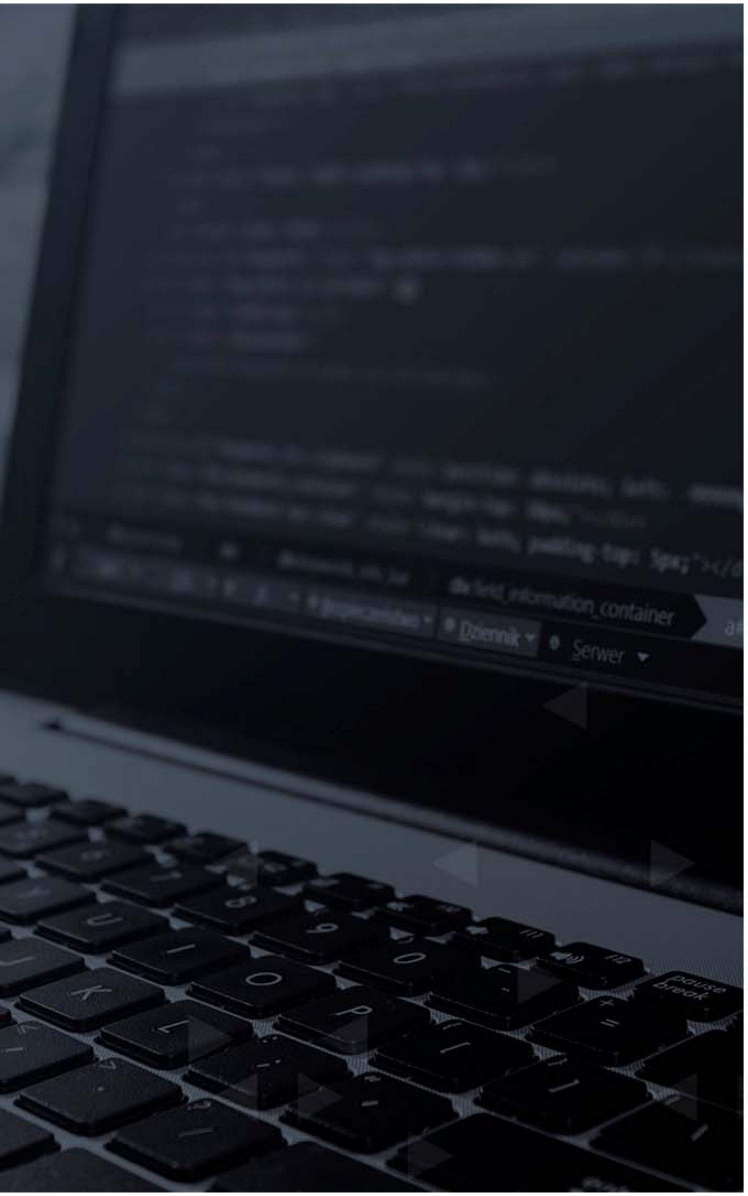
Cybersecurity

BKD
CPAs & Advisors

Everyone needs a trusted advisor. Who's yours?



State of Cyber Attacks - The Human Element

Hackers have come a long way

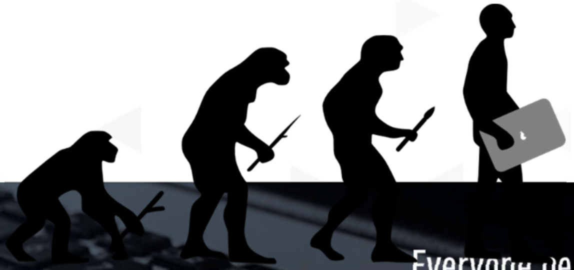
Evolution of Hackers & Their Motivations

Old Tactics:

- Highly sophisticated technical attacks
- Required advanced training, intelligence

Current Tactics:

- Social engineering
- Understanding of human nature & psychology
- Social media, phone, email are primary tools
- They let us do most of the work for them



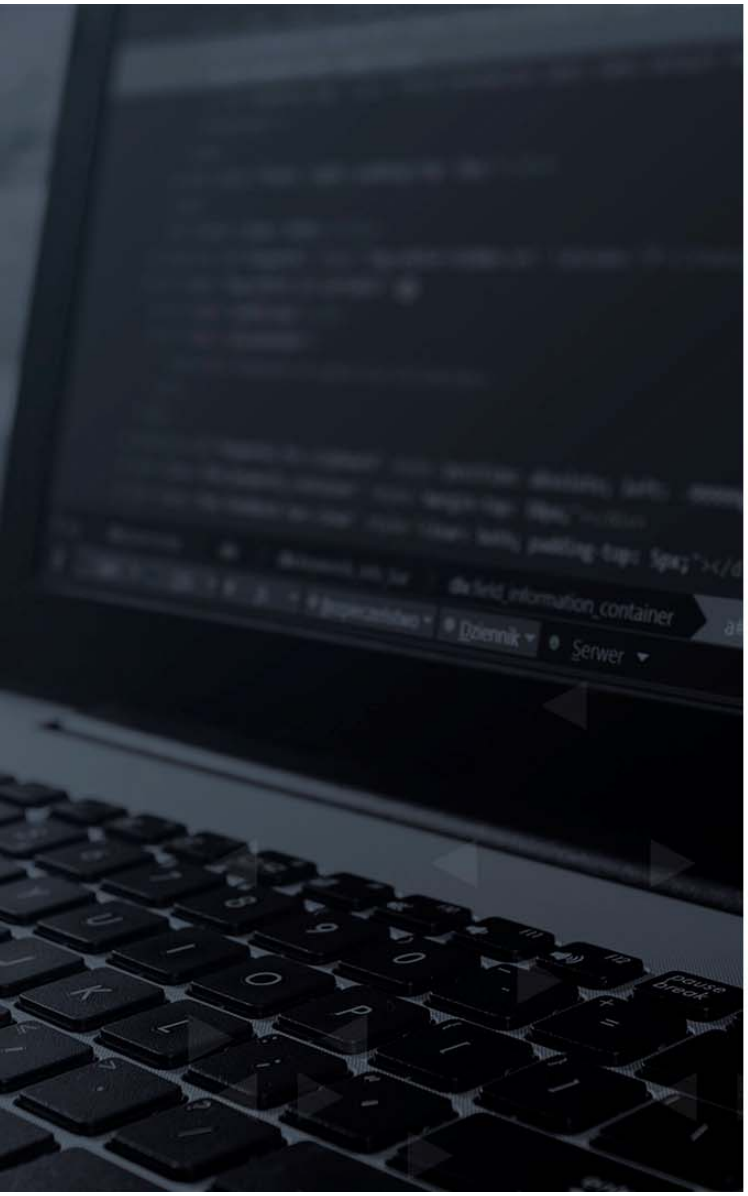
Social Engineering is the Game Changer

- Social engineering attacks ultimately lead to a type of insider threat known as user error.
- 33% of breaches included social attacks
- Often a user clicking a malicious link in a phishing email or in a text message.
- User error can also be the result of someone leaving a laptop unattended. Requiring a physical presence.

Sources: Verizon, 2019 Data Breach Investigations Report &
How Social Engineering is Changing the Insider Threat Game, InfoSecurity Magazine, Jan. 7, 2020 https://www.infosecurity-magazine.com/opinions/social-engineering-insider-threat/

What is Physical Social Engineering?

- Goal is to gain physical access to an organization’s premises
- Key tasks include:
  - Access into the facility’s restricted areas
  - Connection to the network (wired and Wi-Fi)
  - Planting of devices (thumb drives, network devices, etc.)
  - Observe unlocked computer screens and sensitive information on desks



Case Study

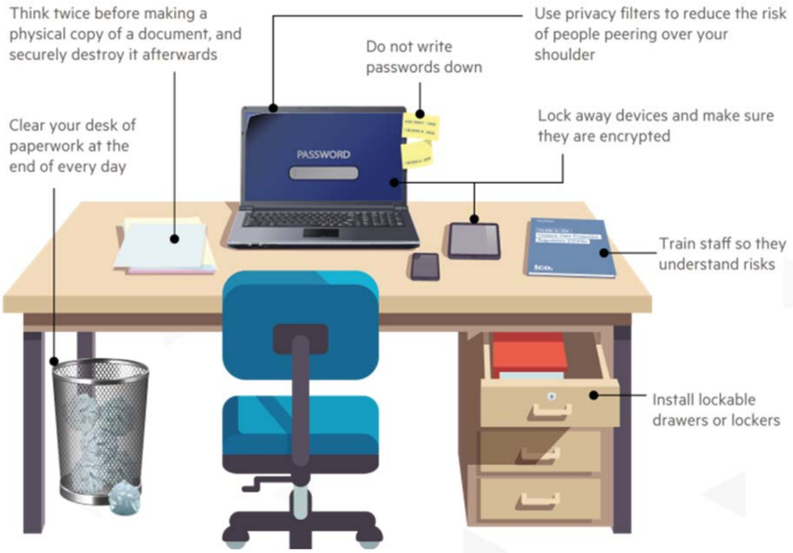
Compromise of health care organization

The Engagement

- Client was a healthcare provider with multiple clinics in two states:
- Team was engaged to perform technical and physical cybersecurity assessment
  - External and Internal Network Penetration
  - Phishing Emails
  - Phone Pre-Text Calls or Vishing
  - Physical Social Engineering

Physical Social Engineering

- Selected seven locations within two states
- Team attempted access to sensitive areas
- Attempt to connect to open data ports
- Observe “clean desk” violations
  - Unlocked screens
  - Post-it notes
  - Files
- Any other targets of opportunity


Think twice before making a physical copy of a document, and securely destroy it afterwards
Do not write passwords down
Use privacy filters to reduce the risk of people peering over your shoulder
Clear your desk of paperwork at the end of every day
PASSWORD
Lock away devices and make sure they are encrypted
Train staff so they understand risks
Install lockable drawers or lockers

Clinic 1

- Posed as flower delivery man
- With a college intern who said she was his “daughter”
- Reception area excited to see their colleague get flowers

Photo of the actual flowers

Clinic 1 Response

- Front staff distracted by the flowers and left workstations
- The “daughter” was able to observe no one locked their screens
- Noticed unattended files and post-it notes with potential passwords
- Then, he asked to use the restroom, they scanned him in the back without an escort…

Clinic 1 Back Area

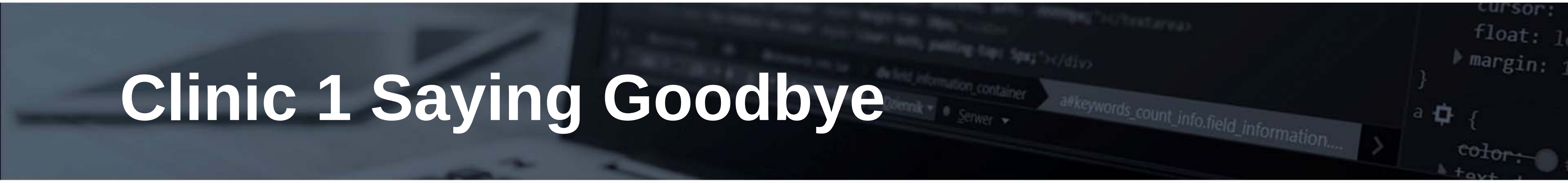
- Easy access to ultrasound room
- All systems were unlocked
- Access to network ports

Clinic 1 Back Area

- Access to a treatment room
- Open ports
- Copier
- Unattended USB drive
- Patient files left unattended

Clinic 1 Back Area

- Main power box
- Unattended systems
- One employee smiled and nodded to at us as we walked by
- Easy access to back door exit if we were caught

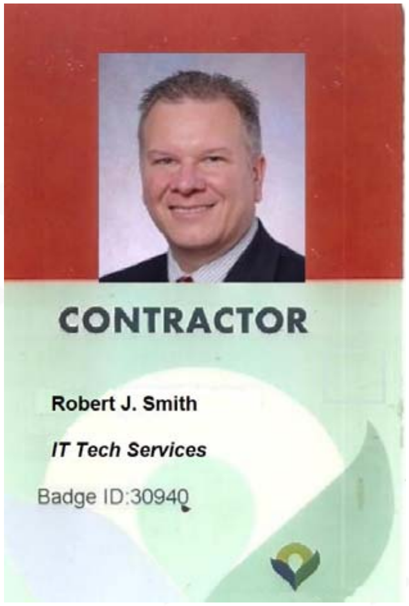


Clinic 1 Saying Goodbye

- After about 8 minutes, he came back up to the front
- Clinic staff said “thank you”
- Wished them well
- They left without clinic staff knowing anything
- Hardest part was having management explain to the lady that the flowers were not from a real guy

Clinic 2

- Team member had photo badge with word “Contractor”
- Walked in main lobby and went to back area without being challenged
- Observed similar rooms
  - X-Ray
  - Radiology
  - Employee Only Areas
  - Printer Areas
- Network ports locked on main level
- However…



CONTRACTOR

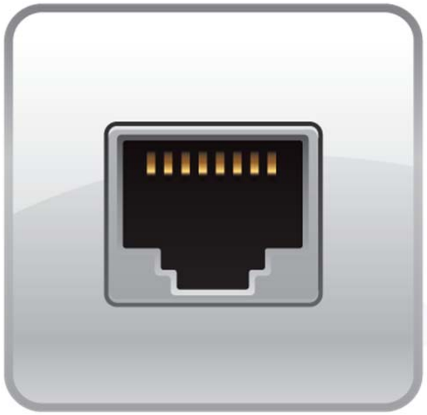
Robert J. Smith

IT Tech Services

Badge ID:30940

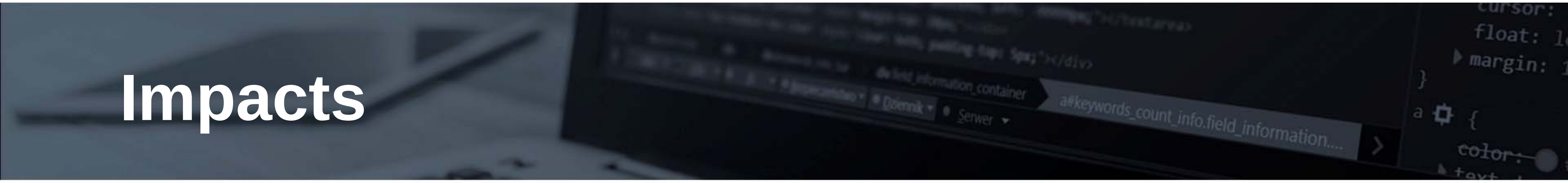
Clinic 2

- Greeted by a man named “Fred”
- Talked way into second floor data center
- Connected to network
- Told “Fred” we were authorized to visit two other clinics
- “Fred” wanted to be helpful, so called them to let them know we were coming



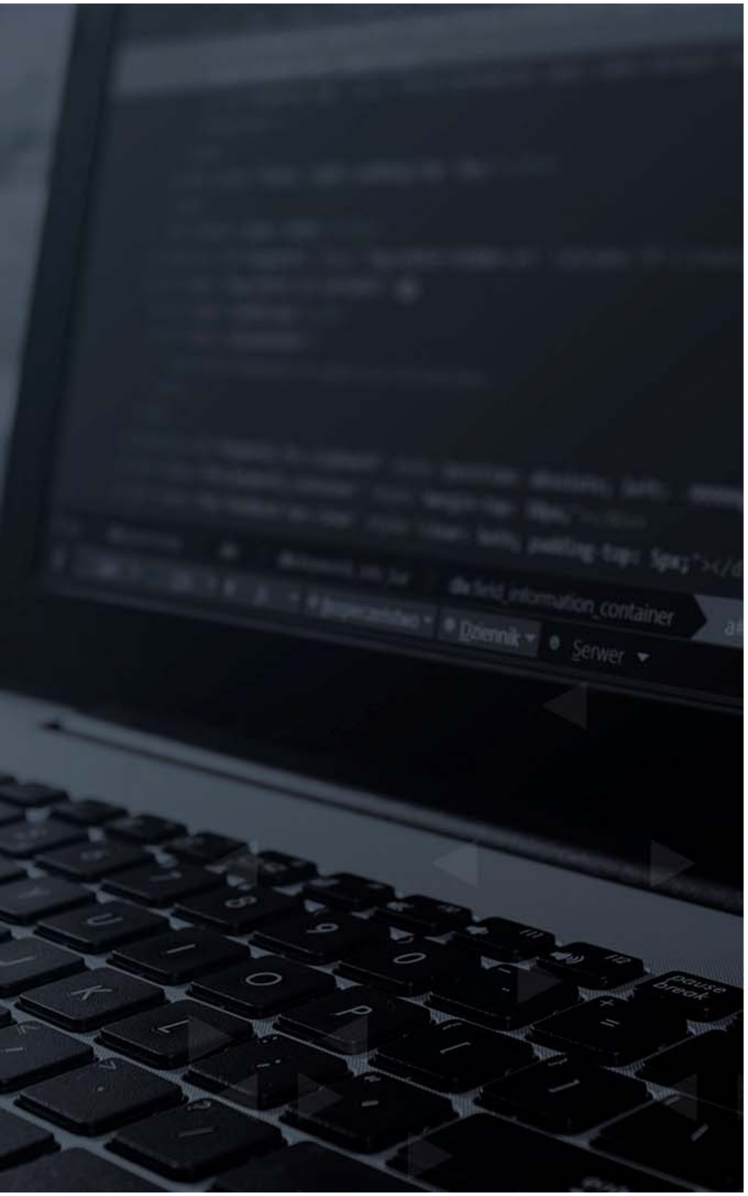
Clinics 3 & 4, Thanks to “Fred”

- Clinic 3
  - Entered through unlocked back door
  - Waked about back area without being questioned
- Clinic 4
  - Walked behind check-in counters
  - Unplugged VoIP phone, connected Kali laptop
    - Accessed AD
    - Captured all usernames
  - Also files with PHI left unattended
  - Approached by a VP who just asked why he was there
  - Left facility unchallenged



Impacts

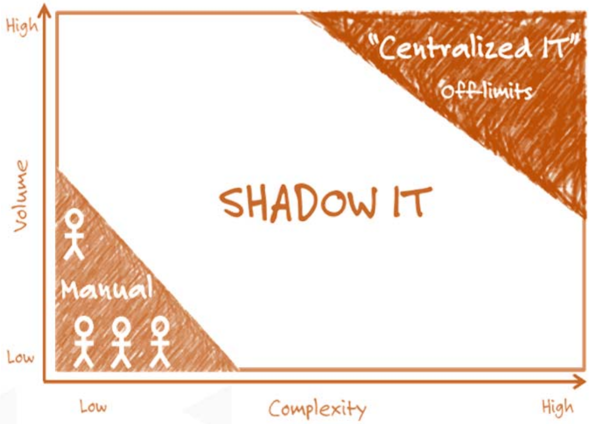
- Able to compromise four of seven facilities
- Access to network to include IP ranges and usernames
- Access to sensitive information:
  - PHI files
  - Passwords
- Majority of people were very accommodating



Other Concerns

Shadow IT

- Shadow IT refers to IT devices, software & services outside the ownership or control of IT organizations
- Departments will often do this to
  - Circumvent bottlenecks
  - Avoid slow processes
  - Rely on familiar software
  - Compatible with mobile devices
  - Work with legacy applications that are no longer supported
- It is easy to attain software as a service (SaaS) solutions



Source: Gartner IT Glossary, https://www.gartner.com/it-glossary/shadow

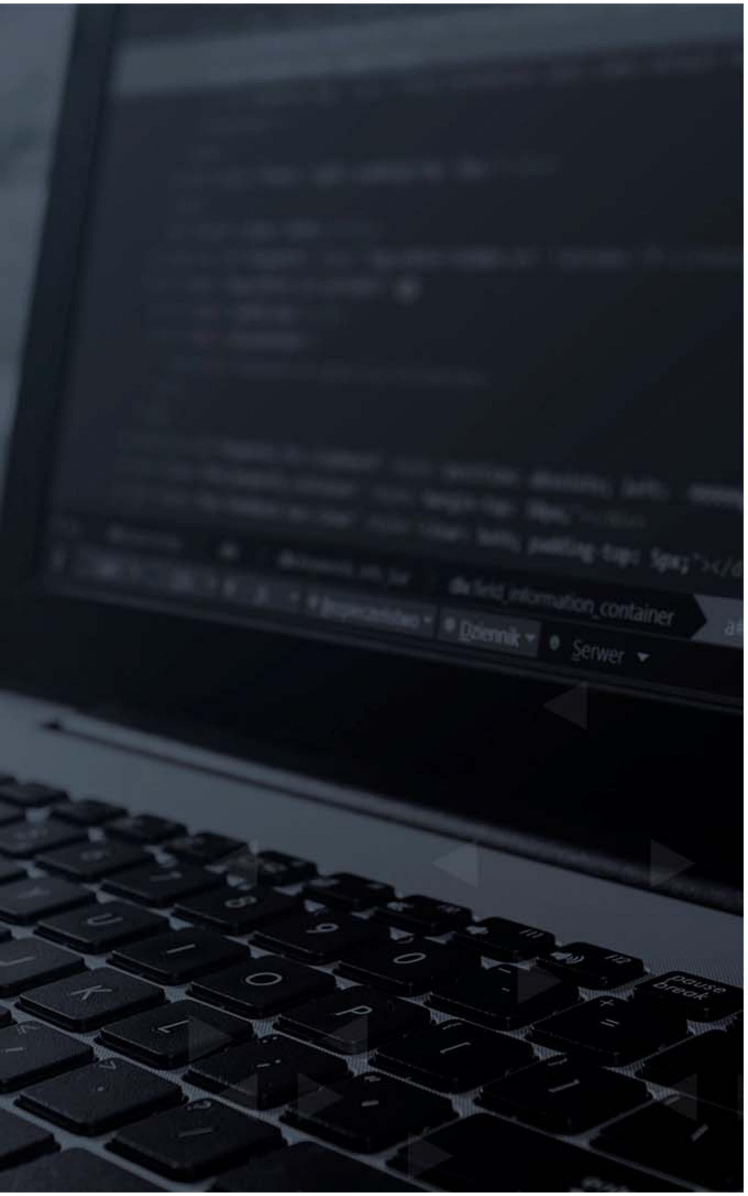
Getting The Job Done, But At Risk…

- In the early 2000’s a young Soldier in the National Guard was tasked with writing stories for the newsletter
- Supply did not have laptop to issue him
- He used his own, but could not connect to the network port to send his stories off
- Purchased a Wi-Fi router, which allowed him access
- Put a DoD network at risk

Risks of Shadow IT

- Rutter Networking study identified
  - Increased risk of data loss
  - Increased risk of data breach
  - Inefficiencies
  - Cybersecurity risks
- Since acquired outside of IT procurement channels, security is often overlooked
- Gartner predicts that a third of all successful attacks will be against their shadow IT resources

Source: https://www.rutter-net.com/blog/4-security-risks-of-shadow-it



Mitigation Steps

Restrict and Limit Access

- Limit access based on need-to-know (least privilege) for both logical and physical access
- Do not let people piggyback, especially if you do not know them
- Ask why someone is there if you are suspicious
- Get evidence of who they are
- Call headquarters or trusted source to inquire

Educate Your Team

- Technology is no substitute for employee education
- Include the board, executives & vendors
- Document & distribute security policies
- Protocols for personal devices
- Encourage a culture of security
- Develop a program that includes them in the security solution

System and Device Protection

- Know you inventory
- Ensure that only approved technology is used
- Vet user devices
  - Mobile Device Management policies
  - VPN
  - Ensure appropriate patch management
- Consider a guest network or DMZ (segmented network)

Do Planned Security Assessments

- Set up a program for planned security assessments
- Assess the effectiveness of the safeguards’ key controls, systems & procedures
- Consider a rotation approach, where different things are tested over a three year cycle
- Provides a more thorough program

Have an Incident Response Plan

- No substitute for a solid IR plan
- Designed to promptly respond to & mitigate any cybersecurity incident
- Defines roles including those with decision making authority
- Manages internal & external communication
- Provides a way for documentation and

  lessons learned

Cybersecurity Insurance

Are You Actually Covered?

- Do not fill the application out alone
  - Management, IT management & legal council should be involved
  - Wrong, partial or inadequate answers can void the policy
- Does the policy cover phishing incidents that result in financial loss or physical breaches?
- Perform annual reviews of the policy
- Determine if strong cybersecurity controls are in place

Criminals Exploit Behaviors

- Social engineering is one of the most effective means of cyber attacks
- Does not necessarily require technical skills
- Relies on the human nature, preying on greed, fear, curiosity, and even the desire to help others
- Cybercriminals do their homework, and may spend weeks or months planning an attack

Source: Social Engineering Explained: How Criminals Exploit Human Behavior. Sep. 25, 2019, https://www.csoonline.com/article/2124681/what-is-social-engineering.html

BKD Thoughtware®

- Webinars, seminars & articles
- Many are CPE-eligible
- *Payment Card Industry (PCI) Compliance*
- *Cybersecurity: Preventing & Mitigating the Effects of Identity Theft*
- *Business Email Compromise Schemes – How to Avoid Becoming an Unwilling Participant*
- *Cybersecurity and Emerging Threats*
- *Phishing Scams & Tax-Related Identity Theft Revealed*

Questions?

Thank You!

Jessica Richter, CPA.CITP, CISA| jrichter@bkd.com

@BKDAdvisory **@jessrichter_cpa**