GIBRALTAR®
DRIVING DIGITAL TRANSFORMATION

ebook

Cybersecurity Survival Guide

Everything you need to know to prepare and protect your digital estate

Are you operating with confidence?

In today's digital world, the volume of cyberattacks continues unabated. But, even more concerning, the technical sophistication of these attacks is also increasing. Due to these combined factors, cyberattack damage will amount to about $10.5 trillion annually by 2025[1]—a 300 percent increase from 2015. As a result, Microsoft includes security as one of five digital imperatives, urging organizations to prioritize their cybersecurity strategy and proactively protect their networks and data.

The challenge is that the security landscape is incredibly complicated; more numerous and advanced threats, more nebulous and complex compliance requirements, and more challenging and intricate infrastructure to secure. As a result, for even the most adept IT, cybersecurity can be difficult to manage.

In this eBook, we will help you navigate the top cybersecurity threats facing your organization and provide fundamental tips to ensure your organization is secure by design.

The Risks of Poorly Managed Cybersecurity

Operational Disruption

A cybersecurity incident can cause widespread disruption. It often makes accessing critical systems and services difficult or sometimes impossible. Every minute that your operations are offline is damaging to your company. It increases expenses, impacts your reputation and reduces employee productivity.

Financial Loss

A data catastrophe can be extremely costly. A single disaster can potentially force your company to close down due to ransoms, legal penalties from compromised personal information, and loss of income and productivity.

Legal Ramifications

Data breaches involving clients', partners' or prospects' personal information can lead to lawsuits against the affected company. In the case of regulated businesses, authorities may even restrict companies from carrying out certain operations until legal investigations are concluded.

Customer Retention

Nobody wants to do business with a company that is not secure. Unplanned downtime or data breaches can significantly damage your company's reputation and jeopardize its long-term viability.

TOP CYBERSECURITY THREATS

Cyber threats are malicious acts that seek to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property, or any other form of sensitive data. Cyber threats can come in many forms and from within an organization by trusted users or from remote locations by unknown parties.

MALWARE

Malware is harmful software that disrupts or manipulates an electronic device's regular operation. Malware can infect personal computers, smartphones, tablets, servers and even equipment — any device with computing capabilities.

75% of organizations experienced malware activity that spread from one employee to another[2]

How It Works

Malware typically infects a machine by tricking users into clicking or installing a malicious program from the Internet. When the click or installation occurs, the malicious code executes actions that the user doesn't anticipate or intend, which could include:

- Self-replication in different parts of the file system
- Installing applications that capture keystrokes or commandeer system resources, often running without the user being aware, while slowing the system down considerably
- Blocking access to files, programs or even the system itself, sometimes forcing the user to make a payment to regain access
- Bombarding a browser or desktop with ads
- Breaking essential system components and rendering a device inoperable

Types of Malware

A virus attaches to a program or document and reproduces itself, spreading from one file or program to another and, less frequently, to other computers on a network.

Trojan horses masquerade as harmless programs, but when activated, they damage their host computer. Unlike a virus, a Trojan horse does not replicate itself; this malware usually attempts to steal files or passwords.

Worms replicate themselves to spread through a network. A computer worm will spread across computer networks, unlike viruses that usually spread from file to file on a single computer.

Spyware infects and operates on a user's computer to monitor user activity, extract personal data without consent, and relay it to advertisers, data firms or external users.

Rootkits allow users to maintain privileged access and control within a system and remain undetected.

Ransomware encrypts a user's files and data, rendering them inaccessible until the user pays a ransom.

Adware displays unwanted pop-up advertisements on a user's device intended to generate clicks.

PASSWORD ATTACKS

A password attack is when cybercriminals attempt to guess or brute force their way into a victim's account by trying different combinations of usernames and passwords.

81% **of hacking related breaches are a result of compromised passwords[3]**

How It Works

Cybercriminals often implement various techniques to exploit personal passwords, including brute force, guessing, and more. Once the attacker solves the password, they use that information to log into the user's account (typically multiple accounts) and gain access to their personal data to use or share with external sources.

Types of Password Attacks

Credential Stuffing is when an attacker attempts to access an online account using previously leaked credentials from a different account. For example, the attacker will use a list of credentials from a data breach to log into multiple accounts on the same website or service.

Keyloggers is a program that records every keystroke a computer user makes to gain fraudulent access to passwords and other confidential information.

Man-in-the-Middle attacks are when a perpetrator is positioned between the user and the system to intercept and alter personal data in transit.

Brute Force attacks use trial and error to crack passwords, login credentials, and encryption keys.

Dictionary attacks filter through common words and phrases that users might incorporate into their passwords.

Password Spraying is when a hacker attempts to log into accounts using commonly used passwords such as 'Password1.'

Rainbow Table attacks take advantage of precomputed hashes to crack passwords. The attacker creates a database of plaintext passwords with their corresponding encrypted hashes, which are then used to speed up attempts to crack passwords.

PASSWORD SECURITY TIPS

Use Complex Passwords
Set Minimum Password Length
Utilize Passphrases
Mandatory Password Resets
Restrict Password Reuse
Set Min and Max Password Age Limits
Establish Password Audits
Send Reminders

SOCIAL ENGINEERING

Social engineering uses influence, persuasion and observation to trick users into revealing personal information about themselves, which the hacker then uses for fraud.

98% **of cyber attacks involve some form of social engineering[4]**

How It Works

Social engineering aims to exploit the victim's personal interests or emotional intelligence. This technique tricks the victim into revealing sensitive information or performing actions to help the cybercriminal access systems or data.

For example, a cybercriminal may use fear by convincing the victim they are under criminal investigation for tax fraud or empathy by requesting the victim provide login credentials quickly. Otherwise, employees will not be paid this week.

Types of Social Engineering

Baiting uses a false promise to pique a victim's greed or curiosity. Then, they lure users into a trap that steals their personal information or inflicts their systems with malware.

Scareware bombards victims with false alarms and fictitious threats. As a result, users are deceived into thinking their system is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or is malware itself.

Pretexting is when an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim to perform a critical task.

Phishing uses emails, texts, or other forms of communication that ostensibly comes from a trustworthy entity (such as a bank or known company) to trick users into providing personal information or downloading malware.

Tailgating is when a hacker follows an authorized person into a password-protected or otherwise off-limits physical location.

$130,000

The average cost of a social engineering attack as a result of money theft or data destruction[4]

ZERO DAY EXPLOITS

A zero-day exploit is when hackers take advantage of a software program's vulnerability before developers can address it, allowing them to steal information, launch denial-of-service attacks, and disrupt operations.

80% of successful breaches were Zero-Day attacks in 2021[5]

How It Works

Zero-day attacks exploit many vulnerabilities — including buffer overflows, broken algorithms, URL redirects, SQL injection, and password security issues. Once a hacker identifies a security flaw, they quickly determine the most efficient plan of attack and develop a malicious program to exploit it. Then, they infiltrate the system, remotely executing false code to compromise the machine.

Common System Targets

Operating Systems: The most attractive target for zero-day attacks due to their ubiquity and the possibilities they offer attackers to gain control of user systems.

Web Browsers: An unpatched vulnerability can allow attackers to perform drive-by downloads, execute scripts or even run executable files on user machines.

Office Applications: Malware embedded in documents or other files often exploits zero-day vulnerabilities in the underlying application used to edit them.

Open Source Components: Some open source projects are not actively maintained or do not have sound security practices. Software vendors may use these components without being aware of their vulnerabilities.

Watering Holes: Software programs widely used by organizations or home users are under scrutiny by attackers who search for unknown vulnerabilities.

Hardware: A vulnerability in a router, switch, network appliance, or a home device such as a gaming console, can allow attackers to compromise these devices, disrupting their activity or using them to build massive botnets.

Internet of Things (IoT): Connected devices, from home appliances and televisions to sensors, connected cars and factory machinery, are all vulnerable to zero-day attacks. Many IoT devices do not have a mechanism for patching or updating their software.

DDOS ATTACKS

A DDoS attack is when a cybercriminal attempts to take down websites, slow down and crash the target servers and make online service unavailable by flooding them with traffic from multiple sources. These attacks often target popular or high-profile sites, such as banks, news and government websites, to thwart or deter target organizations from publishing important information or weaken them financially.

67% **increase in ransom DDoS attacks in 2022[6]**

How It Works

DDoS leverages hundreds or thousands of infected "bot" computers located all over the world. Known as botnets, these armies of compromised computers will execute the attack simultaneously for full effectiveness. The hacker or group of hackers that control these infected computers become botmasters, infecting vulnerable systems with malware, often Trojan viruses. When enough devices are infected, the botmaster gives them the command to attack and the target servers and networks are bombarded with requests for service, which in turn effectively chokes them and shuts them down.

Common Red Flags

Symptoms of a DDoS attack can resemble non-malicious availability issues, such as technical problems with a particular network or a system administrator performing maintenance. However, the following symptoms could indicate a DoS or DDoS attack:

- Unusually slow network performance
- Unavailability of a specific network service or website
- An inability to access any website
- An IP address makes an unusually large number of requests in a limited timespan
- Server responds with a 503 error due to a service outage
- Log analysis indicated a significant spike in network traffic
- Odd traffic patterns, such as spikes at odd hours of the day or practices that appear to be unusual

Notable DDoS Attack in History

To date one of the most significant DDoS attacks happened in 2018 against online code management system GitHub. GitHub was hit by an onslaught of traffic, which at its peak clocked in at a rate of 1.3 terabytes per second, sending packets at a rate of 126.9 million per second. In this attack, the botmasters flooded memcached servers with spoofed requests, which gave them the ability to amplify their attack by 50,000x. Fortunately, administrators were alerted to the attack and it was shut down within 20 minutes.

REMOTE WORK VULNERABILITIES

As the COVID-19 pandemic swept the world, most organizations quickly transitioned to a remote workforce and focused more on serving customers through digital channels. However, while this digital transformation has many benefits, like improved employee morale and productivity, it also opened a pandora's box of security vulnerabilities.

61% **of organizations experienced a jump of 25% or more in cyber threats or alerts since the start of COVID-19[7]**

The increased adoption of hybrid work models means security teams are continually challenged to keep users connected and networks secure. Securing devices is a growing problem for organizations now as they're unable to rely on connecting endpoints to campus networks for visibility and pushing updates. At the same time, employees are connecting to corporate resources with more personal, unmanaged devices, which creates blind spots for security teams.

Types of Remote Work Vulnerabilities

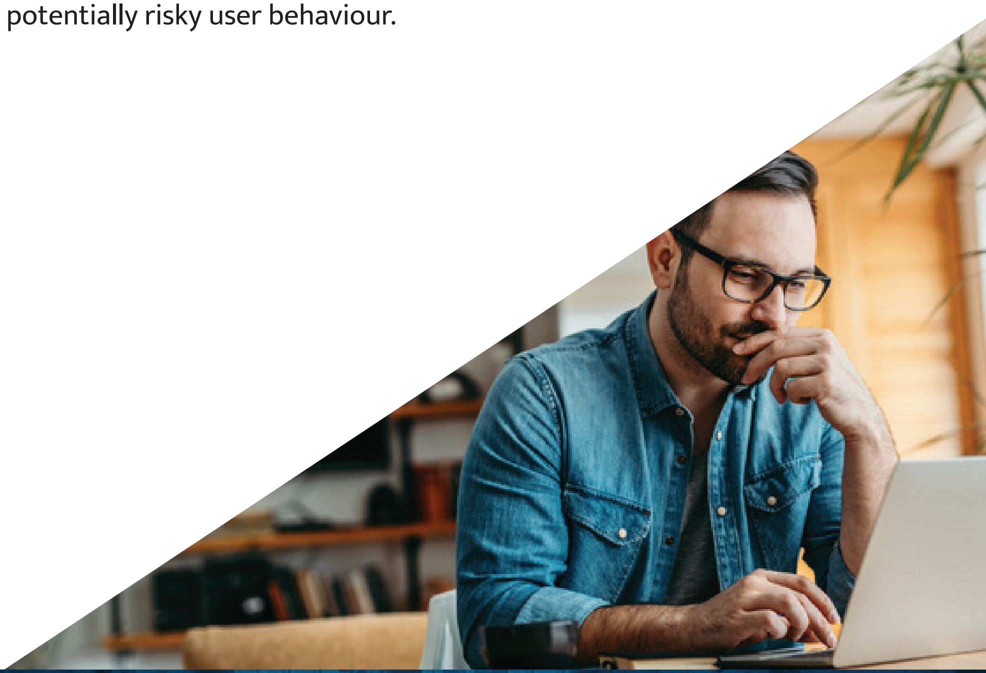
Unsecured Wi-Fi Networks: Accessing corporate data and systems from poorly secured public or home Wi-Fi networks could open a corporate network to unauthorized access.

Bring Your Own Device: The increasingly common practice of using personal devices such as laptops or smartphones for work creates a proliferation of devices that may not adhere to corporate security protocols.

Human Factors: Employees who lack an understanding of security risks may be susceptible to cyber attacks such as phishing scams. Likewise, distracted employees could unknowingly publicly expose their login credentials or lose their devices.

Lack of Training: A lack of remote work security awareness and training. Employees not trained in security best practices are more likely to use weak passwords and expose their company to risks in other ways.

Decreased Visibility: When employees work in remote locations, the IT staff lacks visibility into the endpoints employees use and potentially risky user behaviour.



CYBERSECURITY CHECKLIST

With the ever-growing threat of online security breaches, businesses must maintain a robust security posture. Whether you’re a small business just starting or an established enterprise, this comprehensive cybersecurity checklist provides essential steps to help protect your business from the latest cyber threats.

1 Conduct a Cyber Risk Assessment

The first step to mitigating cybersecurity risk is to complete a cybersecurity risk assessment. Risk assessments seek to answer various information about your technologies, operations, assets and people. This will help you identify vulnerabilities, gaps, and loopholes in your current security architecture and help you understand the measures you need to take to protect your business-critical assets.

A cybersecurity risk assessment may be split into many parts, but the five main steps are as follows:

Scope: Identify the assets that define the scope of this assessment (i.e. servers, databases, key people, sensitive documents)

Threats: Identify the tactics, techniques, and methods used by threat actors that have the potential to cause harm to your organization's assets.

Vulnerabilities: Identify threats an actor can exploit to perform unauthorized actions such as data theft, modification, deletion or further infiltration. Use network penetration testing, web application penetration testing, mobile pen tests or vulnerability assessments.

Risk Impact: Determine the likelihood of a given threat exploiting a given vulnerability.

Prioritize & Recommend: Prioritize risks by giving each vulnerability a risk rating so that you can prepare your remediation plans.

Document: Record each threat, vulnerability, value, mitigation step, and ownership to keep track of the progress and for future reference.

2 Implement Zero Trust

The Zero Trust approach is the most effective security control. This security framework entrenches the principle of "never trust, always verify." Every activity within the organizational network undergoes thorough, ongoing security checks, with strict permission settings ensuring verified access only to sensitive data. In addition, Zero Trust leverages robust authentication methods, network segmentation, "least privileges" policies, and layered threat prevention techniques to prevent threat actors from moving laterally across a network at ease and speed.

Key Defense Areas

Identity: Zero Trust starts with identity, verifying that only the people, devices and processes granted access to your resources can access them.

Endpoints: Next comes assessing the security compliance of device endpoints – the hardware accessing your data – including the IoT systems on the edge.

Applications: This oversight applies to your applications, too, whether local or in the cloud, as the software-level entry points to your information.

Network: Next, there are protections at the network layer for access to resources – especially those within your corporate perimeter.

Infrastructure: This includes data hosted on on-premises or in the cloud – physical or virtual, including containers and micro-services and the underlying operating systems and firmware.

Data: And finally, data protection across your files and content, as well as structured and unstructured data wherever it resides.

3 Limit the Number of Network Admins

No employee outside your IT department should be able to change details about the network or install applications outside your company's approved list. Limiting the number of network administrators will significantly reduce security risks and give your company more visibility over its devices.

60% **of data breaches are caused by insider threats**[8]

4 Audit Disabled Accounts

Whether it's an email account, marketing and sales tool or software developer program, work accounts may be disabled for various reasons. Unfortunately, disabled accounts provide security risks since malicious actors can access them along with all permissions and privileges. Your system administrator should audit and delete accounts from employees who have switched roles or responsibilities or are no longer employed by the organization.

5 Keep Software Up-to-Date

It is critical to identify endpoints that require updates and patches made to the OS, applications, and security software they have installed or need to have installed. The most up-to-date security software will aid in blocking and removing malware from your endpoints. In addition, vulnerability patches from OS and app vendors are only effective if your endpoints are kept up to date regularly.

6 Execute a Patch Management Program

Cybercriminals constantly evolve their methods and search for new ways to infiltrate your systems. Therefore, a formal and proactive patch management strategy is critical. Patch management ensures you upgrade, optimize, or secure existing software, computers, servers, and technology systems before hackers can exploit them to mitigate cybersecurity risk, maintain compliance and ensure business continuity.

7 Conduct Regular Penetration Testing

Penetration testing is an authorized simulated cyberattack to access or exploit your computer systems, networks, websites, and applications. The primary purpose of penetration testing is to identify exploitable issues and implement adequate security controls. However, you can also use penetration testing techniques to test the robustness of your security policies, regulatory compliance, employees' security awareness, and ability to identify and respond to security issues and incidents such as unauthorized access.

8 Perform 24/7 Network Monitoring

Routers, switches, virtual servers, wireless devices, and applications need 24/7 network monitoring. Continuous network tracking and traffic monitoring can reveal early indications of cyberattacks, such as unexpected traffic, unknown devices and uncharacteristic application usage. These tools enable the organization to proactively contain threats and limit damage during the early stages of an attack.

$682,000

The amount your company can save with cybersecurity prevention[9]

9 Ensure Automatic Computer Lock Screens

Whether working remotely or at the office, your employees should turn off their work devices manually or set up an automatic screen lock that activates within a few minutes of inacvtivity. Locking your display screens will help prevent unauthorized users from accessing the device and your network in extension.

10 Establish a Robust Password Policy

A password policy is a set of rules and regulations dictating how employees should create and use passwords. Password policies outline requirements such as minimum length, composition and complexity, expiration dates, storage, etc. Creating and implementing a comprehensive password security policy will help secure your organization's assets.

11 Implement Multi-factor Authentication

Multi-factor authentication (MFA) offers considerably more security than the traditional single password. This cybersecurity measure requires users to provide multiple factors verifying their identity before accessing a network, account, or online operating system. For example, MFA users must provide a password and verify access by inputting a code (often sent to another device) or confirming access with biometric data, such as a fingerprint or facial recognition.

99.9% **of modern automated cyber attacks are blocked by MFA**[10]

12 Install a Network Firewall & Antivirus

A network firewall is essential for your business because it can stop hackers from accessing sensitive information, disrupting operations, or holding your company's ransom for data. In addition, it can also help you monitor employee activities and ensure compliance with corporate policies.

It is also essential to protect your devices from viruses and malware. Antivirus software is a low-cost way to secure your technical assets and avoid expensive problems in the future.

13 Data Encryption & Backups

A data breach or ransomware attack is still possible despite all security efforts. If this happens, your company needs the ability to restore data quickly. To ensure business continuity, you should perform regular verified, air-gapped backups and enable encryption for sensitive data and critical applications, whether on-prem or in the cloud.

14 Develop an Incidence Response Plan

Some cyber events can lead to massive network or data breaches that can impact your organization for days or months. Therefore, you need a well-documented, detailed course of action to stop, contain, and control the incident quickly. An incident response plan ensures the right personnel and procedures are in place to deal with a threat effectively.

15 Educate Employees

Security awareness training should not be overlooked on your cybersecurity checklist. Employees will always be the weakest link in every cybersecurity program. Regular Security Awareness Training helps educate and empower your team to prevent and detect common cyber threats. It also cultivates a robust security-aware mindset and culture that prioritizes protecting sensitive information so you can feel confident that your team can quickly adapt to the ever-changing, complex world of cyber threats.

52% **of data breaches at small businesses are attributed to employee error[11]**

16 Keep Up with the Latest Security Threats

Staying current on cybersecurity news is not just about knowing where the latest data breach happened. It also requires following the rapid changes in the industry and knowing which companies are at the forefront of information security. Staying on top of cybersecurity news also helps security teams ensure their teams are well-informed and aware of emerging threats. Knowing what's happening in the cyber industry today helps your team prepare for tomorrow.

17 Consider a Managed Service Provider

Managed security services are an excellent way for organizations that need more expertise or in-house resources to better plan, monitor and secure their digital estate. From 24/7 systems monitoring and proactive threat detection to compliance management and disaster recovery, MSPs provide a complete security solution to defend your organization and help minimize cybersecurity-related costs.

Benefits of Managed Services Provider

Managed security services, offered by an MSP is a highly effective strategy for businesses that need help monitoring and defending their networks without draining in-house resources. Here are a few key benefits of managed security services:

✓ Access to Seasoned Experts & Innovative Technologies

MSPs offer a range of security experts certified and well-versed in the latest threats and technologies to ensure your company is always secure.

✓ Save Money and Improve Productivity

You can retain an MSP at a fraction of the cost of training and certifying a security team in-house. MSPs can also free your staff members to focus on their core roles and responsibilities.

✓ 24/7 Proactive Threat Detection

With advanced 24/7 monitoring and threat intelligence, managed security services constantly hunt for malicious activities that might attack your network in the future.

✓ Faster Incidence Response

MSPs provide a wealth of knowledge and experience in handling threats and can act fast in the event of a cyber incident. Even a few seconds between threat detection and response could make all the difference in an attack's severity.

✓ Scalability

MSPs adapt to the ever-evolving needs of your business. Your company can quickly scale up with an already trained and knowledgeable team that can handle the dynamic volume of business.

✓ Guaranteed Compliance

MSPs are experts in risk management and compliance who can implement specific security controls and ensure your organization's compliance with ever-evolving regulations.

Prepare & Protect Your Digital Estate with Gibraltar

Whether you're challenged with overcoming skills shortages, fighting new threats or are looking for more efficiency, Gibraltar Managed Security Services helps you strengthen your environment quickly and become more resilient over time.

Sources
https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers
https://www.mimecast.com/resources/ebooks/the-state-of-email-security-2022/
https://enterprise.verizon.com/resources/reports/dbir/
https://firewalltimes.com/social-engineering-statistics/
https://www.illumio.com/cybersecurity-101/zero-day-attacks#:~:text=According%20to%20the%20Ponemon%20Institute,breaches%20were%20Zero%2DDay%20attacks.
https://www.infoq.com/news/2023/02/cloudflare-ddos-attack/#:~:text=The%20number%20of%20volumetric%20attacks,a%20peak%20in%20November%202022.vv
https://umbrella.cisco.com/info/ebook-how-modern-security-teams-fight-todays-cyber-threats?utm_medium=search-paid&utm_source=google&utm_campaign=UMB_23Q3_NA_EN_GS_Nonbrand_Threats&utm_content=UMB-FY22-Q3-Content-Ebook-How-Modern-Security-Teams-Fight-Todays-Threats&_bt=648480029902&_bk=security+risks+of+remote+working&_bm=p&_bn=g&_bg=122023015112&gclid=CjwKCAiAjPyfBhBMEiw
AB2CCIvW4bkU6TgcDZ7WX2GLyahUqN89Rbfe3UVlnXzvFDiHGUGCMwsHpIxoCluwQAvD_BwEv
https://financesonline.com/insider-threat-statistics/#:~:text=In%20the%20US%2C%20the%20most,%25)%20(Securonix%2C%202020).
https://www.techrepublic.com/article/cybersecurity-prevention-can-save-your-company-682k/
https://www.zippia.com/advice/mfa-statistics/#:~:text=Between%202017%2D2021%2C%20the%20MFA,skyrocketed%20to%2078%25%20of%20accounts.
https://www.electric.ai/blog/cybersecurity-statistics

GIBRALTAR®

☎ 1-877-895-2474 ✉ info@gibraltarsolutions.com