SECURECYBER
DEFENSE

The First 48 Hours

Critical Steps During a Data Breach

Shawn Waldman – CEO – Secure Cyber Defense

It's better to be prepared for an eventual cyberattack than to have to deal with it in the moment without a plan or a support network able to get your company back online

We Are

Experienced

- Founded in 2015
- Span Multiple industries

Accessible

- Affordable access to advanced cybersecurity solutions
- US Based staff and management

Responsive

- No Off-shoring
- 24/7 Alerting and Response

FortiNet Advanced Partner

- Areas of Discipline
- FortiGate
- FortiMail
- FortiSIEM
- FortiSOAR
- FortiAnalyzer
- FortiManager
- FortiEDR – Largest MSSP in North Central US


CYBERTHREATS IN THE NEWS
Baltimore Ransomware Attack Disables City
Experian Experiences Major Breach
Louisiana Forced to Declare Cyber State of Emergency
Cloud Computing Hit Hard by Cyberattacks
Ransomware Costs Hit $11.5 Billion
Email Continues to be Top Cyberthreat
Small Businesses Top Cyber Target

Agenda

- Top 9 Steps to a Data Breach
- (2) Case Studies
- Critical Recommendations
- Q&A

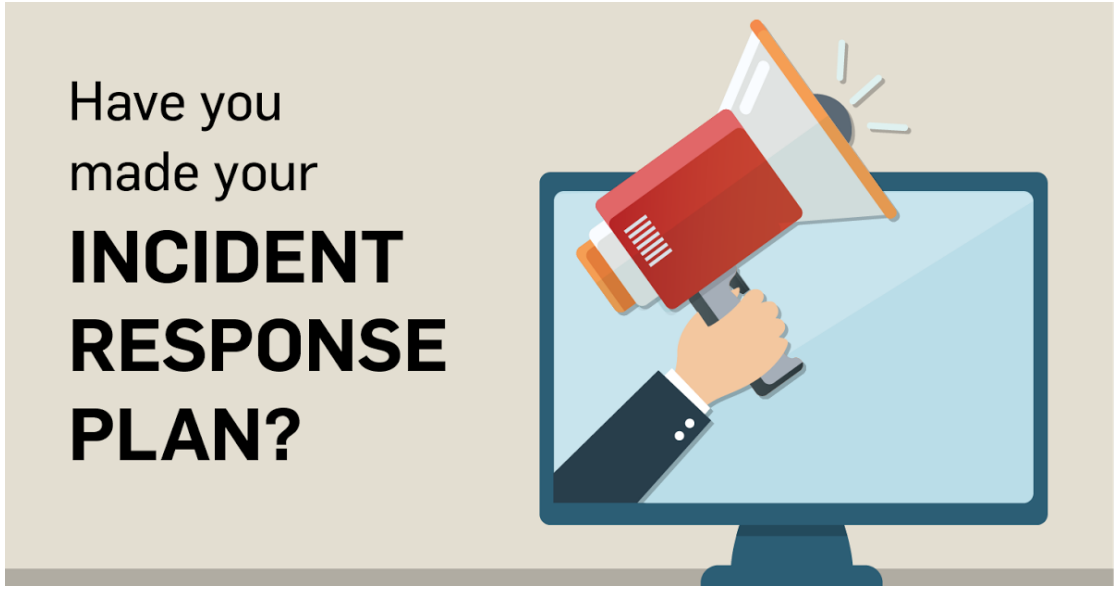
Top 9 Tasks to a Data Breach

Task 1: Call Insurance

- This should be the first call
- Insurance company may offer help with Task 3
- Watch your Exclusions
- Have a relationship with your agent

Task 2: Activate the IRP

- Notify Executive Leadership
- Media Relations
- Watch Social Media
- Consider announcing the event publicly
- Don’t hide it



Task 3: Call a Incident Response Company

- Sometimes provided by insurance
- Take Forensic Images
- Establish Timelines
- Interface with Insurance
- Attempt to answer the Who, What, When, Where, Why and How

Task 4: Notify Federal Law Enforcement

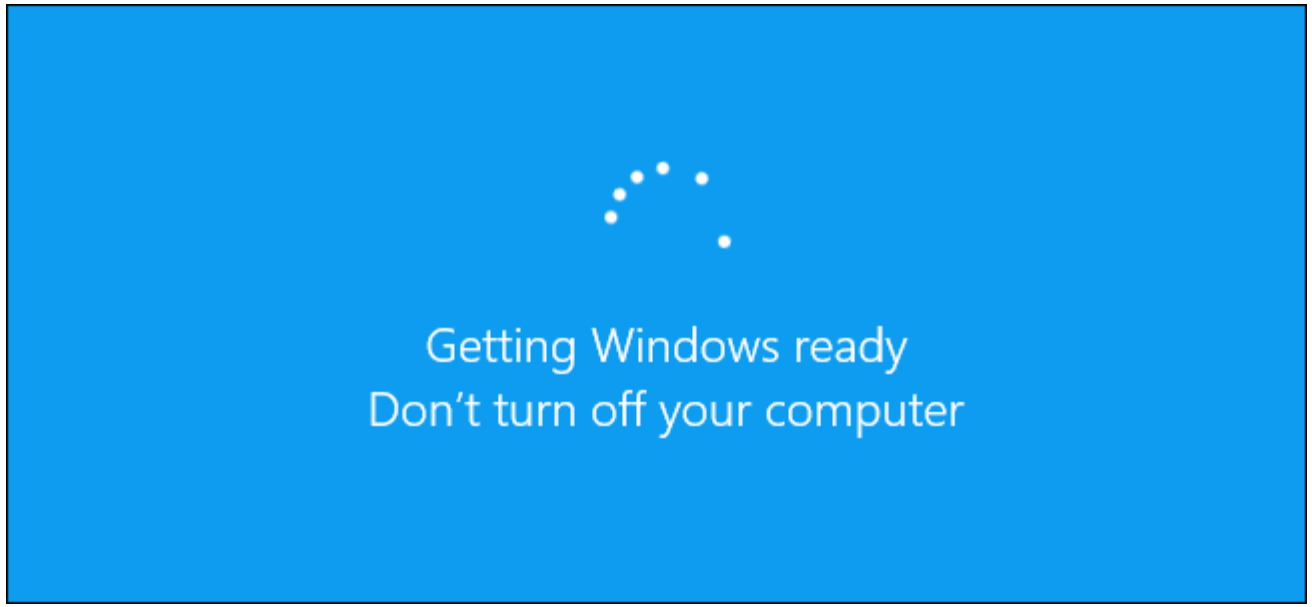
- Notifying Local Law Enforcement won't be helpful
- Recommendation is US Secret Service
- They typically Respond Onsite
- Criminal File is Open

Task 5: Kill The Internet

- This will stop further communication externally
- Don’t turn the firewall off

Task 6: Don’t Turn Devices Off

- Turning off a device will erase in-memory evidence
- You can unplug the network cable



Task 7: Start Documenting

- Exact timelines are critical
- Date/time with details
- Investigators will need this detail

Task 8: Find Patient 0

- Have FTK imager handy
- Don’t unplug patient 0
- Take photos of screen images

Task 9: Don’t Respond to the Bad Actor

- Let insurance or legal handle this
- Don’t connect to the Dark Web

Case Study #1
Ransomware

SECURECYBER DEFENSE

Case Study #1: Ransomware Attack

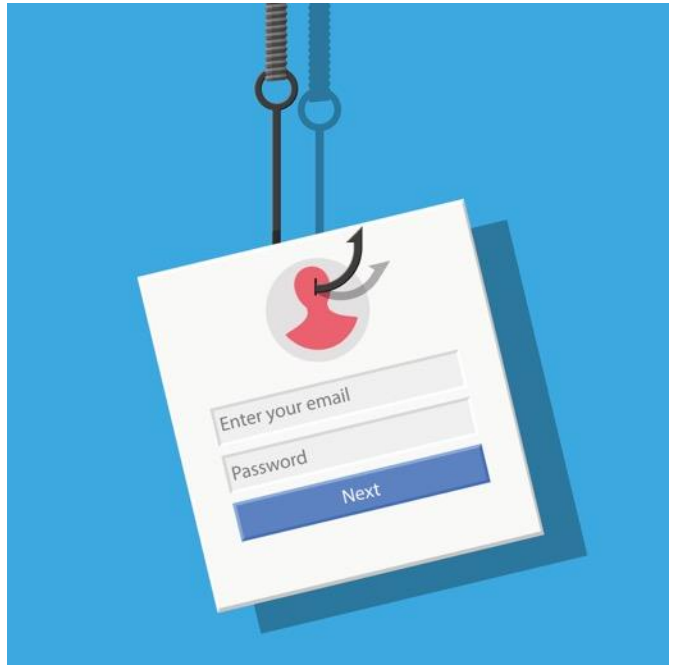
- MALWARE: Sodinokibi
- Compromised VPN
- Backups Domain Joined
- No Offline Copy
- FortiEDR Used in Hot Environment
- Ransomware was Paid
- EDR was able to stop 16 new infection attempts

Case Study #2
Business Email Compromise

SECURECYBER DEFENSE

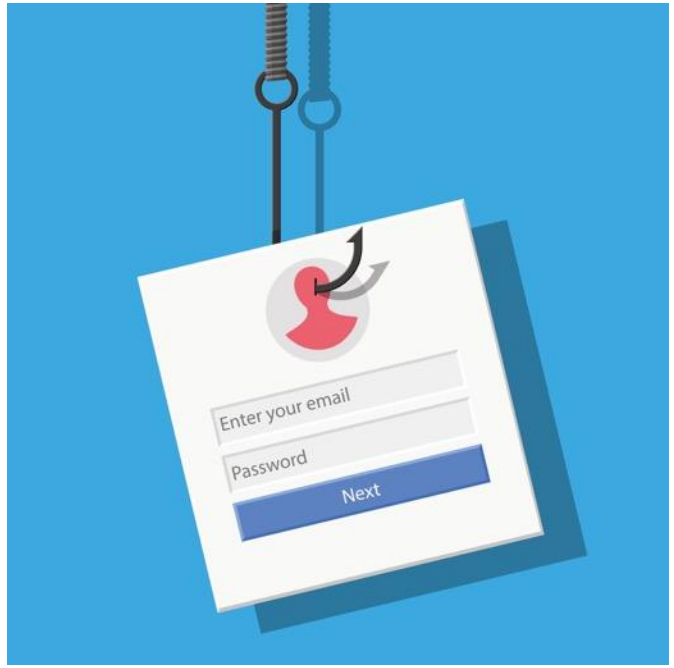
Case Study #2: Business Email Compromise

- CFO Googled Hunting Bank
- CFO Presented with fraudulent site link
- Provided Username/Password/MFA
- Hacker Proceeded with 16 wire transfers
- Client also had a DDoS attack on phone system
- US Secret Service Responded



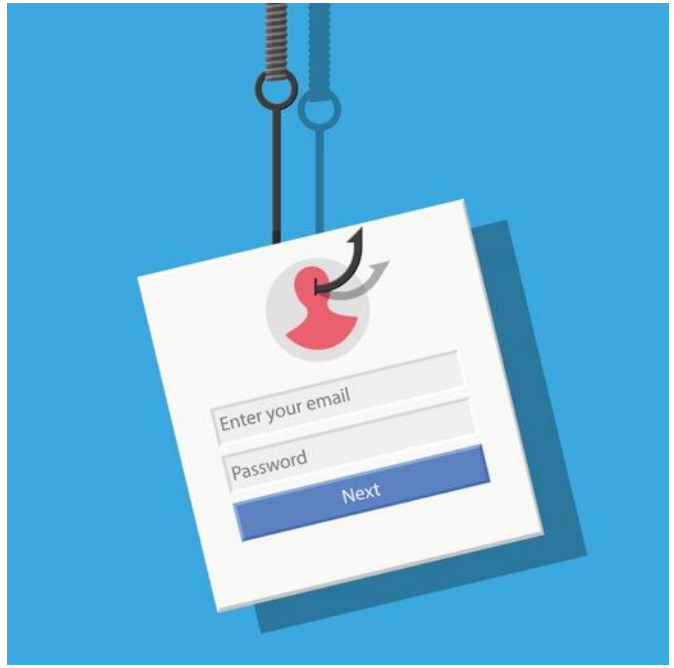
Case Study #2: Business Email Compromise

- US Secret Service executed the Kill Chain from FinCEN
- 900k of 1.3 million was recovered



Case Study Summary

- Both cases took 3-4+ weeks to fully recover
- Financial impact in both cases was in excess of $500k



Final Recommendations

Final Recommendations

- Establish a relationship with a IR company ahead of time
- Work out details with your insurance company
- Have a IR plan and practice it
- Use MFA
- Train your employees
- Use the 3-2-1 Rule for Backups
- Inspect East/West Traffic

Final Recommendations

- Use network segmentation
- Replace Windows XP/2003
- Patch
- Remove Unsupported Applications
- Beef up AD Policies
- Consider configuration logon hours
- Deploy a SIEM

Connect on LinkedIn
https://www.linkedin.com/company/secure-cyber-defense-llc

Questions?

Secure Cyber Defense

Shawn Waldman – CEO
@cyberwaldman
Secure Cyber Defense
www.secdef.com
937-388-4405

Connect on Twitter:
@secdefllc

SECURECYBER DEFENSE