Cybersecurity for Small Business

Andrew Green
Lecturer of Information Security and Assurance
Kennesaw State University

Cybersecurity for Small Business

- What to protect
- Where are the threats coming from
- How to defend against them
- General tips
- Resources
- Summary

What to protect

- Banking accounts
- Credit cards
- Employee records
- Customer data
- Intellectual property (IP)
- Sensitive company data

What to protect

- Banking accounts
- Credit cards
  - Organization
  - Customers

What to protect

- Employee records
  - Contain sensitive/protected data about your people
  - Used in identity theft and tax return fraud scenarios
- Customer data
  - Contain data about your lifeblood – treat it as such!
  - Data breach notification laws differ from state to state
  - Customer's state dictates your requirements

What to protect

- Georgia breach notification law
  - Full name, or first initial and last name
  - PLUS…
  - One of these attributes
    - SSN
    - DL or state ID card number
    - Account, credit card or debit card number
    - Account password, personal ID number or other access codes

What to protect

- Intellectual property
  - Inventions
  - Literary and artistic works
  - Designs
  - Symbols
  - Names and images

What to protect

- Sensitive company data
  - Sales prospect list
  - Sales projections
  - Customer feedback
  - Future project list
  - Competitor analysis

Where are the threats coming from

- Ransomware
- Social engineering (SE) attack
- Password reuse
- Remote access to business network

Where are the threats coming from

- Ransomware
  - Malware which encrypts systems and data until a ransom is paid
  - Payment typically made in Bitcoin
  - Enter organization through phishing attack or vulnerable systems exposed on the Internet

Where are the threats coming from

- Social engineering (SE) attacks
  - “Hacking the human”
  - Phishing and spear phishing
  - Telephone calls as setup for other attacks
  - SMS-based attacks

Where are the threats coming from

- Password reuse
  - Employees use same password for multiple corporate and personal accounts
  - Allow for credential stuffing attacks

Where are the threats coming from

- Remote access to business systems
  - Necessary for remote work
  - Necessary for IT support

How to defend against them

- Banking accounts
  - Bank in-person when possible
  - Use MFA on your online accounts
  - Only do online banking from a trusted system
  - Commercial accounts are regulated differently than consumer accounts
  - Forget your “personal” experience in fraudulent transactions
  - Federal Reserve Regulation E is only for consumer accounts
  - Verify vendor payment changes “out of band”

How to defend against them

- Credit cards – Company
  - Issue company cards sparingly
  - Routinely audit accounts
  - Install spending limits

How to defend against them

- Credit cards – Customers
  - Monitor readers for skimmers and shims
  - Meet PCI-DSS compliance by offloading CC processing
  - Require chip and pin on in-person transactions
  - If online business, routinely scan website code for malware

How to defend against them

- Employee records
  - Outsource HR functions where possible
  - Transmit data via encrypted channels
  - Tax season – exercise greater care!

How to defend against them

- Customer data / intellectual property / sensitive company data
  - Establish written policies about where and when data can be accessed
  - Build technical controls which support written policies
  - Restrict access based on job roles and responsibilities

General tips

- Establish written policies for data and device use
- Establish technical controls to support written policies
- Develop an incident response (IR) plan
- Require 2FA wherever possible

General tips

- Train your employees on how to spot SE attacks
- Periodic security audit of your network from the inside AND the outside
- Pay for password manager software for all employees
- Develop data backup plan AND TEST IT!

Resources

- Small Business Administration
  - https://www.sba.gov/managing-business/cybersecurity/introduction-cybersecurity
- FCC
  - https://www.fcc.gov/general/cybersecurity-small-business
- Homeland Security
  - https://www.dhs.gov/publication/stopthinkconnect-small-business-resources
- National Cyber Security Alliance
  - https://staysafeonline.org/cybersecure-business/

Remember…

- Risk is part of doing business
- No solution will make you 100% “safe”
- More work “left of bang”
- No, the firewall won’t stop it all…