VIRTUAL GUARDIAN

THE TOP 10 MOST COMMON SECURITY MISTAKES BUSINESSES MAKE

Contents

FOREWORD

Cybersecurity, a Major Challenge Not to Be Neglected

Cybersecurity is often seen as a technology problem that requires technology answers. With thousands of vendors selling tools to detect, prevent and recover from cyberattacks and global cybersecurity spending expected to top $150 billion this year, there is plenty of money being spent on solutions.

But the reality is that the vast majority of security problems result from human error, lack of knowledge and poor policies. Rather than acquiring new technology, organizations need to do a better job of using the tools they already have.

Virtual Guardian, a wholly-owned subsidiary of ESI Technologies, provides cybersecurity products and services to North American enterprise organizations ensuring their digital assets and technologies are protected against internal and external threats. Virtual Guardian is a partner of choice to help protect Canadian enterprises and SMEs against modern threat vectors with a full range of IT security services, from one-time consulting projects to 24/7/365 security monitoring.

ESI tapped into its security team's many years of experience to develop this list of the 10 most common cybersecurity flaws they've encountered. While technology is obviously part of the solution to counter threats, most of these gaps can be filled by developing robust policies, training users and following best practices, without neglecting the monitoring and detection of your organization's activities on known malicious Dark Web sites.

With the increasing number of data breaches, taking care of your passwords is as essential as ever. One of the key elements of a strong password is its uniqueness.

Cybernews

MISTAKE N° 1

Overlook Enforcement of a Strong Password Policy

This is the number one most common cybersecurity mistake, and also the easiest one to correct. Despite years of warnings about the importance of choosing passwords composed of random strings of characters, many people persist in using names of family members, birth dates, sequential number strings and other easily guessed codes.

Meanwhile, the software that criminals use to crack passwords is constantly improving. Even brute-force algorithms – which simply run through combinations of random characters until a successful match is found – can process up to 350 billion guesses per second.

The statistics on password failures are alarming. According to the Verizon Data Breach Investigations report, 81% of the total number of breaches leveraged stolen or weak passwords.

A Cybernews analysis of more than 15 billion passwords reveals that nearly 30% of all passwords are eight characters long, while six-character passwords come in second and account for just under 20% ot the total number.

An equally dangerous practice is to use the same password across multiple accounts. Billions of passwords have been stolen in breaches over the past few years. An attacker who can compromise one account with a stolen password can frequently break into numerous other accounts held by the same user.

There are good reasons why people make these mistakes. Memorizing or writing down different passwords for each account is laborious and error-prone. Storing them in a consolidated electronic file offers little protection unless the document is encrypted.

A better option is to use one of the many digital password managers that are available at little or no cost. These products store passwords in encrypted vaults, automatically fill forms and can even store credit card information and other sensitive personal information. They can also suggest passwords that are nearly impossible to crack. Users need to remember only one password to get access to their entire vault.

Implementing Corporate Best Practices

Organizations can help enforce good password security with a few basic procedures.

1

Force immediate change of default password whenever new devices such as network equipment are installed. Leaving defaults in place on a router, for example, can enable an attacker to easily gain access to an organization's entire network.

2

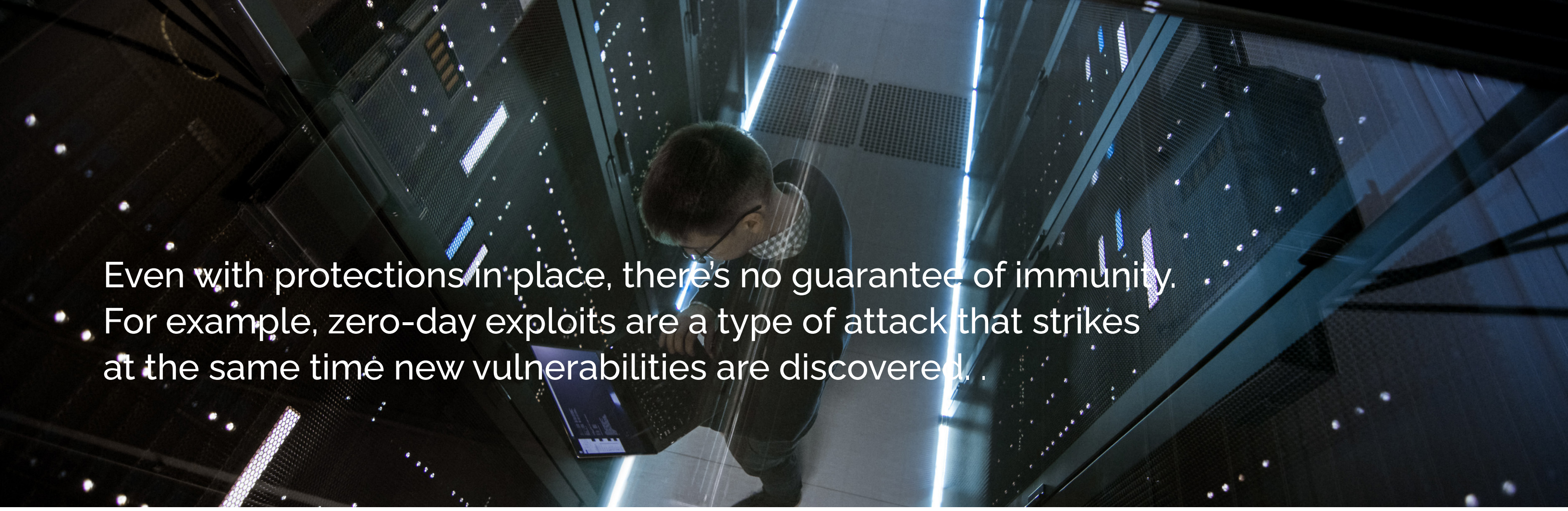
Define rules that users must follow, such as changing passwords for critical applications every quarter, using a password manager to allow administrators to enforce password changes on a predefined schedule.

3

Provide employees with guidance on selecting good passwords. Password hacking software has become so sophisticated that experts now say a minimum length of 13 characters is required. An increasingly common practice is to adopt very long passwords, such as memorable quotes or passages from books.

4

Encourage employees to use two-factor authentication whenever possible. This technique, which supplements the password with a second form of verification, such as a text message to the user's cell phone, is becoming more and more common. According to a 2019 report from Microsoft, using multifactor authentication blocks 99.9% of account hacks.



Even with protections in place, there's no guarantee of immunity. For example, zero-day exploits are a type of attack that strikes at the same time new vulnerabilities are discovered. .

MISTAKE Nº 2

Use Outdated and Unpatched Software

Keeping current with software patches and updates is a significant challenge for even the most resource-rich enterprise IT organizations. For smaller companies on a limited budget the task is nearly impossible. A scan of the National Vulnerability Database at the NIST illustrates the scope of the problem. Literally hundreds of patches are issued every month (which are not all critical) and impossible to keep up with. Those that do need to be applied must often be downloaded, tested and deployed in a rigorous manner that ensures that the fix doesn't break something else.

The renowned Ponemon Institute estimated that 60% of organizations experiencing a data breach over a two-year period were victims of an exploit of a known, but unpatched, vulnerability.

The prevalence of older PCs and operating systems is a significant problem. As of April 2021, a study conducted by Kaspersky found that as many as 22% of personal computer users are still using Windows 7, which Microsoft ended support for in January 2020.

The Challenge of Mobile Devices

A further complication is the growing number of mobile devices that organizations must support. Laptops, smart phones and tablets in the field are difficult to corral, and traveling users are more susceptible to viruses introduced through channels like open Wi-Fi networks and USB sticks.

Keeping up with the patch deluge requires automation and priority-setting. Server administrators should subscribe to all relevant alerts from their strategic software providers and give priority to those patches deemed most critical. A good testing strategy is to use a second server in a virtual partition that mirrors the production environment.

Endpoint Protection Security

Endpoint security is a more difficult problem. Organizations should audit all potential network entry points on a regular basis, ideally once per quarter. This includes desktops, laptops and network equipment connected to the public Internet. Any systems running unsupported operating systems such as Windows XP or Windows 98 should be immediately removed and replaced. PCs running Windows 7 should be upgraded to Windows 10 with automatic patching turned on.

MISTAKE Nº 3

Use Vulnerable Edge Devices

Many organizations offer free wireless service to their guests and clients, but failing to follow a few basic protections can turn this courtesy into a security nightmare.

The Risk of Wireless Services

Public-facing Wi-Fi access points should never be connected or bridged to the corporate network. Organizations may overlook this basic bit of blocking and tackling for the sake of cost or convenience, but they do so at their peril. Adding password security to public access points is a weak protection for all the reasons noted in item 1 above. The better approach is to contract with a commercial Internet service provider whose network is independent of your own.

Most public Wi-Fi access points are unencrypted, meaning that data transmitted through them remains in plain text format. Cybercriminals can easily "sniff" this traffic to capture all packets that traverses the network. For this reason, employees, contractors and even customers should be cautioned against using public hotspots for business purposes.

With their proliferation, companies struggle to maintain an inventory of all their potentially vulnerable access points.

One factor that contributes to this blindness is the ease with which individual devices can now create vulnerabilities without the knowledge of the IT organization. For example, many PCs and smart phones come with a default option to configure them as open wireless access points. Employees may use this convenient feature to set up ad hoc workgroups or save on wireless data costs but then forget to turn it off. Upon connecting at work, they essentially create an open on-ramp to the corporate network.

The Danger of IoT

Unfortunately, the Internet of things will make matters worse. Organizations are increasingly installing devices like programmable thermostats, smart cameras and intelligent lighting systems and connecting them to their network. These devices may come with little or no security, making them easy prey for criminals. It certainly won't be the last. As a basic protection, change the default passwords on all devices added to your network, and use network segmentation to limit access to critical infrastructure and information.

For a hacker, creating rogue access points which mimick the names of common open Wi-Fi access points is the easiest way to track nearby devices and conduct MITM attacks.

Varonis

Phishing attacks account for more than 80% of reported security incidents.

CSO Online

MISTAKE Nº 4

Neglect Email Monitoring and Protection

Despite security administrators' best efforts to enforce good password practices and plug holes in corporate networks, there's little they can do to protect users from their own mistakes. The inbox remains a most stubbornly persistent threat to security.

The statistics speak for themselves. According to CSO Online, 94% of malware is delivered via email. Verizon's 2020 Data Breach Investigation Report indicates that 30% of data breaches involve internal actors.

Increasingly Sophisticated Attacks

Email-based attacks have changed over the past few years as criminals have honed their ability to target messages. Spam filters are now so good that few users even see spam messages any more, but through a technique known as "spear phishing", criminals can bypass even the best controls.

The root of the problem is trust. Email is such an essential utility to business professionals that it's easy for people to fall into the trap of believing that every message is genuine.

Spear phishing preys on this complacency. Criminals mine personal information from social media profiles and match it to email addresses. They might also scan a person's recent activity to find points that establish trust, such as membership in an organization or recent purchases. And they look at friend networks to find the names of people their targets already know. Armed with this information, attackers can easily spoof the "from:" field of an email message to make it appear to be from a friend. Including a little personal information gleaned from a social media site puts the recipient's mind at ease.

The message includes a link to a malicious website that either installs malware or asks for login information. Spear phishing practitioners are so skilled today that even cybersecurity professionals have admitted to falling prey.

Email-borne attacks are extremely difficult to defend against because they are specific to each user on the network. A single click on an attachment or malicious link can unleash a flood of malware that quickly spreads throughout the organization.

Ransomware is a particularly noxious factor. It instantly encrypts a user's hard drive and demands a ransom payment in cryptocurrency in exchange for the decryption key. Some of them also copy themselves to other PCs on the network and encrypt them as well.

Ways to Enhance Protection

Applying an employee awareness and training program is a must do. Implement a program based on cybersecurity event simulation exercises to increase employee vigilance and better prevent attacks.

Fortunately, defending against email-borne attacks is fairly simple. It consists of educating people about a few basic practices:

Never click on links or attachments in email messages unless you're absolutely certain about the identify of the sender. That information can be easily verified by looking at the email header, which is different than the "from:" field.

Never send personal information like financial account numbers or passwords by email. No reputable organization will ever ask you to do so.

If directed to a login page from an email, verify that the web address is what's expected. Attackers can construct fake web pages that look exactly like legitimate banking, commerce and social networking site.

Be judicious about what information you share publicly on social networks..

It took organizations an average of 280 days to discover a breach in 2020. The average cost savings of containing a breach in less than 200 days vs. more than 200 days is $1.12 million.

2020 Cost of Data Breach Report
Ponemon Research

MISTAKE N° 5

Have a Poor Visibility of the Network

You can't prevent attacks from devices you don't see. Unfortunately, many organizations lack a comprehensive view of their networks. Perhaps they can see IP addresses, but they have little information about what those devices are.

Poor visibility increases the risk that attackers can penetrate a network and remain undiscovered for weeks or months, a metric known as "dwell time." During that period, intruders can siphon off large amounts of information in small, steady streams that evade detection.

Information Sharing

The problem is made worse by the open nature of IP networks. The Internet Protocol was designed to make information freely discoverable, meaning that devices willingly share information about other devices on the same subnet, including such things as OS versions and running applications. A cyberattacker can exploit this information to find unpatched software that can be exploited to take over additional machines.

Network Segmentation Failures

Poor network segmentation practices compound the problem. Segmentation is a useful way for administrators to limit access to certain kinds of information by grouping devices into subnets with different permission levels.

However, many organizations don't bother to create subnets, effectively exposing their entire network to anyone who can breach a single firewall. Conversely, over-segmentation creates complexity that can also expose vulnerabilities. For example, 30 subnets with 25 permission policies each creates 750 rules to administer. Errors and oversights are easily missed in such a complex environment..

MISTAKE Nº 6

Mismanage Mobile Devices

Nearly everyone now carries a smart phone, but many businesses are behind the times when it comes to treating them as part of their IT infrastructure. The BYOD policies that dominated the early years of the smart phone revolution are dangerously inadequate to govern the use of today's powerful devices.

Regardless of whether users bring their own phones to work or the company provides them, mobile devices demand the same security considerations as desktop and laptop PCs. In fact, they demand additional attention because of the ease with which they are lost or stolen, as some 70 millions each year.

Mobile devices present some unique new security threats. Because of their built-in cameras and audio recorders, compromised phones can become listening and video recording devices without the user's knowledge. Their built-in GPS also makes them vulnerable to location tracking, a feature that is particularly useful to criminals engaging in corporate espionage.

Mobile phone security is improving, but IT organizations shouldn't rely on built-in features alone for protection. Researchers have shown that PIN codes and swipe patterns can be detected from up to 15 feet away and no biometric protection has been shown to be foolproof. A better practice is to use two forms of authentication.

While some of these rogue programs make their way into legitimate app store channels, many are spread through phishing schemes that send text messages to unwitting users directing them to websites that plant malware on their devices.

Effective mobile security begins with sound policies that are communicated thoroughly. Basic steps include keeping devices up-to-date with the latest operating system versions and security patches, regularly backing up data and using encryption for data both on the device and in transit. Users should avoid public Wi-Fi hotspots and never click on unknown links in emails and text messages.

> In their campaigns to infect mobile devices, cybercriminals always resort to social engineering tools, the most common of these passing a malicious application off as another, popular and desirable one. All they need to do is correctly identify the application, or at least, the type of applications, that are currently in demand. Therefore, attackers constantly monitor the situation in the world, collecting the most interesting topics for potential victims, and then use these for infection or cheating users out of their money.

Mobile Malware Evolution 2020 - Securelist Kaspersky

MISTAKE Nº 7

Neglect Application of Access Privilege Policies

Amid the pressure of day-to-day business, details are easily forgotten, or loose ends left untied. When those details concern access privileges, it's a problem.

Many end-users don't understand how file permissions work or don't pay attention to guidance the IT organization provides. The result is that sensitive information can easily be left in the open for anyone on the network to see.

The 2021 Data Risk Report by Varonis for financial services compiled data of 4 billion files across 56 financial services organizations.

Among its findings:

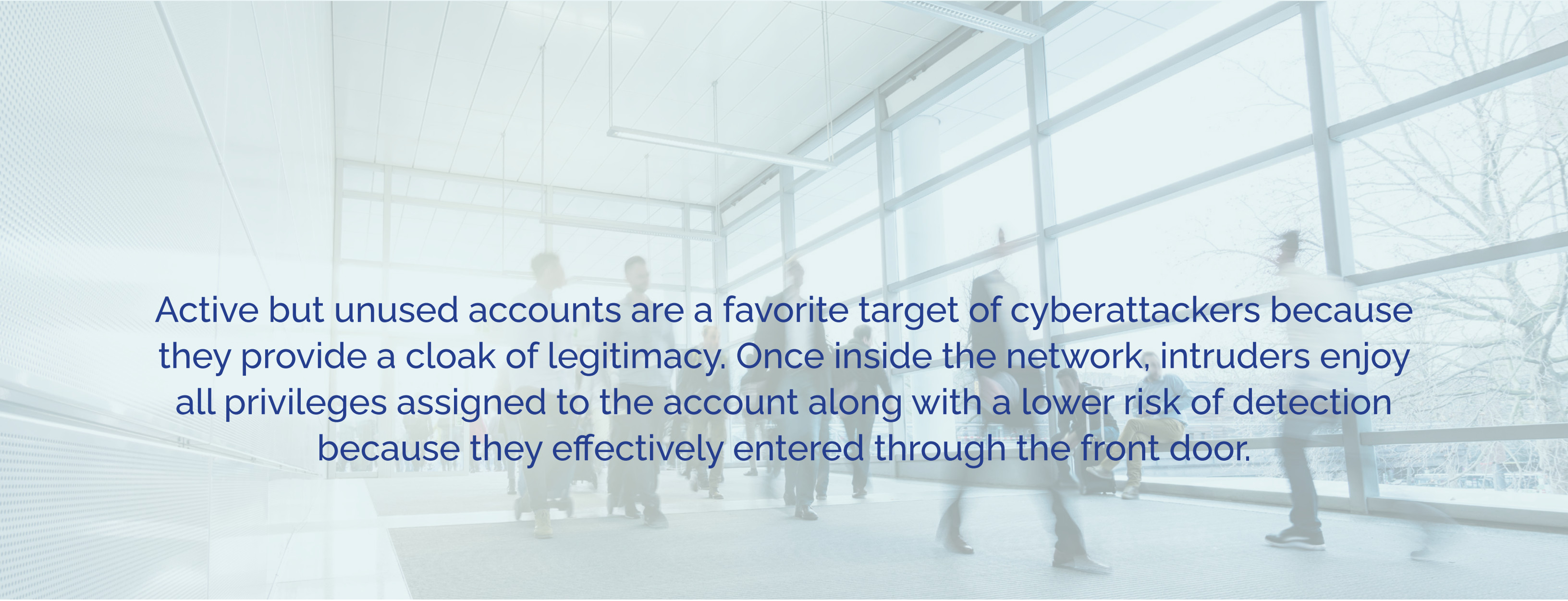
- Every employee has access to nearly 11 million files;
- Nearly two-thirds of companies have 1,000+ sensitive files open to every employee; and
- About 60% of companies have 500+ passwords that never expire.

These oversights are significant in light of the fact that CyberAngel found that about 90% of data breaches are due to employee or third-party negligence with only 10% of leaks being perpetrated by malicious actors.

Lack of knowledge is the biggest culprit. Employees may be unaware of procedures for assigning permissions or may drop files into insecure folders thinking they're protected. Folders deep in a file system may contain permissions that aren't visible at higher levels, causing administrators to mistakenly assume that protections are in place.

Awareness and training are the best remedies. The IT organization should demonstrate how to assign file and folder permissions and convey best practices, such as assigning access at the group level and never to individual users. An even more secure approach is to limit creation of new folders to IT administrators, although that isn't practical in every case.

Technical solutions are available in the form of enterprise content management systems, which regulate access to and distribution of content throughout the organization. These systems often also include sophisticated workflow management capabilities that can streamline processes and enhance efficiency.



Active but unused accounts are a favorite target of cyberattackers because they provide a cloak of legitimacy. Once inside the network, intruders enjoy all privileges assigned to the account along with a lower risk of detection because they effectively entered through the front door.

MISTAKE N° 8

Mismanage Directories

When an employee leaves the company, managers are understandably more concerned about getting work done and filling the open position than deactivating access privileges. Unfortunately, over time this can create a big hole in the organization's defenses.

With people today posting their entire job history on social networks like LinkedIn, it's easy for hackers to identify candidates by looking for people who have recently changed jobs and whose credentials might therefore still be valid. They can cross-correlate that information with the billions of stolen user names and passwords available on the dark web to narrow down their list of candidates.

Turnover isn't the only vulnerability. Accounts are often set up for contractors and temporary workers without careful attention to access privileges, and administrators either forget to shut them down when the assignment ends or leave them open in case the temporary worker returns.

The Varonis report cited above refers to these directory entries as "ghost accounts." Its survey found that one-third of accounts are enabled but unused and 65% of companies have more than 1,000 ghost accounts.

Other common directory-related problems include granting overly generous permissions and assigning group memberships without properly vetting access requirements.

To deal with the ghost account problem, organizations should designate a person within the human resources department to ensure that access privileges are revoked for departing employees. It's also a good idea to audit the list of accounts annually and remove any that are unused. Directory administration should be confined to a few individuals who are trained in best practices for the chosen directory service.

MISTAKE Nº 9

Poorly Protect Cloud Services

Data Encryption

Most software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS) providers offer excellent security, but that doesn't mean customers should assume that the burden is lifted from their shoulders.

For example, IaaS providers may support data encryption but leave the responsibility for encrypting data and maintaining decryption keys in the hands of their customers. Or they may provide controls to prevent the downloading of information but leave that option disabled by default. Each provider has its own policies, and it's up to the customers to do their homework.

Data Leak Prevention

User error is the most common cause of cloud security breakdowns.

According to a survey by Ermetic, nearly 80% of businesses have experienced at least one cloud data breach in the last 18 months. The three biggest causes were:

- Security configuration errors (67%)
- Lack of adequate visibility into access settings and activities (64%)
- Identity and access management (IAM) and permission errors (61%)

Organizations should limit the number of cloud storage providers they use and apply administrative controls to limit what users can share and download.

Password Selection

Poor password selection can leave applications and critical data exposed to anyone on the Internet. Requiring the use of two-factor authentication can minimize this risk. Users should also be educated about best practices for sharing cloud data. For example, sensitive data should only be shared with named individuals rather than through a global URL that enables edit access.

It's usually dangerous to assume, especially when it comes to cloud services. Employees can walk down the hall to ask security-related questions of their IT administrators, but most people never even speak to the companies that provide cloud services, which can lead to dangerous assumptions about who is in charge of what.

MISTAKE Nº 10

Use Inadequate Data Disposal Practices

Equipment that has reached the end of its useful life can be a significant security risk if proper disposal practices aren't employed. Many people believe simply deleting all the data on a disk drive or formatting the media is enough protection, but neither measure actually removes much data.

Rather, they remove pointers from directories, but leave up to 90% of the data intact and easily recoverable using special software. Even multiple formatting passes can still leave significant amounts of data in place.

IT asset disposal (ITAD) is a specialized discipline for destroying data. ITAD providers employ techniques ranging from erasure with high-powered magnets to physical destruction of media using machinery that grinds disk drives into powder.

Professional services also provide a certificate of destruction that satisfies most regulatory inquiries. Some can also refurbish equipment and recover some value through sale on secondary markets.

ITAD services can be expensive and aren't necessary in every scenario. Organizations should have a process for evaluating end-of-life equipment and identifying that which merits specialized handling.

This process should apply to any equipment that contains data, including servers, PCs, smart phones and USB drives.

Common-Sense Security

Small business owners may think they're protected from cyberattacks because their size makes them an unattractive target, but more than 55% of ransomware attacks now involve companies with fewer that 100 employees.

Criminals assume that smaller companies are resource-constrained and lack the sophisticated detection and prevention technology of large enterprises. While large organizations are well-equipped to withstand even large data breaches, the impact can be devastating on companies operating on thinner margins. In fact, according to a survey conducted in early 2021 by the Canadian Federation of Independent Business, small and medium-sized businesses are more exposed that ever to computer fraud; 25% report being victims of attempted fraud, and 56% of entrepreneurs surveyed are more worried about their business since remote work has become more widespread.

Cybercriminals want to have an impact on the daily operations of an organization. IT leaders must rethink and improve the resilience of their organization by implementing IT Recovery and Business Continuity Plans that will ensure that operations continue. This is one of the last lines of defense when a security event occurs.

More than ever, paying attention to the 10 issues listed here can thwart the vast majority of risks and dramatic consequences to your business.

Looking for advice from a team of cybersecurity experts? Virtual Guardian offers you a **free one-hour consultation** to discuss your company's cybersecurity issues and evaluate with you how to mitigate the risks identified in this book. Contact us to book an appointment!

Virtual Guardian

Service Centre:
1-800-401-TECH (8324)

Talk to a representative:
514 745-3311

1550 Metcalfe, # 1100, H3A 1X6
Montreal, Quebec, Canada

www.virtualguardian.com