As part of a continuing education series, the Independent Office Products and Furniture Dealers Association (IOPFDA) presents...

CYBER ATTACKS: IS YOUR BUSINESS PROTECTED?

Presented by:
Juan Fernandez, CIO, ABM Federal and Mike Tucker, President & CEO, IOPFDA

March 12, 2020

Key Topics

The Extent of the Problem

Types of Security Threats Facing Businesses

- ➢ Malware and Ransomware
- ➢ Social Engineering and email Spoofing
- ➢ Unpatched Server and Software Vulnerabilities
- ➢ Account Takeover
- ➢ Virus
- ➢ Cloud Stack, Shadow IT, Mobility Vulnerabilities

Why The Problem Continues

ABM Federal's Strategy for Addressing These Issues

- ➢ The Checklist

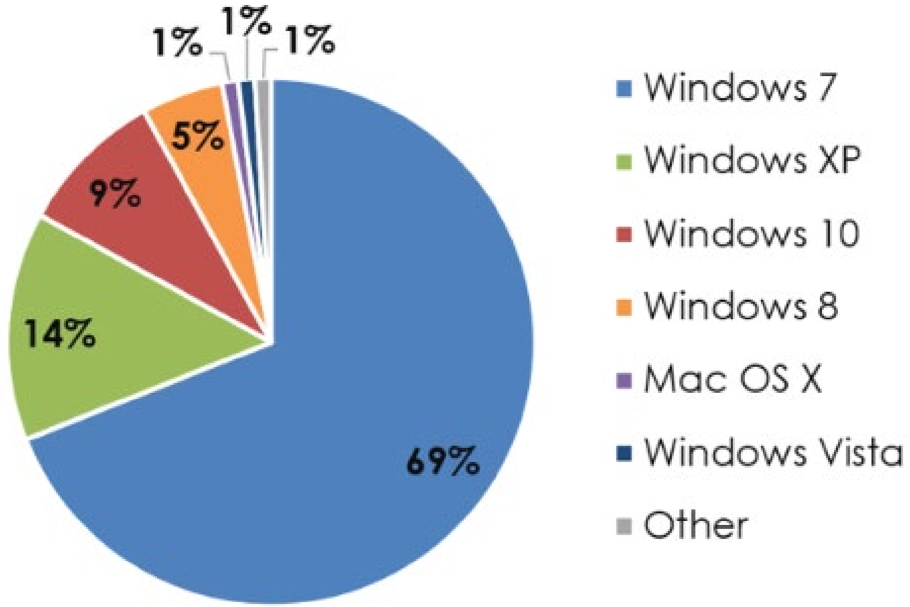
The Extent of the Problem

To better understand the problem, Spiceworks conducted a survey and found that

69% **of businesses worldwide are currently running Windows 7**

5% **run Windows 8**

14% **still run Windows XP**, which Microsoft stopped supporting in 2014



Share of Laptop/Desktop Operating Systems in Businesses Worldwide

IOPFDA
Independent Office Products and Furniture Dealers Association

The Extent of the Problem

What's more, a recent ServiceNow survey (conducted by Ponemon) highlighted some alarming trends. Of the 3,000 companies surveyed:

48% **Almost half admitted that their organization suffered a data breach in the last two years**

60% **Of those that suffered a breach, almost 60% were due to an unpatched vulnerability**

34% **Finally, of those that suffered a breach, 34% knew they were vulnerable but did nothing**

Cybercrime is on the Rise

Data breaches have run at a record pace in 2019. Consider these statistics for the first half of the year:

3,800: The number of publicly disclosed breaches

4.1 billion: The number of records exposed

+54%: Increase in number of reported breaches
(vs. first six months of 2018)

+54%

vs first six months of 2018

IOPFDA
Independent Office Products and Furniture Dealers Association

CNN BUSINESS

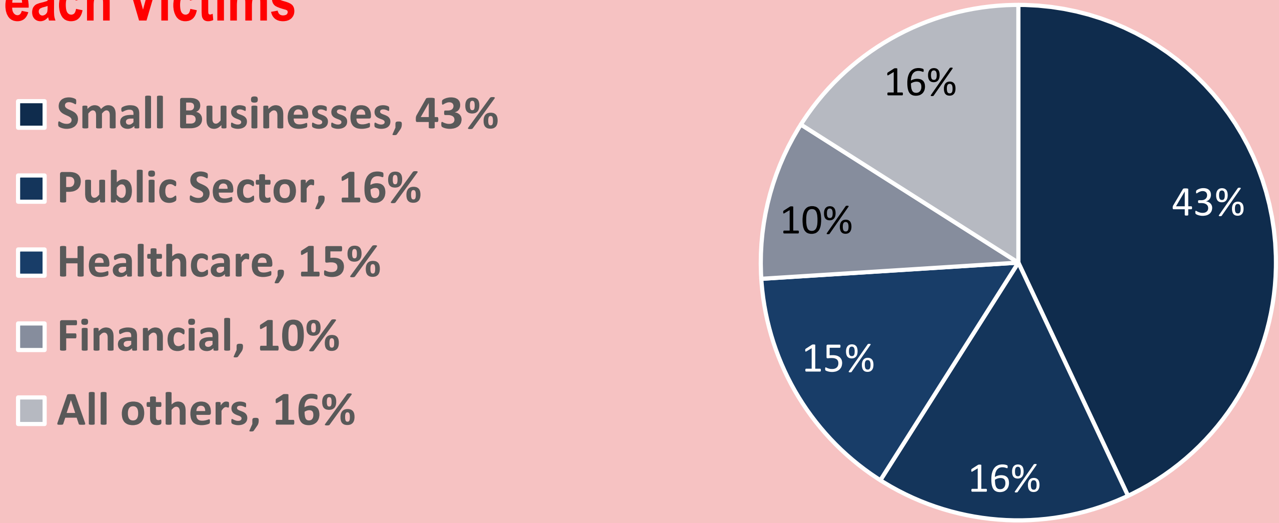
News Headline:

“Capital One hacked, 106 million customers records exposed”

Capital One

While Large and high-profile companies garner the most media attention as cybercrime victims, **small and medium sized businesses are squarely in the cybercriminals crosshairs**

Data Breach Victims



Verizon “2019 Data Breach Investigations Report”

IOPFDA
Independent Office Products and Furniture Dealers Association

CNBC *News Headline:*

“Cyberattacks now cost small companies $200,000 on average, putting many out of business”

The consequences of cyberattacks on Small Business

- 43% of cyberattacks are **aimed at small businesses**, but only 14% are prepared to defend themselves
- These incidents now cost small businesses $200,000 on average, with **60% of them going out of business** within six months of being victimized
- More than half of all small businesses suffered a breach within the last year, with **4 in 10 having experienced multiple incidents**

It’s critical for small businesses to adopt cybersecurity strategies for fighting threats

IOPFDA
Independent Office Products and Furniture Dealers Association

Why Hackers Target Small & Medium Sized Business?

Increasing online business

Easy Target – “Our company is too small”

- Valuable Data – Customer Info, Login, Payment, etc.
- Minimal or Lack of Cybersecurity Protocols
- Less Resources

To get to a larger business – your customer

Not all attacks are for financial gain

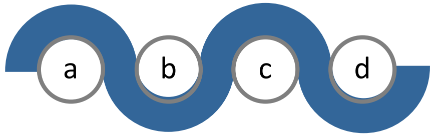
What is Cybersecurity?

People, Process and Technology working together to protect you, your business and your customers

Also known as "**Information Technology Security**".

A Multilayer strategy that consists of technologies, processes, and practices designed to protect networks, devices, programs, and data from unauthorized access, damage or attack.

People



Process

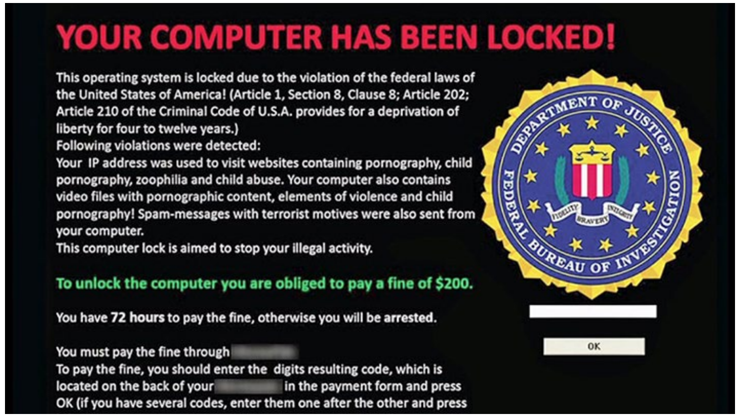
Technology

Types of Security Threats Facing Businesses

Malware and Ransomware

Malware and Ransomware, which come in several forms, share the characteristic of self-installing on a computer and running in the background without the user's knowledge.

While malware hides and steals valuable information, ransomware locks the user's machine or encrypts files and then notifies the user with a ransom demand in order to unlock the machine or decrypt the files.



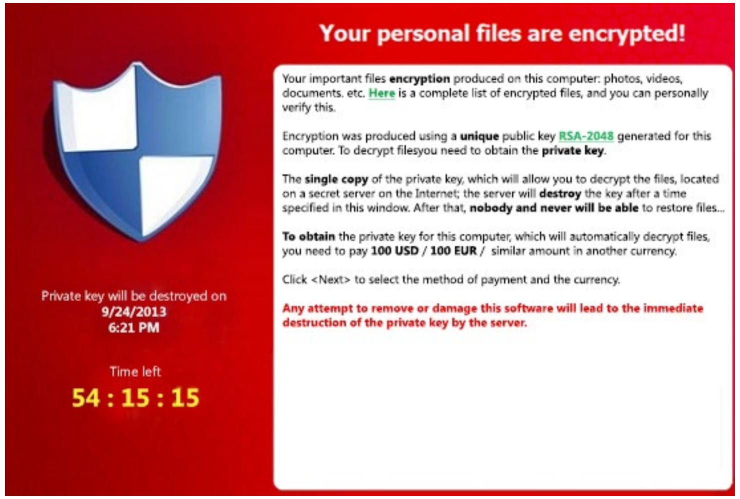
YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents. etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR /** similar amount in another currency.

Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

Private key will be destroyed on
9/24/2013
6:21 PM

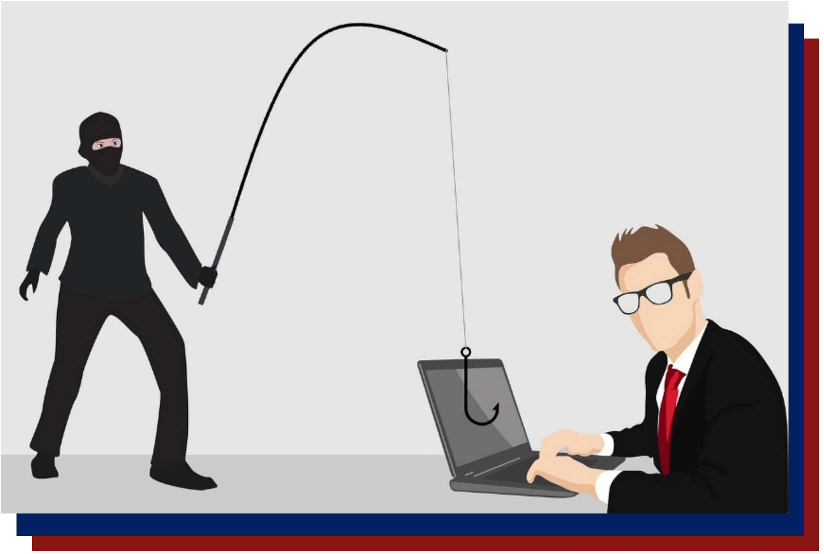
Time left
54 : 15 : 15

Types of Security Threats Facing Businesses

Social Engineering and email Spoofing

Attackers will use social engineering to pose as a colleague or business partner and send fake requests for information or the transfer of funds.

These emails can be quite convincing as the attacker makes a significant effort to identify an appropriate victim and register a fake domain, so that at first glance the email appears to belong to a colleague or supplier.



IOPFDA
Independent Office Products and Furniture Dealers Association

Types of Security Threats Facing Businesses

Unpatched Server and Software Vulnerabilities

One of the common ways for many of the previously mentioned types of security threats to gain access is via unpatched server and software—in short, legacy hardware and software where security patches and updates are either missed or beyond end of life. This can manifest in Remote Desktop Protocol attacks or distributed denial-of-service attacks (DDoS) among others.

DATA
BREACH
IMPLEMENTING A SUCCESSFUL PATCH MANAGEMENT PROCESS:
DON'T BE THE NEXT EQUIFAX

The biggest threat to businesses in terms of cybersecurity vulnerabilities is data loss, especially where regulatory compliance is concerned, including personal health or financial data loss which can cripple a business if breached.

Types of Security Threats Facing Businesses

Account Takeover

Here, attackers use information-stealing malware and keyloggers to gain access to and hijack a corporate email account, which they then use to make fraudulent requests to colleagues, accounting departments and suppliers.

They can also alter mailbox rules so that the victim's email messages are forwarded to the attacker, or emails sent by the attacker are deleted from the list of sent emails.

Types of Security Threats Facing Businesses

Virus

A virus program works by replicating and inserting itself into other applications where it can slow computers, destroy data, disable software, and delete files.

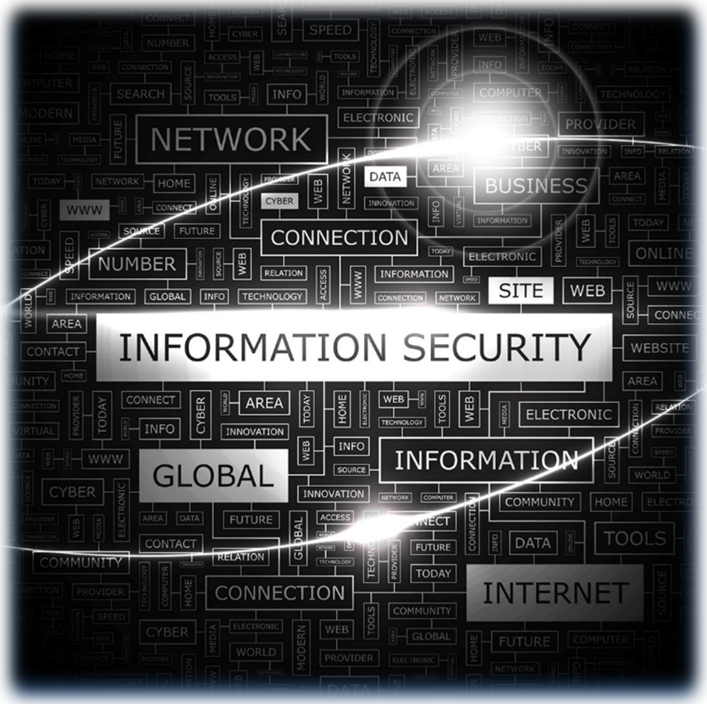
It can be introduced via an email or file download onto an infected computer or portable storage device and by visiting malicious websites.

Types of Security Threats Facing Businesses

Cloud Stack, Shadow IT, Mobility Vulnerabilities

Use of the cloud in its various forms has introduced new challenges such as the access vulnerabilities of “bring your own device” (BYOD) endpoint devices and operating systems.

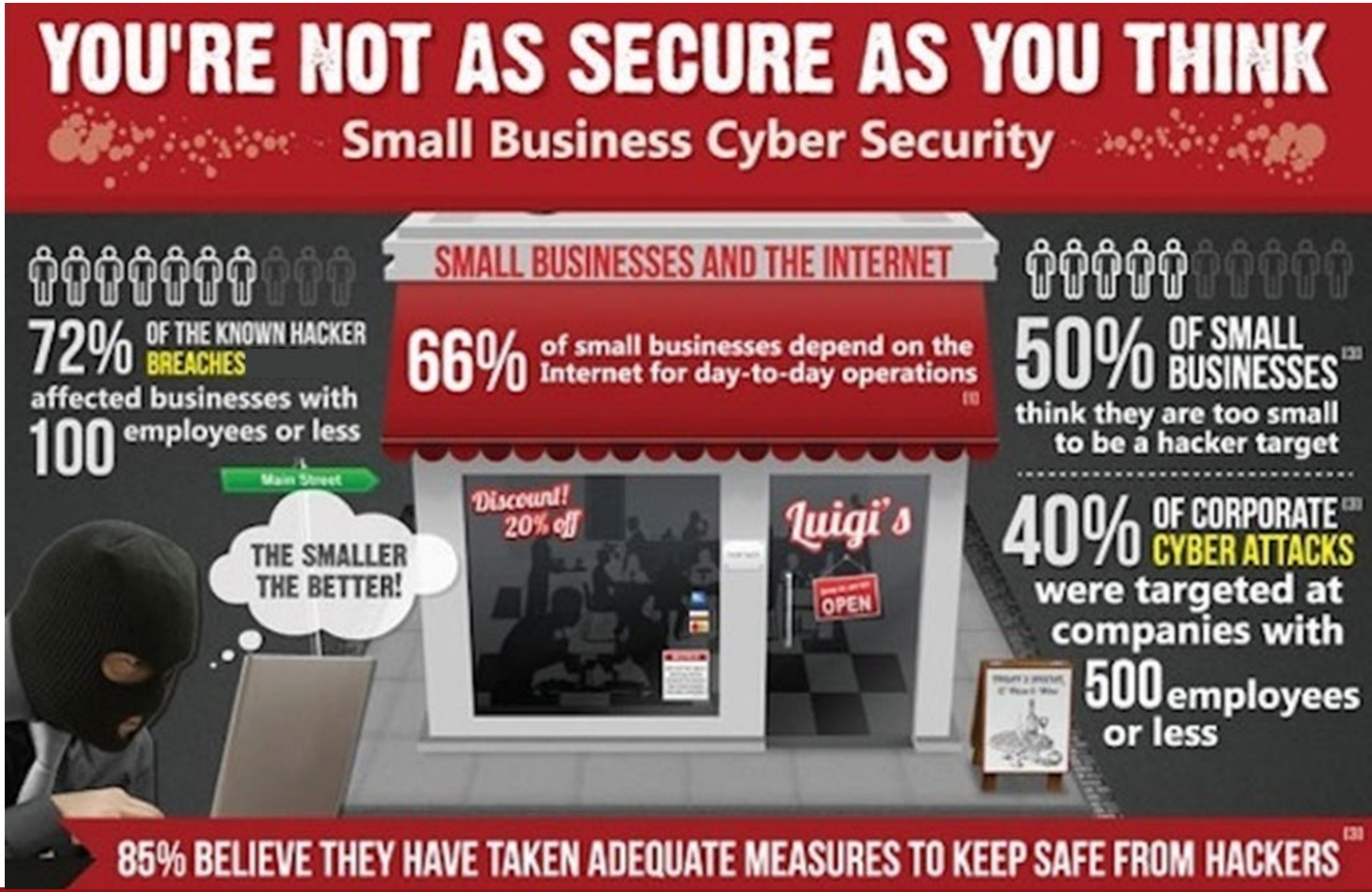
In addition, the use of unauthorized software or cloud services by internal business employees (known as “shadow IT”) can introduce additional security vulnerabilities to the business.



Why The Problem Continues

Despite billions of dollars spent each year on sophisticated technology to help protect critical information assets, hackers and malicious insiders continue to steal information with seeming impunity.

The vast majority of breaches in cybersecurity are the result of human errors or actions that often occur without people even being aware of what they have done.


YOU'RE NOT AS SECURE AS YOU THINK
Small Business Cyber Security
SMALL BUSINESSES AND THE INTERNET
72% OF THE KNOWN HACKER BREACHES affected businesses with 100 employees or less
66% of small businesses depend on the Internet for day-to-day operations [1]
50% OF SMALL BUSINESSES think they are too small to be a hacker target [3]
40% OF CORPORATE CYBER ATTACKS were targeted at companies with 500 employees or less [3]
Main Street
THE SMALLER THE BETTER!
Discount! 20% off
Luigi's
OPEN
85% BELIEVE THEY HAVE TAKEN ADEQUATE MEASURES TO KEEP SAFE FROM HACKERS [3]

SMALL BUSINESS CYBERSECURITY UPDATE

CYBERSECURITY REALITY

$415,000 : The average cost of a cyber intrusion to organizations able to estimate monetary loss.

3 out of 4 organizations detected a security event in prior 12 months.

SMALL BUSINESS NETWORK SECURITY REALITY

40% of small businesses outsource their security to a third party.

33% of small businesses have their own on-premise firewall equipment.

17% of small businesses do NOT have a network security solution because it's not a priority for them and **10%** do not have a solution because they don't know who to work with.

BENEFITS OF A MANAGED SECURITY SERVICE FOR SMALL BUSINESSES

A managed internet router and security service can deliver **UP TO 84%** lower total cost of ownership (TCO) compared to an internally managed approach.

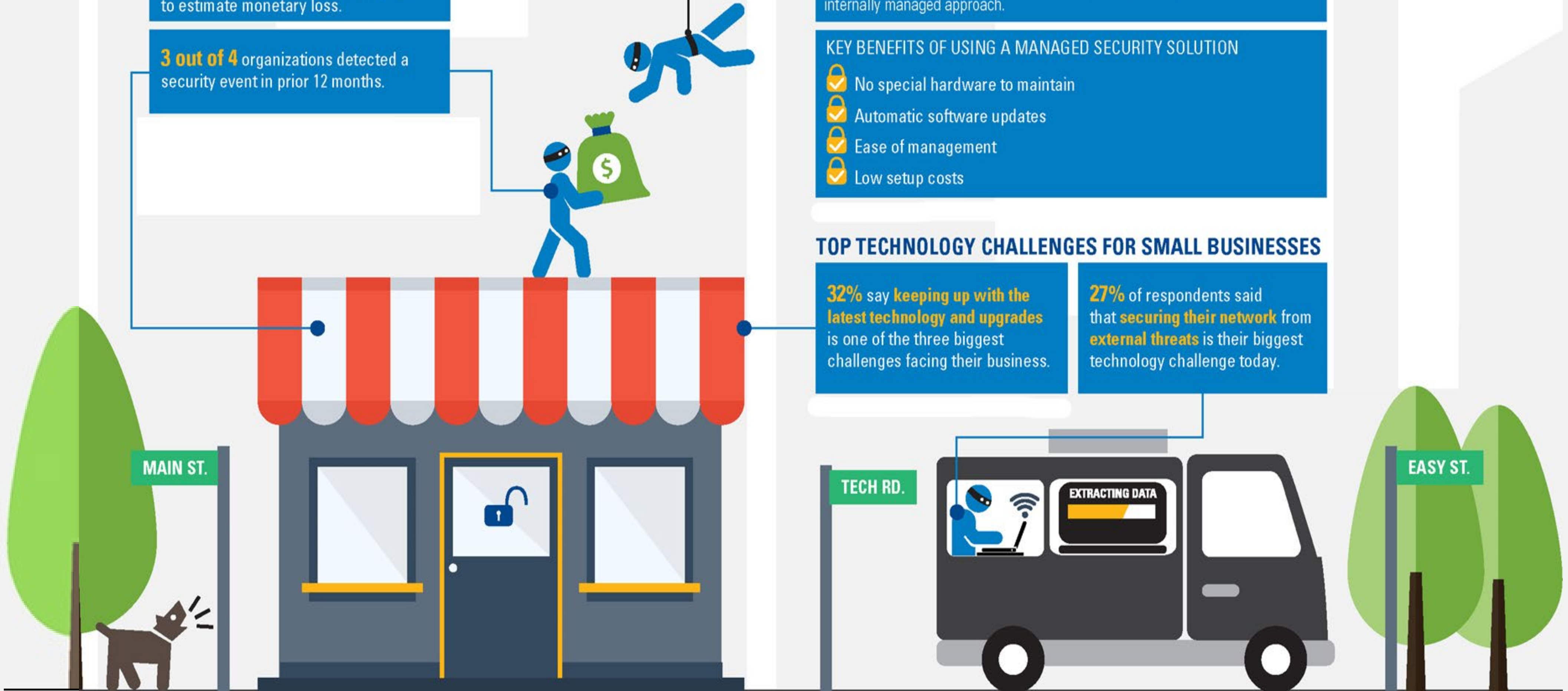
KEY BENEFITS OF USING A MANAGED SECURITY SOLUTION

- No special hardware to maintain
- Automatic software updates
- Ease of management
- Low setup costs

TOP TECHNOLOGY CHALLENGES FOR SMALL BUSINESSES

32% say **keeping up with the latest technology and upgrades** is one of the three biggest challenges facing their business.

27% of respondents said that **securing their network** from **external threats** is their biggest technology challenge today.



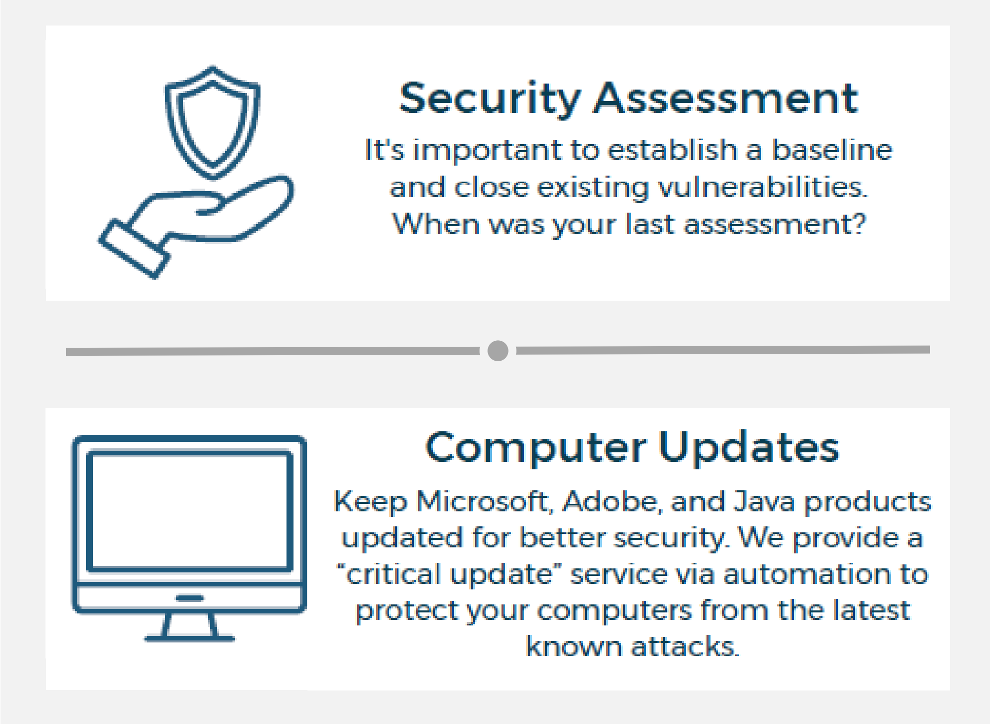
ABM Federal’s Strategy for addressing these issues?

Security Assessment

- Identifies the risks and needs of the customer to set a baseline of issues that need attention.

Continuous monitoring and protection

- Configuration management software that manages computer and server patching to maintain the highest level of protection.



Security Assessment

It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?

Computer Updates

Keep Microsoft, Adobe, and Java products updated for better security. We provide a “critical update” service via automation to protect your computers from the latest known attacks.

ABM Federal’s Strategy for addressing these issues?

- Next-generation firewall features that enable application control across the network
- Intrusion Prevention System (IPS) to identify the attacks coming from inside and outside the network
- Anti-spam technologies for threat detection using techniques such as blocking spammed IPs and spammed emails, conducting DNS lookups, IP comparison, etc.
- Data Loss Prevention System (DLP) for prevention of data leaks to and from the organization
- Web security gateway solutions protect web-surfing PCs from infection and enforce company and regulatory policy compliance
- Cloud Access Service Broker (CASB) to secure data in the cloud by enabling centralized control and enforcement of security policies wherever the data is stored, shared, or accessed

Firewall

Turn on Intrusion Protection and Intrusion Prevention features. Send log files to a managed SIEM. And it your IT team doesn’t know hat these things are, call us today!

Backup

Backup local. Backup to the cloud. Have an offline backup for each month of the year. Test your backups often. And if you aren’t convinced your backups are working properly, call us ASAP!

Advanced Endpoint Detection & Response

Protect your computers and data from malware, viruses and cyber attacks with advanced endpoint security. Today’s latest technology (which replaces your outdated anti-virus solution) protects against file-less and script-based threats and can even rollback a ransomware attack.

THE CHECKLIST: *15 Ways To Protect Your Agency From A Cyber Attack!*

☑

Security Assessment

It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?

Date: _______________

☑

Spam Email

Secure your email. Most attacks originate in your email. We'll help you choose a service designed to reduce spam and your exposure to attacks on your staff via email.

☑

Passwords

Apply security policies on your network. Examples: Deny or limit USB file storage access, enable enhanced password policies, set user screen timeouts and limit user access.

☑

Security Awareness

Train your users – often! Teach them about data security, email attacks and your policies and procedures. We offer a web-based training solution and "done for you" security process.

☑

Multi-factor Authentication

Utilize Multi-factor Authentication whenever you can, including on your network, banking websites, and even social media. It adds an extra layer of protection to ensure that even if your password does get stolen, your data stays protected.

☑

Computer Updates

Keep Microsoft, Adobe and Java products updated for better security. We provide a "critical update" service via automation to protect your computers from the latest know attacks

☑

Advanced Endpoint Detection & Response

Protect your computers data from malware, viruses and cyber attacks with advanced endpoint security. Today's latest technology (which replaces your outdated anti-virus solution) protects against file-less and script-based threats and can even rollback a ransomware attack.

Did you know?

1 in 5 Small businesses will suffer a cyber breach this year

81% Of all breaches happened to small and medium size businesses

97% Of breaches could have been prevented with today's technology

☑

Dark Web Research

Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach. We scan the Dark Web and take action to protect your business from stolen credentials that have been posted for sales.

☑

SIEM/Log Management

(Security Incident & Event Management)

Uses big data engines to review all event and security logs from all covered devices to protect against advanced threats and to meet compliance requirements.

☑

Web Gateway Security

Internet Security is a race against time. Cloud based security detects web and email threats as they emerge on the internet and blocks them on your network within seconds – before they reach the user.

☑

Mobile Device Security

Today's cyber criminals attempt to steal data or access your network by way of your employees' phones and tablets. They're counting on you to neglect this piece of the puzzle. Mobile device security closes this gap.

☑

Firewall

Turn on Intrusion Protection and Intrusion Prevention features. Send log files to a managed SIEM. And it your IT team doesn't know hat these things are, call us today!

☑

Encryption

Whenever possible, the goal is to encrypt files at rest, in motion (think email) and especially on mobile devices.

☑

Backup

Backup local. Backup to the cloud. Have an offline backup for each month of the year. Test your backups often. And if you aren't convinced your backups are working properly, call us ASAP!

☑ **Cyber Insurance**

If all else fails, protect your income and business with cyber damage and recovery insurance policies.

Thank You!

Questions

Independent Office Products and Furniture Dealers Association (IOPFDA)
3601 East Joppa Road
Baltimore, MD 21234
P: (410) 931-8100 | E: info@iopfda.org | W: NOPAnet.org | OFDAnet.org

IOPFDA
Independent Office Products and Furniture Dealers Association