Cybersecurity

Protecting Your Business and Your Customers

Trent Martin, Director of IT Services, CHR Solutions

It Only Takes a Single Click

* At Least 50% of Data Breaches are the result of Phishing or other Social Engineering Campaigns

The Headliners

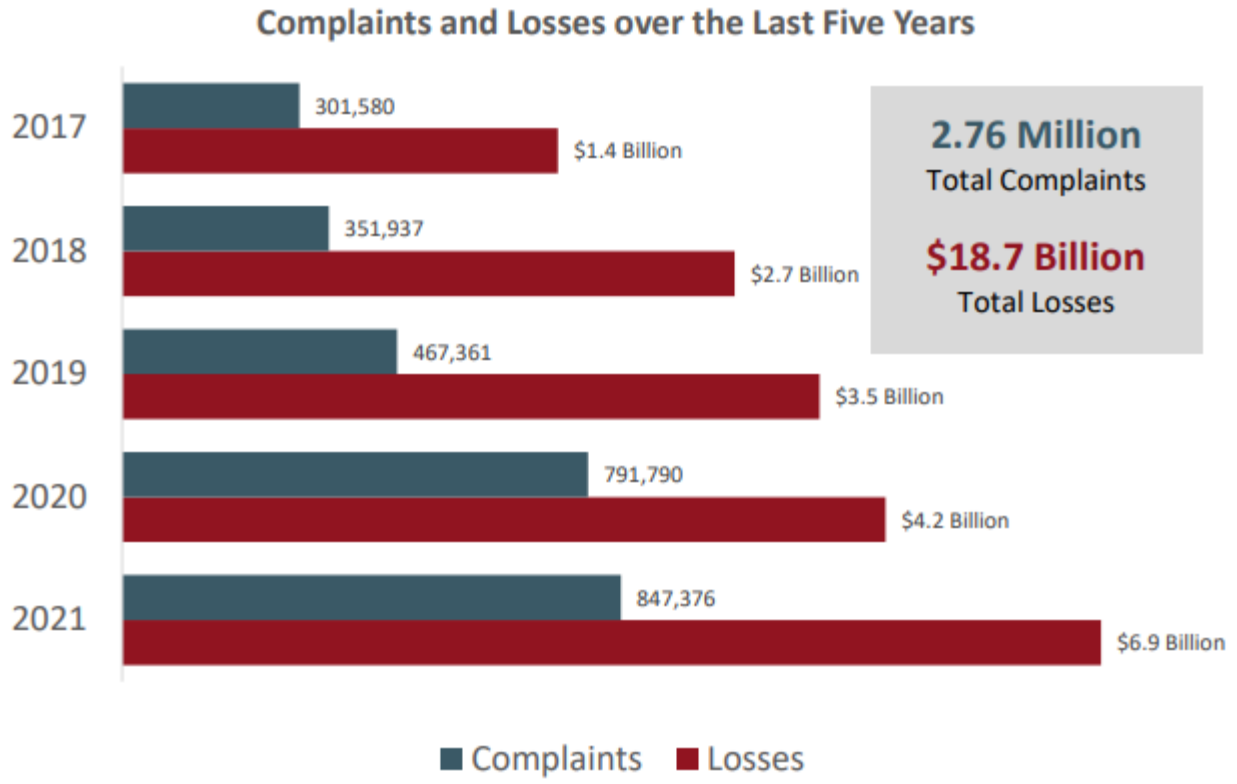
- **CNA (March 2021)**
  - CNA is the 6th largest insurance carrier in the U.S.A.
  - Encryption included remote worker machines that were connected via VPN
  - Insurance carriers that offer Cybersecurity Insurance are valuable targets
  - Bloomberg reported that an estimated £30 Million in ransom was paid to regain access to their networks

- **Colonial Pipeline (May 2021)**
  - Pipeline that carries over 100 million gallons of fuel a day went offline.
  - Darkside Group
  - Average price of a gallon of gas in the US increased to more than $3 for the first time in over 7 years
  - $4.4 million was paid to recover the data

- **Irish Health Service (May 2021)**
  - Shutdown of all HSE systems forcing hospitals to cancel appointments
  - 15 Million in ransom was demanded which HSE refused to pay
  - HSE reports that the total cost of the ransomware attack was 98 million dollars (85 million pounds)
  - Penetration tool was used to deploy Conti Ransomware

The Reality of Cyber Attacks

- Average of 552,000 *reported* attacks per year (ic3.gov)
- Double Extortion is now the norm



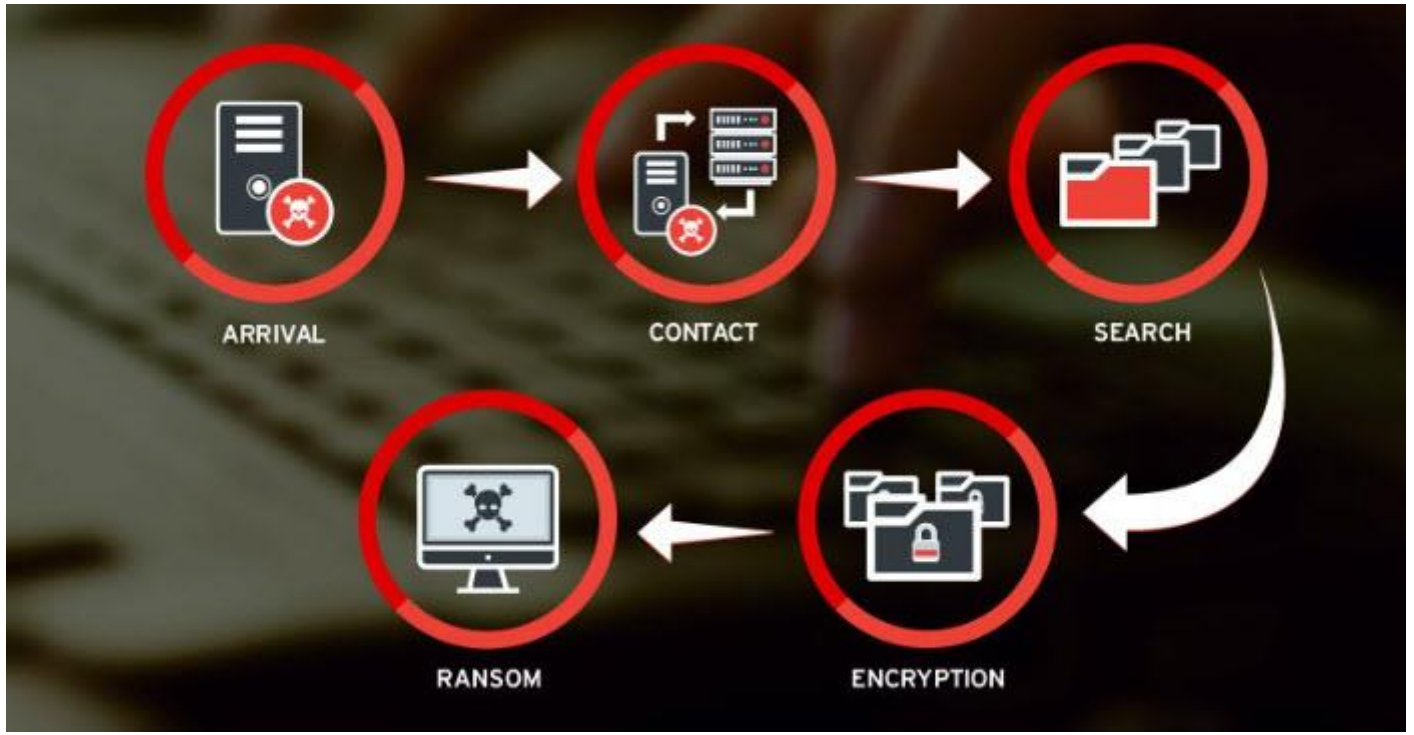
The Cost of Ransomware

Ransomware – The Worst of the Worst

- Staff Can't Work
- Customers are Impacted
- Revenue is Impacted
- Sales are Impacted
- Potential Loss of Customers
- Reputation is Impacted
- Ransom (Double Ransom?)
- Possible Legal Ramifications
- Unplanned Costs of Hardening the Network
- Cybersecurity Insurance that may not pay out fully

How Does Ransomware Work

- Acquisition of Credentials
- Access to Network
- Sit and Steal Passwords
- Elevated Privileges
- Scripts for Data Searches
- Data Exfiltration
- Script Encryption – Servers
- Encrypt Backups
- Leave a Nice Note



Cloud Models Make It Easy for Bad Actors

RaaS model

- Developer creates specific ransomware code
- Code is sold to affiliates
- Affiliates spread malware and pay with cryptocurrency
- Money is divided between developer and affiliates

How Do They Get In?

- Phishing Campaigns and Other Social Engineering
- Credential Stuffing from Other Breaches are More Targeted
- Password Spraying
- Keylogging (Malware)

What Happens When You are Ransomed?

- Everything HALTS
  - Network will need to be shutdown immediately
- You won't see it coming and the timing will not be convenient
- FBI will likely only take a report and provide (and request) IOC's
- Lots of "experts" will be involved
- Everything that runs on a server STOPS
- Very Long Days Ahead for IT and Leadership Groups
- Decisions will be made
- There is no free speech

Be Prepared

- **Have a Plan!**
  - Not the same as your DR Plan
- **Test and Update Your Plan Annually**
  - Tabletop Exercises with all key areas
- **Cybersecurity Insurance (Be honest…)**
- **Cybersecurity Training for ALL**
- **Friendly Phishing Campaigns**
- **NIST Compliance**
  - Formal Policies and Procedures
  - Security Reviews
  - Encryption used where possible
- **Secure Your Border**
  - MFA
  - SPAM and AI Phishing Protection
  - Geofencing and URL Filtering

Be Prepared

- **Network Separation**
  - Corporate Network and ISP Network should not be able to access one another
  - Guest Networks should talk to neither
- **Backups and Storage**
  - Local and Cloud Copies
  - Immutable SAN storage
- **Internal Security**
  - Monthly Patching
  - Vulnerability Scanning
  - Next Generation Endpoint Protection
  - Secure Password management
- **Monitoring**
  - SOC
  - Dark Web Monitoring
- **Cloud Applications**
  - 365/G-Suite
  - Use MFA
  - Allows communications to continue

Be Prepared

- **Staffing**
  - Are you staffed properly?
  - Are they trained to protect and respond
- **Watch for Information Silos**
  - What are you going to do if Fred is out?
  - What if multiple groups need Fred's help?
- **Documentation**
  - Could outside hands help you?
  - Do they know your systems?
- **De-Hoard Your File Servers**
  - This data will likely be exfiltrated
- **Create a Security Culture**
- **Ask the hard questions!!!**

Customer Education

- **Cybersecurity Email Campaigns**
  - Monthly email campaigns to customers to educate them on threats and how to avoid them
    - Passwords
      - Long
      - Complex
      - Do Not Reuse
      - Password Managers
    - Phishing
    - Malware
    - Suspicious Links
    - Browser Extensions
    - Keep Browsers and Computers Up to Date
    - Using Complex Passwords
    - Don’t Re-Use Passwords
    - Use of Password Managers
    - Next-Gen Endpoint Protection

Value Added or Premium Services

- **Anti-Virus / Malware Protection Software**
  - Many home users do not have up to date antivirus
- **Dark Web Scanning**
  - Link Scanning like “Have I been Pwned” (haveibeenpwned.com)
- **WiFi Mesh Systems with Added Security**
  - Sell or Lease Wifi Mesh Systems that provide some protection against Cyber threats such as Plume with Homepass.
- **Cloud Backup Services**

QUESTIONS?