

# Protecting Small and Medium-Sized Businesses from Cyber Attacks

HOW CYBERSECURITY AWARENESS KEEPS YOU IN BUSINESS

JANUARY 23, 2020    HARRISONBURG, VIRGINIA

DAN OBRIEN, CYBER SECURITY INSTRUCTOR

BLUE RIDGE COMMUNITY COLLEGE

# INTRODUCTION

## Background:

- Dan OBrien- Years of experience with US Departments of Treasury and Justice performing cyber security audits of critical infrastructure using best practices
- GO Virginia cyber security program at Blue Ridge Community College, providing cyber security assistance to valley businesses and municipalities



# Why are Small and Medium-sized Enterprises targeted for cyber attacks?

*Smaller businesses have more digital assets to target than an individual consumer but have less security than a larger enterprise*



# What are the risks?



*60% of businesses that are hacked go out of business within 6 months of a cyber attack*

Source: UGA Small Business Development Center



# Hacking up the Supply Chain



UNIVERSAL MUSIC GROUP  
INTERNATIONAL



UNDER ARMOUR.



# Will you pay the ransom?



- *Many more SME owners are likely to pay a ransom to get their data back than ever before*
- *Global Ransomware Damage Costs Predicted To Hit \$11.5 Billion By 2019 (source: Cybersecurity Ventures)*

# Types of Cyber Attacks

Denial of Service Attack

Ransomware

Inside Attack

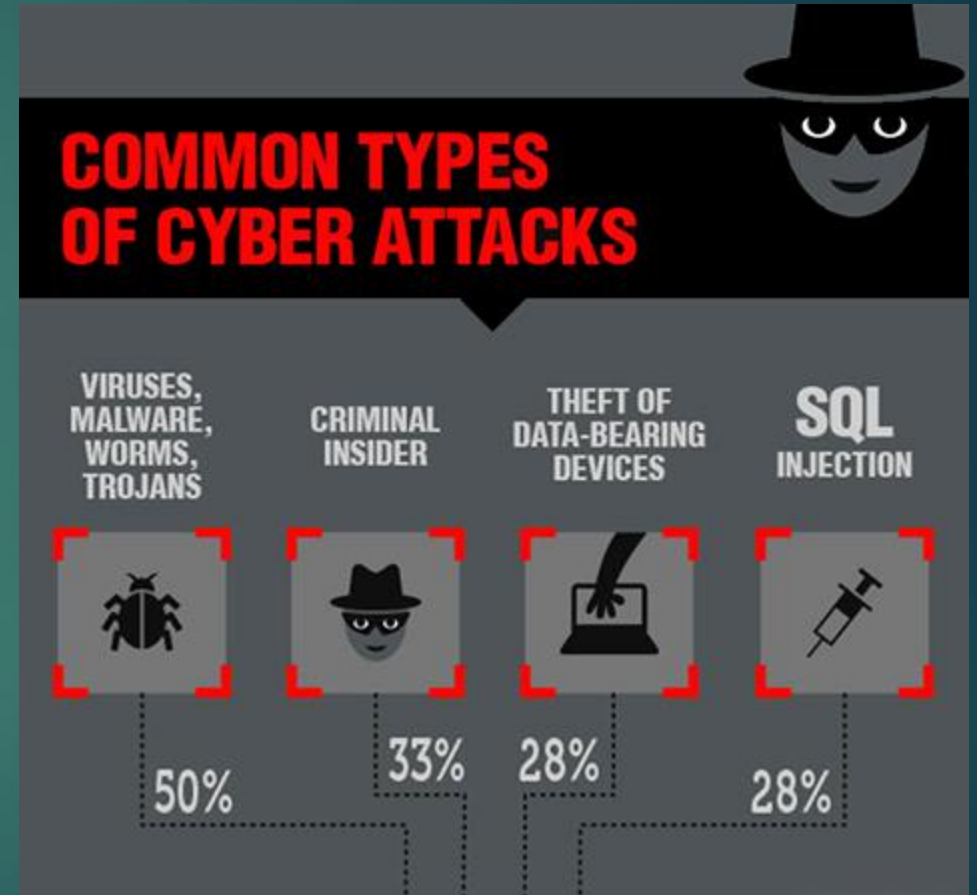
Malware

Phishing

Password Attacks

Website Attacks

The Next New Threat..



# Crimeware: Toolkits for Cyber Thieves

Wake up to the fact that attackers are far more sophisticated than ever before. The infection of hosts and stealing of data is now a point-and-click smart phone exercise, with many of the tools costing less than \$100 each, and several of them are available free of cost.



# How can you protect your business from cyber loss?



*You're here today, so let's get started!*

# Evaluation and Planning- Creating a Business Impact Analysis



# Protect Against Malware



1. Protect against viruses, spyware, and other malicious code

Make sure each of your business's computers are equipped with antivirus software and antispyware and update regularly. Configure all software to install updates automatically.

# Keep the Network and Wi-Fi Secure



## 2. Secure your Wi-Fi networks

If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted, and hidden. Hide your Wi-Fi network, avoid broadcasting all over the neighborhood. Password protect access to the router. Make sure the latest firmware version is always in use. Use the highest grade encryption and security available.

# Train Employees



## 3. Train employees in security principles

Establish basic security practices and policies for employees, such as requiring strong passwords, and establish appropriate Internet use guidelines that detail penalties for violating company cybersecurity policies. Establish rules of behavior describing how to handle and protect customer information and other vital data.

# Firewall Security



## 4. Provide firewall security for your Internet connections

A firewall is a set of related programs that prevent outsiders from accessing data on a private network. Make sure the operating system's firewall is enabled or install free firewall software available online. If employees work from home, ensure that their home system(s) are protected by a firewall.

# Mobile Device Action Plan

YOUR WEEKLY TECH TIP

**Create a Mobile Device Action Plan: Protect Your Devices, Encrypt Data, and Install Security Apps.**



## 5. Create a mobile device action plan

Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password protect their devices and encrypt their data. Be sure to set reporting procedures for lost or stolen equipment.

# Backup, backup, backup



## **6. Make backup copies of important business data and information**

Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Backup data automatically if possible, or at least weekly and store the copies either offsite or in the cloud.

# Control access to data, equipment, and accounts



## 7. Control physical access to your computers and create user accounts for each employee

Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so lock them up when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.

# Protect Sensitive Information



- ▶ **8. Establish security practices and policies to protect sensitive information**
- ▶ Establish policies on how employees should handle and protect personally identifiable information and other sensitive data. Clearly outline the consequences of violating your business's cybersecurity policies.

# Passwords and Authentication



## 9. Use Strong Passwords

Require employees to use unique passwords and change passwords every three months. Consider implementing multi-factor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multi-factor authentication for your account.

# Perform Cyber Security Audits



## 9. Cyber Security Assessment and Review Process

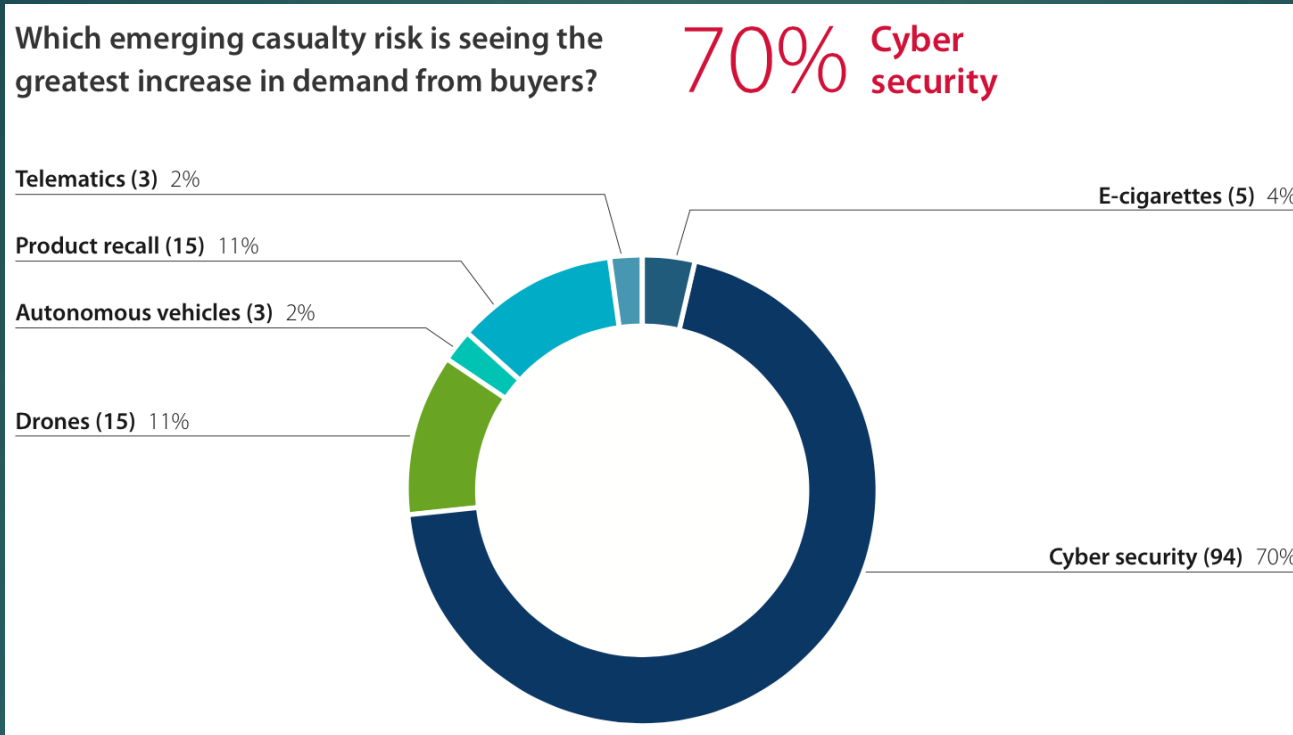
Use the National Institute for Standards and Technology MEP (Manufacturing Extension Partnership) online assessment survey:

***[nist.gov/mep/cybersecurity-resources-manufacturers](https://nist.gov/mep/cybersecurity-resources-manufacturers)***

Hire a professional firm to perform your cyber security review

Download the NIST MEP Handbook 162 for SME self-assessment

# Cybersecurity Insurance



Source: Risk Management Monitor

## Investigate Cybersecurity Insurance

One important solution that doesn't involve hardware or software is cybersecurity insurance. Your general liability policy will not help you recoup losses or legal fees associated with a data breach. A separate policy covering these types of damages can be hugely helpful in case of an attack.

# Protecting Small and Medium-Sized Businesses from Cyber Attacks

Dan OBrien

GO Virginia Cyber Security Program  
Manager and Instructor- Blue Ridge  
Community College

