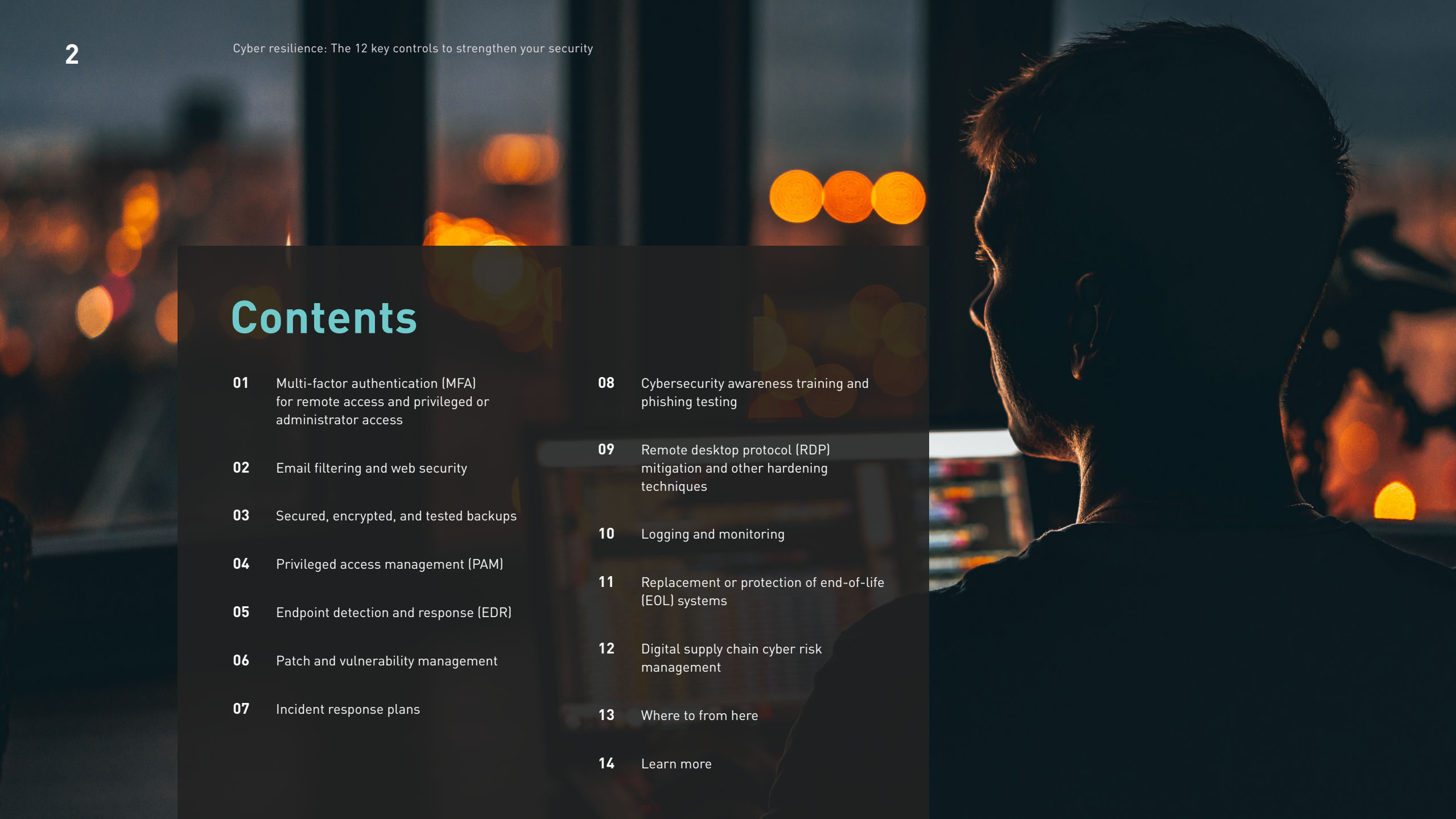
VICTOR

Cyber resilience:

The 12 key controls to strengthen your security



Contents

Cyber resilience: The 12 key controls to strengthen your security

Cyberattacks continue to dominate news headlines, driven by a surge in ransomware events, which increased by an overwhelming 148% in 2021.[1] The perpetrators of these attacks now demand multi-million dollar ransom payments as they cripple a business' operations, bringing them to a standstill until a payment is made.

As cyberattacks become more prolific, related insurance claims follow, meaning underwriters have been able to identify a correlation between certain controls and corresponding cyber incidents. Through this analysis and the continuous examination of relevant data points, the insurance industry has a rich understanding of the technical steps that organizations can take to build their cyber resiliency.

However, due to the growth in attritional losses, consequently insurers are now taking a much more cautious position. Insurers are tightening their underwriting terms, carefully analyzing all cyber insurance applications, and asking more questions than ever before about an applicant's cyber operating environment and risk controls.

The adoption of certain controls has now become a minimum requirement of insurers, with organizations' potential insurability on the line. Organizations are undoubtedly placing more emphasis on controls than ever before to help mitigate their ransomware risks and improve their overall cybersecurity position and resilience.

While these controls have been established best practice for several years, some companies are still struggling to adopt them — most often because they have been unable to justify the cost of implementation, did not deploy them comprehensively, or did not understand or see the need for controls. In many regulated industries where cyber resilience controls have been required for years, the effort was often more about checking a box, than enhancing security.

Organizations are recommended to implement a number of cyber hygiene controls that are key to achieving cyber resilience and insurability. In this report, we present 12 recommended cybersecurity controls and their characteristics and requirements.

1. SonicWall: 'The year of ransomware' continues with unprecedented late-summer summer surge

Multi-factor authentication (MFA) for remote access and privileged or administrator access

WHAT IS THIS CONTROL?

Multi-factor authentication (MFA) is an additional login security layer to verify a user's identity when requesting access to a computer resource. MFA requires the user to provide two or more pieces of evidence to be authenticated from the following categories: "something you know" (such as a password/PIN), "something you have" (for example, a cryptographic identification device or token), and "something you are" (for example, a biometric).

WHY SHOULD THIS CONTROL BE ADOPTED?

According to findings published in "The Changing Face of Cyber Claims 2021," 80% of all cyber incidents are malicious and often start with compromised user credentials. MFA is an essential part of a strong identity access management (IAM) strategy, preventing unauthorized remote access to computer resources.

MFA should be enabled in all systems, applications, and accounts that are accessible remotely, for all access by privileged and administrative users, and for all access to critical or sensitive data.

In many cases, correct MFA implementation can help prevent cyber incidents — such as a costly ransomware attack. Insurers are requiring organizations to be more cyber resilient, with MFA as a key starting point. Ultimately, this will strengthen their security and will assist them in becoming better candidates for cyber insurance cover.

At a minimum, companies should look for the enforcement of MFA on:

- Critical assets.
- Privileged accounts.
- Remote applications.

WHAT A COMPANY NEEDS TO DO TO PUT THIS CONTROL IN PLACE

In order to implement this control accordingly, businesses are recommended to:

1. Require MFA for all remote logins to the corporate network by using secure remote access, such as virtual private network (VPN) and remote desktop protocol (RDP).
2. Require multi-factor authentication and encrypted channels for all administrative account access, irrespective of a user's location.
3. Require MFA for access to the most critical or sensitive data or systems, irrespective of a user's location.
4. Enforce complex long passwords that are longer than 14 characters and use upper and lowercase letters, numbers, and symbols.

As a basis to meet and implement the aforementioned requirements, an organization is advised to:

- Identify:
  - All systems and applications that are accessible remotely.
  - Critical and sensitive data, as well as all systems and applications that it is stored on.
  - All high-privileged and administrative users.
- Implement risk-based authentication, which is a method of applying varying levels of stringency to authentication processes based on the likelihood that access to a given system could result in it being compromised.
- Combine the VPN and any remote solutions with MFA.
- Identify all corporate devices, especially those that accept biometrics (such as laptops and mobile phones), for potential use as an additional factor.
- Check local regulation regarding data protection, privacy, and biometrics data. There may be limitations in using private devices, or biometric data, as a means to achieve the additional factor.
- Deploy factors in all devices to avoid a compromise affecting them all.
- Train and inform employees on the value of additional layers of security before implementation of MFA to reduce resistance and avoid any misunderstandings.

Please refer to NIST 800-63 for further guidance.

Ransomware events increased an overwhelming 148% in 2021.[1]

1. SonicWall: 'The year of ransomware' continues with unprecedented late-summer summer surge

Email filtering and web security

WHAT IS THIS CONTROL?

Email filtering software is used to scan inbound or outbound email traffic for undesired content. This can be less harmful spam emails approaching the recipient regarding specific actions — for example, selling a product or asking for donations — or phishing emails which represent a serious cybersecurity threat.

These detected emails would automatically be filtered out, so they do not reach the user, or be flagged so the user is sensitized to the potentially malicious or unwanted content. Via email security software, suspicious and potentially malicious email attachments are additionally tested in a secure "sandbox" environment.

Web content filtering can be implemented by using either hardware- or software-based solutions, as well as tracking, and regulating access to websites that users are not supposed to enter. The reason for that can be because the content is subject to compliance regulations — as is often the case with material on gambling websites — or is suspected to be malicious content. Domain name system (DNS) filtering, meanwhile, is a special type of content sifting that uses the DNS layer to regulate website access based on IP addresses, in order to filter web use and reduce malware exposure.

WHY SHOULD THIS CONTROL BE ADOPTED?

Malicious links and files are the primary way to insert malware into organizations' systems, or to steal user passwords, and eventually access critical systems. Web and email filtering is seen as a "first line of defense" in defending against email- or web-browsing-related cyberattacks, even before the users — the "second line of defense" — can fall victim to a phishing attack or enter websites with malicious content.

Filtering is needed as email phishing is one of the top initial attack vectors leading to severe cyber incidents, especially ransomware attacks. Cybercriminals often use phishing campaigns to steal their victims' usernames and passwords, which provide the attackers with initial access to a victim's IT environment. By implementing email security and web-filtering technologies, a large percentage of potentially severe cyberattacks can be stopped at the outset.

At a minimum, organizations should pre-screen emails for potentially malicious attachments and links, and to use tools to monitor web content to block access to vulnerable websites.

Insurers are also imposing stringent cyber resiliency requirements on policyholders to evaluate them as insurable. The implementation of email security and web-filtering technology will allow an organization to improve its profile in relation to presenting its cyber risk to insurance underwriters. These controls are a key element of eligibility for cyber insurance cover as, if they are implemented, insurers predict seeing a decrease in the total number of severe — and therefore costly — cyber incidents.

WHAT A COMPANY NEEDS TO DO TO PUT THIS CONTROL IN PLACE

Security controls related to malware protection, email security, and web–filtering that could be put in place can encompass the following:

- Using technology to scan and filter incoming emails for malicious attachments and links.
- Preventing macro-enabled files from running by default.
- Evaluating email attachments in a sandbox environment prior to user delivery, in order to determine whether files are malicious.
- Using technology to monitor web content and to block access to malicious websites or web content.

Secured, encrypted, and tested backups

WHAT IS THIS CONTROL?

Secure, available, and accurate backups are essential to ensure business resilience. Backups should be secured, preferably by isolating them from the network, or by implementing multi-factor controlled access and encryption. Regular testing is also critical to ensure the integrity and availability of data.

WHY SHOULD THIS CONTROL BE ADOPTED?

As organizations increasingly move to cloud-based backup solutions, attackers look for administrator credentials to gain access to them, before deleting or encrypting them. A lack of available backups increases the likelihood of a victim paying a ransom, in order to recover systems and data, as they have no other option.

Regularly testing backups is critical — there is no point in having backups if they are unavailable, or incomplete, when you need to restore your systems. Regular tests also enable IT and business resilience teams to understand the complexity of the restoration process and identify external partners that may be required to assist them. It is not usually as simple as flicking a switch.

Viable backups enable organizations to recover from attacks more quickly and effectively. In the case of ransomware, having backups reduces the leverage that threat actors have over the victim and can greatly reduce the need to pay a ransom.

Where systems are encrypted, businesses are usually unable to operate and so incur significant business interruption losses. Secured backups can reduce recovery time and enable a return to business as usual more quickly than negotiating with threat actors for dubious decryption keys. Tested backups enable the business to place more trust in the backed up data — errors or failures in the backup process will be picked up and rectified quickly.

3

WHAT A COMPANY NEEDS TO DO TO PUT THIS CONTROL IN PLACE

Organizations should review their critical systems and assets, and ensure that backup procedures are adequate and tested regularly. It also is essential to ensure that one copy of the backup is stored offline and is unconnected from the network.

Disaster recovery, business continuity, and incident response plans should be put in place to accurately document the process that would be taken to recover systems from backups.

There are myriad different backup solutions and it can be difficult to assess the best provider and proposition for an organization. Focusing on providing a solution for the systems, data, and assets that are truly critical — the "crown jewels" — is a good place to start.

In terms of cybersecurity, humans are often the weakest link.

Privileged access management (PAM)

WHAT IS THIS CONTROL?

Privileged access management (PAM) is a security technology that offers an elevated or "privileged" level of access to protect accounts, credentials, and operations. Privileged access differs from "normal" access because it can allow security or maintenance functions, system- or application-wide configuration changes, and the bypassing of established security controls through super user access.

WHY SHOULD THIS CONTROL BE ADOPTED?

In terms of cybersecurity, humans are often the weakest link, making any organization vulnerable to an attack. PAM tools control privileged access of machines (systems or applications) for internal or machine-to-machine communication, including for people who administer or configure systems and applications. It runs on the principle of "least privilege," meaning the users only receive the minimum level of access required by them to perform their job functions. Components within a typical PAM solution monitor sessions that are used by administrator accounts and generate alerts for any anomalous session usage. Anomalies may include an account trying to access areas outside of its responsibility domain or outside of its window of operations.

4

WHAT A COMPANY NEEDS TO DO TO PUT THIS CONTROL IN PLACE

At the outset, an organization needs to identify the use case — that is, the actions or event steps it wants to invest in a PAM for. For example, it can adopt a risk-based approach to identify critical assets that are at the highest risk of exposure, as a result of the compromise of privileged accounts, and then only implement the solution for those assets.

Once PAM is in place, to overcome any misconception about the solution, an organization can distribute content to its employees on its different components, their purpose, and why they are required as part of the overall cybersecurity mix.

An organization also should establish a governance and monitoring program for PAM so that performance does not degrade over time. This should include setting selection and performance criteria for vendors and products and conducting post-implementation performance evaluations.

Regarding the scalability of PAM, roadmaps for business growth can factor in additional relevant assets requiring this control, so that licenses are available to accommodate them when implemented.

Endpoint detection and response (EDR)

WHAT IS THIS CONTROL?

Endpoint detection and response (EDR) is a threat detection and response mechanism for an endpoint — a remote device such as a desktop, laptop, mobile phone, server, or Internet of Things (IoT) that communicates with an internal network, externally.

As endpoints are the entry points for virtually any type of malicious attack on a network, their monitoring is vital to detect and stop a strike before it spreads to the wider internal network. An EDR solution continuously monitors endpoints, collects data from devices, and provides a response based on defined rules.

WHY SHOULD THIS CONTROL BE ADOPTED?

According to a study[2] published by the Ponemon Institute in 2020, 68% of organizations have experienced one or more endpoint attacks that successfully compromised data and/or their IT infrastructure. The same report noted that 68% of IT professionals found that the frequency of endpoint attacks had increased since the previous year. Monitoring of endpoints is critical to detect and stop an attack before it spreads to the wider internal network.

Additionally, when EDR is in place, it monitors and records activity on those endpoints. That data can be analyzed to detect persistent threats, or "zero day" vulnerabilities — in other words, flaws not yet patched — that have been compromised. If a security threat is detected, the log can be reviewed to determine when that threat began, the scope of the compromise, and the root cause.

For example, an organization that is the victim of a ransomware attack will take longer to recover without EDR in place. This is because it will not have visibility into the extent of the event, and specifically, on how many endpoints have been infected. The organization will be unable to detect if there are any payloads still operating on the backend, and if relevant configuration settings are working as expected, or need to be implemented. All of this means that the recovery effort will take longer and need to be more in depth.

2. 2020 State of Endpoint Security (morphisec.com).

WHAT A COMPANY NEEDS TO DO TO PUT THIS CONTROL IN PLACE

Having a strong baseline of cybersecurity best practices usually enables an organization to implement EDR seamlessly. It is also vital to find an EDR solution that can provide the maximum level of protection while requiring the least amount of effort and investment, ultimately adding value to your security team without demanding a lot of resource. Key aspects organizations should look for in a solution include:

- Endpoint visibility across all your endpoints. It should provide real-time visibility for you to view suspicious activities, even as they attempt to breach your environment, and stop them immediately.
- A solution that collects a significant amount of telemetry from endpoints, so it can be mined for signs of attack with a variety of analytic techniques.
- Effective endpoint detection and response requires behavioural approaches that search for indicators of attack (IOAs), so you are alerted of suspicious activities before a compromise can occur.
- A solution that integrates threat intelligence, including details on the attributed adversary that is attacking you or other information about the attack.
- A quick-response, solutions should operate in real-time, provide accurate alerting, and automate threat response. This requires detection engines that produce minimal false positives and the ability to set automated response policies.
- Having a cloud-based endpoint detection and response solution is the only way to ensure zero impact on endpoints. This solution should smoothly integrate with current systems and provide intuitive remote access to controls.

Patch and vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization.[3]

3. According to NIST SP 800-16. However, there are multiple risk definitions. Although we have included the simplest way to define a risk, this definition considers the most important characteristics: probability of occurrence, threat or event, vulnerability, and impact.

Patch and vulnerability management

WHAT IS THIS CONTROL?

Vulnerability management is a capability that identifies vulnerabilities on software and hardware devices that are likely to be used by attackers to compromise a device and use it as a platform from which to further compromise the network.

Patch management is the systematic notification, identification, deployment, installation, and verification of an operating system and application of software code revisions. These revisions are known as patches, hot fixes, and service packs.

Not all vulnerabilities have related patches. Therefore, a proper vulnerability management process will consider other methods of remediation, or temporary workarounds — such as software configuration change and employee training — to limit or isolate the exposure.

WHY SHOULD THIS CONTROL BE ADOPTED?

Organizations will always have a certain level of risk due to vulnerabilities in their IT environments. A risk can be defined as the probability that a particular security threat will exploit vulnerability in a system.[3]

Vulnerabilities can be exploited by several cyber threats in software and hardware devices that are frequently used by an organization. Therefore, without having a clear and continuous view of existing vulnerabilities, organizations will struggle to identify and respond to threats in a timely manner.

On the other hand, each organization will have a unique risk tolerance based on its financial health, reputation exposure, and compliance requirements. Establishing a relationship between proper IT vulnerability management and risk tolerance is complex, and can be hard to advocate for in front of a board, as management may not fully understand which IT vulnerabilities present the greatest risk.

A proper patch and vulnerability management function will reduce, or eliminate, the potential for exploitation and involve considerably less time, effort, and money than the response following an exploitation.

Unpatched vulnerabilities remain a leading cause of intrusions into systems, with hundreds of vulnerabilities revealed every month for multiple applications and systems. When technology environments are not patched in a timely fashion, attackers will seek to exploit vulnerabilities.

3. According to NIST SP 800-16. However, there are multiple risk definitions. Although we have included the simplest way to define a risk, this definition considers the most important characteristics: probability of occurrence, threat or event, vulnerability, and impact.

4. These steps are enlarged upon in the SANS Institute paper: "Implementing a vulnerability management process."
5. Exception process: a condition that is not aligned with formal security expectations as defined by policy, standard, and/or procedure — for example, a patch isn't applied.
6. CVE stands for common vulnerabilities and exposures. It is a program launched by MITRE to identify and catalog vulnerabilities in software or firmware.

WHAT A COMPANY NEEDS TO DO TO PUT THIS CONTROL IN PLACE

While the implementation of a vulnerability management process is very complex, it can be summarized in five steps:[4]

1. **Preparation.** Conduct a vulnerability analysis, define the scope of assets, inform stakeholders and asset owners, and plan vulnerability scans.
2. **Identification and detection of vulnerabilities.** This can be achieved through a vulnerability scan.
3. **Definition of remediating actions.** To properly define the remediating actions, an IT risk assessment must be conducted. Depending on the remediation (such as a patch or a change in configuration), software restrictions, and availability of solutions, different options can arise including:
   - Mitigate — by implementing remediating actions.
   - Accept — by launching an exception process[5] and investigating potential indicators of compromise (IOC).
4. **Implementation of defined actions.** Deployment of the tasks identified in the previous activities.
5. **Monitoring of vulnerabilities.** As new vulnerabilities arise every minute, committing to real continuous monitoring is essential to properly manage them.

Most vulnerabilities can be remediated by patching and updating systems. IT systems with known vulnerabilities with constraints to install the patch, or without an available solution, can be investigated for the presence of indicators of compromise. And, if these systems are compromised, incident response and recovery plans should be initiated. In addition, an isolation plan for legacy systems can also be applied. Ultimately, if the IT risk assessment indicates a delay in remediation due to operational constraints, an exception process should be in place.

Insurance companies are also likely to require the following actions:

- Periodic performance of a vulnerability analysis.
- Performance of penetration testing — that is, a simulated cyberattack to check for exploitable vulnerabilities — at least annually.
- Ongoing maintenance and updating of the information technology and communications landscape.
- Patches with CVE[6] 8 or above to be applied in less than three to seven days, after their publication, on exposed IT systems.
- Non-critical patches are expected to be applied in less than 30 days after their publication.

The frequency and detail of these actions is tied to an organization's cyber risk profile, industry, and cyberattack environment.

Incident response plans

WHAT IS THIS CONTROL?

Incident response plans document a "predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyberattack against an organization's information systems."[7] They need to be in line with other available related plans and capabilities, including:

- An IT disaster recovery plan (DRP), which describes how an organization recovers data during and after a crisis or disaster.
- A business continuity plan (BCP), which sets out how an organization ensures that essential business processes are available during and after a crisis or disaster.

Incident response will only work smoothly when all relevant stakeholders are familiar with the response plan. Therefore, regular testing of procedures is an essential part of this control.

WHY SHOULD THIS CONTROL BE ADOPTED?

Incident response plans are an integral part of increasing an organization's cyber resiliency. These programs are not isolated frameworks — they need to reflect the specific and unique risk profile of an organization and require integration within an overall cyber risk management strategy.

In order to mitigate cyber risk, the first approach and line of defence will always be technical and organizational prevention measures. When cyber incidents do occur, it is crucial to detect them as early as possible, and respond to them in a fast and professional way.

An up-to-date incident response plan and a trained team provides efficiency, speed, and quality in response to cyber incidents. When combined with a holistic organizational approach to the 12 key controls — as well as the implementation of appropriate technical controls and incident and disaster recovery (such as secured, encrypted, and tested backups) — an incident response program significantly helps to mitigate the impacts of a cyber event on operations and an organization's reputation.

7. As defined by the Computer Security Resource Center.

WHAT A COMPANY NEEDS TO DO TO PUT THIS CONTROL IN PLACE

Organizations are advised to encompass the following core capabilities in their approach to incident response planning and testing:

- The incident response plan must contain defined processes and procedures for performing cyber incident handling, reporting, and recovery.
- The incident response team members' roles, tasks, and responsibilities during a security incident must be clearly defined. Additionally, strong definitions of escalation paths and decision making processes/ responsibilities are obligatory.
- The parts of incident response that will be covered externally (such as IT forensic investigations) should be planned and documented, and the relevant contact information noted.
- Due to the significant uptick in ransomware incidents and their enormous loss potential, a specific response playbook tailored to the ransomware crisis scenario should be defined.
- Incident response plans are only valuable when the response team members are familiar with their roles and responsibilities, and when there is clarity on the underlying processes. An annual table top exercise should be conducted to train the team for specific scenarios, and to evaluate an organization's incident preparedness.
- Additionally, the plans need to be reviewed and updated periodically, incorporating recent developments, such as staff changes and new anticipated threats.

Businesses are operating in a world in which 95% of cybersecurity issues can be traced to human error.[8]

8. Mee, P. and Brandenburg, R. 2020: "After reading, writing, and arithmetic, the fourth 'r' of literacy is cyber-risk." World Economic Forum Global Agenda, December 17, 2020.

Cybersecurity awareness training and phishing testing

WHAT IS THIS CONTROL?

Cybersecurity awareness training is a control used to educate employees and IT users on cyber risks and threats. It helps them identify and recognize the various attacks, and equips them with the necessary information on how to protect themselves and their organizations by preventing events in the first place, and doing the right thing after an attack or an attempted breach.

Phishing testing is part of a security awareness training program which simulates phishing attacks by sending bogus, but very realistic, phishing emails to employees to measure their awareness. It tests the effectiveness of security awareness training, by evaluating employee reaction to the emails, and determines the behaviors that require further improvement.

WHY SHOULD THIS CONTROL BE ADOPTED?

Business is about people, process, and technology. Investing in securing process and technology is very important, but insufficient, if the human aspect is ignored. Businesses are operating in a world in which 95% of cybersecurity issues can be traced to human error.[8]

Despite very advanced IT security, human factors such as workload, stress, lack of skillset, the increased use of the hybrid working model, and basic human nature can all lead to human error. However, this weakest link of the security chain can turn into the best layer of defense, when it gets the right focus and attention.

The human element is also a concern for regulators. Some regulations — including, but not limited to, Payment Card Industry Data Security Standard (PCI-DSS), National Institute of Standards and Technology (NIST), HIPAA, and General Data Protection Regulation (GDPR) — may require employees to undergo regular security awareness training.

In order to establish a secure culture, make people part of the cybersecurity program, comply with regulations, and ultimately protect an organization from the impacts of a possible cyber incident, cybersecurity awareness training and phishing testing have become extremely important.

8. Mee, P. and Brandenburg, R. 2020: "After reading, writing, and arithmetic, the fourth 'r' of literacy is cyber-risk." World Economic Forum Global Agenda, December 17, 2020.

WHAT A COMPANY NEEDS TO DO TO PUT THIS CONTROL IN PLACE

Organizations should take the following actions when establishing cyber awareness training:

1. Perform an annual analysis to identify gaps in their cybersecurity skillset and develop and implement training roadmaps and/or project plans to close identified gaps.
2. Establish annual (at a minimum) cybersecurity training and a cybersecurity awareness program that:
   - Are mandatory for all employees, vendors/contractors, and third party partners with access to the corporate network.
   - Train users to avoid common cyber risks and threats, such as social engineering and phishing.
   - Provide frequent — at least annual — updated content to embody the latest attack and social engineering techniques.
3. Conduct, at least annually, internal phishing campaigns.
4. Have a process to report suspicious emails to an internal security team to investigate.
5. Have a process to respond to phishing campaigns.
6. Tag external emails to alert employees that the message originated from outside the organization.

NIST in the US also focuses on security awareness and training under the "protect function" of its cyber framework. For further guidance please see: "NIST Special Publication 800-50."

Remote desktop protocol (RDP) mitigation and other hardening techniques

WHAT IS THIS CONTROL?

Hardening is the process of applying security configurations to system components including servers, applications, operating systems, databases, and security and network devices, in line with best practices. These configurations are defined in order to reduce an organization's surface attack by limiting the exposure of each platform on the internal network or that may be facing to the internet.

WHY SHOULD THIS CONTROL BE ADOPTED?

Through hardening techniques, companies can minimize their attack surface by disabling unused or insecure services, mitigating vulnerabilities, and improving weak configurations that could be used by malicious actors to compromise their systems.

WHAT A COMPANY NEEDS TO DO TO PUT THIS CONTROL IN PLACE

Normally, organizations define a set of secure configurations for their main systems and services, based on best practices, commonly known as security baselines or hardening guides. A process is implemented to deploy these configurations, and review them periodically, in order to identify any misconfiguration or deviation.

Although they vary between each platform, the configurations that commonly are part of these security baselines may include the following:

- User and access management.
- Password policies.
- Secure services and protocols.
- Firewall configurations.
- Network configurations.
- Remote access.
- Log management and audit policies.
- Antivirus/antimalware protections.
- Application control.
- Security updates.
- Encryption.
- Other platform-specific security configurations.

To ensure the timely deployment of these configurations, organizations may use images of systems with security configurations or tools already applied and then perform a gap analysis periodically.

An important topic that insurers are concerned about is the exposure of weak or commonly attacked protocols or services to the internet, such as remote desktop protocol (RDP), server message block (SMB), secure shell (SSH), file transfer protocol (FTP), as well as database ports. Organizations need to have a strict hardening process in order to eliminate the usage of these kinds of ports exposed to the internet. If they are needed, as a result of a specific business requirement, organizations should implement compensating controls to mitigate the associated risk.

One of the most common barriers to implementing a hardening process is the absence of a comprehensive asset inventory, providing an organization with detailed knowledge of the technologies in place on the network, which may be supporting critical processes.

Organizations are advised to define a structured change management process to deploy these security baselines. Without a proper process, some of these arrangements may affect the availability of the systems by disabling configurations that are required at the moment of deployment. They may need a deeper analysis in order to find a secure method to function or may even require a change on an application. Today, vendors and cybersecurity organizations are constantly releasing security baselines for the most common systems and services. The Center of Internet Security (CIS) is one of the most important sources of baselines that all organizations can access.

Logging and monitoring

WHAT IS THIS CONTROL?

In order to react to a cyberattack in a timely manner, organizations need to establish strong logging and monitoring capabilities that enable them to identify any suspicious activity on the network. These capabilities require specific knowledge, tools, and processes to be able to detect malicious activities. All of these factors are normally executed by a security operations center (SOC) or an external managed security service provider (MSSP). The SOC or MSSP may include different capabilities, depending on their level of maturity and sophistication.

WHY SHOULD THIS CONTROL BE ADOPTED?

The current global threat landscape requires companies not only to implement a set of controls in order to protect their organizations from a cyberattack, but also to identify any suspicious activity that may indicate a potential attack in progress in a timely manner and that could trigger a cyberincident response plan. This can only be performed by an adequate logging configuration on the main systems and applications of the company, the appropriate tools to collect, correlate, and alert in case of a situation, as well as the right team capable of analyzing and acting in case of an incident.

WHAT A COMPANY NEEDS TO DO TO PUT THIS CONTROL IN PLACE

Companies are recommended to:

1. Outline and implement the audit logs and systems or platforms to be monitored, including firewalls, intrusion prevention systems and intrusion detection systems, active directory, antivirus/antimalware, endpoint security technologies such as EDR and XDR, data loss prevention (DLP), applications, Microsoft 365, and other important platforms defined by the organization.
2. Implement a security incident and event management system (SIEM) and integrate the main platforms into this system. Logs should be accessible for at least the last three months and backed up for a minimum of one year.
3. Analyze the logs in the network and define a set of use cases or common patterns that the organization would like to monitor and react to, in the instance that they are found. The information should also be used alongside threat intelligence information.
4. Define processes for reviewing, periodically, the administrators' or high-privileged users' activities on critical systems.
5. Define and train a team of professionals specialized in the monitoring of security events and incident response.
   - Specific processes or playbooks should be defined in order for the SOC and MSSP to react if a cybersecurity incident is detected. If this service is outsourced, these procedures should also include the tasks that the organization would need to execute in order to contain, eradicate, and restore the operations to normality.
   - Define and monitor key performance indicators for continuous improvement.

The development of adequate logging and monitoring capabilities may require significant investment and resources from the organization. Also, establishing these capabilities requires continuous review to ensure that the processes put in place are able to detect suspicious activities in real life scenarios.

Replacement or protection of end-of-life (EOL) systems

WHAT IS THIS CONTROL?

End-of-life (EOL) or end-of-support (EOS) products are those that reach the end of their lifecycle, preventing users from receiving updates. These products create risk because patches and other forms of security support are no longer offered by the vendor. Once the technology is unsupported, it will be exposed to unfixable vulnerabilities.

The only fully effective way to mitigate this risk is to stop using the obsolete product and replace or upgrade it with a newer solution that continues to provide support. Where this is impossible, EOL/EOS systems will need to be protected by compensating controls, such as restricting access to those systems, ensuring they are not internet facing, and are "air gapped" — that is, physically isolated from other connected systems.

EOL/EOS products and systems are often used by organizations with large legacy estates, particularly where systems are used to control operational technology (OT), which can be difficult and costly to upgrade regularly.

WHY SHOULD THIS CONTROL BE ADOPTED?

Vulnerabilities in EOL/EOS products will remain unpatched and become increasingly exploitable by hackers looking for easy ways to gain access to systems. Known vulnerabilities are openly discussed on forums, and hackers are able to scan easily for EOL systems that continue to be in use.

While open ports and email phishing remain popular attack vectors, known software vulnerabilities are also a common entry point, offering an easy route into systems. Once inside, hackers will try to gain access throughout a network, looking for valuable data to steal and systems to encrypt.

WHAT A COMPANY NEEDS TO DO TO PUT THIS CONTROL IN PLACE

Ideally, organizations should stop using any obsolete products. If this is unfeasible, it is essential to ensure that legacy systems are protected. Limiting access to these products from outside the environment is a critical step — if attackers cannot reach a device, the risk of exploitation is significantly reduced. Where possible, network air gaps should be implemented. If this is not possible, a discrete network firewall and monitoring of data flows to obsolete servers should be considered. A good rule of thumb is to treat all access from the internet as untrusted.

Steps can also be taken to limit the potential impact of compromise, such as preventing those EOL systems from accessing or storing critical and sensitive data or systems, meaning that a compromise of the EOL device would not be as damaging.

Upgrading EOL systems and products will come with a potentially hefty price tag. For organizations with significant legacy estates and operational technology systems, an EOL product may mean that the whole system needs to be overhauled, upgraded, or replaced.

Where organizations opt to continue to use the EOL product, the necessary protection and risk mitigation steps will require thorough implementation and will typically necessitate the collaboration of both the IT and OT security teams, and may also call for external expertise and tools. For manufacturers and other organizations with extensive OT systems, this implementation can be complex and time-consuming.

Digital supply chain cyber risk management

WHAT IS THIS CONTROL?

The digital supply chain encompasses all information technology (IT) and operational service (OT) providers that together with an organization's teams deliver digital services. In terms of cyber risk, the digital supply chain poses an increasing challenge. There have been instances of various large digital supply chain vulnerabilities having major effects — for example, the recent Log4J and Kaseya vulnerabilities, or breaches such as the hacking campaign Operation Cloud Hopper. Even the infamous NotPetya attack resulted from a digital supply chain risk.

A digital supplier can present the perfect entry point to hundreds of companies and their sensitive data. By successfully breaching a vulnerability within one single digital supplier, cybercriminals can gain access to a multitude of their clients' networks and devices.

A robust framework for managing digital supply chain cyber risk is required.

WHY SHOULD THIS CONTROL BE ADOPTED?

The continuously increasing digitalization and the use of information and communications technology to deliver critical functions has introduced new aspects of cyber risk that need to be managed. Organizations are consuming new and different digital services from various service providers, offering software packages to complete outsourced and software-as-a-service[9] products. At the same time, the fact that supply chains have become so global has created new risk, in terms of confidentiality, integrity, and availability.

Given the pervasiveness of digital services, it is becoming increasingly complex to manage the digital supply chain. IT teams may not be aware of all services consumed by the organization, caused by the issue of "shadow IT[10]." But also, it is not always apparent what exactly constitutes a service and the potential vulnerabilities embedded in it. Cybercriminals use these digital supply chains as a mechanism for cyberattacks. Indeed, most software products rely on thousands of prewritten packages produced by vendors. The most commonly used third-party software supply chain components are highly-prized targets for cybercriminals, as breaching one digital service provider can allow access to its many customers.

Hence, this control aims to protect the cyber risk heritage from digital suppliers by a set of activities focused on analyzing, managing and responding to the cyber risk.

9. Software-as-a-service (SaaS) is a software distribution model in which a cloud provider hosts applications and makes them available to end users over the internet.
10. Shadow IT refers to information technology programs, projects, or systems implemented outside of the IT or information security departments.

WHAT A COMPANY NEEDS TO DO TO PUT THIS CONTROL IN PLACE

Organizations are advised to consider the following actions to manage digital supply chain risk:

- Adopt a digital supply chain risk management framework, including risk rating of first tier vendors/suppliers, based on an advanced risk quantification. This will help an organization take strategic decisions on risk management and capital allocation.
- Implement a cybersecurity framework. This can include, but is not limited to:
  - Account management based on "zero trust" expectations and the "need-to-know" principle. Strict limitations of privileged and generic accounts apply.
  - Enforced appropriate risk-based multi-factor authentication (MFA).
  - Engagement with the internal security operations center to develop specific use cases for monitoring third party accesses.
- Develop and test an incident response playbook for vendor/digital supply chain scenarios and include third parties in this playbook.
- Assess contracts, service agreements, and escalation protocols for each vendor or digital supplier.
- Engage with the procurement department to include appropriate cybersecurity hygiene controls and responsibilities in new contracts and renewals. This can include security trainings and certifications.

Where to from here

At Victor, we believe the new cyber risk paradigm requires organizations to become more comfortable with the reality that the connective tissue of modern business is digital. As such, organizations need to adopt new methods of understanding, measuring, and managing cyber risk on a continuous basis. With discipline, foresight, and agility to shift focus, organizations can achieve improved outcomes, as we collectively embrace new cyber risks.

When an organization implements the recommended controls, they will either prevent, or be equipped, to respond to the majority of cyberattacks, in a way that minimizes their impact. They will be well prepared to defend themselves and feel more confident with their cyber resiliency. Given the current cyber landscape and the increasing threat to every organization, cyber resiliency can no longer be an afterthought or tick-the-box exercise — it has become a minimum requirement.

Learn more

Faster, smarter, stronger cyber coverage.

In an increasingly digitized world, no business can avoid cyber risks. When you experience cybercrime, business interruption and privacy threats, you need protection that's always looking to evolve.

Our Victor Cyber solutions provide far-reaching protection for small to medium-sized businesses to large organizations across Canada.

Visit victorinsurance.ca/cyber or email info.ca@victorinsurance.com.

About Victor

Victor Insurance Managers Inc. (Victor Canada) is a subsidiary of Victor Insurance Managers LLC and a leading managing general agent in Canada. Victor Canada has a rich history in specialty insurance, and offers a unique range of products and programs distributed through independent brokers and advisors. With specialized underwriting and claims expertise, the company provides a wide range of insurance solutions — from specialty property, casualty and professional liability insurance to group and retiree benefits.

For more information, visit: victorinsurance.ca.