A Practical Approach to Cybersecurity

Presented by:
Martin Straub
Threats!

- Malware
- Key loggers
- Viruses
- Spear Phishing
- Phishing
- Denial of Service
- Man-in-the-Middle
- Password Attacks
Worldwide Attacks??
Costly...

Types of attacks
Cyber incident type; CNA Claim Data, 2016–2017:
- Ransomware: 10%
- Social engineering: 20%
- Hacking: 30%
- Human error: 31%
- Other: 9%

Costs in time and money
- Average days to identify a data breach: 191
- Average days to contain a data breach: 66
- Average cost per record of a data breach in the United States: $225

Professionals at risk
- 58% of victims of data breaches were categorized as small businesses.
- 68% of breaches took months or longer to discover.
- 60% of breaches for the Professional Services industry were discovered by an external party.
- The Professional Services industry is the 4th most common industry to be targeted by social breaches (phishing/pretexting).

Path to Better Security

• Is client data at risk?
• What are our vulnerabilities?
• Is our network “hackable”? 
• What can we improve?
  – Best practices
  – Cost-effective opportunities
  – Ongoing monitoring
Challenges…

Mandient, Fireeye, RSI, Arctic Wolf, etc.

• Very expensive (starting at $20k)
• Industry expertise?
• Generic assessment
• Not holistic
  – White hat hack ≠ assessment
  – Incident response ≠ assessment
• Scare approach / jargon
Better Approach?
"Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence."

In other words…

What are all the bad things that could happen to us, how likely is it that any given thing could happen, and how bad would it be if it did happen?
Assessing Risk

Low
- No internet presence
- Limited data, no PII
- Limited geography
- Limited financial $
- Low IT dependence
- Few employees/partners

Medium
- Web transactions / portal
- Some attractive data
- Regional footprint
- Some financial $
- Important IT systems
- Many partners

High
- Public website and PII
- Attractive (mineable) data
- Multinational presence
- Significant assets
- Critical IT systems
- Widespread employees/partners
Risk and Vulnerability Management
(External Controls)

• Firewall / network traffic controls
• Remote access controls
• Wireless security
• Physical control of assets
• Partners/vendors access controls
Recommendations

- Secure wifi networks and isolate guest network
- Do not use public or unsecured wifi
- Use a business class router with a security subscription (eg Fortinet, Sonicwall)
- Encrypt notebook PC hard drives
- Secure remote access with complex / multifactor passwords, VPN, etc
- Do not allow unattended vendor remote access
Data Loss Prevention
(Internal Safeguards)

• Organization security policies
• Access controls to PII (personal info)
• Network security controls
  – Passwords, MFA (multi-factor authentication)
• Virus protection
• Patch management
• Disaster recovery planning
Recommendations

• Limit employee access to sensitive internal data
• Passwords
  – Complex and change regularly
  – Multi-factor authentication, especially for cloud apps
• Centralized antivirus and Windows patching
• Encrypt backups and store offsite or in cloud
Regulatory Compliance

Review applicable standards

- PCI
- GDPR
- HIPAA
- FINRA
- SOX
Security Framework

Company Culture

External controls

Internal safeguards

Regulatory compliance
Company Culture

• Do you have a Cybersecurity Plan?
• Does it address all cybersecurity components?
• Do you carry cybersecurity insurance?
  – Have you addressed prerequisites?
Company Culture

- Do you have an IT security policy?
  - Are employees required to read and acknowledge?
  - Is it modified periodically?
Company Culture

• Does your IT security policy address:
  – Appropriate use
  – Client confidentiality
  – Mobile devices
  – Remote work / telecommuting
  – Password policies
  – Partners/vendors access to data
  – Breach response
Employees

- Greatest asset or biggest liability?
- Employee espionage
- Unintentional breaches
- Do they understand security policy?
- Consequences for non-compliance?
Phishing / Spear Phishing

• Biggest risk
  91% of breaches begin with spear phishing

• Constantly evolving / sophisticated

• May originate from a “trusted sender”

• Office 365, G Suite = significant threat
Phishing / Spear Phishing

• How to prevent / mitigate?
  – 3rd party filtering
  – Tag subject line on [External] emails
  – Forward all phishing emails / Outlook add-in
  – Office 365 branding
Office 365 Branding

Typical Sign-in

Branded
User Awareness

• Onboard training
• Periodic phishing tests
• Internal awareness program
  – Employee presenters at team meetings
  – Security webinars / videos
  – Encourage employee “hackers”
• Review breach response
Training Resources

• Phishing
  – Knowbe4.com
  – Phishme.com
  - https://phishingquiz.withgoogle.com/

• Security awareness
  – knowbe4.com/automated-security-awareness-program
Suggested Next Steps

• Appoint a “CISO” (Chief Security Officer)
• Implement employee awareness program
• Cybersecurity evaluation
  – External vendor or self-assess
  – Penetrating testing
  – Repeat periodically
• Ongoing monitoring
  – Security Operations Center?
Additional Resources

• Microsoft Phishing Protection Guide

• Center for Internet Security
  https://www.cisecurity.org/controls/

• FCC Cyberplanner
  https://www.fcc.gov/cyberplanner