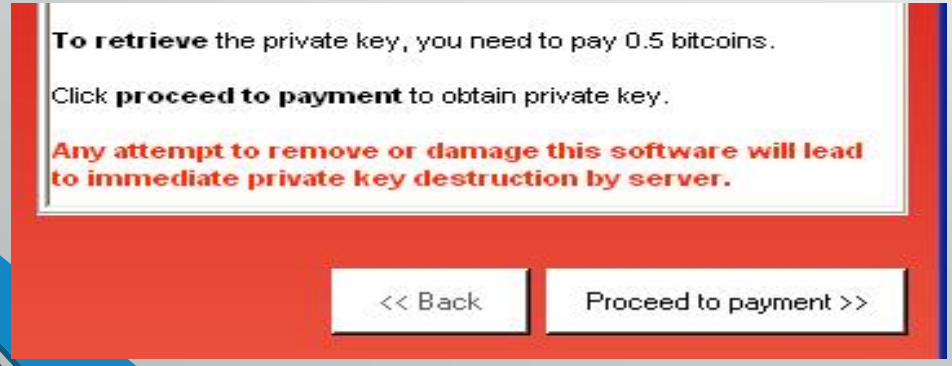
July 11, 2016 — The Health and Human Services (HHS) Office for Civil Rights (OCR) released new HIPAA guidance to help health care entities better understand and respond to the threat of ransomware.

https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

OTHER SIGNS YOU'RE A VICTIM OF RANSOMWARE

Signs of Ransom.doc

Signs of Ransom. xvu



1. A splash screen blocks access
2. Files that won't open
3. Odd or missing file extensions
4. You've received instructions for paying the ransom

Source: CSO 8.9.2016

RANSOM ATTACK – PDF RESUME

IMPACT ON THE PRACTICE

No EHR

No email

No access to digital imaging

Lab results interrupted — unable to access results

Documentation disruptions

Billing and collections interruptions

RANSOMWARE CASE STUDY

2018 – 7:30 a.m.

Arriving at work, the practice is unable to login to the network.

It notified and discover a ransom notice on the server.

Unable to access records the clinic opened using a paper process to see the patients.

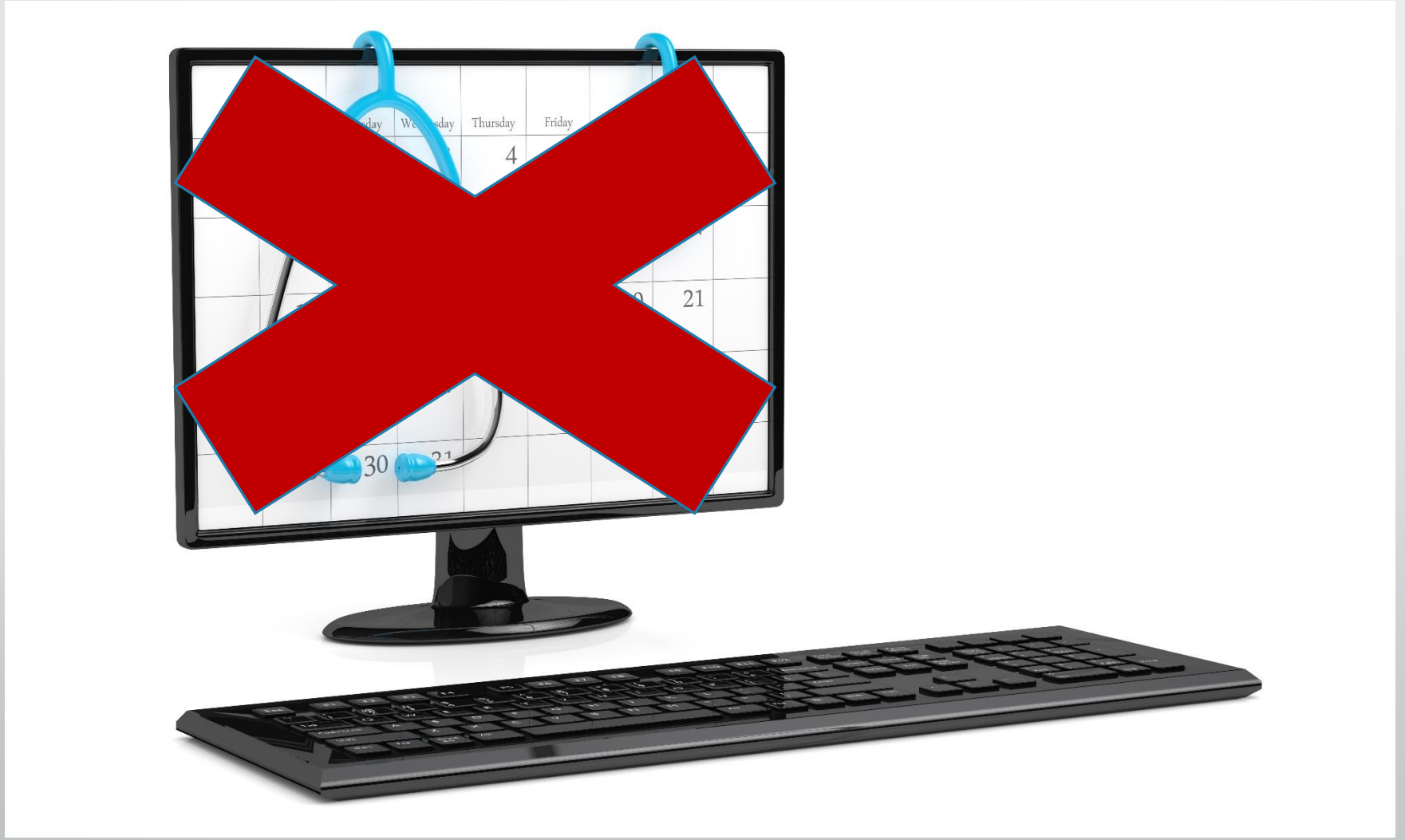
RANSOMWARE CASE STUDY

"The FBI does not condone paying ransom, bu
its agents acknowledge that businesses are
often left with a tough choice."

Source: "Under pressure to digitize everything, hospitals are hackers biggest new target." *The Washington Post*, April 1, 2016

RANSOMWARE CASE STUDY
THE REST OF THE STORY

HACKING/RANSOMWARE
CASE STUDY: PRACTICE MANAGEMENT



HACKING/RANSOMWARE CASE STUDY

HACKING/RANSOMWARE CASE STUDY

- The practice had an inadequate backup process
- The practice had never had a Risk Assessment and Risk Management Plan
- The practice had policy and procedure templates dated 2013 that had never been customized
- There was no recent training of staff
- There had been no training on social engineering

HACKING/RANSOMWARE CASE STUDY

- Cost to Notify Patient and Credit Monitoring and Forensics **$92,000**
- Cost related to OCR Investigation **$29,000**
- IT Cost increased by 170% per month
- **$15,000** to mitigate the effects of the breach (out of pocket)

Total cost of the breach ≈ $ 138,000

OCR Investigation closed after 16 months with no fines or penalties

BUSINESS CONTINUITY

Business continuity considerations:

- Back up data regularly. Verify the integrity of those backups and test the restoration process to ensure it is working.
- Conduct an annual penetration test and vulnerability assessment.
- Secure your backups. Ensure backups are not connected permanently to the computers and networks they are backing up.
- **Backups are critical in ransomware recovery and response; if you are infected, a backup may be the best way to recover your critical data**.

HIPAA AND RANSOMWARE

If You Are a Victim Of Ransomware, Does That Constitute a HIPAA Breach?

It

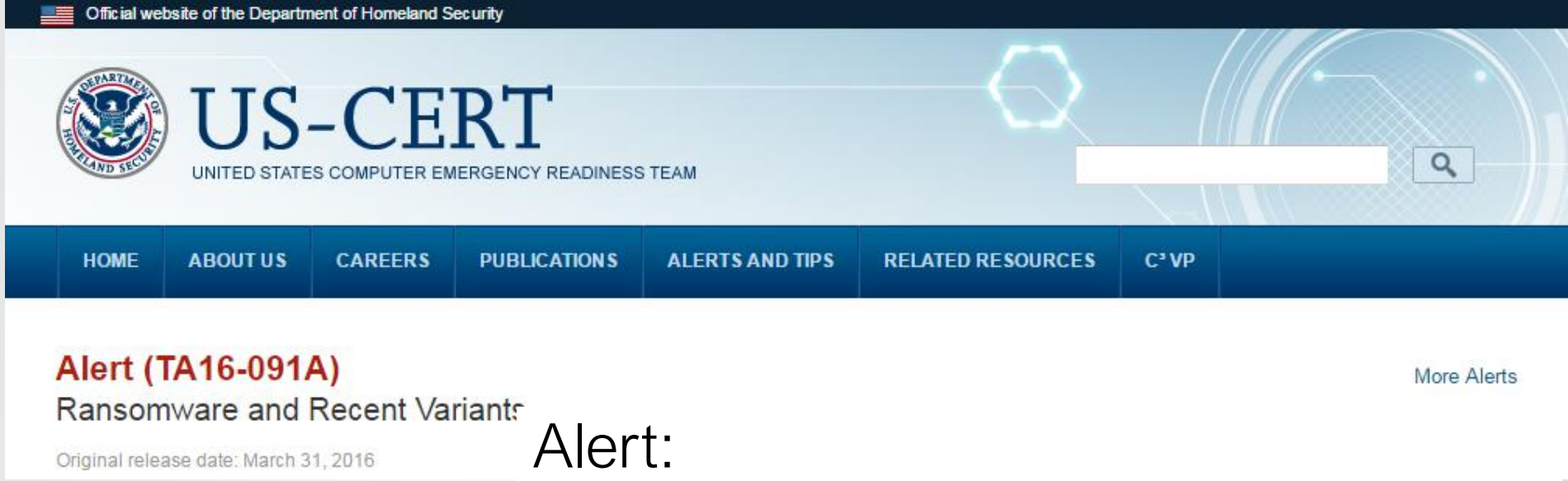
Depends!

IT RESPONDS TO PRESSURE TO RESTORE DATA

LESSONS LEARNED

Practices must:

- have a Data Backup process
- have an Emergency Plan
- have a Contingency Plan
- must test your processes and plans at least annually
- train workforce how to respond to IT issues
- preserve evidence



US-CERT — for information on safely handling email attachments, see *Recognizing and Avoiding Email Scams*. Follow safe practices when browsing the web. See *Good Security Habits* and *Safeguarding Your Data* for additional details.

Alert:

- 2016 increase in destructive ransomware
- Infecting computers — individuals and businesses — including health care
- Provides guidance on user prevention and mitigation

www.us-cert.gov/ncas/alerts/TA16-091A

BASIC HEALTHCARE CYBERSECURITY TIPS

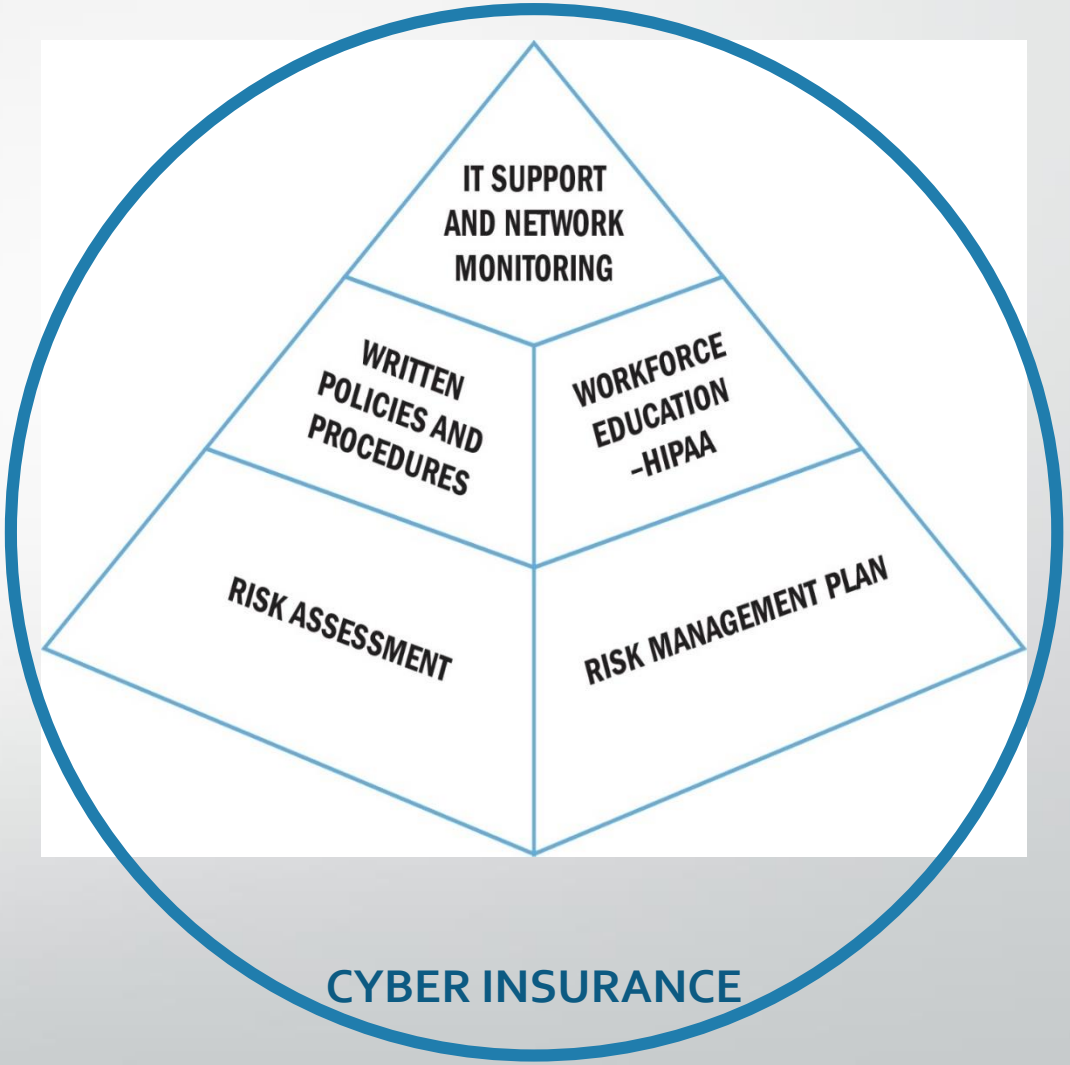
- Establish a security culture
- Encrypt/protect data on mobile devices
- Backup data in real-time & store it off-line
- Use a firewall
- Immediately install updates/patches
- Control access to all PHI
- Use strong passwords & change them regularly
- Limit network access
- Control physical access

CYBER RISK MANAGEMENT

- **Everyone has a role in Cyber Risk Management**
  - Physicians
  - Leadership
  - Clinical Staff
  - Operations

- **Cyber Risk Management must address People – Processes – Technology**

- **Risk Transfer – Cyber Insurance is your safety net when something bad happens despite all the hard work you have done.**



RISK TRANSFER IS NOT RISK MANAGEMENT

Cyber insurance is not a substitute for a good cyber risk management program, as all losses may not be covered by an insurance policy.

Increasing cyber risks and regulatory violations *require* cybersecurity to be integrated into your business risk.

Complacency is not a risk management strategy!

TMLT
Texas Medical Liability Trust

As leaders in your practice you must work to:

- ✓ Understand that Medical Privacy and Security is federal law, but it is also good for business
- ✓ Understand the level of compliance/documentation the OCR expects
- ✓ Know that TMLT Cyber Risk Management services assist your practice ***proactively*** to become HIPAA Compliant or ***reactively*** in the event of an OCR Audit or Investigation
- ✓ Know how to report a Cyber Incident to TMLT
- ✓ Understand your Insurance coverage

- ✓ **Do not assume**
  - IT Company not your Security Officer
  - Employees do not know the Current Threats
- ✓ **Know how to report a Cyber Incident**
- ✓ **Risk Assessment by a Third Party**
  - Every 2 Years
  - 2/3 of all hacking and ransomware from Remote Desktop Connections (RDP)
- ✓ **Separate Privacy and Security Officers**
- ✓ **Train Your Staff**
  - Phishing campaigns
  - Interoffice newsletters or memos
  - Sanctions policy
- ✓ **Have good resources for HIPAA Information**

RESOURCES FOR

CYBERSECURITY RISKS AND REQUIREMENTS FOR PHYSICIANS

TMLT

https://www.tmlt.org/tmlt/products-services/cyber-consulting-services.html

TMA

https://www.texmed.org/Search/Content/?searchtext=CYBERSECURITY

HEALTH AND HUMAN SERVICES CYBERSECURITY GUIDANCE

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

Achieved 2016 and 2017

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/cybersecurity-newsletter-archive/index.html

OFFICE OF NATIONAL COORDINATOR

https://search.usa.gov/search?utf8=%E2%9C%93&affiliate=www.healthit.gov&query=CYBERSECURITY

Cathy Bryant

Cathy-Bryant@tmlt.org

512-425-5910

CYBER@TMLT

Quarterly e-newsletter focusing on the latest cyber security news and trends in health care.

TMLT
Texas Medical Liability Trust

PROTECTION FOR A NEW ERA OF MEDICINE.

First Name* Last Name*

Email Address*

Are you a physician?*
Yes
No

Please list your specialty or occupation.

Are you a TMLT policyholder?*
Yes
No

SUBMIT

ABOUT CYBER @TMLT

The Cyber @TMLT e-newsletter focuses on the latest cyber security news and trends in health care. Our ultimate goal is to help you keep your patient data safe by offering security best practices and guidance, along with the latest risk alerts and updates from HIPAA and the U.S. Department of Health & Human Services. Articles and resources are geared specifically to physicians, but group administrators and IT professionals will also find the newsletter's content relevant and useful.

The newsletter is emailed quarterly with the next issue sending August 10, 2017.

ABOUT TMLT

With more than 20,000 health care professionals in its care, Texas Medical Liability Trust (TMLT) provides malpractice insurance and related products to physicians. Our purpose is to make a positive impact on the quality of health care for patients by educating, protecting, and defending physicians.

WWW.TMLT.ORG/CYBERNEWS

- ✓ **Become invested in Cybersecurity as owners and leaders in the practice**
  - Can get sued in Texas for a Privacy Breach / Medical Board Complaint
  - Will have to do it anyway and it will
  - Lower any potential fines and penalties
- ✓ **Make a Budget – Money and Time**
  - Budget 2 Days of Time per Quarter for HIPAA – 8 Days Total
- ✓ **Do a Risk Assessment and make a Risk Management Plan**
- ✓ **Spend Time and Money on Policies & Procedures**
- ✓ **Understand what your Cyber Insurance covers**

PRACTICES MAY NEED EXPERT GUIDANCE

As the forms of connected technology used by healthcare providers increase—so will your cybersecurity risks.

Therefore, providers will need assistance in mitigating the proliferation & diversity of cyber risks, including help with their:

- ✓IT Systems;
- ✓HIPAA Privacy and Security Risk Assessments;
- ✓Staff Privacy Training; and
- ✓Risk Transfer (cyber insurance).

QUESTIONS

Cathy Bryant

Cathy-Bryant@tmlt.org

512-425-5910