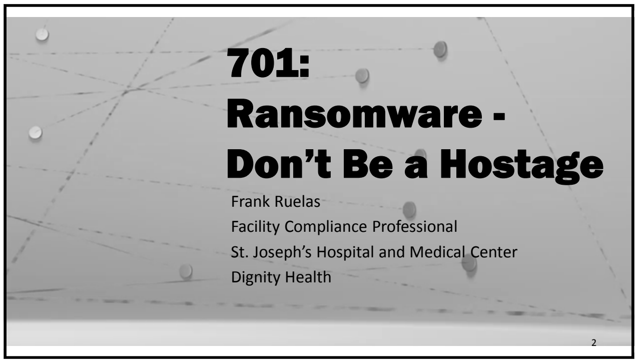
Clinical Practice Compliance Conference

October 15-17, 2017 | Phoenix, AZ

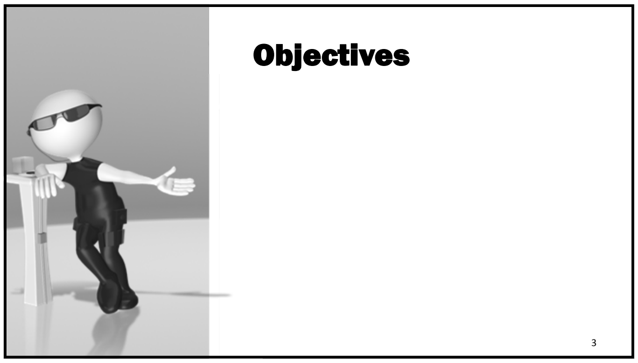
1



701: Ransomware - Don’t Be a Hostage

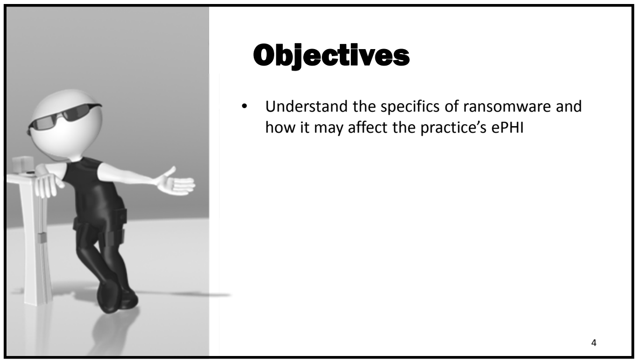
Frank Ruelas
Facility Compliance Professional
St. Joseph’s Hospital and Medical Center
Dignity Health

2



Objectives

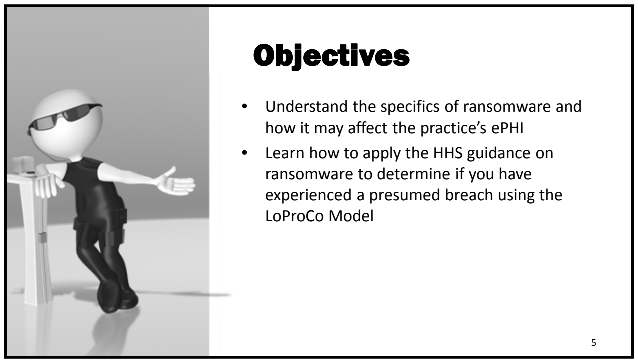
3



Objectives

- Understand the specifics of ransomware and how it may affect the practice's ePHI

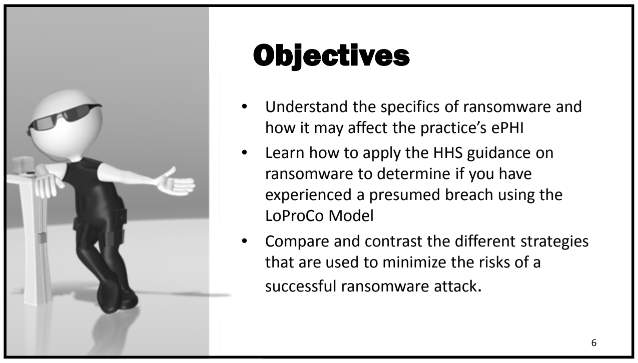
4



Objectives

- Understand the specifics of ransomware and how it may affect the practice's ePHI
- Learn how to apply the HHS guidance on ransomware to determine if you have experienced a presumed breach using the LoProCo Model

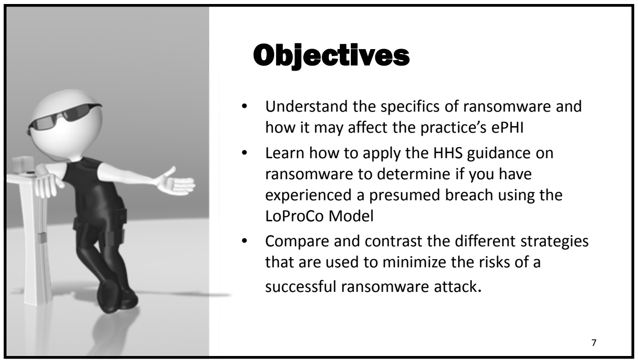
5



Objectives

- Understand the specifics of ransomware and how it may affect the practice's ePHI
- Learn how to apply the HHS guidance on ransomware to determine if you have experienced a presumed breach using the LoProCo Model
- Compare and contrast the different strategies that are used to minimize the risks of a successful ransomware attack.

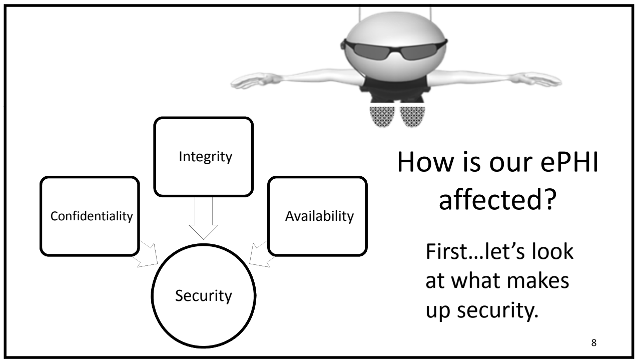
6



Objectives

- Understand the specifics of ransomware and how it may affect the practice’s ePHI
- Learn how to apply the HHS guidance on ransomware to determine if you have experienced a presumed breach using the LoProCo Model
- Compare and contrast the different strategies that are used to minimize the risks of a successful ransomware attack.

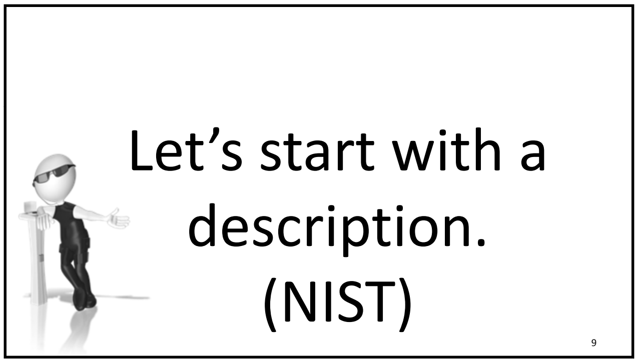
7



How is our ePHI affected?

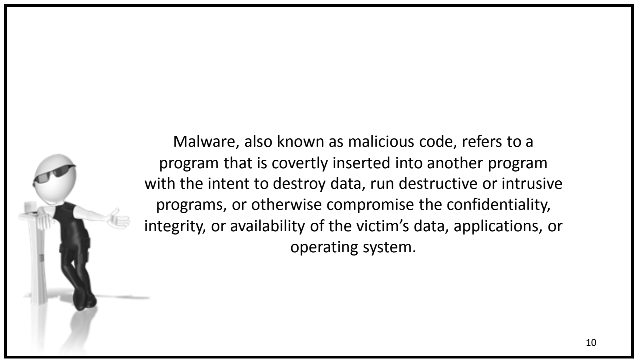
First…let’s look at what makes up security.

8



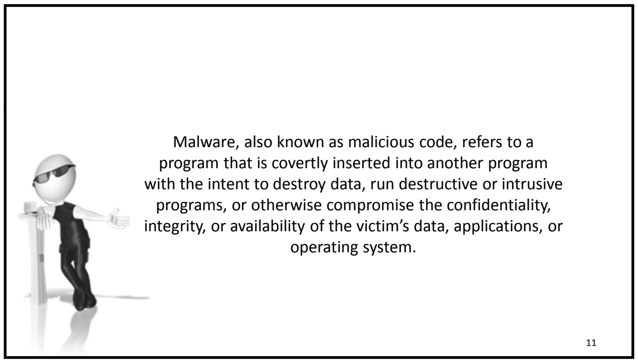
Let’s start with a description. (NIST)

9



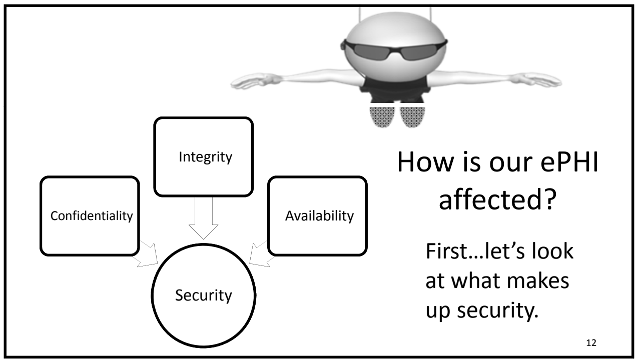
Malware, also known as malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

10



Malware, also known as malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

11



Integrity

Confidentiality

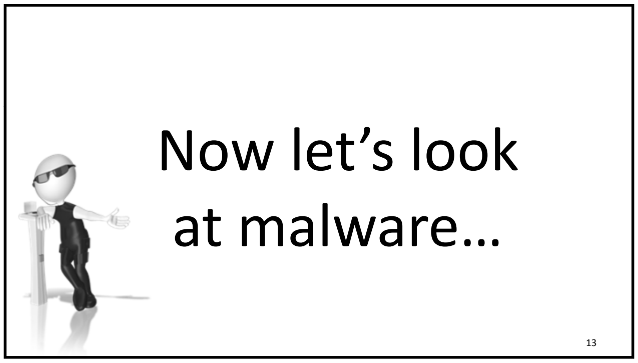
Availability

Security

How is our ePHI affected?

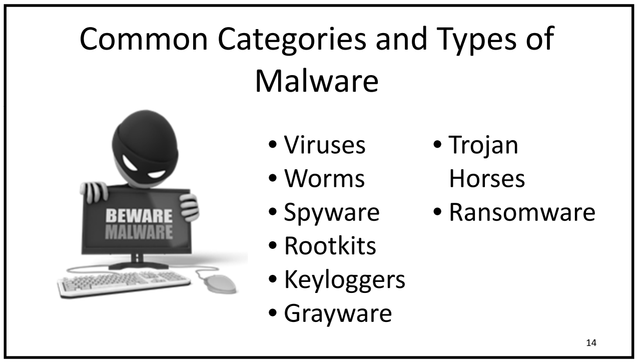
First…let's look at what makes up security.

12



Now let's look at malware…

13

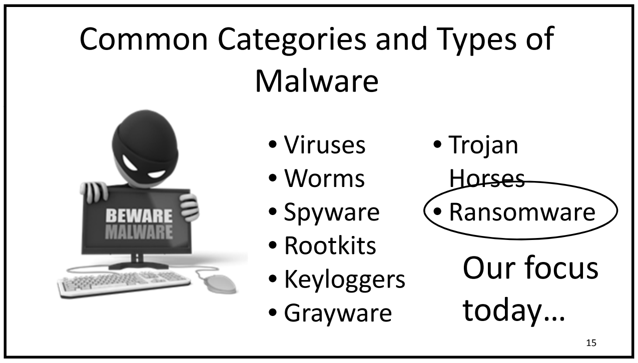


Common Categories and Types of Malware

- Viruses
- Worms
- Spyware
- Rootkits
- Keyloggers
- Grayware
- Trojan Horses
- Ransomware

BEWARE
MALWARE

14



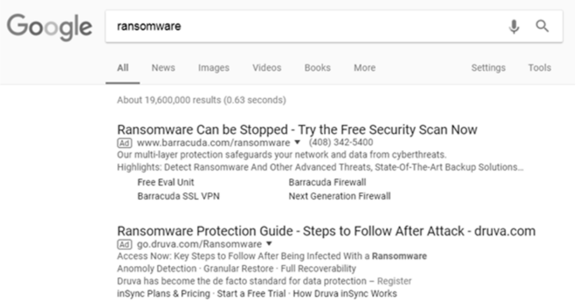
Common Categories and Types of Malware

- Viruses
- Worms
- Spyware
- Rootkits
- Keyloggers
- Grayware
- Trojan Horses
- Ransomware

Our focus today…

BEWARE
MALWARE

15



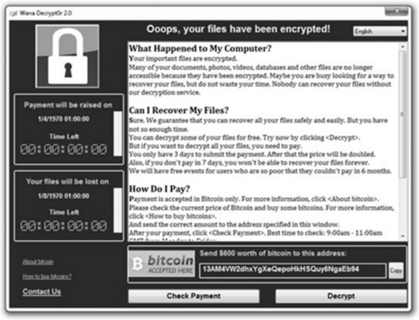
About 19,600,000 results (0.63 seconds)

Ransomware Can be Stopped - Try the Free Security Scan Now
Ad www.barracuda.com/ransomware ▾ (408) 342-5400
Our multi-layer protection safeguards your network and data from cyberthreats.
Highlights: Detect Ransomware And Other Advanced Threats, State-Of-The-Art Backup Solutions...

Free Eval Unit	Barracuda Firewall
Barracuda SSL VPN	Next Generation Firewall

Ransomware Protection Guide - Steps to Follow After Attack - druva.com
Ad go.druva.com/Ransomware ▾
Access Now: Key Steps to Follow After Being Infected With a **Ransomware**
Anomoly Detection · Granular Restore · Full Recoverability
Druva has become the de facto standard for data protection – Register
inSync Plans & Pricing · Start a Free Trial · How Druva inSync Works

16



Ooops, your files have been encrypted!

Payment will be raised on
1/4/1970 01:00:00
Time Left
00:00:00:00

Your files will be lost on
1/8/1970 01:00:00
Time Left
00:00:00:00

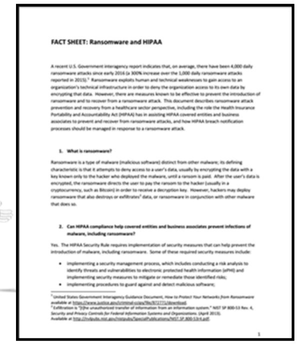
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $600 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

17



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 ransomware that also destroys or exfiltrates[2] data, or ransomware in conjunction with other malware that does so.

2. **Can HIPAA compliance help covered entities and business associates prevent infections of malware, including ransomware?**

Yes. The HIPAA Security Rule requires implementation of security measures that can help prevent the introduction of malware, including ransomware. Some of these required security measures include:

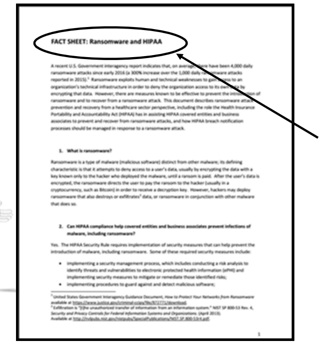
- implementing a security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI) and implementing security measures to mitigate or remediate those identified risks;
- implementing procedures to guard against and detect malicious software;

[1] United States Government Interagency Guidance Document, *How to Protect Your Networks from Ransomware* available at https://www.justice.gov/criminal-ccips/file/872771/download.

[2] Exfiltration is "[t]he unauthorized transfer of information from an information system." NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. (April 2013). Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

1

18



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 ransomware that also destroys or exfiltrates[2] data, or ransomware in conjunction with other malware that does so.

2. **Can HIPAA compliance help covered entities and business associates prevent infections of malware, including ransomware?**

Yes. The HIPAA Security Rule requires implementation of security measures that can help prevent the introduction of malware, including ransomware. Some of these required security measures include:

- implementing a security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI) and implementing security measures to mitigate or remediate those identified risks;
- implementing procedures to guard against and detect malicious software;

[1] United States Government Interagency Guidance Document, *How to Protect Your Networks from Ransomware* available at https://www.justice.gov/criminal-ccips/file/872771/download.
[2] Exfiltration is "[t]he unauthorized transfer of information from an information system." NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, (April 2013). Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

1

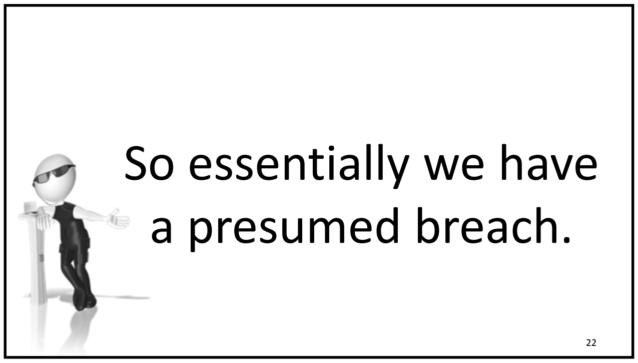
Browser Tip:
Search terms

Unless the covered entity or business associate can demonstrate that there is a "…low probability that the PHI has been compromised," based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred. The entity must then comply with the applicable breach notification provisions, including notification to affected individuals without unreasonable delay, to the Secretary of HHS, and to the media (for breaches affecting over 500 individuals) in accordance with HIPAA breach notification requirements. See 45 C.F.R. 164.400-414.

This applies to each of the four "impermissibles"…

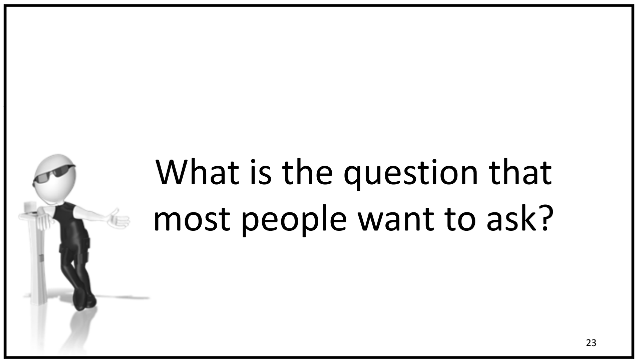
What are the four impermissibles?

- Access
- Acquisition
- Use
- Disclosure



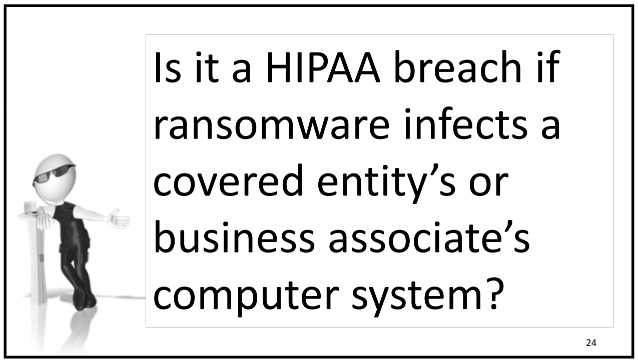
So essentially we have a presumed breach.

22



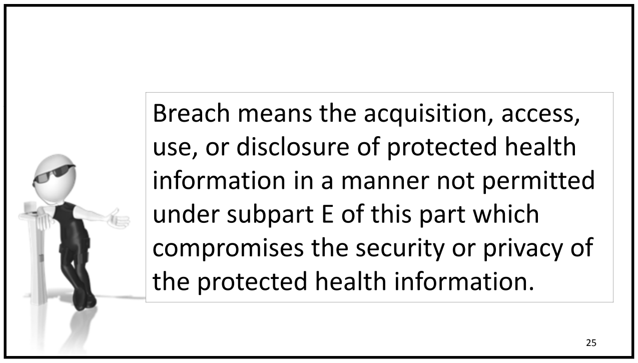
What is the question that most people want to ask?

23



Is it a HIPAA breach if ransomware infects a covered entity’s or business associate’s computer system?

24



Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

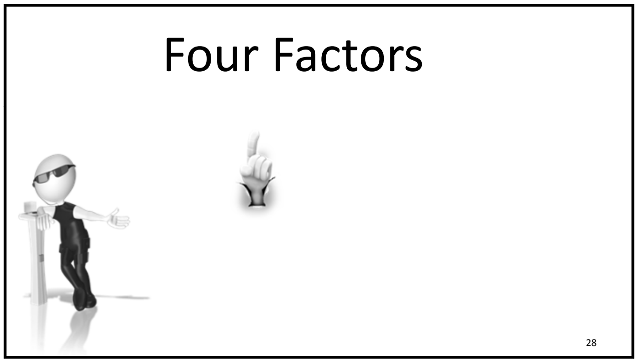
25

Let’s do a LoProCo for a ransomware attack…

26

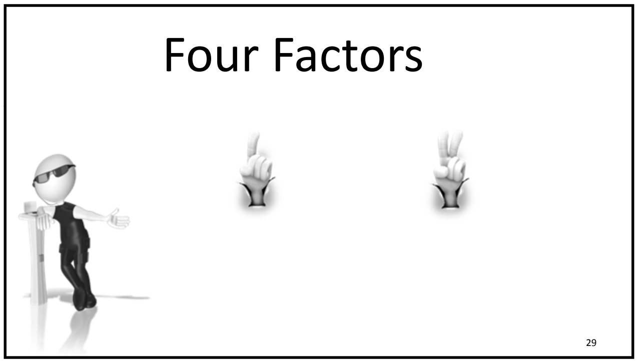
Four Factors

27



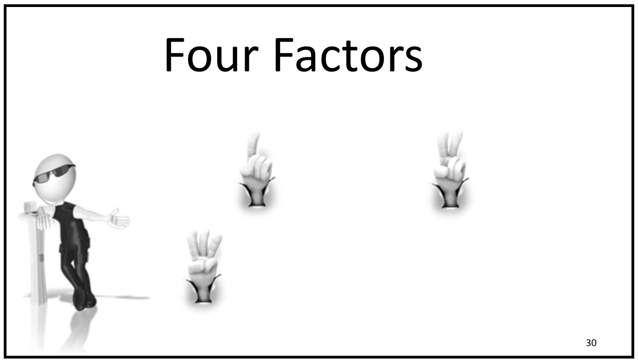
Four Factors

28



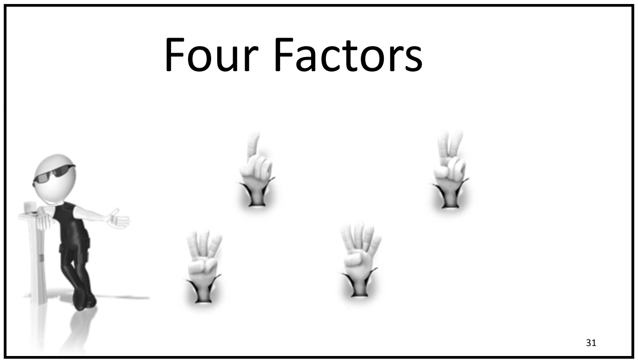
Four Factors

29



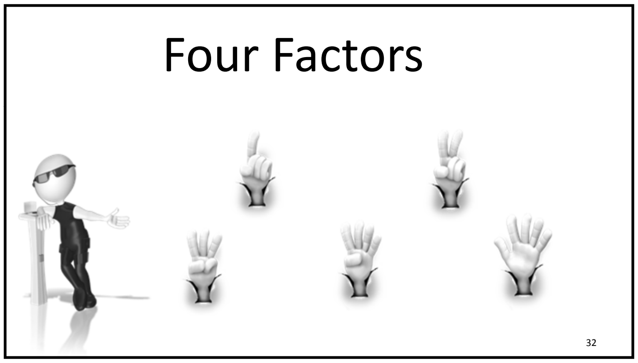
Four Factors

30



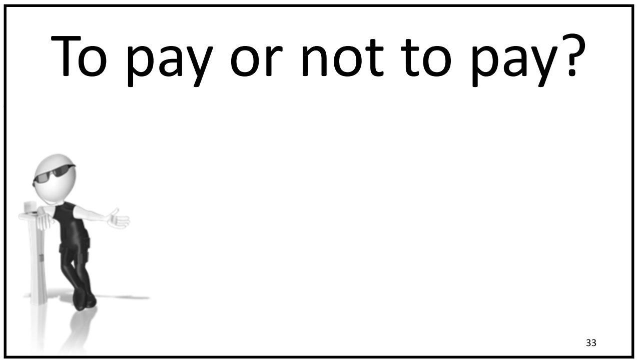
Four Factors

31



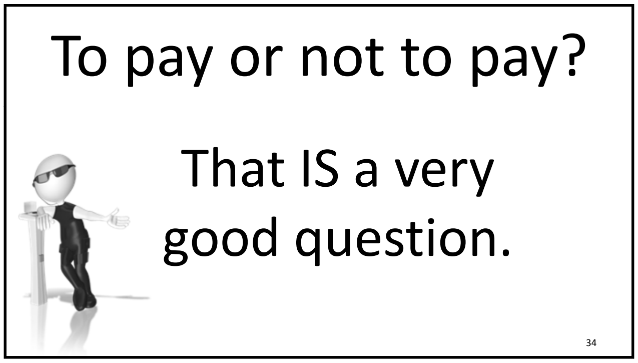
Four Factors

32



To pay or not to pay?

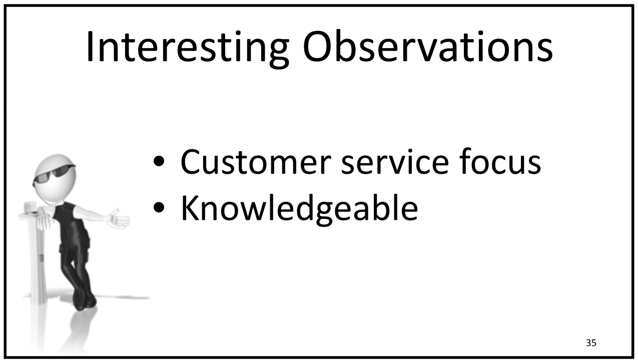
33



To pay or not to pay?

That IS a very good question.

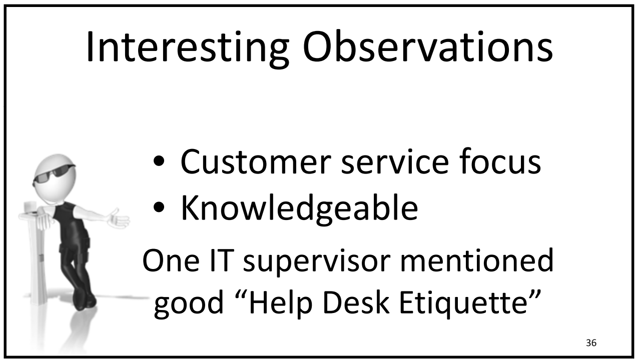
34



Interesting Observations

- Customer service focus
- Knowledgeable

35



Interesting Observations

- Customer service focus
- Knowledgeable

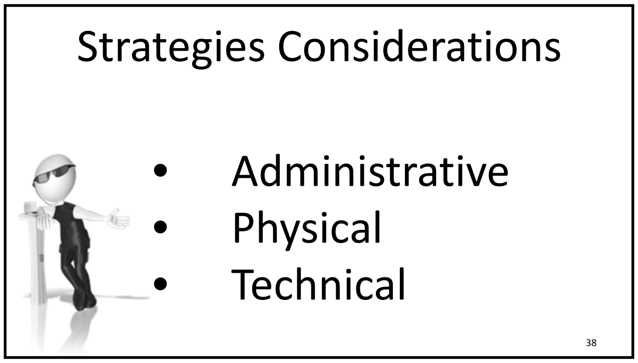
One IT supervisor mentioned good “Help Desk Etiquette”

36

Strategies Considerations

Safeguards

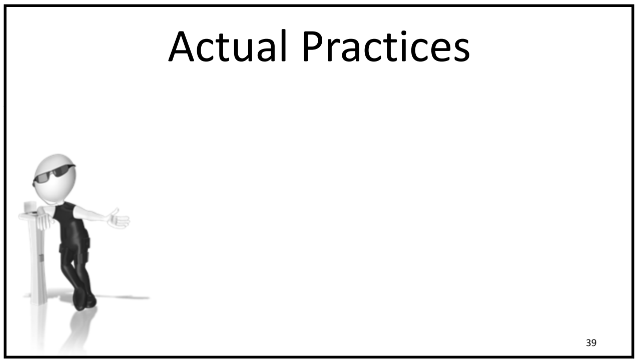
37



Strategies Considerations

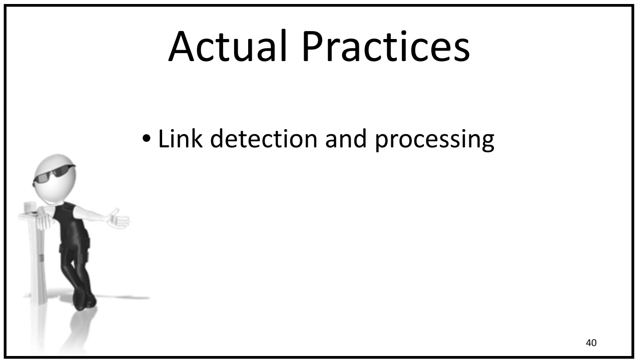
- Administrative
- Physical
- Technical

38



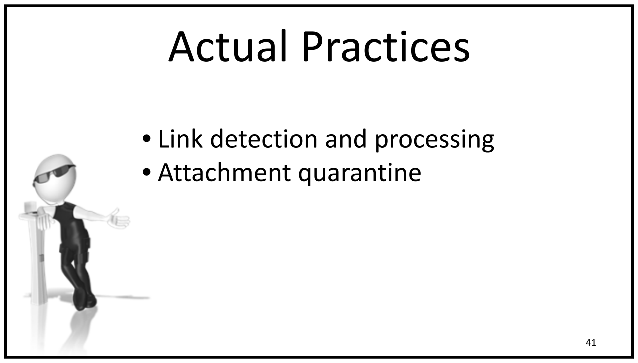
Actual Practices

39



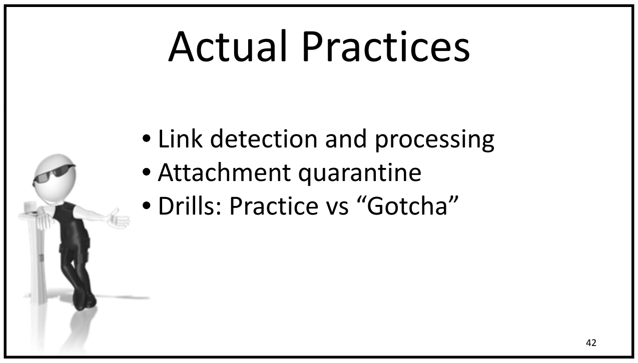
Actual Practices

- Link detection and processing



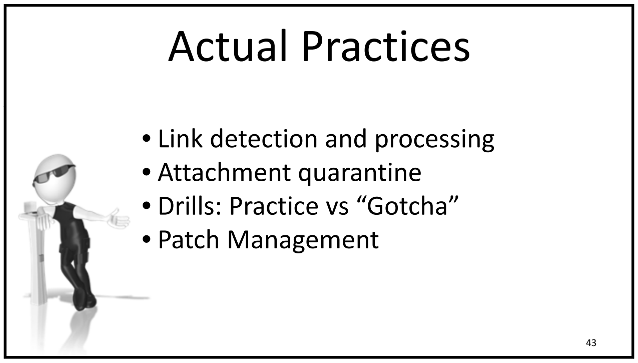
Actual Practices

- Link detection and processing
- Attachment quarantine



Actual Practices

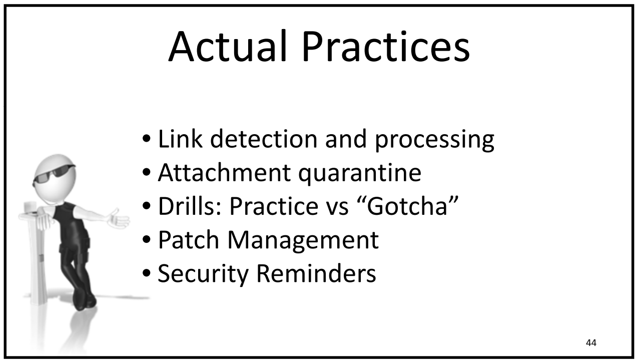
- Link detection and processing
- Attachment quarantine
- Drills: Practice vs “Gotcha”



Actual Practices

- Link detection and processing
- Attachment quarantine
- Drills: Practice vs "Gotcha"
- Patch Management

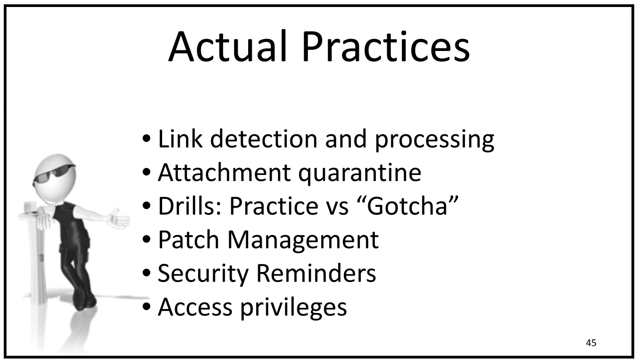
43



Actual Practices

- Link detection and processing
- Attachment quarantine
- Drills: Practice vs "Gotcha"
- Patch Management
- Security Reminders

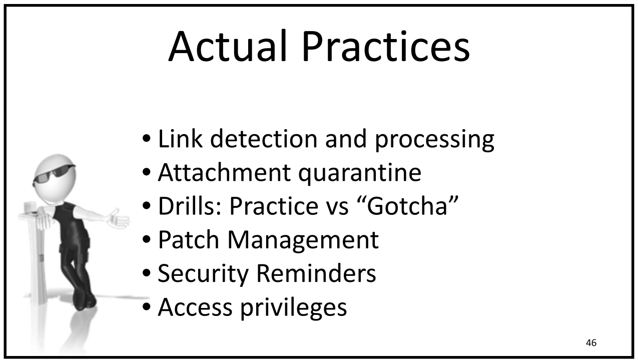
44



Actual Practices

- Link detection and processing
- Attachment quarantine
- Drills: Practice vs "Gotcha"
- Patch Management
- Security Reminders
- Access privileges

45



Actual Practices

- Link detection and processing
- Attachment quarantine
- Drills: Practice vs “Gotcha”
- Patch Management
- Security Reminders
- Access privileges

46