EVERYDAY SECURITY

INFORMATION SECURITY FOR YOUR BUSINESS

TIM PADGETT – TECHNOBILITY.US

THE SECURITY PROBLEM

Many layers, but some are more likely than others

RUSSIAN HACKERS? YOU BET… BUT THEY'RE NOT AFTER YOU.

SOPHISTICATED ATTACKERS

- High value targets
- Usually other-than-economic motives (espionage, warfare, political)
- State-sponsored, unlimited budget
- Almost impossible to prevent (Equifax, Target, OPM, and well, you know…)

OPPORTUNISTS

- Whatever's easy
- Curiosity or money - mostly money
- They look for weaknesses, openings, and opportunities
- Can be prevented by denying opportunity and value

YOU ARE THE TARGET OF OPPORTUNISTS, AND THEY'RE GETTING STRONGER

- Ignorance and carelessness are the enemy – these provide opportunities
- You, your employees, and your systems are the biggest **opportunity**
- Systems are easier to secure than people
- "the growing number and sophistication of cyber threats poses a critical risk to U.S. businesses, and the impact of a successful attack can be devastating to small businesses in particular." Howard S. Marshall, Deputy Director, FBI Cyber Division
- Zogby survey – 60% of businesses close within 6 months of a successful attack
- DENY THE ATTACKER **OPPORTUNITY** AND/OR **VALUE** – **Here's how**

YOUR EXPOSURE TO THE PROBLEM

You have a great degree of control over this

USING THE WEB

- It's called a "network" because it's structured like a net, or a web
- You can't get from your business to your customer directly, you have to move through the net
- This fact presents an **opportunity – deny it**
  - Can't secure the nodes, but you CAN secure the lines
    - Use SSL and VPN
  - Stay away from risky neighborhoods, stick with the well-known
    - There is no reason to use the Dark Web
  - Be careful about what you give the web, and to whom you give it.
  - Some neighborhoods are better than others, your browser can help

USING EMAIL

- Email is NOT different from the web – same net structure applies, same problems
  - Every message passes through nodes you know nothing about, and a copy is made
- Additionally, the shady can be trickier to spot
  - Email addresses are NOT identities – many ways to falsify
  - Messages can appear to originate from trusted sources
  - Messages can have unseen payloads and purposes
- Targeted communication is an **opportunity** to attack your systems and steal your information
  - Be SURE who you're talking to, where you're going, and what you're opening
  - Simple to launch an attack, your trust is a vulnerability, and a vulnerability is an **opportunity**
  - Use the tools – spam filters, VPN, virus scanners, security packages

ACCEPTING CREDIT CARDS

- Treat credit cards as if they are hand grenades – use them, and then get as far away as you can, as fast as you can. Fastest way to blow up your business.
- NEVER store them in any form or fashion, anywhere. Doing so properly is beyond the capability of most small businesses
- They are a proxy for money, the number one reason for an opportunistic attack
- Access to money in a hidden way is an **opportunity** to steal money
- You are not the target - your customer is
  - Do they watch their credit cards?
- Outsource this risk and cost to those that can handle it (PayPal, Square, etc.)

ANOTHER PERSPECTIVE

Information Assurance – more than security

INFORMATION ASSURANCE

- Larger than Information Security
- Emphasis on Preparation and Readiness
- Wider universe of threats – many of them are not attackers, but circumstances
  - Weather
  - Business Environment (Power network, infrastructure, etc.). Causes hardware failures, disk drives especially vulnerable
- Are you liable? 60% in 6 months…
- Lack of readiness is an **opportunity** to damage your equipment and cause money loss
  - Heard of Mr. Murphy?
- Have a plan

INFORMATION ASSURANCE

- Don’t store anything you don’t have to store
  - Credit cards, inventory, cash
- Limit access
  - Systems AND Facilities
- Backup, backup, backup
  - Data AND power
  - Don’t keep your backups in the primary location
    - Online backups (IDrive, Backblaze, etc.) – benefits and limitations

GREAT. NOW WHAT?

You can do a lot for a little

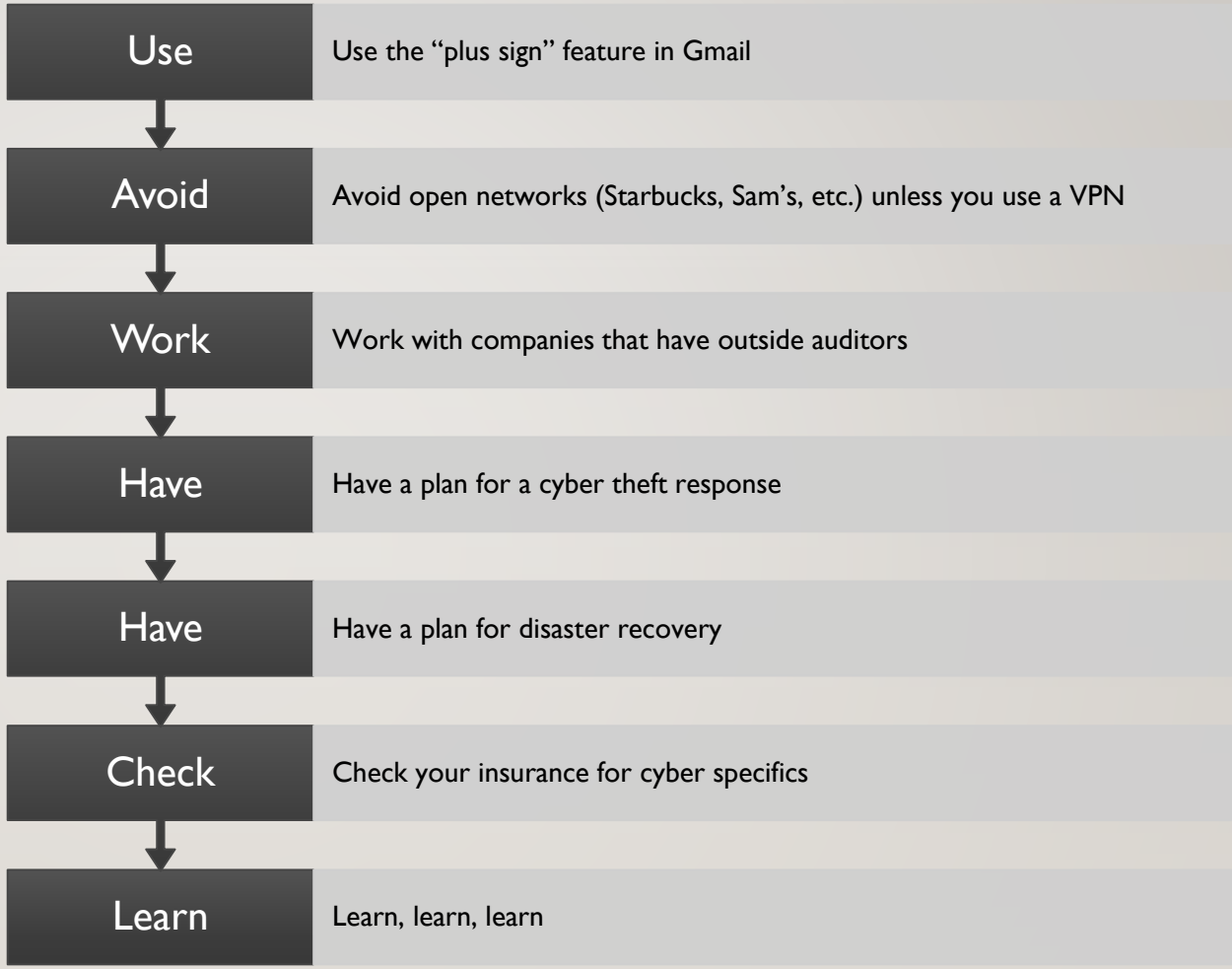
OK – WHAT'S THIS GONNA COST ME?

- Next to nothing, or thousands, or millions
- Cost directly related to the number of **opportunities** you present
- Learning is cost-effective, and being smart is free
- The smart thing to do is make sure what YOU care about is protected
  - Do you care if someone uses your WiFi for free?
- Your legal duty is to take "reasonable and customary" measures
- Trade-off: Cost to secure vs. impact of a breach

FREE STUFF TO DO

- Two-factor Authentication (TFA) – Bad Guy has to have your password AND your phone
- Use a password manager (LastPass, etc.)
  - Generate and keep random passwords and other information there
- Hide your WiFi
- Don't use your business/public email address as a username anywhere
- Don't answer security questions honestly
  - "What's your mother's maiden name?" – SmithGNXLUB

FREE STUFF TO DO



USEFUL PLACES AND THINGS

- Hotspot Shield VPN https://www.hotspotshield.com/
- LastPass Password Manager https://www.lastpass.com/
- HubSpot CRM https://www.hubspot.com/products/crm
- Payment Card Industry (PCI) Merchant Types (you're probably A, B, or B-IP) https://www.pcisecuritystandards.org/documents/Understanding_SAQs_PCI_DSS_v3.pdf
- PCI Self-Assessment Questionnaires (SAQs) https://www.pcisecuritystandards.org/document_library?category=saqs#results

USEFUL PLACES AND THINGS

- Stay Safe Online (National Cyber Security Alliance) https://staysafeonline.org/cybersecure-business/
- Testimony before the Small Business Committee, Howard S. Marshall, FBI Deputy Director https://www.fbi.gov/news/testimony/small-business-information-sharing-combating-foreign-cyber-threats
- Stop/Think/Connect – Homeland Security/FBI/NSA effort https://www.stopthinkconnect.org/
- Payment Card Security Standards https://www.pcisecuritystandards.org/

ABOUT TIM AND TECHNOBILITY

- 25 years experience in IT
- Master of Science, Information Technology (focus on Information Assurance)
- MBA, Information Technology
- Certified Project Management Professional (PMP)
- Technobility's Goal – making technology useful by making it understandable
- tim@Technobility.us
- www.Technobility.us