First Line of Defense

Wednesday May 15, 2019
2:45pm 3:45pm
Waconia IV
Lord of the Rings III – The Siege of Gondor
Under Siege

• Attackers probing for weaknesses in your defenses - automated

• Malware – Cleveland Hopkins International Airport. Week of 4/22.
  • Disabled flight and baggage information screens

• Ransomware – 60 Minutes 5/5/2019
  • In 2017, 1700 Successful Ransomware attacks were reported
  • Hospitals – Hancock Regional Hospital (suburb of Indianapolis)
  • Municipalities – Leeds, Alabama (Pop. 12,000). Atlanta, GA

• Everyone is a target
  • Manufacturing, Government Agencies, & Financial Services
Multiple Fronts

• Technical Front
• Physical Front
• Human Front

Based on Verizon’s 2018 Data Breach Investigation Report, companies are nearly three times more likely to get breached by social attacks than via actual vulnerabilities, emphasizing the need for ongoing employee cybersecurity education.

All employees need to be engaged and empowered as they are the First Line of Defense.

Key learning points:
• The human factor is still the weakest link of any security strategy
• An annual security training session isn't enough
• Avoid the trappings and take the steps necessary to instill security as part of your culture
First Line of Defense

Who am I? – Jerry Widenhofer

• Consultant - Getronics

• Consulting Company – Glenwood Solutions
  • Helping healthcare providers achieve CMS EHR incentive payments
  • Became immersed in HIPAA – Security Rule
  • Conducted over 100 risk assessments & implement resulting management plan
  • Teach online privacy & security and health information technology courses for Normandale Community College in Bloomington, MN.
First Line of Defense – Vulnerability

**Vulnerability** = An inherent weakness that could be exploited by a threat

Have 400 employees – 400 vulnerabilities (points of access)

4% of people will click on any given phishing campaign

Source: Verizon’s 2018 Data Breach Investigations Report

*Only 4% = 16 potential incursions.*

Once behind your “walls”, past your defenses – free reign
First Line of Defense – Breaches

Biggest U.S Healthcare Data Breaches of 2018


Following involved employees:

10. HEALTHEQUITY: 190,000 INDIVIDUALS
Data of 190,000 customers breached after a hack on two employee email accounts

8. MED ASSOCIATES: 270,000 PATIENTS
Discovered a hacker accessed an employee workstation

6. AUGUSTA UNIVERSITY HEALTH: 417,000 PATIENTS
Fell victim to two phishing attacks. Solicited usernames and passwords to gain access to internal email accounts
First Line of Defense – Breaches

Biggest U.S Healthcare Data Breaches of 2018


Following involved employees:

3. CNO FINANCIAL GROUP: 566,217 CUSTOMERS
Hackers accessed several employee credentials

2. UNITYPOINT HEALTH: 1.4 MILLION PATIENTS
A phishing attack on the Iowa-based health system’s business email system compromised the data of 1.4 million patients.

Hit with a series of highly targeted phishing emails that looked as if they were sent from an executive from within the organization.
First Line of Defense – Weakest Link

Build A Strong Cybersecurity Posture With These 10 Best Practices

3. Plan for the weakest link: your people.
When you plan to overhaul your cybersecurity infrastructure, it’s important to keep the weakest link in mind: the people in your organization. Yes, you should invest in the right technology that takes your network and endpoint security to the next level, but make sure your organization’s workforce is aware of the cyberthreats they face and how they must address these threats. Conduct security awareness training programs that establish a culture of cybersecurity awareness.
First Line of Defense – Steps to Strengthen

1. **UNDERSTAND THREATS**
   a. Social Engineering – Phishing
   b. Ransomware
   c. Denial of Service

**Goal:** Target the Human Front to bypass defenses
First Line of Defense – Steps to Strengthen

Example 1:

Why have you sued me? WTF is this?
I am attaching the subpoena.

Example 2: Black Mail

Your account was recently infected! Renew the password right this moment!
You probably do not know me and you obviously are probably wanting to know for what reason
you’re receiving this particular electronic message, proper?
I’m hacker who burst your email box and digital devices two months ago.
Do not waste your time and make an attempt to talk to me or seek for me, it’s impossible, since I sent
you a letter from YOUR hacked account.
I created a virus to the adult vidoes (porno) website and guess you watched this website to have some fun
(you realize what I want to say).
Whilst you were taking a look at films, your browser began operating like a RDP (Remote Control)
with a keylogger that provided me authority to access your monitor and camera.
Consequently, my software program acquired all data.
First Line of Defense – Steps to Strengthen

2. MAKE SECURITY CULTURAL PRIORITY FOR THE ORGANIZATION
   a. Top Down
   b. Let employees know committed – Actions Speak Louder than Words
   c. Communicate efforts
First Line of Defense – Steps to Strengthen

b. Let employees know the organization’s committed
   ➢ Have the necessary staff (CSO) and technology
   ➢ When starting projects, involve security
   ➢ Make it easy to report (ex. PhishAlert button – forwards to security team)
   ➢ Staged Attacks
     o Share Results
     o Phishing Attacks (Participation)
       ▪ Report suspicious emails
       ▪ Click → Training

Tout Your Efforts
First Line of Defense – Steps to Strengthen

c. Communicate Efforts
   ➢ Include in Annual, Quarterly, Departmental meetings - provide updates
      o Ex. Security Budget
      o Testing Results
      o Transparency – make it real
   ➢ Positive Message
      o Internally
      o Externally – Clients \ Customers \ Partners

Tout Your Efforts

Secure360.org | #SEC360
First Line of Defense – Steps to Strengthen

3. Training
   a. Once a year is not enough
      i. “Nuggets” – reminders (Ex. Newsletter)
   b. Know how to report – keep it simple
   c. Understand threats
   d. Impact to business \ clients
      i. Loss of data
      ii. Unable to service clients
      iii. Divert funding to respond to breach
      iv. Reputation in the market
      v. Client \ customer confidence
First Line of Defense – Steps to Strengthen

3. Training
   e. Awareness when dealing with sensitive data
      i. Minimize mistakes
      ii. Report suspicious activity – Insider attacks 28% (Verizon)

4. Tie security to job responsibilities & evaluations
   (Ex. Facebook – Incentivize employees to prioritize safety & security)
   a. Carrot & Stick
      i. Incentives
      ii. Employee Audits
First Line of Defense – Steps to Strengthen

5. Stay Diligent
   a. Physical
   b. Technical
   c. Administrative
      i. Policy Reviews
First Line of Defense – Wrap Up

Closing Comments:
• You are a TARGET
• Do It Right – Actions Speak Louder Than Words
• Security Culture
  o Make it a priority

Contact Information:
Jerry Widenhofer
Gerald.Widenhofer@Normandale.edu
440-346-9950
First Line of Defense – Questions???