THE VISION COUNCIL

CYBERSECURITY

Vision Expo West

September 18, 2019

CYBER SECURITY

OVERVIEW OF CYBERTHREATS

THE VISION COUNCIL

Who does this and Why?

- Kids/amateurs. General malice, show off to friends
- Reacting out of revenge or vendetta against company/group
- Politically motivated. May be individuals or hacktivist groups. Some state-sponsored?
- Plain old thieves/con men

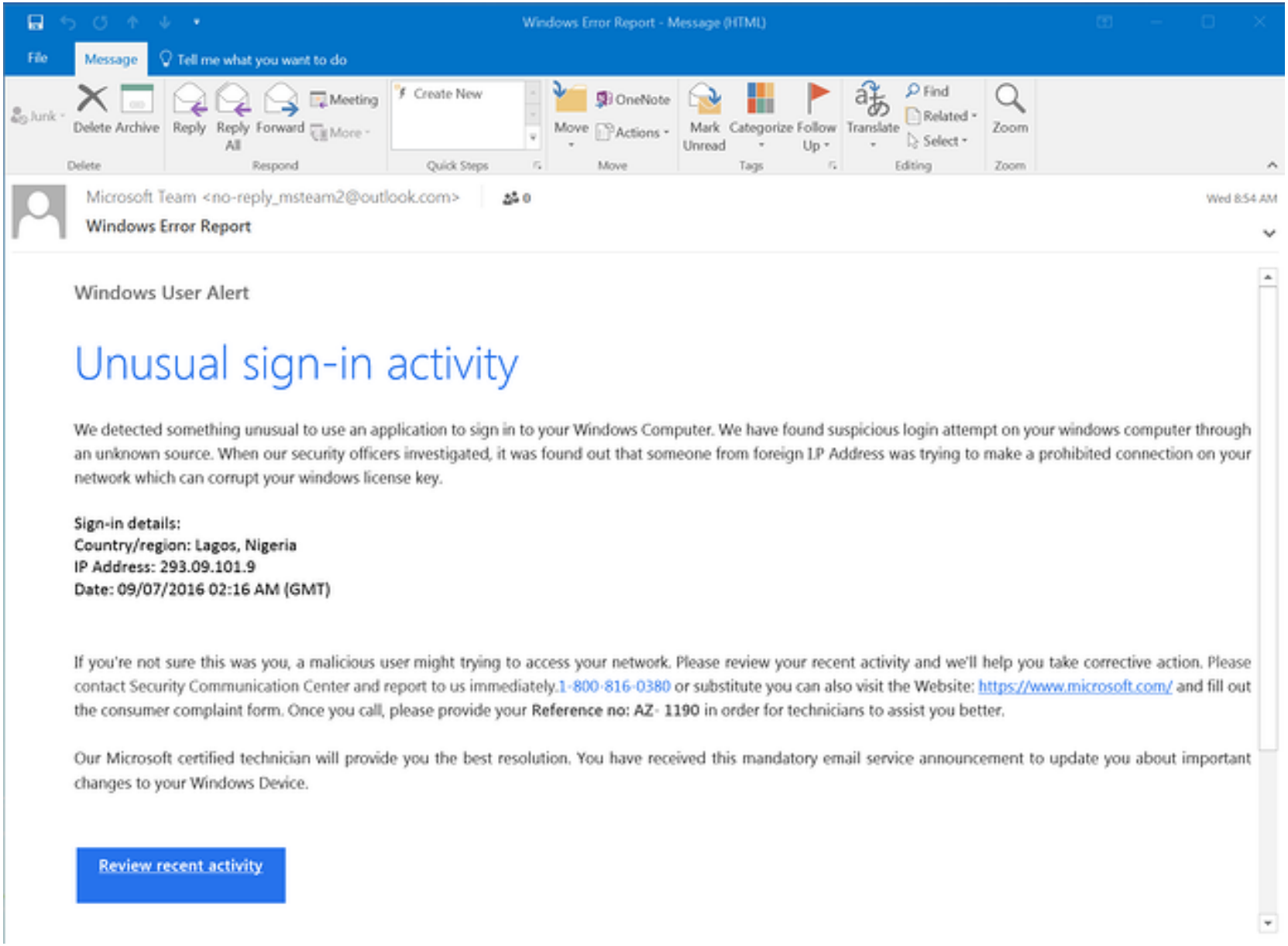
What is Malware

- Short for Malicious Software
- Virus: like a natural virus, describes any malware that self-proliferates
- Trojans: Disguised as legit software, delivered via trickery.
- Spyware: used in a stealthy manner, monitoring activity on a computer.
- Ransomware: Not stealthy, holds data for Ransom

How Attacks Happen or Spread

- Brute Force: Repeated attempts with different login credentials, hoping one will work.
- Email
  - Spam vs Spear Phishing, or Shotgun vs Rifle
- Websites
- Portable Devices

THE VISION COUNCIL


Windows Error Report - Message (HTML)
File
Message
Tell me what you want to do
Junk
Delete
Archive
Reply
Reply All
Forward
Meeting
More
Create New
Move
OneNote
Actions
Mark Unread
Categorize
Follow Up
Translate
Find
Related
Select
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Zoom
Microsoft Team <no-reply_msteam2@outlook.com>
0
Wed 8:54 AM
Windows Error Report
Windows User Alert
Unusual sign-in activity
We detected something unusual to use an application to sign in to your Windows Computer. We have found suspicious login attempt on your windows computer through an unknown source. When our security officers investigated, it was found out that someone from foreign I.P Address was trying to make a prohibited connection on your network which can corrupt your windows license key.
Sign-in details:
Country/region: Lagos, Nigeria
IP Address: 293.09.101.9
Date: 09/07/2016 02:16 AM (GMT)
If you're not sure this was you, a malicious user might trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately.1-800-816-0380 or substitute you can also visit the Website: https://www.microsoft.com/ and fill out the consumer complaint form. Once you call, please provide your Reference no: AZ- 1190 in order for technicians to assist you better.
Our Microsoft certified technician will provide you the best resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.
Review recent activity

Lab Affects Summary

Lab System	Likely source of attack	Most Typical Type of Malware	At Risk:	Potential Ramifications
Corporate Systems	Phishing via email, web site links, Brute Force	Keyboard Logger, Data Encryption (Ransomware)	All documents, on local and Shared drives; Log in Credentials	Loss of data, release of sensitive data, identity theft
LMS Systems	Cross Infection, Portable Devices, mail servers, Remote access computers	Data Encryption (Ransomware)	All files on the server. Most common are .doc/.xls/.txt/.csv files	LAB DOWN. Possible loss of data, loss of production. Possible release of sensitive data
Manufacturing Systems (Equipment)	Portable Devices (USB), Cross Infection	Data Corruption,	System Resource Utilization, Configuration files	Corruption of data, unstable/Inconsistent system, potential loss of use of equipment, potential to cross contaminate to other machines

Latest Trends

- Much more sophisticated Phishing methods
- ‘Codeless’ installations: code can automatically kick off in the browser, no need to actually click on something to activate it.
- Search Engine Optimization: Hackers manipulate search engines, their bogus phone number goes to the top of the search results. Why? Smart Speakers!
- 2019 Healthcare Industry:
  - 2018: 15M patient records compromised, 3x amount from 2017
  - 2019: YTD, already almost double 2018
  - Third party vendors and Phishing attacks are primary source

Recent Healthcare Related Incidents

- Anthem, 2015: Largest US health data breach in history
  - Stole ePHI and other info of 79M people
  - Hackers gained access via a single employee: employee responded to a spear phishing email
  - Anthem paid:
    - $16M HIPAA settlement to Office for Civil Rights (OCR, part of the US Dept of Health and Human Services)
    - $115M class action civil settlement filed by victims.
- Quest Diagnostics, LabCorp, others, 2019:
  - 25M patients affected; personal and financial data, including SSN
  - Source of breach was at a 3rd party, AMCA, a billing services vendor. Breach affected at least 13 other companies including Quest. AMCA is now bankrupt as a result.

Legal

- There is NO single principal data protection legislation in the US (Digital Guardian).
- Most protections are either to specific industry areas (ex HIPAA), or at the state level.
- Laws from state to state vary.
  - In most states, common protected info include:
    - Full Social Security Number
    - Drivers License Number
    - Bank Account info
    - Credit Card Numbers
    - User Passwords and other security codes
    - Medical ID numbers
    - Any login info that can access any of the above accounts
  - Other medical info may be included in separate statutes (Ex: CA)

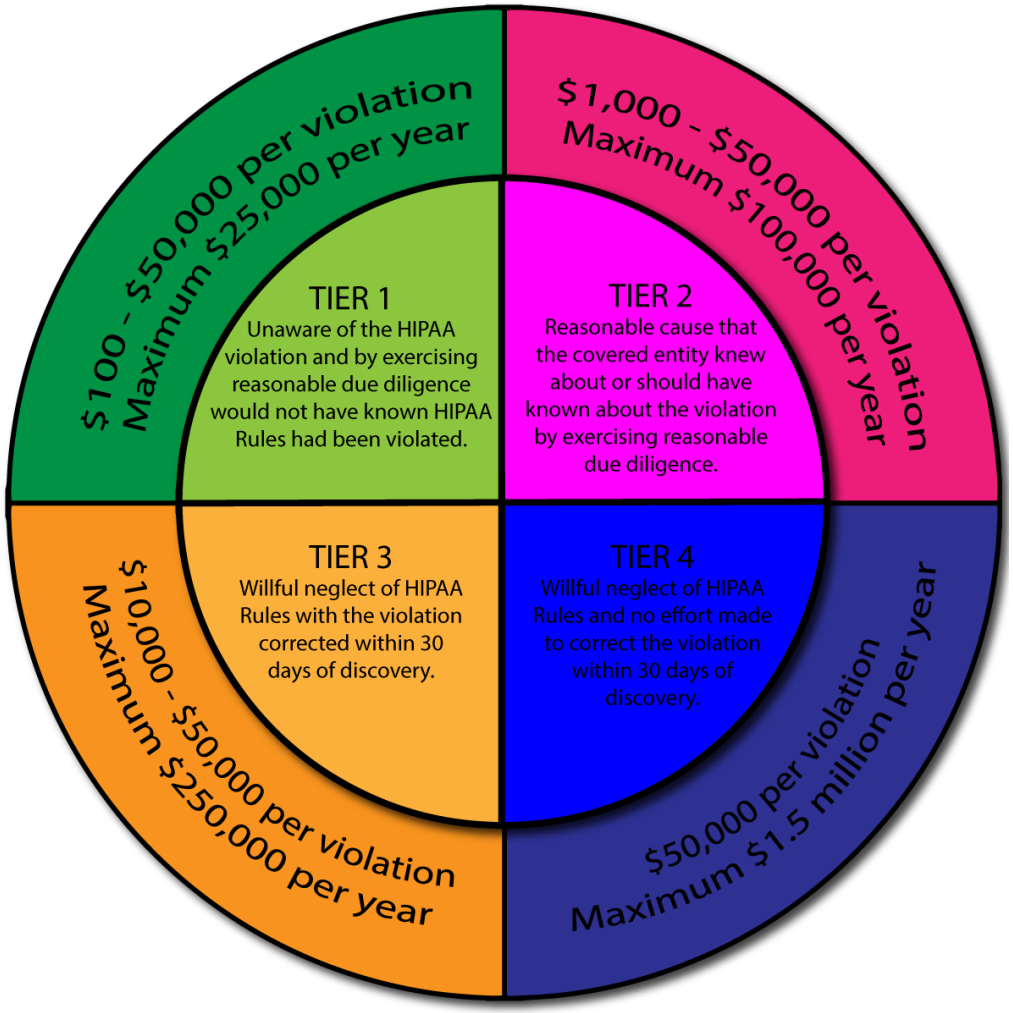
Legal: Notification of Breach

- Each state has their own requirements. Most require:
  - Notification ‘without unnecessary delays’ (unless directed otherwise by law enforcement)
  - Specific information to be shared by affected individuals (ex: Date of breach, description of covered info accessed, etc.).
- Some states may require HOW affected individuals are informed of the breach
- HIPAA requires notification within 60 days.

Legal: Financial Impact

- HIPAA penalties, paid to OCR in the USDHHS, upwards of $50k per violation
- Punitive damages from victims
- Bankruptcy/insolvency: small companies that suffer a data breach: 60% bankrupt within 6 months (Inc. Magazine, May 2018).
  - Cambridge Analytica, Nortel
- Average cost of a data breach: $3.62M (IBM Ponemon Institute Study, 2017

HIPAA Violation Penalties



HIPAA JOURNAL

THE VISION COUNCIL

Cyber Security ACTION ITEMS REVIEW

- Review Previous Presentation for 2017, found on TVC website:
  - https://www.thevisioncouncil.org/members/optical-lab-resources OR: Lab Division, Secure Content, Vision Expo West Lab Division Meeting 2017 Files. OR: PPT, poster and Video links are available.
- Consult your IT group, discuss all vulnerabilities and strategies to mitigate.
- Upgrade all PC's to the latest Operation System (Windows 7 is EOL January 2020!)
- Implement Antivirus on all PC's, ensure they are all kept up to date.
- Coordinate with all equipment vendors to determine best method to update the Operating System (OS) and AV on their equipment.
- Verify Backup Solution is adequate
- Develop USB Use and Remote Access Policies
- Begin/refine/review a BCP/DR
- Post and emphasize the TVC Poster
- Browse TVC site for other resources.
- Key is combination of education+policy+tools

DOWNRIGHT SCARY!

The boogie man may not be out to get you, but cyber-criminals are.

Viruses, phishing attacks and ransomware hidden in emails and other devices can cause loss of data, cripple your network and effectively stop your business—and your job—for days.

- Never open ANY attachment unless you are certain you know the sender.
- Before clicking on a link in an email, verify the sender is legitimate. If on a PC, hover over the link to verify the destination. Always think before you click!
- Never plug a USB drive into a PC unless you know where it came from.
- Don't plug in a USB drive into a piece of manufacturing equipment without it first being scanned for malware.
- Never charge your phone with a USB port on a networked computer or piece of manufacturing equipment.
- Don't visit unknown websites.

If something unexpected happens, report it to your supervisor immediately.

THE VISION COUNCIL

Brought to you by
The Vision Council and danbailey.com

QUESTIONS?

THE VISION COUNCIL