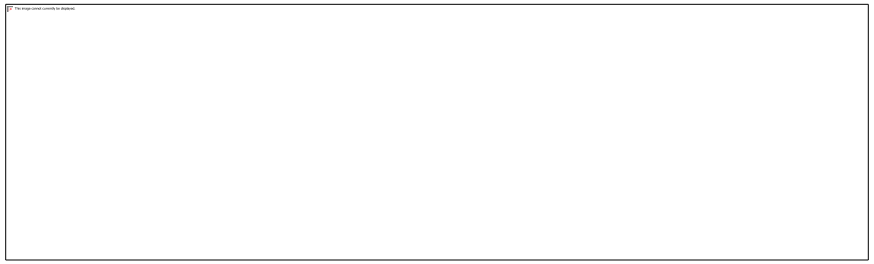


Why Hackers are Targeting Healthcare

Sarah Badahman, HIPAAtrek

Why are We Being Attacked

The Weakest Link

- 72% increase in healthcare attacks since 2013
- Hackers exploit the fact that healthcare professionals are nurturers and caregivers by nature
- Technology has grown faster than security measures

Health Information on the Black Market

- Worth 10x more than credit card information
- Average of $363 per healthcare record

Why are We Vulnerable to Attacks?

Why Haven't We Addressed Security?

- Not viewed as critical to patient care
- Technology shortcuts are culturally "OK" in healthcare
- Budget – Tech is **expensive** to adopt and maintain
- Interruption of existing workflows are met with resistance

Why are We Vulnerable to Attacks?

- Lack of…
  - Authentication
  - Encrypted Data at Rest (Stored Data)
  - Comprehensive inventory
  - Basic security procedures
- Use of insecure emails and outdated technology
- Must train staff on recognizing potential malware!

Hacking/IT Incident Facts

Highest Attacked Locations

- Network Servers
- EMR
- Email
- Desktop Computers

Many of the breaches affected more than 1 location

- Network Server
- EMR
- Desktop Computer
- Email

10 Largest Breaches from 2017 were all Hacking Incidents

Common Social Engineering Techniques

- Ransomware
- Malvertising
- Phishing
- ClickBait
- Pretexting
- Tailgating

Trojan Virus

- Destructive program that masquerades as a benign application or upgrade
- How Trojans Wreak Havoc
  - Harmless messages or "pranks"
  - Stolen passwords
  - Learning of keystrokes
- How to Detect
  - Slow running machines
  - Antivirus
  - Comprehensive monitoring
- How to Prevent
  - Double-check emails
  - Common sense browsing
  - Be sure of every download before opening it

Botnet

- Allows an attacker to take over a computer
  - Affected machines are called zombies
- Stealing of information
  - Identity Theft
- Denial of Service (Dos)
  - Ransomware
- Clickfraud
  - Fraudulently increasing click-based ad revenue

ClickBait

Social Media's Role in Luring Users

- BuzzFeed, Facebook well-known for having clickbait
- Most websites just want your click
  - Can you tell which sites have malware and which don't?
- Automatically posts onto your Social Media page to spread malware to your friends!

X Marks the Spot

Sneaky Hacker Devils

- Remember that X icon that was supposed to close the popup?
  - It was loading a hidden iframe
- The popup is controlled by JavaScript
  - Disable the execution of any scripts by configuration or browser add-ons
- Force quit the browser when a popup appears.
- Never trust the links, especially those clickbait ones!

Bombardment of Ads

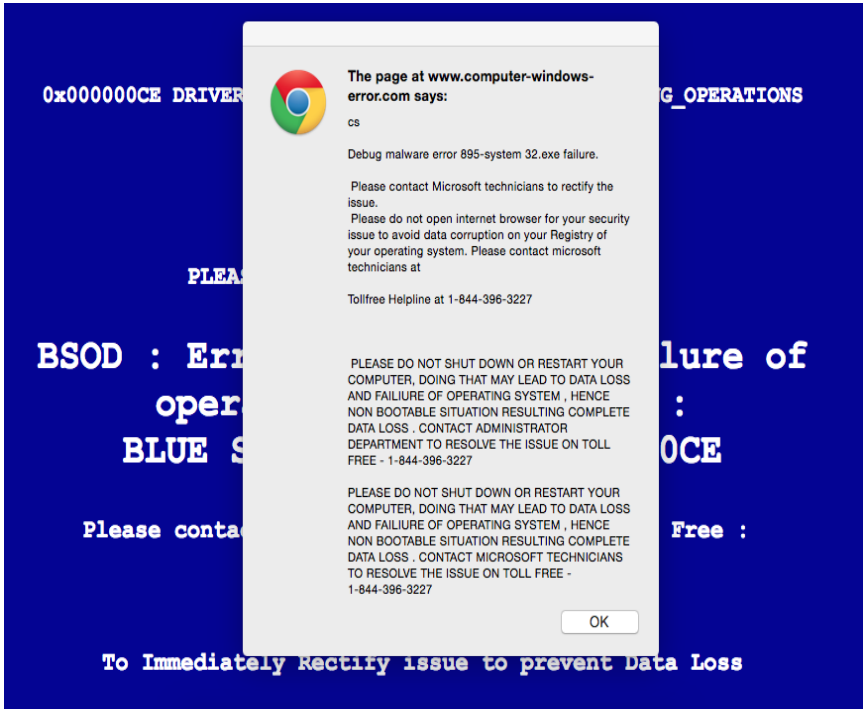
The Dawn of Malvertising

- Malicious ads do not require any type of user interaction in order to execute their payload

- Browsing to a website that has ads is enough to start the infection chain

Malvertising

- Malvertisers bid on keywords that are highly searched
  - Using reputable company names to launch their attack.
- Interested in an ad? Type the name directly in your browser



Ransomware

- A type of malicious software designed to block access to a computer system until a sum of money is paid.
  - CryptoLocker
  - CryptoWall
  - Locky

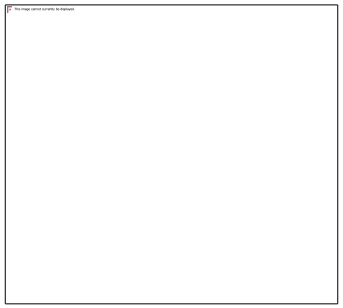
- Ransomware is on pace to be a **$1 billion** a year crime this year.

How to Prevent Ransomware

- Group policy setting
  - Stop applications from installing in temp folder
- Active monitoring antivirus and antimalware
- Don’t allow .exe files in email
  - Active content scanning and filtering on mail servers
- Limit end user access to network drives

Get Your Data Back from Ransomware

- Deploy and maintain a comprehensive backup solution
  - Datto
  - VSS
  - Make sure to validate backup
    - Backups that don't restore data are useless. Don't find out after its too late



DROWN

- **Decrypting RSA with Obsolete and Weakened eNcryption**

- Specific to the legacy SSLv2 protocol
  - Impact of the flaw could be exposing millions of sites to risk today

- Vulnerability that can enable an attacker to decrypt intercepted TLS connections by abusing connections to an SSLv2 server that uses the same private key

Checklist

- Compressive Backup solution
- Business/Enterprise level firewall
- Business level Antivirus and Antimalware
- Keep software up-to-date with Patching
  - Windows
  - Adobe
  - Java
- Follow up with Vendors about their IT security
  - Hosted EMRs
  - Hosted email

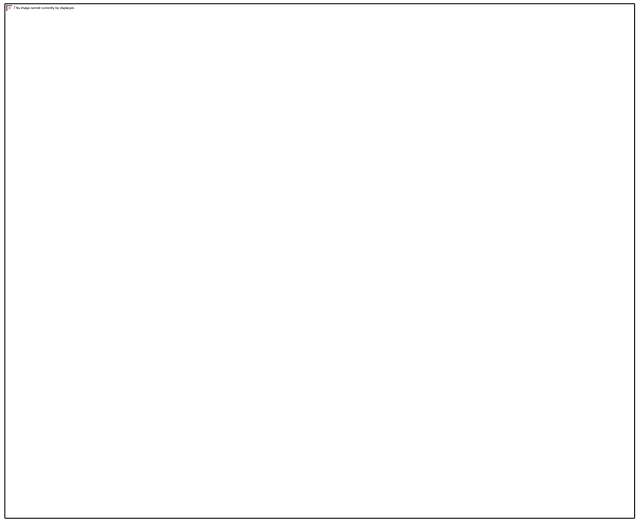
Common Cyber Security Mistakes

Treating Your Work Environment Like Your Home Environment

- Computing habits
  - Browsing
  - Email
  - Social Media
- Physical Security
  - Leaving unlocked and unattended
  - Leaving mobile devices in vulnerable areas
- Security Practices
  - Passwords
  - Firewalls
  - Audit Procedures

Outdated Technology

- Outdated technology costs the health industry $8.3B annually
- Reliance on legacy systems
- Older technology more prone to crashes
- Incapability with newer softwares
- Higher prevalence of cyber attacks and malware
- Less likely to be supported by the manufacturer
- Lost productivity and revenue
- Use of home or non-commercial technology



BYOD Policies Lacking

- Devices included:
  - Laptops, tablets, mobile phones, company owned, employee owned, non-employee owned
- Rules regarding:
  - What is allowed based on operating systems
  - What devices, data types or applications are restricted
  - Monitoring of devices
- Basic controls required for each device
- Enhanced controls required for certain devices

Ignoring Non-Technical Vulnerabilities

- Physical Security
  - Portable Devices
  - Storage
  - Maintenance Records
- Employee
  - Training
  - Hiring
  - Terminating
- Policies and procedures
  - More than just a binder
- Third Parties
  - Business Associate Agreements
  - Security Assessment of third party vendors

Slow to Adopt to Changing Security Landscape

- Healthcare historically lax in security protocols and technology advancements
- Outdated Technology
- Cost major deciding factor for adoption of newer techniques and technologies
  - Less than 6% of operational expenses spent on technology and security
- Lack of education around security

Inadequate Encryption Practices

- Failure to encrypt data at rest
  - Full Disk encryption
    - Only effective on an unbooted computer
    - Files are not protected when moved
  - File Encryption
    - Stay encrypted regardless of where they are stored
    - As long as the file is 'at rest' it is encrypted
- Most thefts involving portable devices and laptops involved unencrypted devices
- Encrypt smart phones and tablets that store, transmit, access ePHI
- Many cost affective solutions
- AES-256 is industry standard in the healthcare industry

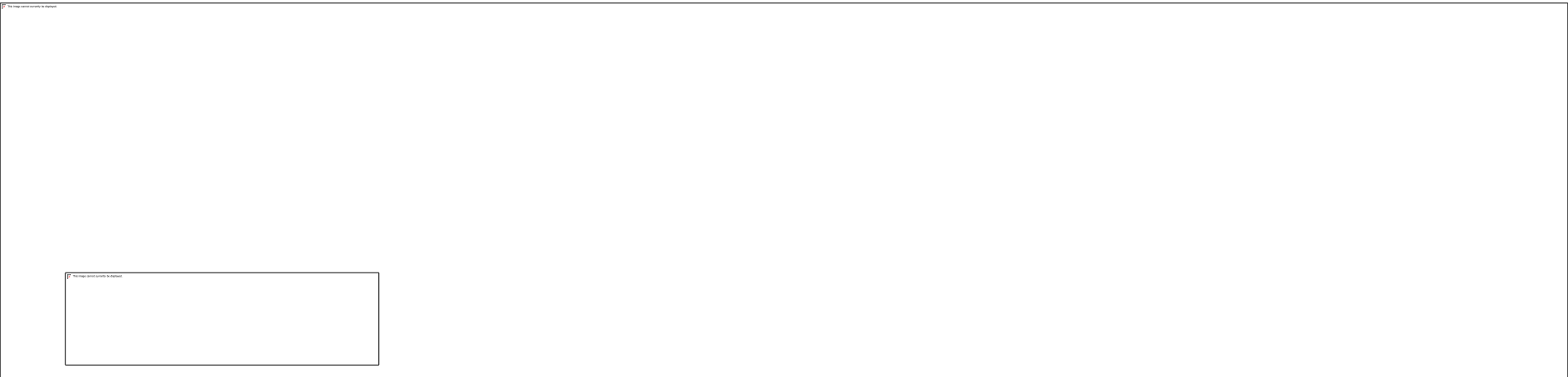
Improper Training Procedures

- Training on HIPAA 101
  - HIPAA requires training on YOUR policies and procedures
  - HIPAA 101 is a good starting place; but not sufficient
- Training as a checkbox vs an opportunity to increase security practices
- Lack of…
  - Routine security reminders
  - Training prior to granting or modifying access to PHI
  - Training when a security/privacy incident occurs
  - Access to policies and procedures

How to Know if Your Network Has Been Compromised

Unusual Outbound Network Traffic

- Monitor firewall logs
  - Unusual traffic
    - Repeated attempts from unusual geographic locations
    - Non-standard ports
  - Malicious patterns
    - Unusual times of day
    - Simultaneous repeated attempts
    - Unusual ports

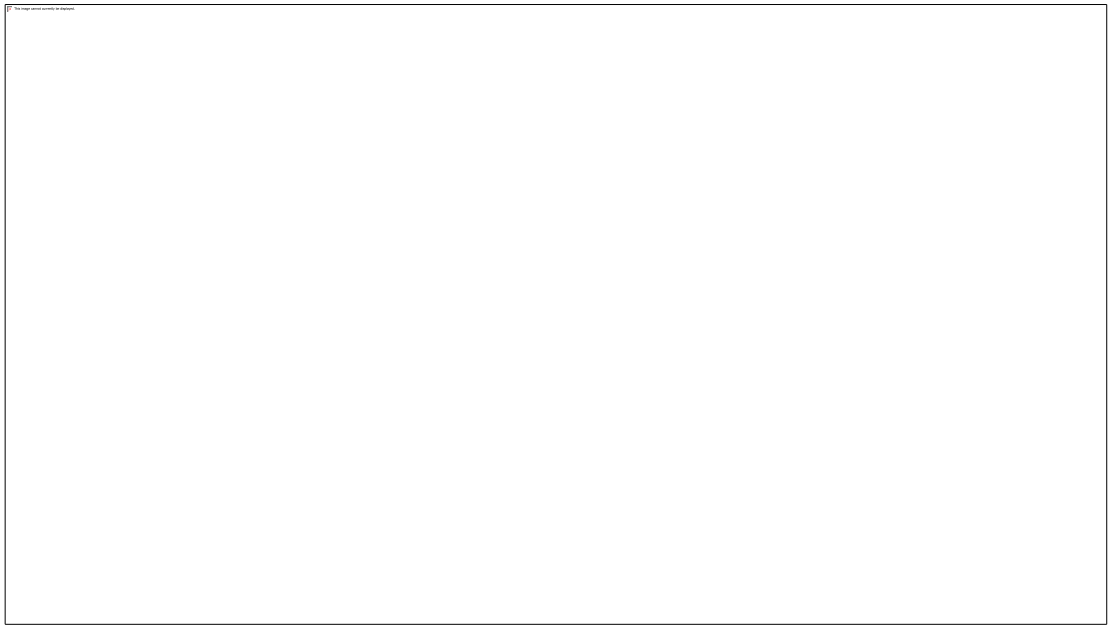


Anomalies in User Accounts

- Social Engineering attacks require interaction
  - Anomaly monitoring powerful tool in recognizing account takeovers
- What to look for
  - Change in personal information
    - Unusual password change requests/executions
    - Unusual date/time logins
    - Work habit changes
      - Accessing or attempting to access restricted files
      - Prolonged activity in off-hours
      - Suspicious geographic logins
      - High volume database queries
    - Unusual download or installation activity

Files in Odd Places

- Large files stored in unusual places
  - Root Folder
  - Recycle Bin
- Hard to detect if you are not monitoring



Focus on Security and compliance will follow

Secure Compliance

Testing Your Vulnerabilities

What are your Weakest Points?

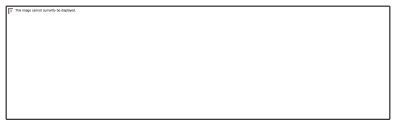
- Human
  - Conduct social engineering penetration testing
    - Email spoofing
    - Pretexting
    - Malicious email attachments
  - Tailgating
    - Technical
    - Non-technical
- Social
  - Find employees on social media
  - Google employees
- Technology
  - Anti-Exploit, Anti-Malware and Anti-Virus installed, up to date, and continuously monitored?
  - Contingency planning in case all fails and you fall victim?

Plan of Action: Implementing Policies

- Project Management
  - Think of procedures as tasks to be completed
  - Compliance is NOT one and done – it is an on-going process
  - *Tying projects together can help staff and providers see the bigger picture and develop a culture of compliance*
- Delegate
  - Compliance is the responsibility of everyone
- Documentation and Tracking
  - Document all efforts – it will help in the event of a breach or audit
  - Review efforts to determine if the procedure is still effective – revise as necessary

Important Steps

- Workforce Training
- Security Reminders
- Social Engineering Penetration Testing
- Evaluating technical and non-technical vulnerabilities
- Social Media Policies are a MUST
- Up-to-date anti-malware that is being monitored for attacks
- Anti-Exploit software
- Use a positive security model and administer privileges with a 'least-access-necessary' mindset
  - Less people with access reduces your risk


This image cannot currently be displayed.