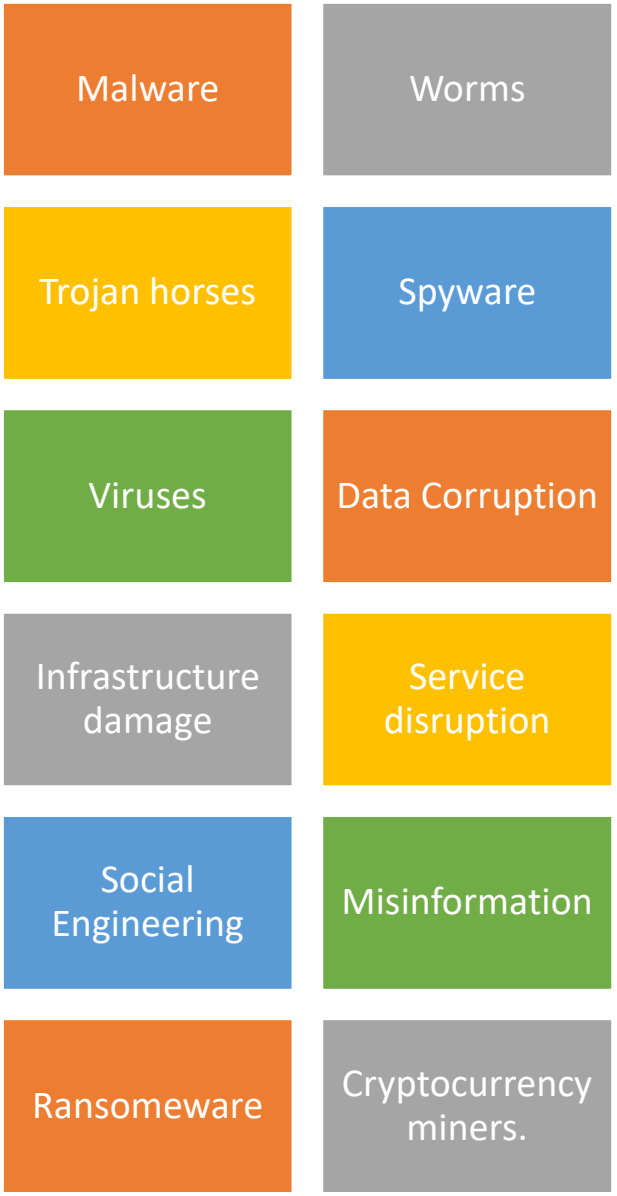
2022 WEBINAR SERIES

Cyber Security; Beyond Insurance

M Penado 2022.03.14

Predators Abound in the Cyber World

Variety of Risks Evolving



Remain Vigilant and Agile

- The weakest are attacked first
- the most often,
- even multiple times.

- Prevention Is Key
- Detection is Vital

Inventory At Least Annually

- Take inventory of your IT equipment annually
- Have employees check in with IT to report equipment
- Personal Computer
- Iphone
- Laptop
- Set up hotline to report lost or stolen IT equipment
- Require return of equipment to IT from separated employees
- Ensure all IT Equipment is accounted for
- Shut off lost or unaccounted for items

2022 WEBINAR SERIES

Are you complete?

IT EQUIPMENT INVENTORY /

WE NEED HELP WITH:

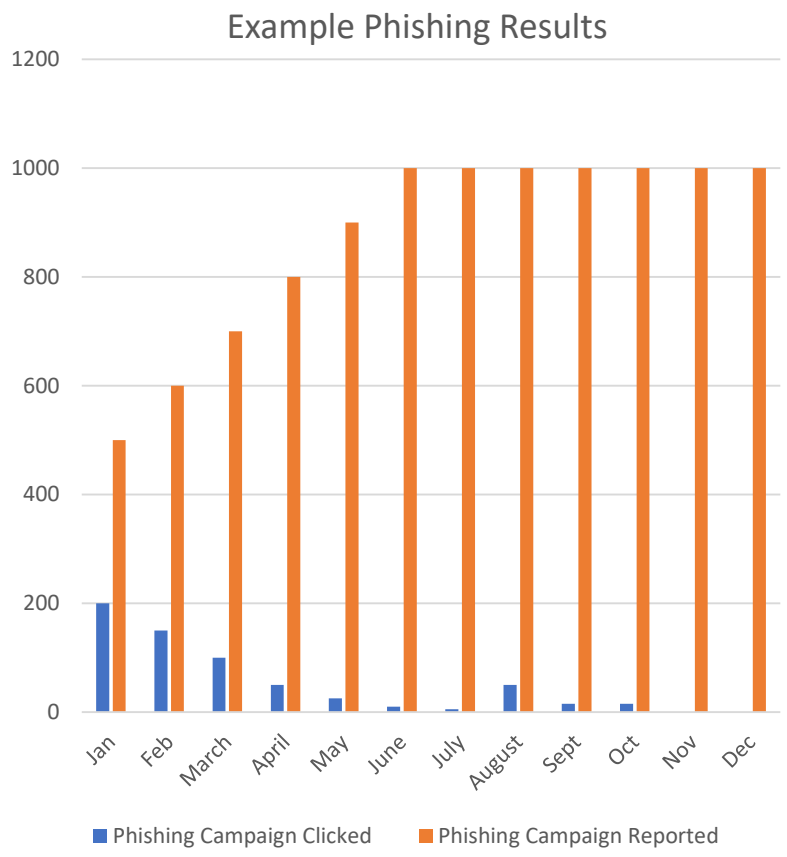
- Register your devices
  - Computers
  - Cell Phone
  - Mi-Fi
  - Tablets

Robust Employee Training and Feedback Loops

- Train every member of your workforce
- If you see something say something
- Create hotline to report IT anamolies or concerns
- Set up an IT Phishing report avenue
- Set up an IT security group

Cyber Training Topics

- New hire and annual training general cyber security
- Spoofing training
- Phishing Campaigns with Feedback
  - How many clicked on it;
  - How many reported it to IT
  - Follow up remedial training for those who clicked
- Strong passwords

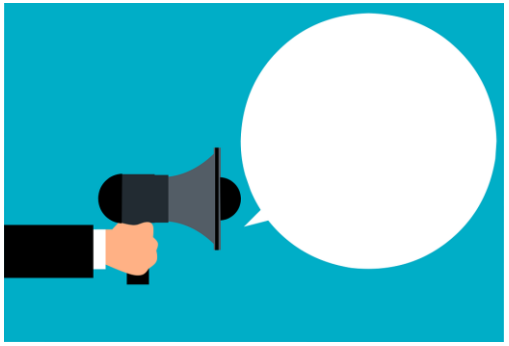


Use Memorable Phishing Tests and Feedback

- Click here to enter to win a free box of 1 dozen doughnuts.
- Your password with a major network provider has expired; click here to update.
- You won; click here.
- Feedback; Here were the warning flags in the phish email. Misspelling, foreign domain address.
- 1,000 reported, only 25 clicked on it. Thank you for your support.

Cyber Alerts: Federal Government Warns of Increased Cyber Attacks

Share Examples Reported



- Sally in Accounting received a suspicious email
- Recount red flags noticed.
- Sally called source to verify
- Found to be fraudulent
- Social Engineering attempt
- Thank you for reporting this to IT. Everyone remain vigilant to guard against similar attacks.

Spoofing Training

- **Require call-back verification** for authorization of wire payments and any requested changes in routing information by third parties. Call the previously known number on file, not a number provided via email request
- Insurance exclusions on employee actions related to this. No coverage for social engineering.

Reporting Structures

- Set up IT hotline
- Have written protocols for IT response
- Have IT report to Cyber Incident Response Team when breaches are suspected.

Zero Trust Architecture

- Implement **Least-Privilege Administrative Models**
- **Limit access to only necessary users.**
- **Need to use only**
- **Zero Trust Model from CISA**

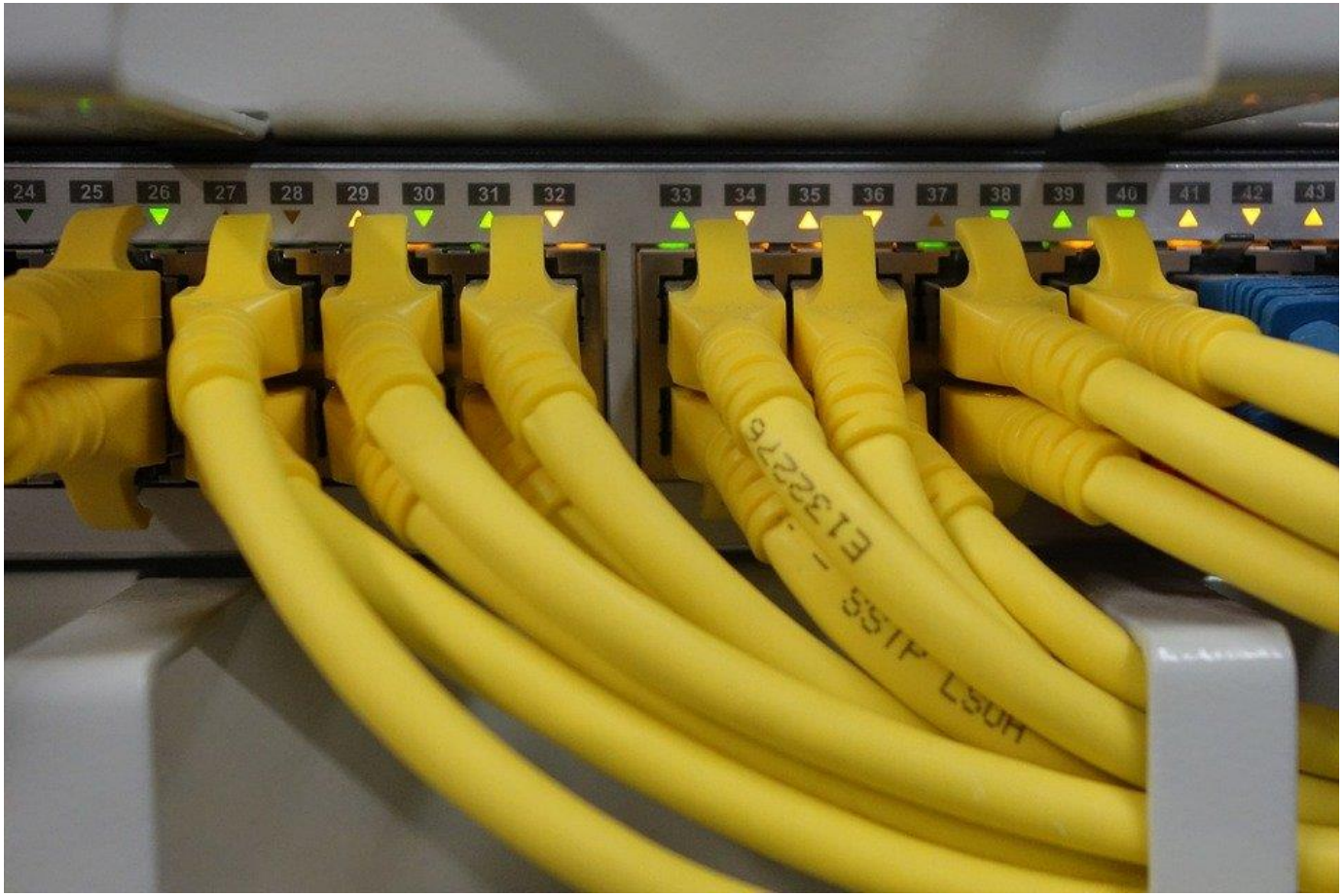
Use Encryption

- Encrypt Data in Transit – Emails Outgoing
- Encrypt Data at Rest – in network storage areas
- Use Secure Portals to Send and Receive Files

Multi Factor Authentication; MFA

- Forces user to provide individual responses to verify their identity prior to access to the network.
- Question based is one level
- Higher level is rolling changing number sequences sent to the user to input.
- Apply MFA everywhere possible
- Advise never to provide an MFA generated access code or individual responses to others.
- Above and beyond dual factor authentication
- Part of the Zero Trust Methodology.

Monitor All Endpoints to the System



Endpoint Detection and Response Software/Hardware

- **EDR**
- A security solution which uses real-time continuous monitoring and collection of endpoint data alongside rules-based automatic response and analysis.
- This category of tools includes antivirus software, firewalls, whitelisting, monitoring for unusual activity tools, etc. to detect threats.

Essential EDR Functions

- Collect data on the number and types of processes being run
- The number of connections to the network
- The amount of data transfers
- The amount of computing activity
- Set up criteria in the EDR software to automatically react when certain trigger points are tipped.
- Send an alert message to IT staff
- Force shutdown of computer
- Force logoff of user.
- Use EDR to diagnose threats based upon activity, and collect data for forensic investigation.
- EDR software searches out patterns to find real or possible threats for action.
- Use EDR software to find malware or other exploits that might lie dormant on an endpoint that could be used for a future attack.

Remote Worker Cyber Challenges

Remote Worker Cyber Security

- Require all in remote work settings to use company issued equipment.
- Cannot rely upon the security level or patching of a personal system, nor know whether it has been infected from online activity.
- Virtual Protected Network. (VPN) tunnel to connect company equipment to the company's secure server.
- Have employees acknowledge equipment is only for company use with a disclaimer on sign in page for every login.

Schedule Weekly Software Patches

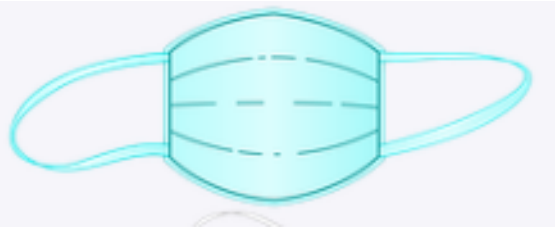
All laptops and computers connected on specific day of the week to receive updates.

Schedule Weekly Software Patching

- Timely, consistent patch management protocols
- Obtain latest software patch criteria from MS-ISAC
- Deploy weekly at a specified time
- Announce patch time to all employees weekly
- Ask that they keep their device connected to receive.

Quarantine end-of-life, unsupported software from primary network

- Old systems which are no longer supported with patches should be separated and no longer used.
- Regularly identify which these are and work with IT department to replace with supported software.
- Support investments needed to acquire updated software rather than continue using old unsupported software systems.



Rising Threat from Internet of Things

- Reasonable Security on Internet of Things in CA
- Internet of things and cyber security.
- Keep separated from Internet whenever possible
- May not yet have basic security firewalls to block cyber intrusions
- Promote security over convenience

Duplication/Segregation/Geo Dispersal

- IT data back up time options are minute by minute, hourly, daily, weekly.
- Place at a different location
- Keep separated from the network
- Have separate logins and passwords for access
- This is separation is known as air gapped

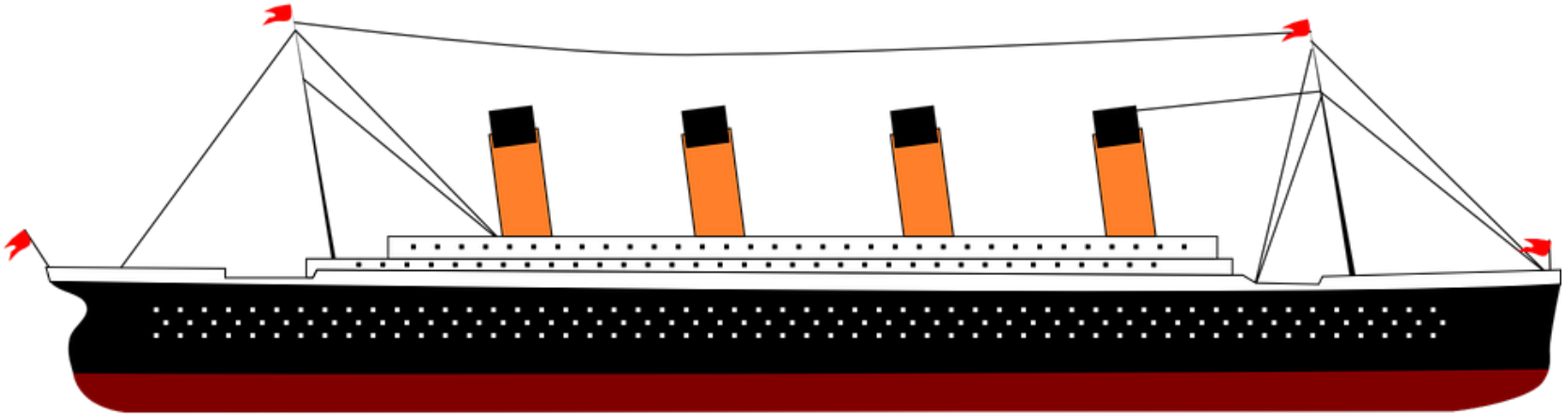
Scan Cyber Traffic; Both Directions

- Filter in-bound web traffic
- Screen and block access to sites
- without SSLs
- Known dangerous sites

Denial of Service Attacks; DNS

- You overwhelm me!
- Forces a shutdown of systems
- May be dealt with by isolating the system from outside communications from specific IPS addresses or domains

Benefits of Segmentation



Network Segmentation

- A network is divided into different parts of the system that don't; need to interact with each other. A subnetwork may be set up for printers, or for data storage.
- Each subnet is a unique system with its own access and security controls. Subnets may also be set up to organize data by type, source, or purpose.
- When attacked, the entity IT department can act to stop all communication from one segment from reaching the others. This acts like a quarantine.
- Segmenting a network limits a threat's ability to move and spread quickly. If a breach is detected in one section of a network, it can be quickly isolated to preserve other segments from infection.

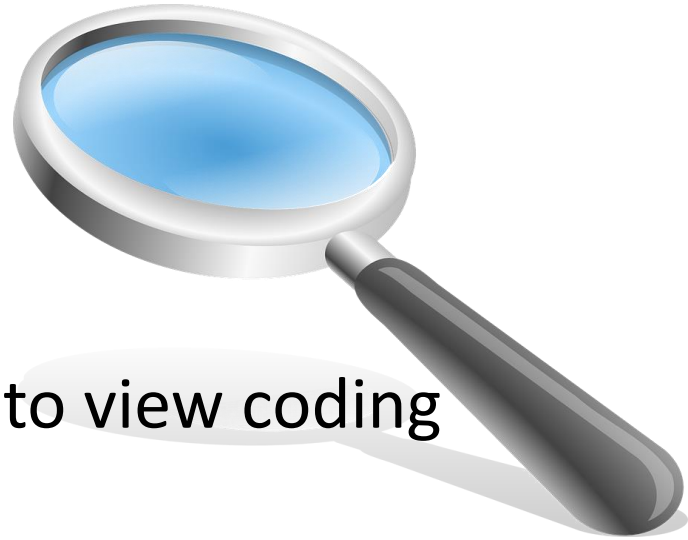
Stay Informed on Cyber News

- Scan news for newly deployed exploits to take action as needed.
- MS-ISAC weekly bulletins and alerts
- Isolate systems if needed
- Monitor for unusual activity,
- Obtain software patches to fix.

ZERO DAY EXPLOITS

- An error in the software code of a program or operating system
- Used as a backdoor to enter and
- Steal data
- Modify data
- Corrupt data
- Modify operating instructions
- Take over control of system or equipment
- Harm operating system or equipment
- Original entity has no prior notice of coding error; zero time to fix it.
- How fast is your organization to learn of zero day exploits?
- How fast is your organization's reaction time to protect against zero day exploits.
- Example; Logjam4 exploit announcement of a few months ago.

Open Source Code



- Nature of software allows anyone to view coding for errors.
- Complexity of coding is now often thousands of lines long.
- Length of complicated software coding increases the possibility of errors within, waiting to be found.

2022 WEBINAR SERIES

Critical Infrastructure Vulnerabilities

- Equipment relied upon by citizenry for essentials
- Water, fuel, electricity, transportation systems, internet
- Can be disabled, or misdirected to harm citizens
- By nefarious hackers or other nation states
- Infrastructure systems were originally built independent of internet without sophisticated security defenses mechanisms.

Audits and Penetration Testing

- Assessments: Cyber Resilience Review (CRR) | CISA
- No cost assessment self audit or assist by DHS
- Annual audits of cyber security recommended

Fed Focus on Cyber Contractors

- In October episode of The Insuring Cyber Podcast.
- “The federal government can’t meet this challenge alone,” President Joe Biden told the executives at the summit. “You have the power, the capacity and the responsibility, I believe, to raise the bar on cybersecurity.”
- **TOPICS** CYBER

Leverage the Power of Cyber Insurers over Contractors with Cyber Exposure

- Increased underwriting standards
- Federal government to require all its contractors to carry cyber insurance.
- Require your vendors to do the same.
- Insurers will hold their policyholders to a higher standard.
- Carve back the limited liability to hold vendors with cyber exposure responsible for cyber security and privacy.

Cyber Requirements for Your Cyber Realm Contractors

- Must carry cyber liability insurance
- Must endorse additional insured status
- Primary and noncontributory basis
- Confidentiality clause for PHI and PII
- Cyber Breach indemnification clause
- Must inform you within 48 hours of a cyber breach affecting them; whether your data involved or not

Operational Parameters for Contractors with Cyber Exposure

- Must use MFA
- Must follow HIPAA logging compliant with 1996 HPAA Act
- Must encrypt all data in transit and at rest
- Must adhere to Federal Information Processing Standards (FIPS) created by the United Sates National Institute of Standards and Technology (NIST) for the Federal Information Security Management Act of 2002 (FISMA)
- Must use Transport Layer Security (TSL) and Secure Socket Layer (SSL) standard industry security protocols to safeguard data sent between computer systems and to prevent unauthorized parties from reading, capturing, modifying or intercepting information transferred.
- must provide all services in a secure manner from within Canada and/or the United States. No operations for services in the scope of this contract may occur outside of Canada or the United States.
- Must not subcontract to any specific other entity without the express written permission of our organization.

Cyber Incident Response Plan

- Outline of action steps that will be taken for potential attacks, including a ransomware attack.
- Exercise your plan for practice
- Conduct after action review of exercises
- Implement improvements as needed.

Essential Cyber Event Response Elements

- Be ready to report to your insurer immediately,
- Have call list ready for
- Cyber Insurer and insurer approved;
- Cyber Lawyer
- Cyber Forensics
- Cyber Call Center and
- Cyber Identity Theft Protection Company

Consider Your Cyber Response and Ransomware Position

- Narrowing ransomware coverage.
- Increasing self insured retention amounts
- State governments and federal governments are proposing to outlaw the payment of cyber ransoms by government entities.
- Cyber currency and ransomware/anonymity and difficulty to trace hackers.
- Set aside reserves to deal with cyber losses as cyber insurance may not be available.