# Protecting your Business: Understanding and Mitigating Cybersecurity Threats

October 30, 2019

SCORE

FOR THE LIFE OF YOUR BUSINESS

# Introductions and Objectives

- Review the cyberthreats landscape facing the small business community.
- Understand the "People, Process, and Technology" aspects of mitigating cyberthreats.
- Demonstrate tools that can help business owners ensure the security of the digital aspects of their business such as malware detection, password managers, backup tools, and strategies, etc.

Make the Small Business Owner a savvy consumer of technology and services

# Agenda

- What are Cyberthreats?
- Costs of Cyberthreats to Small Business
- Small Business Infrastructure Landscape
- People-Process-Technology Mitigation Paradigm
- Practical Steps to Mitigating Cyberthreats
- Question and Answer

# What are Cyberthreats?

SCORE
FOR THE LIFE OF YOUR BUSINESS

# What are Cyberthreats? A Definition

"A cyber or cybersecurity threat is a malicious act that seeks to **damage data**, **steal data**, or **disrupt digital life** in general. Cyber attacks include threats like computer viruses, data breaches, and Denial of Service (DoS) attacks."

# What are Cyberthreats? The Top 8


## RANSOMWARE

Encrypts files and holds your computer hostage for money


## (SPEAR)PHISHING

Lures users into opening emails and/or disclosing personal information


## BYOD DILEMMA

Unsecure devices brought in by users spreading malware or exfiltrating data

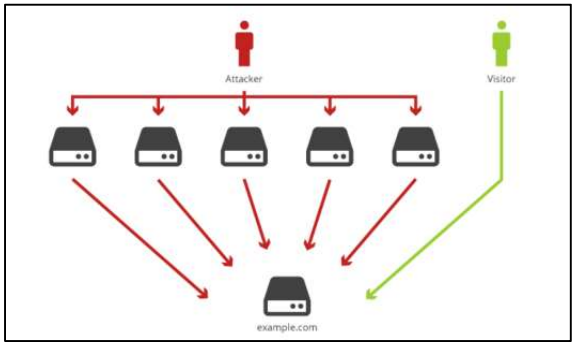
# What are Cyberthreats?


## FRAUDULENT APPS

Applications, even from the app store, that may contain threats


## WEAK PASSWORDS

"123456"
Vs
"7Y*i6dsgy!2$"



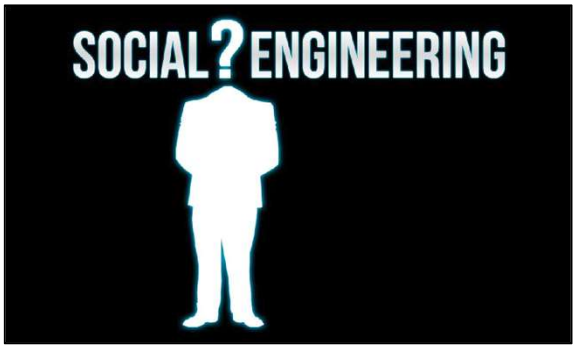

## DDOS ATTACKS

Prevent access to your website by bogging down servers with requests

# What are Cyberthreats?

**LACK OF AWARENESS**

Users doing the wrong thing




**SOCIAL ENGINEERING**

Fraud by impersonation

# What are Cyberthreats? How Attacks Proliferate


- Accessing a malicious website
- Opening an attachment in an email
- Allowing an insecure device to access your network
- Plugging an insecure device into your computer
- Installing and running software from an unknown source
- Having inadequate safeguards

# What are Cyberthreats? Trends

- Ransomware attacks on the decline


**Source:** 2018 Microsoft Security Intelligence Report

Ransomware encounter rates declined approximately 60 percent between March 2017 and December 2018, with intermittent increases across that period.

▲ FIGURE 1.

Ransomware encounters from March 2017 to December 2018

SCORE
FOR THE LIFE OF YOUR BUSINESS

# What are Cyberthreats? Trends

- Cryptocurrency mining on the rise
  - With Bitcoin, miners use special software to solve math problems and are issued a certain number of bitcoins in exchange. This provides a smart way to issue the currency and also creates an incentive for more people to mine.
  - Some forms of malware install bitcoin miners in victim's machine to run the mining algorithms.
  - This can slow down the victim's computer while generating revenue for the miner

**Source:** 2018 Microsoft Security Intelligence Report

# What are Cyberthreats? Trends

- Phishing continues to be a preferred attack vector
  - The share of inbound emails that were phishing messages increased 250% between January and December 2018.


**Source:** 2018 Microsoft Security Intelligence Report

SCORE
FOR THE LIFE OF YOUR BUSINESS

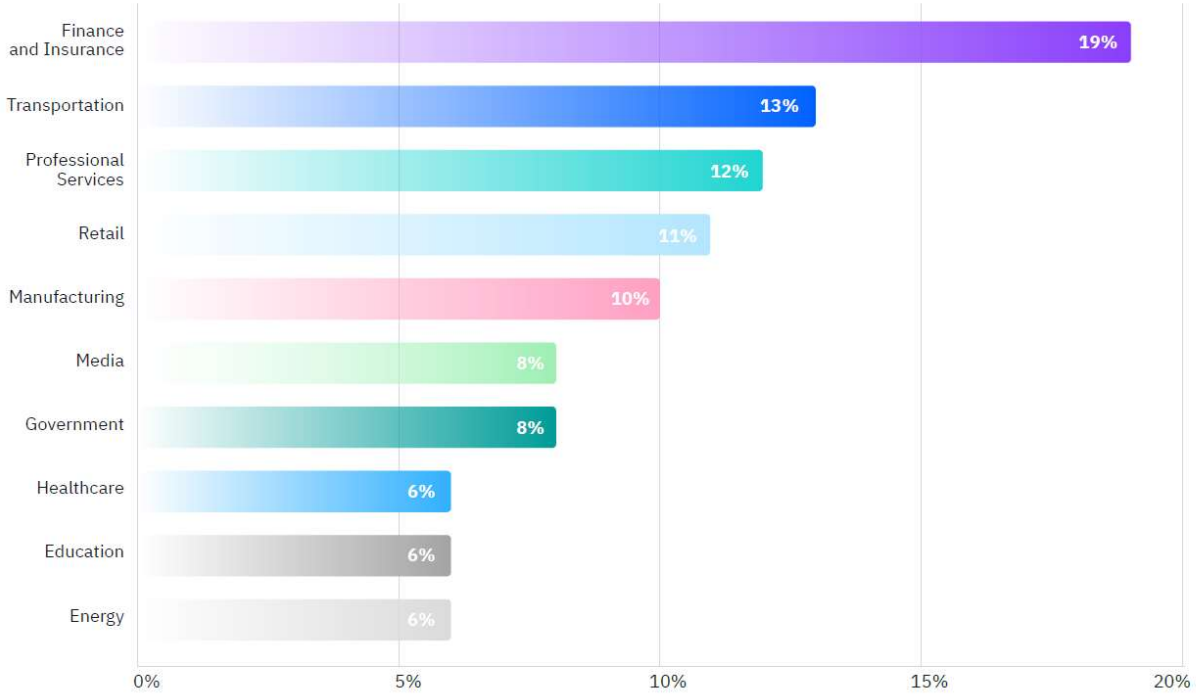
# Costs of Cyberthreats to Small Business

SCORE
FOR THE LIFE OF YOUR BUSINESS

# Costs of Cyberthreats to Small Business

## Most Frequently Targeted Industries in 2018

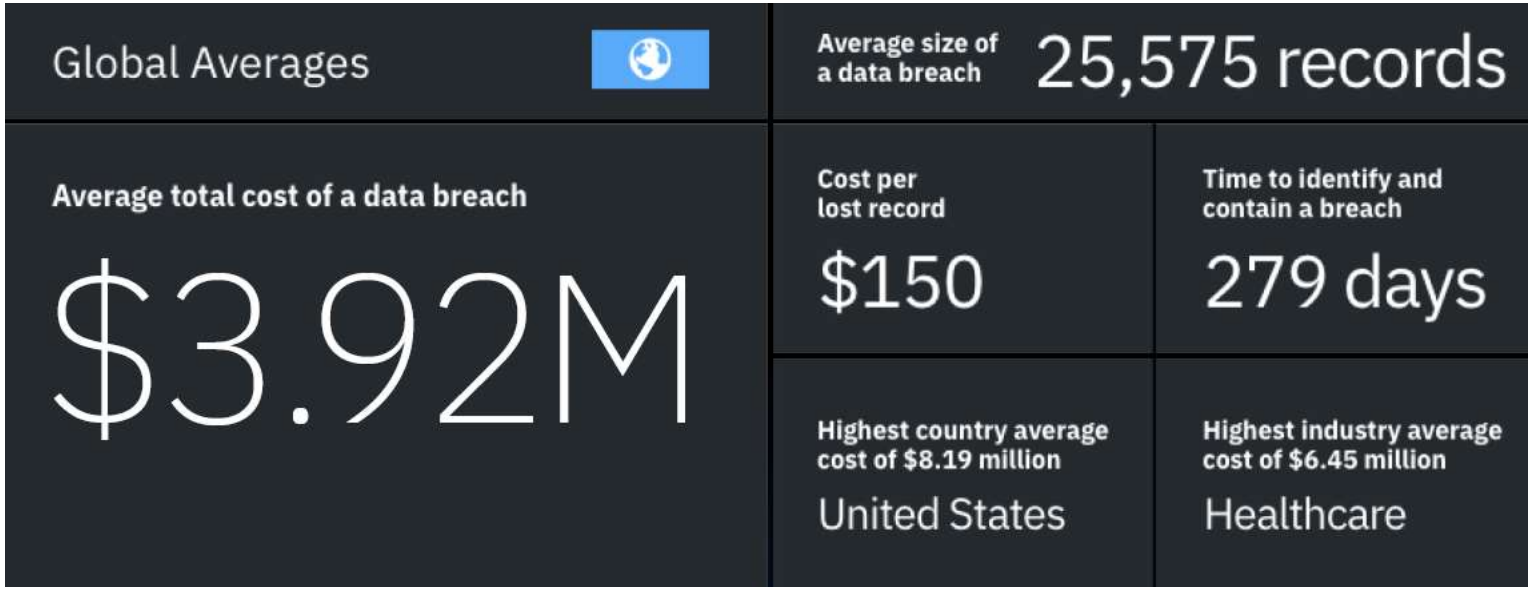
Source: IBM X-Force




**Source:** 2019 IBM X-Force Threat Intelligence Index

SCORE
FOR THE LIFE OF YOUR BUSINESS

# Costs of Cyberthreats to Small Business




507
companies studied

3,211
individuals interviewed

**Source:** 2019 IBM X-Force Threat Intelligence Index

SCORE
FOR THE LIFE OF YOUR BUSINESS

# Costs of Cyberthreats to Small Business

- Lost business was the biggest contributor to data breach costs
- Data breaches impacted organizations for years
- Small businesses face disproportionately larger costs relative to larger organizations
  - Organizations > 25,000 employees - $204/employee
  - Organizations 500-1000 employees - $3,533/ employee

**Source:** 2019 IBM X-Force Threat Intelligence Index

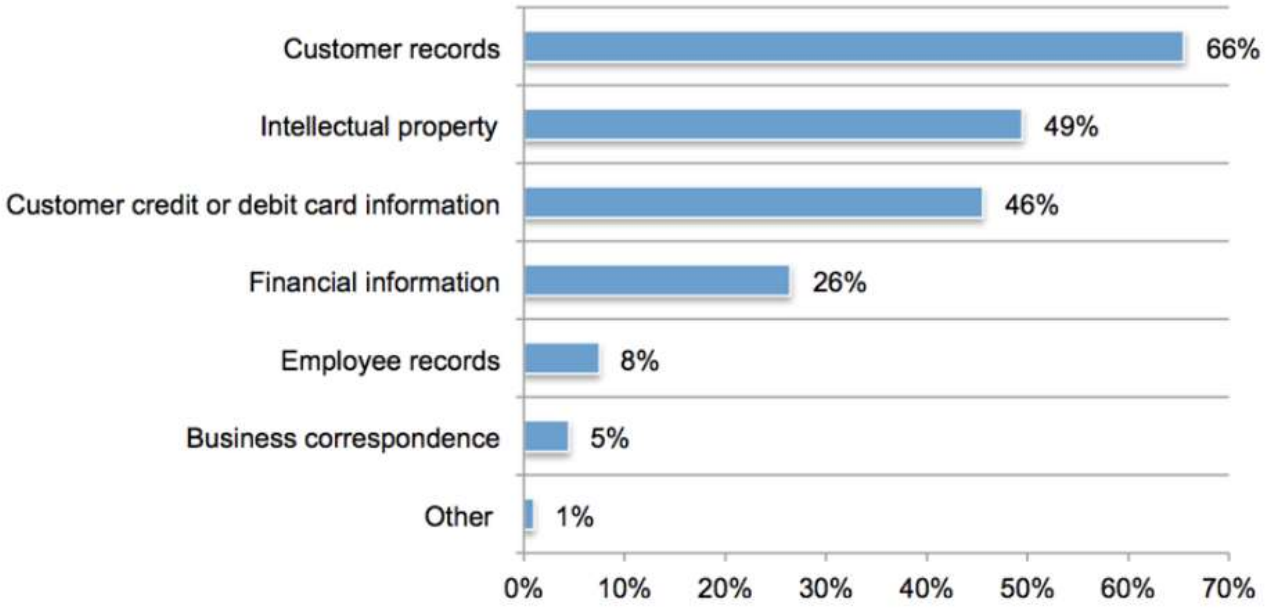
# Costs of Cyberthreats to Small Business

- 43% of cyber attacks target small businesses
- Only 14% of small businesses rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective.
- 60% of small companies go out of business within six months of a cyber attack.
- 48% of data security breaches are caused by acts of malicious intent. Human error or system failure account for the rest.

**Source:** August 2019
Small Business Trends

# Costs of Cyberthreats to Small Business

- Types of information small business owners are most concerned about

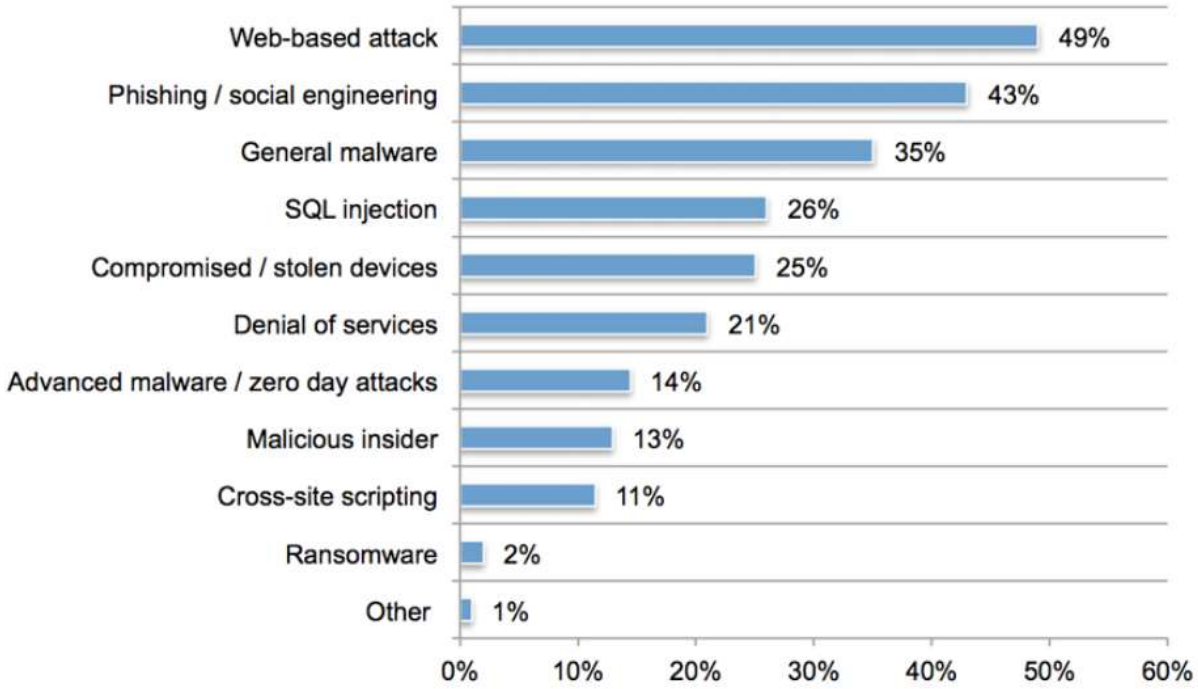



**Source:** August 2019 Small Business Trends

SCORE
FOR THE LIFE OF YOUR BUSINESS

# Costs of Cyberthreats to Small Business

- Types of attacks experienced by small businesses

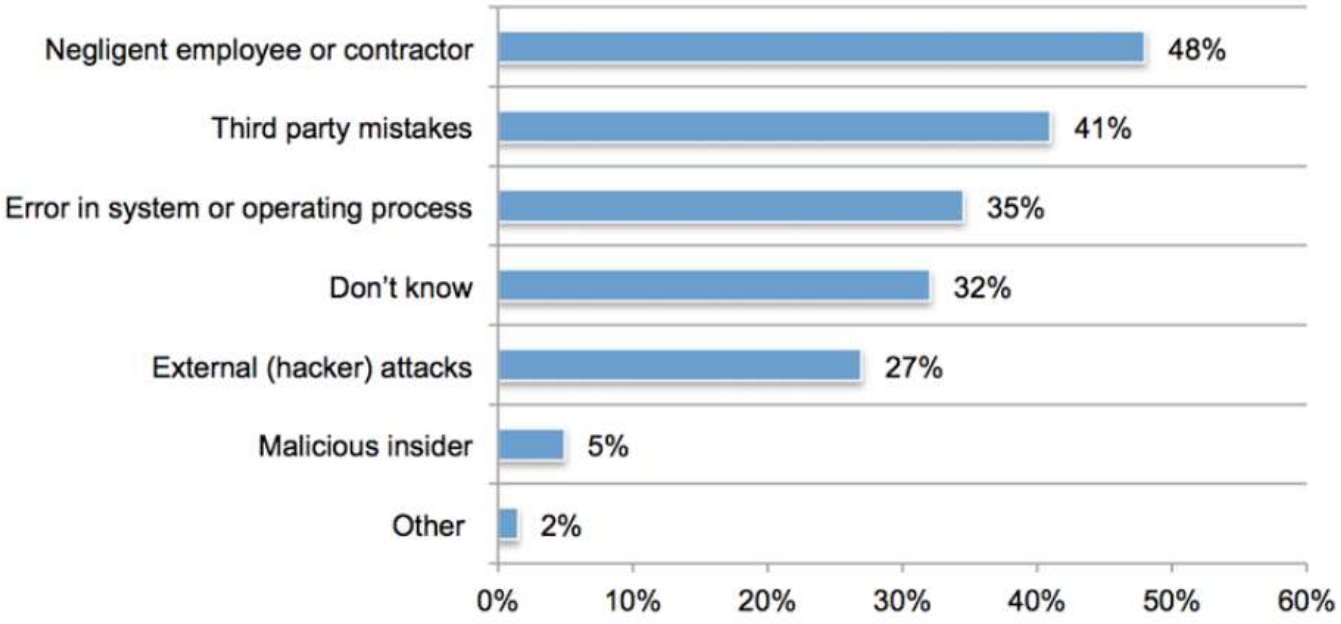



**Source:** August 2019 Small Business Trends

SCORE
FOR THE LIFE OF YOUR BUSINESS

# Costs of Cyberthreats to Small Business

- Root causes of data breaches for small businesses



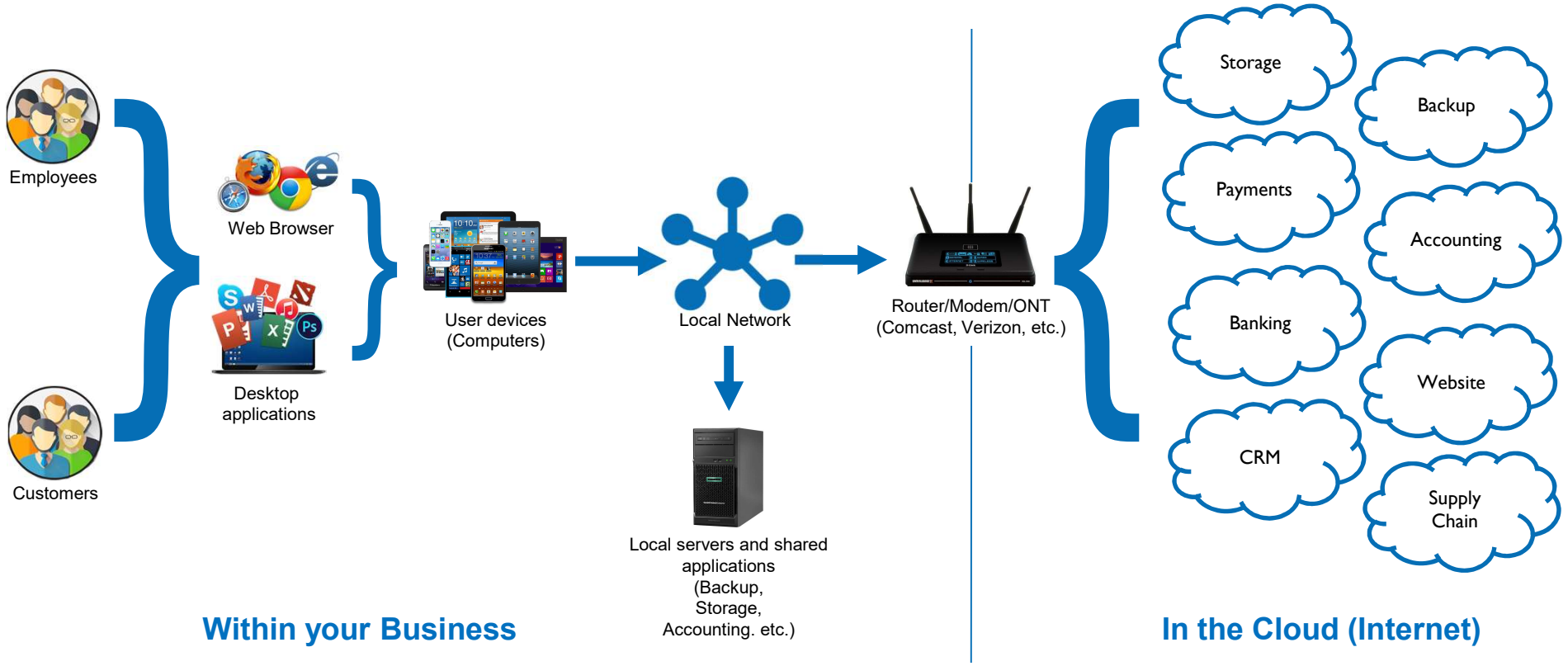

**Source:** August 2019 Small Business Trends

SCORE
FOR THE LIFE OF YOUR BUSINESS

# Small Business Infrastructure Landscape

SCORE
FOR THE LIFE OF YOUR BUSINESS

# Small Business Infrastructure Landscape



# Small Business Infrastructure Landscape

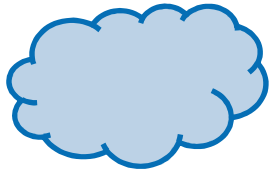
- **Within your Business**
  - Software
    - Browsers
    - Desktop Applications
    - Server Applications

  - Computers
    - Laptops/desktops
    - Servers
    - Mobile devices

  - Local network (router)

CyberSecurity Punch List

- **In the Cloud**
  - Software
  - Servers



- **Human Factors**
  - Employees
  - Customers

SCORE
FOR THE LIFE OF YOUR BUSINESS

# People-Process-Technology Mitigation Paradigm

SCORE
FOR THE LIFE OF YOUR BUSINESS

# People-Process-Technology Mitigation Paradigm

## People

- People do the work
- Without people, nothing can happen
- People make decisions and take actions whether, or not they are informed enough to do so (Subsidarity)
- The most important part of the paradigm

## Process

- Actions or steps that need to happen in order to achieve a particular goal
- Identify key steps
- Provide training on processes
- Ask yourself how to measure success

## Technology

- Technology by itself does not solve problems and should be applied judiciously
- Be sure to get buy-in from those who must use technology
- Beware the "solution in search of a problem" trap

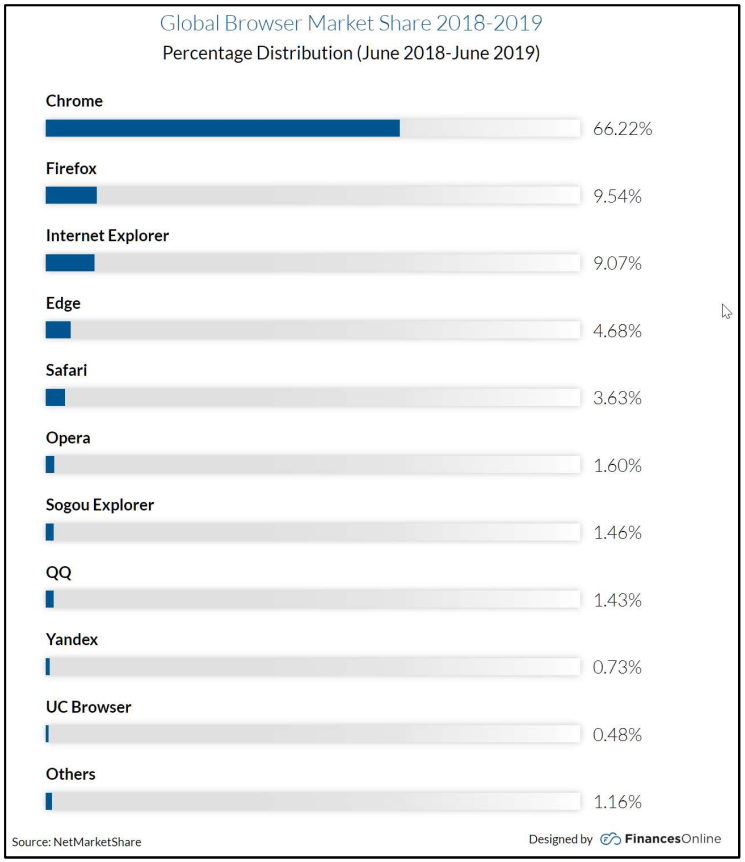
SCORE
FOR THE LIFE OF YOUR BUSINESS

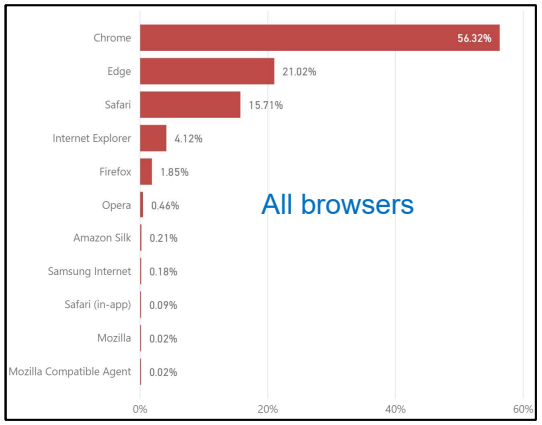
# Practical Steps to Mitigating Cyberthreats

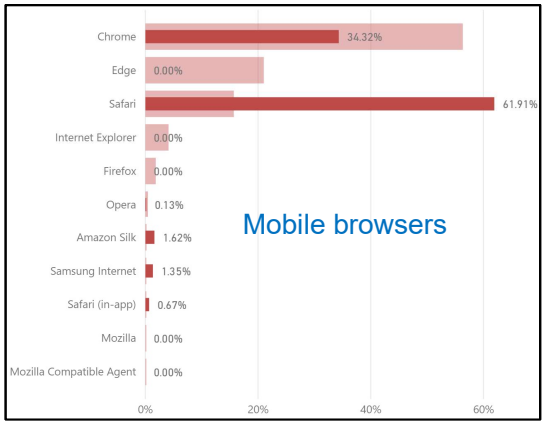
SCORE
FOR THE LIFE OF YOUR BUSINESS

# Practical Steps to Mitigating Cyberthreats

Web Browser




SCORE
FOR THE LIFE OF YOUR BUSINESS

Bucks County
2019

SCORE
FOR THE LIFE OF YOUR BUSINESS

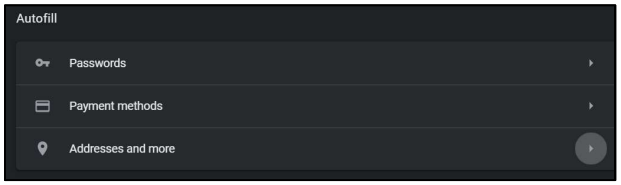
# Practical Steps to Mitigating Cyberthreats

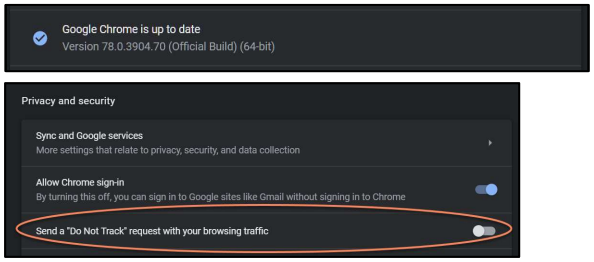

- Recommended
  - Chrome for compatibility, performance, cross-platform, and add-ins
  - Firefox for security, cross-platform, and add-ins
  - Safari if you have an Apple eco-system

- Not Recommended
  - Internet Explorer due to lack of compatibility and add-ins
  - Edge since Microsoft is replacing it
  - Any small player due to compatibility
    - E.g. Opera, Yandex, etc.

# Practical Steps to Mitigating Cyberthreats

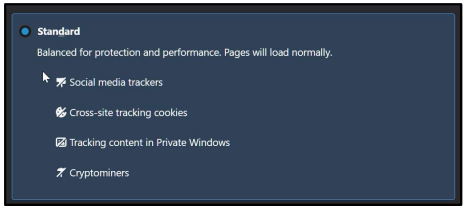

- Browser features that protect you
  - Keep your browser up to date
  - Turn off tracking
  - Block malicious content
  - Only use HTTPS (SSL) sites when possible
  - Block pop-ups
  - Turn off autofill

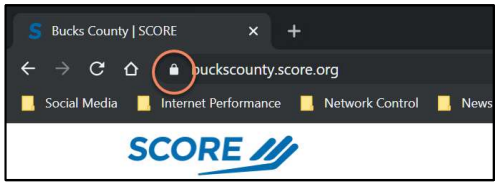








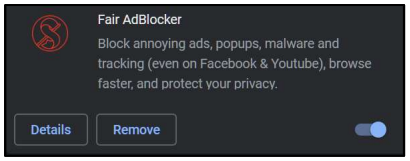



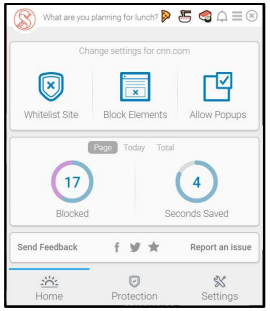


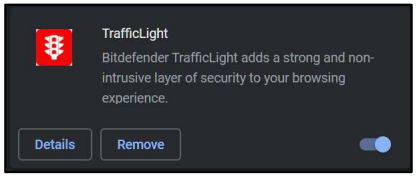
SCORE
FOR THE LIFE OF YOUR BUSINESS

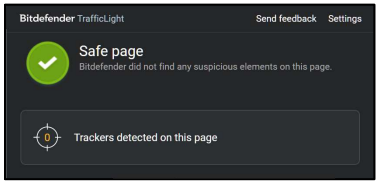
# Practical Steps to Mitigating Cyberthreats

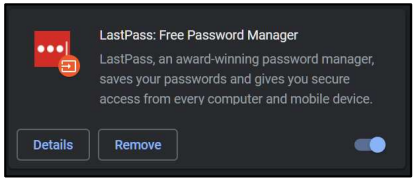

- Useful browser add-ins/extensions
  - Ad blocking
  - Threat detection
  - Password managers
    - More about this later!

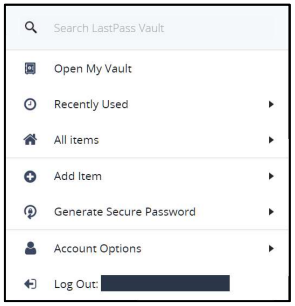


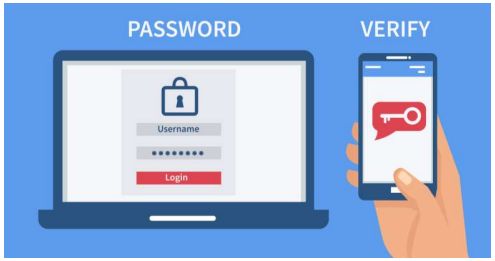




SCORE
FOR THE LIFE OF YOUR BUSINESS

# Practical Steps to Mitigating Cyberthreats


- User account best practices
  - Passwords
    - Weak – Anything common or personally identifiable
      - Pet names, family names, social security numbers, etc.
    - Strong – Contains capitals, numbers, special characters
      - Best to auto-generate these if possible
  - Multifactor (two-factor) authentication
    - Who you are – user name (charles.morris@scorevolunteer.org)
    - What you know – password (0^FW96JuO*b7)
    - What you have – Usually a mobile phone
      - To get pin codes, rolling codes, or use an application


SCORE
FOR THE LIFE OF YOUR BUSINESS

# Practical Steps to Mitigating Cyberthreats


- Password Managers
  - Stores all of your usernames and passwords
  - Local or cloud-based
  - Multiplatform (Laptops/desktops/mobile)
  - Integrates with browsers to autofill
  - Generates strong passwords
  - Emergency access
  - "Freemium" pricing models
  - Web browsers have these, but they are seldom robust


LastPass dashlane 1Password KEEPER True Key™

# Practical Steps to Mitigating Cyberthreats


## People

- Aware of threats posed by web browsers
- Use approved browsers
- Use strong passwords
- Use password managers when possible
- Use work computers for work and limit personal use

## Process

- Training on threats posed by browsers
- Alert appropriate parties if threats are detected
- Keep browsers up to date

## Technology

- Approved browsers
- Extensions to identify threats
- Strong passwords
- Multifactor authentication
- Password managers

SCORE
FOR THE LIFE OF YOUR BUSINESS

# Practical Steps to Mitigating Cyberthreats


- Best practices
  - Only use applications from known sources
    - Microsoft store, Apple store, direct company website, etc.
  - Never use applications from "free" download sites
  - Make sure your malware scanner scans installation packages (usually automatic)
  - Don't allow users to install software if possible
  - Keep applications up to date (usually via automatic updates)
    - Use caution if the application is mission critical
    - Test the upgraded version first if you have concerns

Office 365

LibreOffice

G Suite

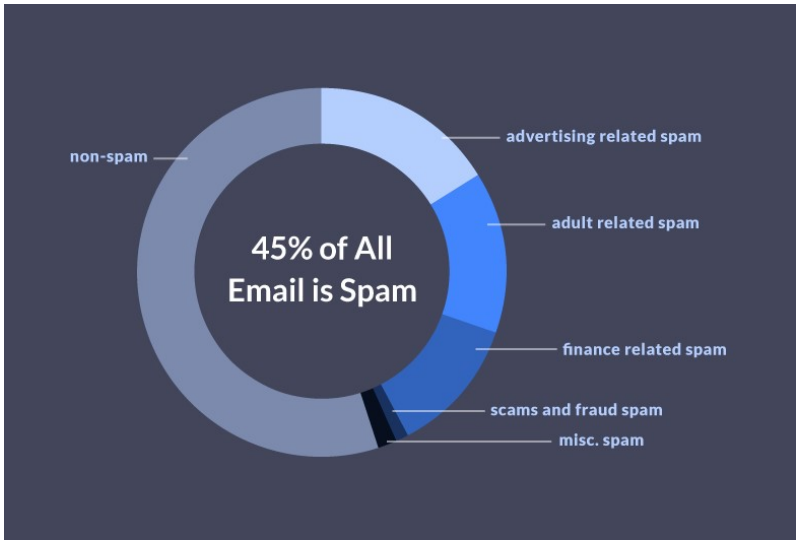
QuickBooks

Adobe

SCORE
FOR THE LIFE OF YOUR BUSINESS

# Practical Steps to Mitigating Cyberthreats


- Notes about email
  - Email is a common vector for phishing and other scams
  - Never open suspicious attachments
  - Never send important usernames and passwords in emails
    - If you must, send them in two separate emails
  - Hover over embedded links to inspect URLs before clicking
  - Use spam blocking settings even if they over-block
  - Vendors will not ask you to verify usernames, passwords, or account information
  - Vendors may ask to verify answers to secret challenge questions after you authenticate to websites




SCORE
FOR THE LIFE OF YOUR BUSINESS

# Practical Steps to Mitigating Cyberthreats


## People

- Aware that application downloads and installations are a prime malware vector
- Use only approved applications on work computers
- Use special caution around email applications

## Process

- Training on threats posed by installing rogue applications
- Alert appropriate parties if threats are detected
- Keep applications up to date (with caution)

## Technology

- Approved applications
- From known sources
- Automate updated where possible
- Automated malware scanning

SCORE
FOR THE LIFE OF YOUR BUSINESS

# Practical Steps to Mitigating Cyberthreats


User devices (Computers)


Local servers and shared applications

- Operating System Distribution

statcounter GlobalStats

**United States**

| Windows | iOS | Android | OS X | Chrome OS | Unknown |
|---|---|---|---|---|---|
| 33.42% | 30.87% | 21.27% | 9.33% | 3.05% | 1.11% |

Operating System Market Share in United States Of America - September 2019

**Global**

| Android | Windows | iOS | OS X | Unknown | Linux |
|---|---|---|---|---|---|
| 40.44% | 35.32% | 14.29% | 6.4% | 1.59% | 0.8% |

Operating System Market Share Worldwide - September 2019

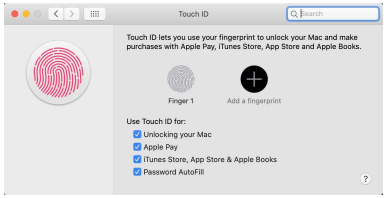
The incidence of malware on operating systems closely follows global operating system market share

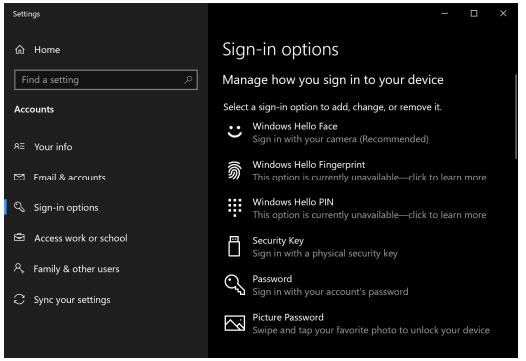
# Practical Steps to Mitigating Cyberthreats

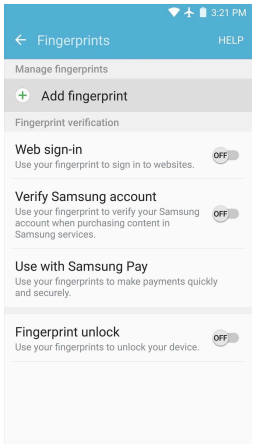

User devices (Computers)

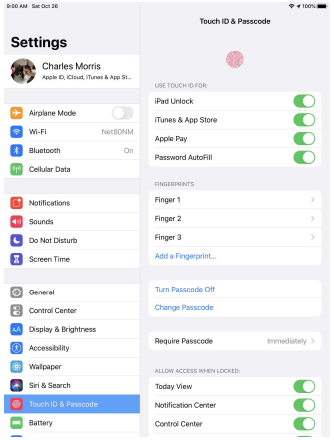

Local servers and shared applications

- Prevention
  - Protect device access
    - Set timeouts requiring login
    - Newer authentication methods
      - Windows Hello – Password, PIN, fingerprint, face recognition
      - Apple Touch ID and face recognition
      - Android Fingerprint recognition and face unlock




SCORE
FOR THE LIFE OF YOUR BUSINESS

# Practical Steps to Mitigating Cyberthreats



- Prevention
  - Use operating system settings
    - Windows
      - User Access Control – prevents applications from accessing the operating system by asking user for permission
    - OSX/macOS
      - Security and Privacy - prevents applications from accessing the operating system by asking user for permission
    - iOS
      - Security built into the core
    - Android
      - Application permissions

Windows

macOS®

iOS

ANDROID

SCORE
FOR THE LIFE OF YOUR BUSINESS

# Practical Steps to Mitigating Cyberthreats



- Prevention
  - Anti-virus
    - Less important than in the past – ***hackers have moved to adware and malware attacks***
    - **Don't run multiple Anti-virus programs!**
    - All products are good based upon industry ratings
    - Your internet provider may offer it for free
    - Don't forget Microsoft Windows Defender
    - OSX/macOS
      - Not a large attack surface due to low market share
      - I'm on the fence about anti-virus for this platform
    - No real anti-virus for iOS – The OS prevents apps from getting the access that they need

McAfee

Symantec.

Bitdefender

kaspersky

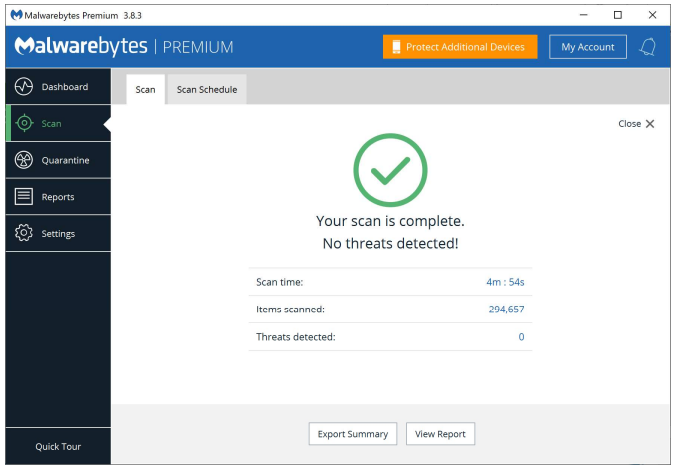
Windows Defender

SCORE
FOR THE LIFE OF YOUR BUSINESS

# Practical Steps to Mitigating Cyberthreats



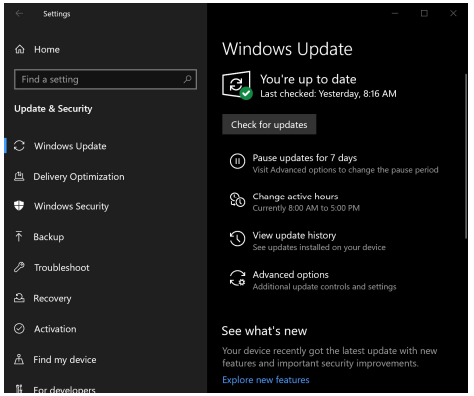
- Prevention
  - Anti-malware
    - More important than in the past – ***hackers have moved to adware and malware attacks***
    - Malwarebytes is the 800 pound gorilla
    - Run in addition to Anti-Virus
    - Multi-platform (Windows, macOS, iOS, Android)
    - Versions
      - Free – cleans devices
      - Pay – cleans and protects devices

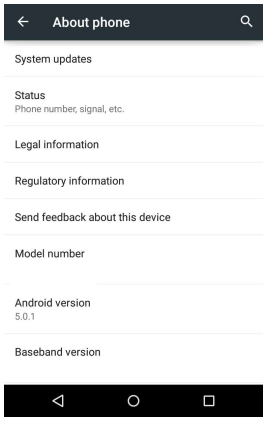


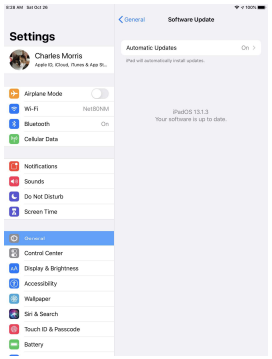
# Practical Steps to Mitigating Cyberthreats



- Prevention
  - Operating System Patching
    - Operating system makers provide periodic updates to enhance security and features
    - Can sometimes select the update cadence
    - Should test major updates to ensure your key applications still work
      - Windows 10
        - Major - "1703", "1809", "1903"
        - Minor - Interim patches
      - macOS/iOS
        - Major - macOS "10.15", "iOS 13"
        - Minor - macOS "10.15.1", "iOS 13.1"
      - Android
        - Major - "9", "Pie"
        - Minor - "9.1"

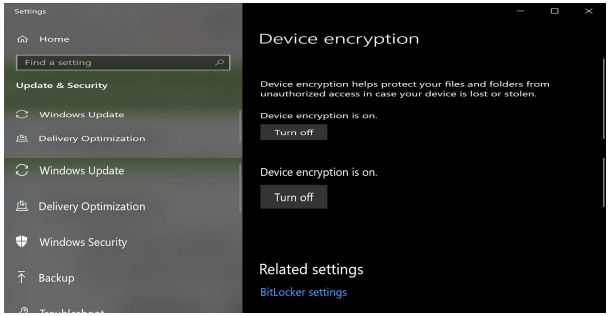



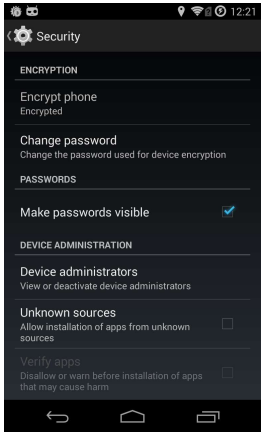

SCORE
FOR THE LIFE OF YOUR BUSINESS

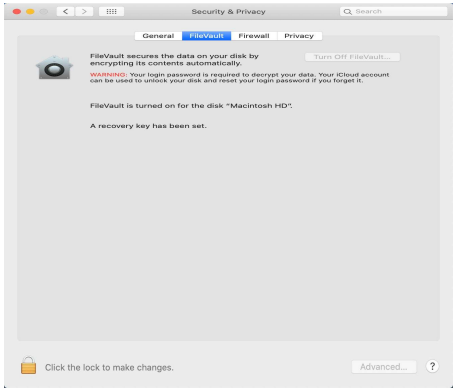
# Practical Steps to Mitigating Cyberthreats



- Planning for an Attack
  - Disk encryption – prevents a thief from stealing your data if the device is stolen
    - Windows – Bitlocker
    - OSX/macOS – FileVault
    - iOS - Encrypted by default
    - Android – Security settings



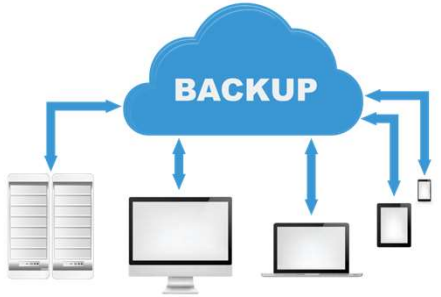




SCORE
FOR THE LIFE OF YOUR BUSINESS

# Practical Steps to Mitigating Cyberthreats



- Planning for an Attack
  - Backing up
    - Ensures your critical data is safe
    - Forms the basis of a disaster recovery strategy in case of attack or natural disaster
    - Basics
      - A planned and disciplined approach
      - Periodic
      - Data stored offsite
      - If you use a third-party, have a Service Level Agreement with guaranteed recovery time




SCORE
FOR THE LIFE OF YOUR BUSINESS

# Practical Steps to Mitigating Cyberthreats



- Backup Topology

User devices
(Computers)

Backup to Cloud

Router/Modem/ONT
(Comcast, Verizon, etc.)

Cloud
Backup

Backup to
Local device

Local storage
device

Hybrid Backup
to Cloud

Offsite Backup

**Within your Business**

**In the Cloud (Internet)**

SCORE
FOR THE LIFE OF YOUR BUSINESS

# Practical Steps to Mitigating Cyberthreats



Cloud Backup

**Pros**

- Single backup provider
- Convenient
- Moves data offsite
- Fixed cost (usually)

**Cons**

- Dependent on internet connection
- Uses internet bandwidth
- Can be slow to backup
- Can be slow to recover

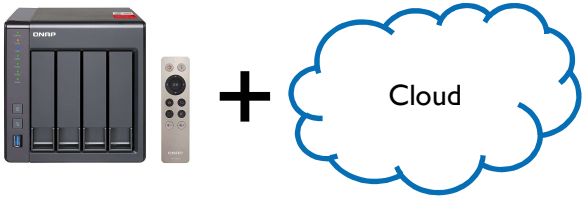
Local Backup

**Pros**

- Very fast backup
- Very fast recovery
- No dependence on internet

**Cons**

- Cost to procure and maintain hardware
- Must take backup offsite daily




Hybrid Backup

**Pros**

- Very fast backup
- Very fast recovery
- Moves data offsite
- Two layers of safety

**Cons**

- Cost to procure and maintain hardware
- Cost of cloud backup provider

SCORE
FOR THE LIFE OF YOUR BUSINESS

# Practical Steps to Mitigating Cyberthreats

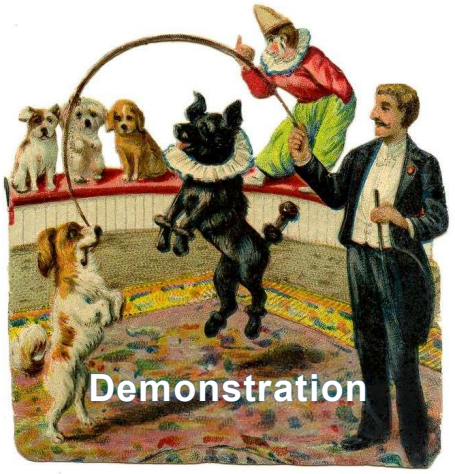


- Planning for an Attack
  - Backup Software
    - Cloud-based solutions
      - Carbonite is the big player
    - Local backup solutions
      - Apple – Time Machine in built-in
      - Acronis has solutions for Windows and macOS
    - Hybrid backup solutions
      - Dedicated storage solutions contain option for cloud backup
      - Acronis offers both local and cloud backup in one package
    - Note about Windows 10 OneDrive Folder Protection

CARBONITE

BACKBLAZE

Acronis


SCORE
FOR THE LIFE OF YOUR BUSINESS

# Practical Steps to Mitigating Cyberthreats



- Other items
  - Bring Your Own Device (BYOD)
    - Make sure foreign devices are patched and have malware protection
    - Isolate foreign devices from your business network (more on this later)
  - Endpoint protection
    - Be careful when allowing users to connect external devices
      - Thumb drives
      - External hard drives
    - Make sure your anti-virus/malware prevention software scans external drives


SCORE
FOR THE LIFE OF YOUR BUSINESS

# Practical Steps to Mitigating Cyberthreats


User devices (Computers)


Local servers and shared applications

## People

- Use passwords and other authentication means
- Be aware of threats posed by external devices

## Process

- Training on threats posed rogue devices
- Alert appropriate parties if threats are detected
- Keep devices up to date (with caution)
- Plan and implement a backup regimen
- Test your backup regimen

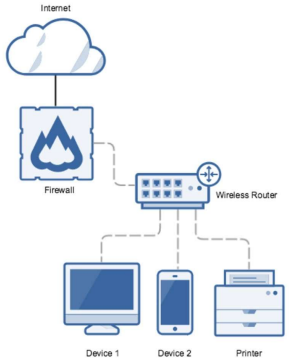
## Technology

- Authentication properly set up
- User access limited
- Anti-virus and Malware protection
- Patching
- Disks encryption in use
- Backup configured and automated

SCORE
FOR THE LIFE OF YOUR BUSINESS

# Practical Steps to Mitigating Cyberthreats

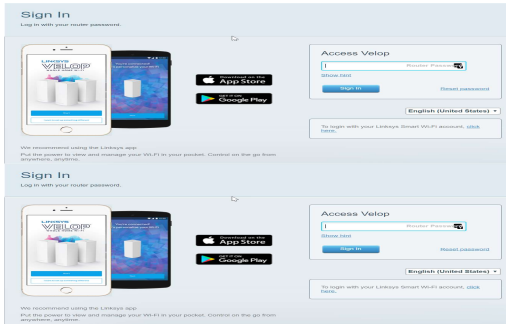

- Securing your network and internet connection
  - Attackers are looking for ways into networks via the internet
  - Routers are the main line of defense
  - Business routers are usually managed by the Internet Service Provider or 3rd Party IT professionals
  - We will review the basics since it gets complicated very fast

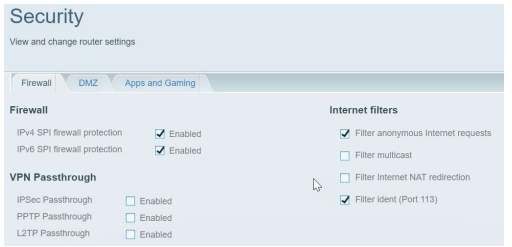



**Network setup, configuration, and maintenance is best left to experts!**

# Practical Steps to Mitigating Cyberthreats

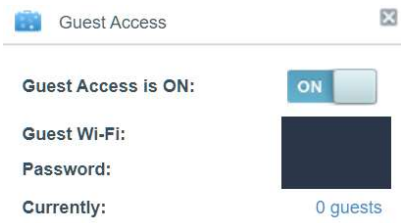

- Network security basics – Internet facing
  - Password protect the router
  - Prevent logins from the internet side of the router
  - Make your router invisible
    - Turn on router firewall – block external sites from "pinging"
  - Only open ports that you use (e.g. web site HTTP = 80, HTTPS = 443)



# Practical Steps to Mitigating Cyberthreats


- Network security basics – Local network facing
  - Turn on encryption
  - Change Default Wi-Fi name
  - Change Default Wi-Fi password
  - Disable Wi-Fi name broadcast (SSID)
  - Use MAC filtering if feasible – limits access to known devices
  - Keep business and guest Wi-Fi separate
    - Keeps customers off of your business network
    - Many business and home routers allow this


SCORE
FOR THE LIFE OF YOUR BUSINESS

# Practical Steps to Mitigating Cyberthreats


- Cloud applications are just applications running on computers running outside of your business
- The same best practices apply to cloud vendor as you would apply within your own business
- Many cloud providers have information security certifications
  - Type I – Processes and Procedures in place
  - Type II – Evidence of following processes and procedures
- Customers can sometimes request and inspect the certifications




The Intuit Online Payroll Services are subject to an annual audit of the control environment following SSAE16/SSAE18 guidance. That results in a SOC 2 Type II report. Distribution of the SOC2 Type II report is limited to external parties who have consented to abide by the SOC specific Non-Disclosure Agreement (NDA). Intuit Online Payroll Services do not undergo an audit for SOC1.

SCORE
FOR THE LIFE OF YOUR BUSINESS

# Summary

- Small businesses are increasingly targeted by cyberattacks
- Cyberattacks cost small business proportionately more than large corporations
- Many attacks occur because due to lack of employee awareness and training
- Prevention requires a layered approach
- Planning enables recovering in case of attack
- It's helpful to procure the services of an IT professional for networking

# Question and Answer

SCORE
FOR THE LIFE OF YOUR BUSINESS

# Thank You for your Time and Attention

SCORE
FOR THE LIFE OF YOUR BUSINESS
Bucks County


## Charlie Morris, SCORE Certified Mentor

SCORE Bucks County
11 Welden Drive, Suite 100
Doylestown, PA 18901
M: (215) 520-2909
E: charles.morris@scorevolunteer.org


SCORE CERTIFIED MENTOR