Less Hackable

For Small to Medium Business Owners

By Danny Jenkins

After nearly 20 years working in cybersecurity, I am still asked the age-old question by business owners: **"How can I make myself unhackable?"** Seldom do they understand when I try to explain that there is no such thing as unhackable.

The purpose of this guide is to help business owners better understand cyber risks and how those risks can be reduced to an acceptable level. Securing your cyber environment is much like securing your house. It is impossible to make your house 100% secure, but you can take steps to reduce the risk of an intrusion. Most people take steps such as installing an alarm, high-grade locks, and a camera system. The rest of the risk is transferred to the insurance company.

The contents of your house will most likely alter your decision on how much money and effort you are willing to put into securing it. If you have a lot of cash, you may decide to install a safe. If you are the President of the United States, you will take more extreme measures, such as putting snipers on the roof and installing ballistic glass. But even the White House is not 100% secure.

Creating a cybersecurity plan follows the same principles: the more important the asset, the more resources you should take to secure it. The problem that many businesses face is they do not understand the risks involved when trying to secure their network. The idea of this whitepaper is to give businesses a better understanding of scoping their security needs and assessing common risks. It will not make you a cybersecurity professional, but it will give you some insight as to the questions you should be asking.

The document will address the basic cybersecurity protections that nearly all businesses use, such as firewalls, antivirus software, password security, email protection, web protection, and backups. It will also give you methods of improving your cybersecurity with little cost and overhead by adding solutions that you should be using.

A big challenge for a small business is the shift of targets for cybercriminals. In 2001 there were two types of cyber threats businesses had to worry about:-
Blanket or net type attacks -- where attackers would send out self-propagating malware, scan a mail server for weak passwords, or attack poorly managed servers. These types of attacks affected large and small businesses, banks, and coffee shops.

Targeted Attacks

Large enterprise businesses also had to worry about targeted attacks, where attackers would take the time to drop footholds, research, plan, and ultimately work a lot harder to get into your business.

This led to a large gap in the tools used by small businesses and large enterprises. Small businesses relied heavily on antivirus, antispam, and other types of detection tools. In contrast, large enterprises prefer to take definitive measures, such as default-deny application whitelisting, dual-factor authentication, and network controls combined with their detection tools.

Over the past two decades, cybercriminals shifted their focus more towards smaller businesses, and focused less on enterprise. They realized that small businesses can often lead to quick wins of lumps of cash, ranging from $10,000 up to millions of dollars. Small businesses are much easier to attack as their defenses were not on par with the larger enterprises.

As a small to medium-sized business, there are many tools you can add that will harden to bring you closer to the defenses of large enterprise. Tools like Advanced Application Control (ThreatLocker® Ringfencing™), ThreatLocker® Default Deny (Application Whitelisting), Dual Factor Authentication, and User Training.

In addition to this document, there are more advanced steps you can take to help secure your environment, but these often cost tens of thousands of dollars and require dedicated cyber teams to manage them.

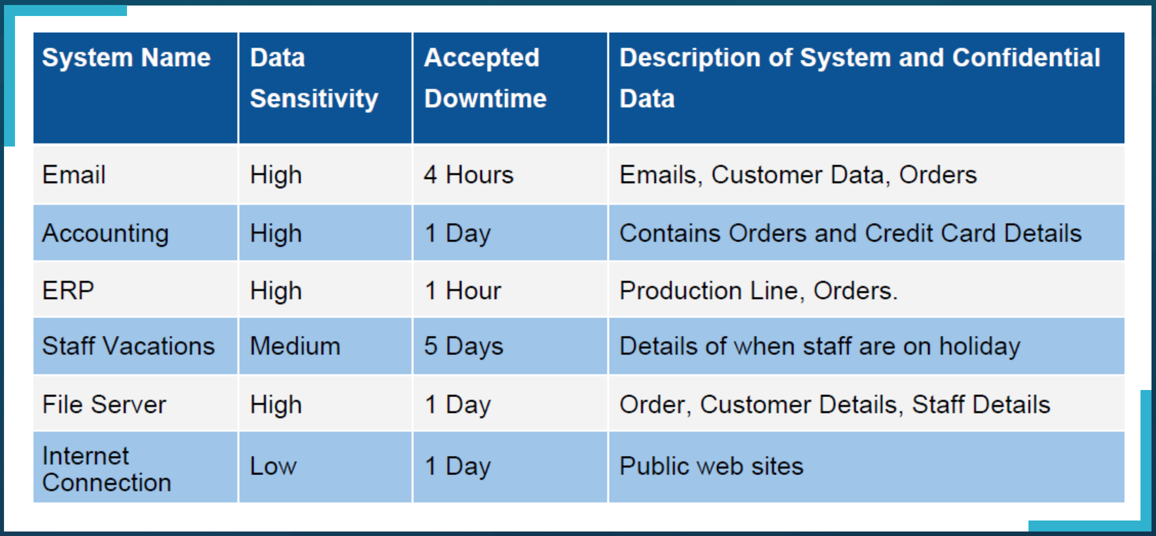
Taking the First Steps in Securing your Business

The first step in protecting your business is understanding what assets you have and what the potential risks are. A good place to start is to look at your day-to-day business processes and how users interact with their computers. There are some common items listed below, but the list may not be complete for what you might see in your business.

Each system and its data should be classified. Some systems are crucial for the operation of the business, while others may be less crucial but still contain sensitive data. When classifying systems, it is worth noting that although data may not be confidential, the applicable system could allow access to another system. For example, even if you do not store confidential data in your email, your email could be used to reset a password to a more secure system.

Take note of all your systems and rate the confidentiality of the data and the importance of each system's continuity. It is a good idea to think about what downtime is acceptable for each of these systems.

Your list should look something like this:



System Name	Data Sensitivity	Accepted Downtime	Description of System and Confidential Data
Email	High	4 Hours	Emails, Customer Data, Orders
Accounting	High	1 Day	Contains Orders and Credit Card Details
ERP	High	1 Hour	Production Line, Orders.
Staff Vacations	Medium	5 Days	Details of when staff are on holiday
File Server	High	1 Day	Order, Customer Details, Staff Details
Internet Connection	Low	1 Day	Public web sites

The next stage is to consider some of the risks associated with each system. One major consideration when dealing with their risks is whether the systems talk to the outside world. For example, an email system gets data from the outside world and can receive data in multiple formats. However, a payroll system most likely only receives data from internal employees and controlled sources. It is important to understand this distinction as systems that can receive external data are more vulnerable.

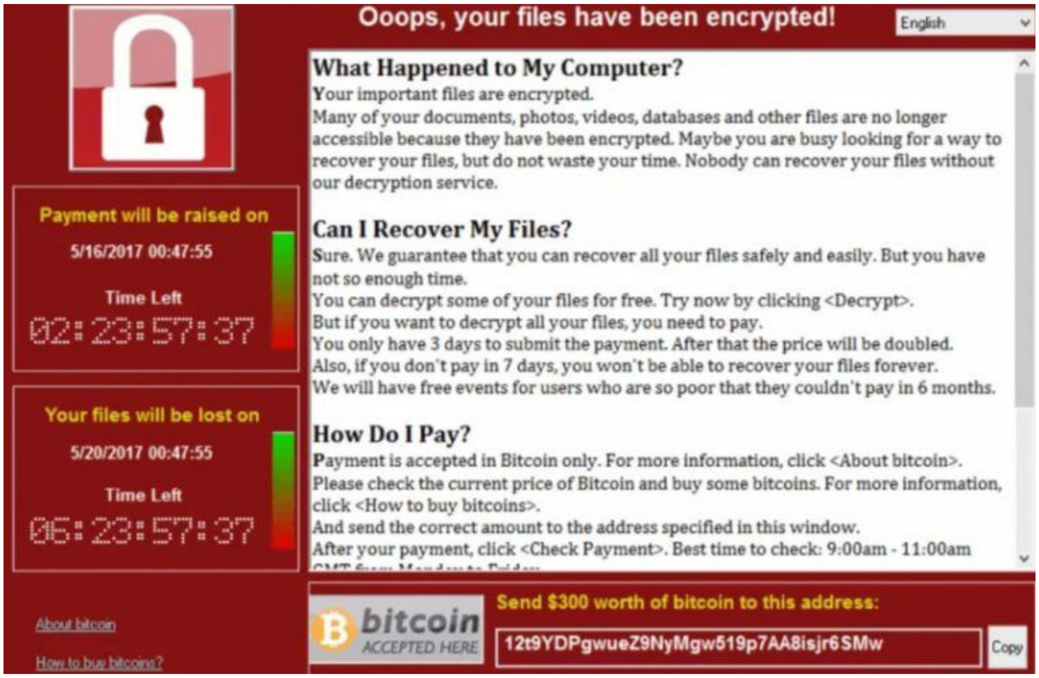
Before going into too much detail about options for reducing risk and protecting your business, consider common threats that small- to medium-sized companies face. Some of these common threats are outlined on the next page.

Most common threats to small businesses

Malware

The most common threat to small businesses is malware. Malware could essentially be any software that is produced with bad intent. Examples range from traditional viruses to ransomware. Malware can get into your system in many ways. The most common way that this can happen is when a user opens or downloads a file. Most often, users think they are opening an email attachment or downloading a legitimate software update. Unfortunately, the impact of malware is worsening each year. Today's malware is no longer just an inconvenience; it is catastrophic and causes real damage. Malware ranges from stealing data to encrypting your files and demanding a ransom payment to using your systems to attack other companies or send emails.

Ransomware has been on the rise. A ransomware attack occurs when all of the files on your computer are encrypted, and a ransom is demanded by an attacker. Normally, the attacker is in Russia or a country that has no consequences for cybercrime.



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

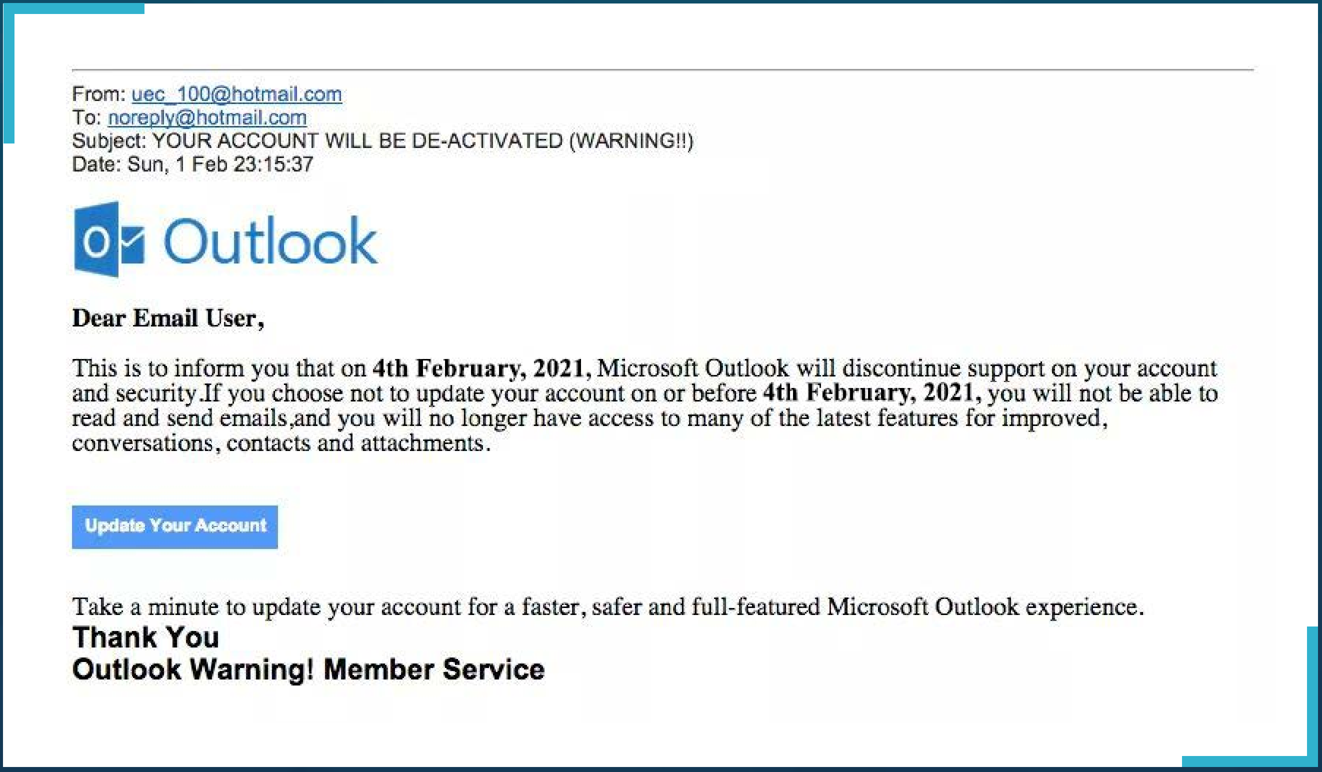
Malware should be a real concern for your business. Once the malware is running on your system, it can exploit other computers on your network, access logins by recording user keystrokes or steal your data. Do not underestimate the risk of **malware**. If you have any suspicion that you have malware, you should power off your systems until the damage can be assessed.

Most common threats to small businesses

Phishing and Spear Phishing

Phishing emails and websites are set up to trick users into entering credentials for a system, such as an email account, bank, or financial account. Once the user enters their details, the attacker collects and then uses them to access the user's information at a later date or time. They could also use users' accounts to reach out to their coworkers and get information from them.

Spear phishing is a little bit more advanced. In these cases, an attacker will engage with a user using a spoofed email address, posing as somebody else in the same company. Typically, they will exchange emails back and forth with the user about incidental and related items initially before then asking them to make a payment. For example, an attacker could spoof a manager's email address and trade emails with accounts payable. Once they have gained trust by email, they could ask them to pay an invoice to a supplier, often leaving the company with thousands of dollars lost.



From: uec_100@hotmail.com
To: noreply@hotmail.com
Subject: YOUR ACCOUNT WILL BE DE-ACTIVATED (WARNING!!)
Date: Sun, 1 Feb 23:15:37

Dear Email User,

This is to inform you that on **4th February, 2021,** Microsoft Outlook will discontinue support on your account and security.If you choose not to update your account on or before **4th February, 2021,** you will not be able to read and send emails,and you will no longer have access to many of the latest features for improved, conversations, contacts and attachments.

Take a minute to update your account for a faster, safer and full-featured Microsoft Outlook experience.
Thank You
Outlook Warning! Member Service

Most common threats to small businesses

Weak Passwords

The use of strong passwords is critical in your organization, especially as more and more data is moved to the cloud. Over 30% of small business breaches involve a weak password.

System Vulnerability or Exploit

In this case, an attacker would use a vulnerability in the software you are running on your computer. Usually, the operating system's vulnerabilities are targeted to gain access to your computer. This would allow the attacker access to your system generally as an administrator where they could install ransomware, steal data, or shut down your operations.

Quite often, these attacks come from guest laptops that are connected to your Wi-Fi. In most cases, the guest does not even know that they are being used as a springboard to attack your network. So do not assume a person who is trustworthy has a computer that is trustworthy.

SQL Injection Attacks

SQL injection attacks are a common threat to the line of business applications, where attackers can insert a database command into the user interface and get more data returned than they have access to. For most small businesses, there is little they can do to stop these attacks, other than ensuring their software vendors follow good programming practices.

Common Security Practices

Most businesses follow the below common security standards to protect their network environment. Unfortunately, while these security practices will protect you, most companies will still be affected by malware and other threats over a two-year period.

Perimeter Firewall

You should have a firewall that separates your network from the Internet. While firewalls have a name for protecting everything, they only perform one function. That function is: to block any network-level traffic from connecting to devices on your network if it has not been explicitly allowed. Network-level traffic has nothing to do with logins or content, it only relates to TCP/IP ports, you can choose to permit e-mail or web traffic but not capabilities such as file shares. A firewall does not filter the content of email or websites, just whether the type of traffic is allowed. However, some unified threat management (UTM) devices that are sold as firewalls may have web and email filtering built-in.

Your I.T. professional should document a list of open ports on your firewalls, as well as the reason they are open. This process should be repeated on a scheduled basis to ensure changes are reflected in the firewall. Ask your IT professional for this information, keep it safe, and don't assume that they will review it.

Anti-Virus Software

Anti-virus software is becoming less and less effective at detecting new malware. Over 90% of businesses have been affected by malware in the last two years, and all of those businesses had an operational antivirus program. Most new and active viruses are not detected in time by standard antivirus software. However, anti-virus protection does play an important role. Computers should be scanned on a scheduled basis to ensure they are not infected by known viruses. Using an antivirus program is essential, and if you choose not to purchase a commercial product, check that your built-in Windows antivirus software is enabled.

Email Security and Filtering

More and more companies are moving their email to the cloud. Products such as Office 365 or GSuite include email protection in their platforms. However, these platforms almost always fall short and only detect about 90% of threats. Using commercial products can increase your detection rates, but don't expect to be completely safe.

Email security products should reduce the spam email, viruses, and phishing emails in your organization.

In addition to filtering emails for threats, you should make sure that your email servers support TLS and that you have published SPF records. If you are using GSuite or Office365, TLS is standard, but if your business has an in-house Exchange or Email Server, ask your I.T. administrator if you have TLS configured.

SPF records help stop other organizations from spoofing your email addresses. Ask your I.T professional if you have SPF records published.

Running Security Updates

The EternalBlue exploit was used by the NSA for years to access computers before it was publicly discovered and fixed. While security updates would not have helped during this time, they would have stopped an attacker from gaining access after it was made public. Microsoft and other vendors race to release security updates as soon as they become publicly known. This will massively reduce your attack surface. Always install security updates as soon as they are deployed.

Don't forget to install updates on your server. Quite often servers don't get patched because businesses don't want downtime. But they are more important than your desktops. Schedule updates on your servers as fast as you can after updates are released.

Personal Firewalls

Windows and most other operating systems come with built-in personal firewalls. Personal firewalls protect your computer's from inbound network traffic. Unlike perimeter firewalls, personal firewalls run on each device. If someone plugs an infected computer into your network, or another user on your network gets a virus, your personal firewall will help protect your computer.

Secure Passwords

This is a challenge for all businesses. Best practice dictates that users should set their own passwords, and those passwords should not be known by anybody. However, quite often users make no effort at all in creating secure passwords. Passwords should be secure; they should not be full words and should contain at least 1 UPPERCASE, 1 lowercase, 1 numeric digit, and 1 special character (e.g. $,!,:). It is essential that users understand this when setting passwords. In systems that are accessible publicly, this need multiplies.

Users should not use the same password for multiple systems and should change their passwords regularly.

Backups

Backups are paramount in any cybersecurity solution. In many cases, the loss or corruption of data is the most significant impact of most breaches. You should have a backup solution in place that involves a copy of data offsite and inaccessible by your network. Your I.T. professional should complete a test restore on a regular basis.

All of the above methods of security are commonly used and in place in most businesses. Unfortunately, while they are going to help you secure your business network if you wish to become part of the 10% of organizations that are not breached you will need to step things up a little bit. Stepping up security adds a burden to your budget and resources. That said, there are many products and solutions that allow you to add security without excessive cost that are not too difficult to use.

Human Behavior

Before considering more advanced methods in your cybersecurity strategy, it is important to understand that the most significant failures in cybersecurity are due to a failure in human behavior. A recent study showed that a large portion of staff voluntarily emailed their credentials to a scammer when faced with a phishing email. While this is hard to believe, it is far easier than you might think. People are often the biggest weakness in an organization's cybersecurity. While it is impossible to change human nature completely, you can improve user behavior through education. The study showed that when organizations put their staff through a cyber awareness training program and repeated a similar test a few months later, the number of users that were tricked was reduced to a handful. Unfortunately, it is unlikely that you will ever be able to reduce this number to zero, but reducing human error and combining it will security tools will lower your exposure massively.

Users giving out their passwords is just one example. There are many other mistakes users can make that could lead to a network compromise. Examples include spear phishing, running applications attached to emails, or clicking on links in emails.

While training is important, you have to plan for failures in human behavior. Adding controls in place like Default Deny, can stop users from knowingly or unknown running malicious software. Dual factor authentication can prevent a breach when a user unknowingly discloses their password.

How you should improve security past the norm

Cybersecurity is not one hat that fits all solutions. Picking the right products and solutions will depend on the level of security you need and the resources at your disposal.

Here are some ways to step up your protection. At the bottom of each item, there is a cost, a complexity, and an importance scale between 1 and 10. While not a complete list, these are the most feasible steps that small-to-medium sized businesses can take to improve security.

Advanced Application Control

Anti-virus software works by trying to detect known threats. Unfortunately, quite often by the time a virus is added to a database, it is too late and you are feeling the pain. Advanced application control techniques such as ThreatLocker® Ringfencing™ controls what applications can do, essentially creating a perimeter around them so they can only access the parts of the system necessary to perform their functions. This is very effective at preventing vulnerable systems from being exploited and handicapping malware by limiting the damage it can do. ThreatLocker® Ringfencing™ was able to stop exploits such as EternalBlue out of the box. The latter was an exploit that the NSA used for years before it became publicly available and patched by Microsoft. The Ringfencing™ software also limits the damage.

Complexity: 1/10 **Importance: 9/10**

Should take less than 5 minutes per computer to install, or 1 hour to deploy organization-wide. Requires no further management.

Dual-Factor Authentication

Dual-factor authentication is a solution that allows businesses to require confirmation that you are who you say you are without just accepting a username and a password. This can be achieved in a few ways. The most common method is sending a text message to your phone with a one-time code when you try to log in to the system. The implementation can vary. For example, it may be that you only need to use a one-time code the first time you log in to your email from the device, but your banking site may require the code each time you log in.

Systems such as Office 365 and GSuite offer dual-factor authentication free of charge and can be enabled relatively easily. Products such as DUO offer dual-factor authentication as a paid extra, and it can be integrated into multiple systems. As a small business, you may not want to invest in a system such as dual-factor authentication for everything, but it might be worth using for systems that are accessible from the public internet, such as your email system.

Complexity: 3/10 **Importance: 7/10**

Takes about 3 hours of I.T. professional time for systems such as Office365 and a little extra work for users. Implementing systems such as DUO could take a few days of an I.T. professional's time.

Segmented WiFi Networks

Your perimeter firewall is extremely important in stopping external attackers from accessing your corporate network. Unfortunately, quite often, internal WiFi networks are used by visitors to your organization. Also, employees bringing personal laptops onto the corporate network often lead to viruses that can springboard onto your servers. Thus, it is generally good practice to have either your entire WiFi separated by a second perimeter firewall or a separate WiFi for guests who are visiting your network. Also, make sure your WiFi password is secure and, if it is internal to your network, lock it down with more than just a key. For example, limit it by a computer's mac address.

Complexity: 1/10 **Importance: 7/10**

Takes about a week to deploy.

Control Data Level Access

This applies in the case where you are using shared data, such as a file server with a common share. Make sure data is segmented on a need-to-know basis. The fewer users who have access to data, the less likely you are to be breached. When considering access, it is not about considering whether you trust employees because quite often, they are unknowingly compromised with malware. It is about making sure that the least privilege is required.

Complexity: 2/10 **Importance: 7/10**

Depends on how much data you have, but your staff will need to review files and data, create a list of who needs access to it, then change permissions based on who needs access. This is a time-based exercise only; no additional products should be required.

Application Whitelisting

Application whitelisting is the holy grail when it comes to stopping malware or unauthorized software. It works similar to antivirus software, but instead of trying to block known threats, it only allows software that is explicitly permitted by your business. Using whitelisting is a major part of large enterprises and government security platforms, although it does come with a tradeoff. The cost of whitelisting is not excessive, generally about $30-$60 per device per year. It does require I.T. Management to manage the items on the whitelist.

In most cases, whitelisting requires a team of I.T. professionals to deploy and requires enormous management overhead. ThreatLocker® offers two application control platforms that can help reduce damage from malware or unauthorized software. Traditional whitelisting products require teams of I.T. professionals to manage, whereas a part-time I.T. service provider can manage ThreatLocker's product.

Complexity: 2/10 (ThreatLocker) **Complexity: 10/10** (Most other solutions)
Importance: 7/10

Once in place, only general I.T. Management is needed.

The above suggestions are just some ways that you can improve your cybersecurity. There are many other ways to improve security, and your security provider may suggest them. Use this whitepaper as a way to check that you are at least heading in the right direction. It is important to remember there is no such thing as unhackable. That said, it is not unreasonable to create an environment that is unattractive to hackers. Many small businesses have or will experience some kind of data breach. Taking steps does not mean killing your bank account or crippling your business, it merely involves taking the right extra steps.

THREATLOCKER

ThreatLocker® is a global cybersecurity leader, providing enterprise-level cybersecurity tools to improve the security of servers and endpoints. ThreatLocker's combined Application Whitelisting, Ringfencing™, Storage Control and Privileged Access Management solutions are leading the cybersecurity market towards a more secure approach of blocking all unknown application vulnerabilities.

To learn more about ThreatLocker visit:
www.threatlocker.com