

# What You Need To Know Now With Cyber Security

**Jay Shelton SVP Executive Risk**

# What Will We Cover

- » Cyber Threat
- » Why Companies Should Care
- » Current Types of Cyber Risks
- » Risk Assessment & Mitigation
- » Steps to Take Now
- » Insurance as a Mitigation

# Cyber Treat

- » Your Computer Connects to Internet – You’re at Risk!
- » FBI Direct Muller – “Two types of companies, ones that have been hacked and ones that don’t know they’ve been hacked”
- » #1 Threat Businesses Face
  - » Intellectual Property
  - » Data & Products
  - » Denial of Service – Ransom or Hacktivist
  - » MONEY – usually the goal
- » Variety of Ways
  - » Third Party Access
    - Internet of Things and Remote Accessing
  - » Insider Threats
    - User errors & IT Security Skills Gap
  - » Phishing, Emails, Websites, Hacking
  - » Connected Devices
    - Mobile Devices and Networks



# State of Cyber Security

- » In 2017, the World Economic Forum rated cybersecurity as one of the top risks facing the world today (NTT Security, 2017).
- » According to Mandiant, a premier American Cybersecurity Firm, “
  - 97% of organizations have already been breached at least once.” “And perimeter security tools, like next generation firewalls, offer little real protection against advanced, targeted attacks.” (Identity Week, 2015)
- » Global Attack Trends (FireEye, 2018):
  - The line between certain financial attackers and state-sponsored attackers no longer exists.
    - Increasing sophistication of financially motivated attacks
    - Email is a major target. Attackers are using interesting ways to get it.
    - Financial attackers tailor phishing email and call victims to ‘help’ them

# Cyber Attack Statistics

50% of small businesses have had data breaches in the past 12 months.



**Svmantec.**

The U.S. had the most data breaches of any other country, by a large margin.



Cybercrime was the 2nd most reported crime in 2016




43%, about half, of all cyberattacks target small businesses.



90% of all customer card data theft attacks occur at small businesses, and these attacks are increasing

# Costs of Cyber Attacks

In 2017, cyber attacks cost small and medium-sized businesses  
 of \$2,235,000.



\$1.5 trillion: The total revenue cybercriminals coaxed out of their victims worldwide in 2017.



\$2.1 trillion: The total global annual cost of all data breaches by 2019, as suggested by Juniper Research



60% Of Hacked SMBs Are Out Of Business 6 Months Later

# Why Should Companies Care

- » Cyber Attacks Continue to Increase
  - » Seen double digit growth every year since 2011
- » Cost of U.S. Cyber Breach Continues to Increase
- » Price of stolen data continues to grow
  - » Credit Card Number - \$.50 per
  - » SSN & W2 - \$50+ per
  - » Bit Coin Exchange – 1 bit coin = \$4,000 and growing
- » Company reputation at risk
- » Significant indirect cost of dealing with cyber attack

Data based: Ponemon Institute 2017 Cost of Cyber Crime Study

# Most Common Types and Goals of Cyber Attacks

1. Social Attacks - Phishing, Smishing, Vishing and Whaling
  - » Use of Email, Texts, and Phone Calls to trick user into clicking on a link, opening an attachment, providing remote connection or obtaining PII
    - 93% of all Breaches begin with Social Attacks
      - 96% of these Breaches involved Email
  - » To deliver Ransomware, Crimeware, Malware, Trojan Horse, Virus, and or Worms
    - 92% of malware is delivered via email, approximately 8% by Web Applications
    - 70% of businesses infected with ransomware have paid the ransom to get their data back.
    - In 2017 Ransomware is up by a staggering 350%



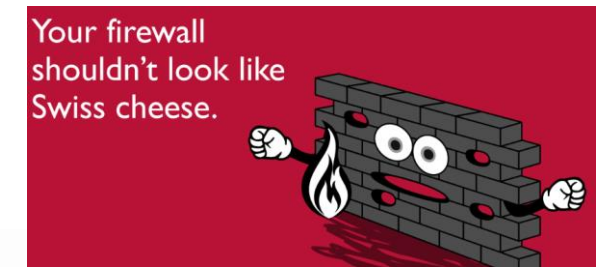
# Most Common Methods and Goals for Cyber Attacks

## 2. Web Application Attacks –

- » Code and Vulnerability exploits, Overcoming authentication
  - Use of Stolen Credentials most frequently the cause then SQL Injection
- » To deliver Ransomware, Crimeware, Malware, Trojan Horse, Virus, and or Worms via Malvertizing, Drive-By Downloads or directly obtain PII from the User
  - 75% of legitimate websites have unpatched vulnerabilities.
  - 18,500,000 websites are infected with malware at any given time
  - 1 in 13 Web requests lead to some type of malware infection

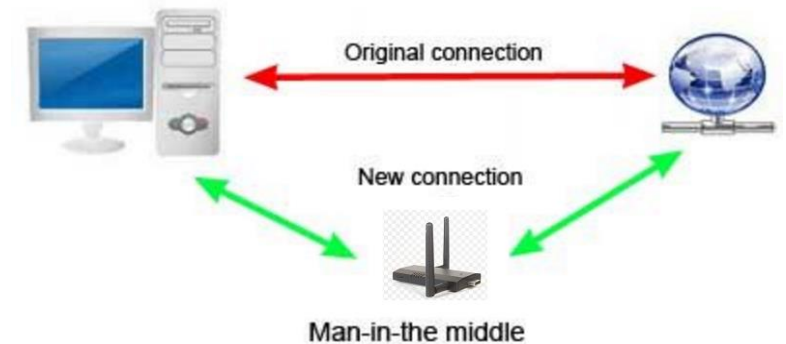
# Legacy Security (Why it Doesn't Work)

- » Compliance doesn't mean **SECURE**.
  - Don't depend on be compliant as a security measure!
- » Yesterday's Firewalls Aren't Enough for Today
  - Firewalls must be configured to allow Smart Phones, Email, Web Pages
  - DDoS attacks over burden Legacy Firewalls leading to loss of service and completed C2C
- » Antivirus is "Dead"
  - Both Symantec and McAfee Executives have said it!
  - Antivirus software only catches 45% of known malware



# Common Vulnerabilities

- » Cyber security skills gaps
- » Configuration Errors – expose equipment to attack
  - » Gain Physical access to the device
  - » Gain logical access via the internet
- » Patch Management & Security Updates
- » Weak Access Controls
- » Lack of User Administration
- » **Lack of Employee Training**
- » **Lack of a Breach Response Plan**



# Risk Assessment & Mitigation

- » Clear Understanding of
  - » Type of information collected
  - » Where it's stored
  - » Who has access
- » Assessing Cyber Risk in 4 Key Areas
  - » Administrative Safeguards
  - » Physical Safeguards
  - » Technical Safeguards
  - » Breach Response – greatest cost saving
- » Key to Any Program
  - » Single person responsible
  - » Give them the authority to make change

# Security (Use Common Sense Methods)

- » **Restrict remote access** - Limit the number of employees who can use remote access to internal devices
- » **Change passwords.** 81% of data breaches used stolen or easy-to-guess passwords..
- » **Update your software and system regularly.** Set your preferences to download updates automatically.
- » **Don't fall for "malware"** – malicious software caused over half of recent breaches. Never respond to suspicious unknown or "phishing" emails, and if you accidentally respond, exit the program and immediately change your passwords.
- » Don't allow use of any device connected to a POS system to surf the Internet.
- » Do **background checks** on vendors and new employees, especially temporary hires.

# Risk Mitigation w/ Insurance

- » Wide variety of Cyber policies
  - » Cyber Risk, Network Security, Privacy Liability, Cyber/Multi-Media
  - » No Standard forms
- » Not every carrier or broker is equal
  - » Pick a carrier with good support structure
  - » Subject matter experts
- » Exclusions & Issues
  - » Limits – make sure their enough & sub-limits
  - » Retroactive coverage
  - » Broadly worded exclusions – look for terms like “all” or “any”
  - » Data Outside of Your Network - cloud
  - » Non-electronic Data - paper
- » What should be covered
  - » Both 1<sup>st</sup> and 3<sup>rd</sup> Party Coverage
  - » Breach Response & Business Interruption
  - » Credit Monitoring & Crisis Management
  - » Cyber Extortion & Data Restoration
  - » Defense & Regulatory Action
  - » Forensic Investigation

# Questions ?