Greenlight
INFORMATION SERVICES

7 CYBERSECURITY TRENDS YOU NEED TO KNOW ABOUT

INTRODUCTION

Maintaining a solid understanding of current cybersecurity trends is crucial for safeguarding an organization's data and privacy. Cyberattacks can range in scope and impact from targeted attacks on individual team members to large-scale breaches affecting an entire organization. The consequences of these attacks can go from disruptive to devastating, as exemplified by the 2013 Target data breach, which resulted in the theft of 40 million credit and debit records and a $18.5 million settlement for the company.

As more businesses digitize their operations and remote work becomes increasingly prevalent, the volume of sensitive information being processed and stored online continues to grow. This article will review the top seven current cybersecurity trends and discuss how organizations can safeguard themselves online.

1 ANTICIPATED RISE IN TARGETED RANSOMWARE ATTACKS

Ransomware attacks have been a persistent threat for some time, but the sophistication of the technology used has increased, leading to more significant risks for businesses. Ransomware is a type of malware that seeks to exploit the victim's data by threatening to publish it or block access to their computer system or digital platform unless a ransom is paid. In recent years, targeted ransomware attacks have become more prevalent and show no signs of slowing down.

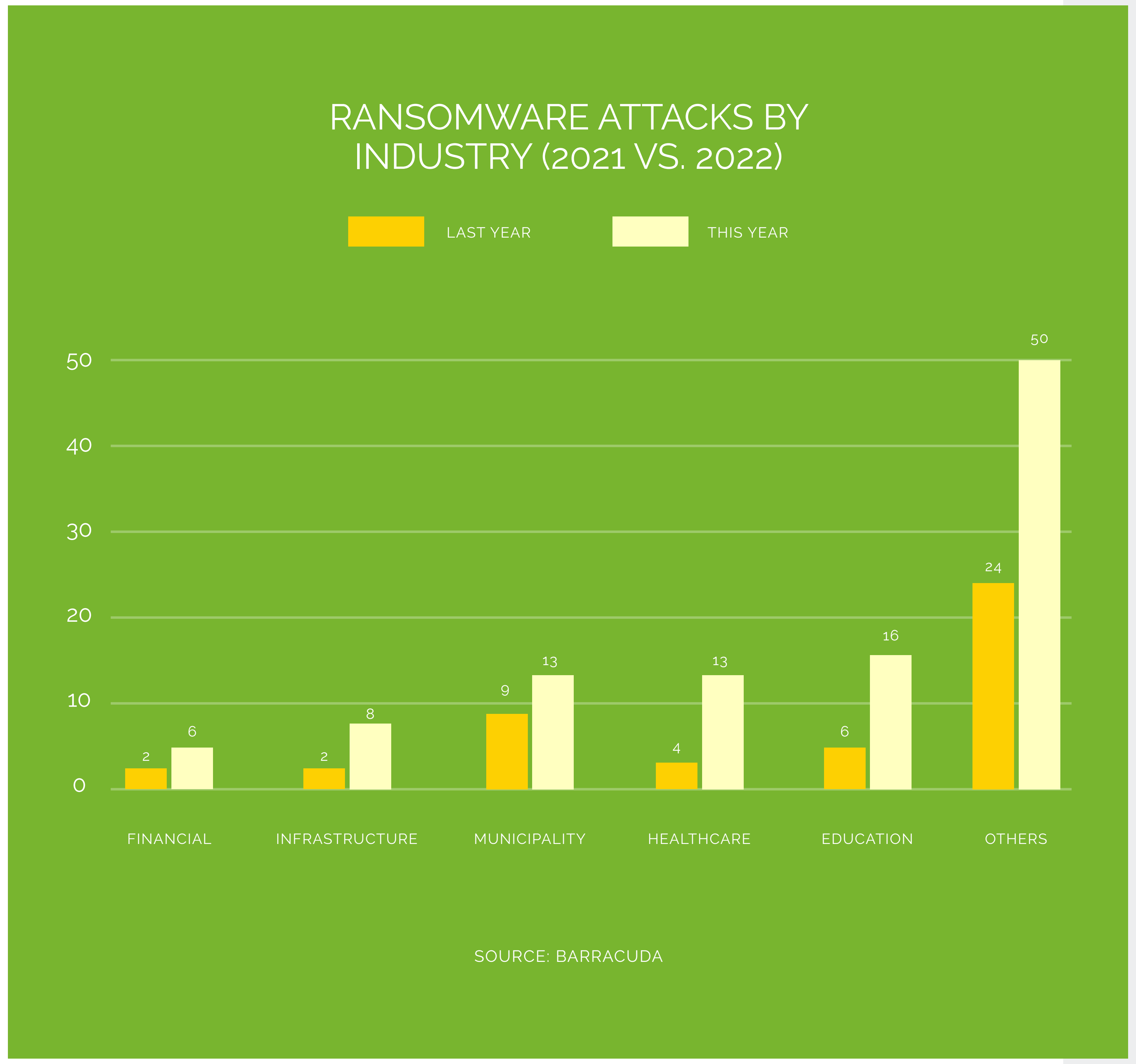
Ransomware attacks on organizations can compromise privacy and data, causing long-term damage and shutdowns. It is essential for businesses to protect against this threat.

Ransomware attacks have experienced a significant increase since the onset of the pandemic, with one report indicating a 105% growth in attacks in 2021. This trend is expected to continue in the foreseeable future. To protect their operations, business leaders should stay informed of the following emerging types of ransomware attacks:

Supply Chain Ransomware Attacks are a growing threat, where attackers target third-party vendors or suppliers to gain access to a company's systems and data. They use ransomware to encrypt files and demand a ransom payment. These attacks can cause significant damage as they exploit trust in vendor relationships and can rapidly spread through the entire supply chain.

Double Extortion Ransomware Attacks typically involve infiltrating a system, encrypting information, and demanding a ransom payment in exchange for a decryption key. However, some attackers are now taking this a step further by threatening to leak sensitive data to the public if the ransom is not paid. This not only increases the financial stakes, but also adds the risk of litigation and reputational damage to the victim.

Ransomware-as-a-Service (RaaS) platforms have made it much easier for attackers to conduct ransomware attacks without needing to write their own code. These pay-for-use platforms provide users with the necessary malware and instructions to launch attacks.



SOURCE: BARRACUDA

In 2022, various industries including financial services, education, and others recorded a minimum of 50% increase in ransomware attacks when compared to the preceding year. Some sectors even experienced more than double the number of attacks compared to 2021.

To protect against targeted ransomware attacks, organizations can take the following steps:

Install the latest security updates and maintain up-to-date security software.

Implement a solid backup and recovery strategy that includes air-gapped and immutable backups. Air-gapped backups are physically disconnected from the network, making them harder to access. Immutable backups are stored in read-only format, so they cannot be modified or deleted, providing multiple layers of protection for data and increasing the chances of successful data restoration.

Adopt Managed Detection and Response (MDR) for continuous monitoring, threat detection, and incident response for your organization. It uses advanced technologies to identify suspicious activity and respond to security threats.

Conduct a cybersecurity audit to identify and address any vulnerabilities in the organization's systems and defenses.

Educate employees on cybersecurity and user safety to help prevent them from falling victim to phishing attacks or other tactics used by attackers.

By taking these steps, organizations can significantly reduce their risk of falling victim to a targeted ransomware attack and minimize the potential impact on their business.

2 INCREASED DIFFICULTY IN DETECTING GEO-TARGETED EMAIL PHISHING THREATS

Geo-targeted phishing attacks have become a prevalent threat in recent years, posing a persistent security risk for organizations and placing additional strain on IT departments. Employees are frequently targeted through phishing email scams, which can result in significant data breaches and security issues if not adequately addressed. To protect against these threats, businesses must be aware of current phishing email trends and implement appropriate measures to prevent them.

Phishing attacks that are tailored to specific individuals or groups by using criteria such as location, industry, and language are becoming increasingly common. These attacks typically use language and terminology that mimic familiar brands and even impersonate colleagues, making the scam more convincing and effective. In a similar way to how companies adapt their marketing and advertising campaigns or products for specific regions, attackers have begun to adopt this strategy. They are designing malware increasingly tailored to their intended targets, making it more challenging for victims to detect.

Phishing is a social engineering attack involving a perpetrator posing as a trusted entity to trick the victim into opening an email or clicking on a malicious link. The victim may then be tricked into divulging sensitive information, or triggering a ransomware attack that blocks access to the system.

47.3% of all the emails sent in 2021 are phising emails

Standard phishing emails are often designed to appear as if they are coming from platforms and services that businesses use on a daily basis, such as Microsoft, Google Docs, invoice providers, and work email providers. Some scammers will conduct research on a company's structure and send emails from fake accounts that appear to belong to high-level individuals, including the CEO. These emails may request sensitive information or access to data that the scammer can use for a ransomware attack.

Sophisticated phishing attacks may include branding, sender email addresses, and content that appears professional and almost identical to the imitated brand. However, upon closer inspection, certain elements may not match the authentic brand's information. As cybercriminals continue to evolve, so do the quality and frequency of their attacks. In 2021, nearly half of all emails sent were phishing emails.

A common technique used by IT and cybersecurity professionals is to block access to their systems from specific countries through the use of Geo-IP filtering. However, cybercriminals are increasingly using VPN services to proxy their connections through the United States to evade these protections, making them less effective.

Additionally, attackers may use geo-targeting phishing, which tailors the scam to specific countries or regions and makes it more believable to the target. This method potentially bypasses geofencing software and may include using specific language or IP addresses.

During the first quarter of 2022, global phishing attacks revealed that financial institutions were the most targeted industry, accounting for 23.6% of all attacks. The second most targeted industry was Software as a Service (SaaS), which accounted for 20.5% of attacks during the same period.

There are several measures that organizations can take to protect themselves from phishing attacks, including:

Train employees to spot phishing attacks and regularly update them on new phishing attack trends. All employees should be aware of the common tactics used in phishing attacks, including geo-targeting tactics. This includes using fake login pages, urgent requests for sensitive information, threats of account deactivation, fake invoices or purchase confirmations, attackers pretending to be well-known brands, etc.

Use spam filters to help block phishing attempts from reaching employees' inboxes. Organizations can also use web filters to prevent employees from accessing known phishing websites.

Regularly review and update security policies and train all employees on any security policy updates.

3 IOT DEVICES ARE AT RISK OF INCREASED ATTACKS

IoT (Internet of Things) refers to the interconnectivity of physical devices and objects embedded with electronics, software, and connectivity, enabling the exchange of data. In a business context, common examples of IoT devices include routers, cameras, and security systems. However, these devices are also vulnerable to cyberattacks, and a study has found that 60% of IoT devices are vulnerable to attacks despite not being widely discussed as other types of cyber threats.

The security threat from IoT devices lies in the possibility of hackers gaining control over the device and using it to access and potentially compromise the network it is connected to. This can pose a major risk to an organization's data security. To mitigate this risk, organizations should be aware of the specific vulnerabilities associated with each IoT device, ensure that all devices are adequately secured, segment networks to isolate IoT devices from company systems, and stay informed about the latest IoT cybersecurity threats and alerts.

As the use of these devices continues to grow, it is likely that they will become a bigger target for cyberattacks in the coming years. To combat this risk, companies must invest in IoT cybersecurity. If these devices are compromised, it could lead to data theft and even more dangerous situations, For example, if a hacker were to gain access to a company's network through a compromised IoT device, such as a connected security camera, they could potentially steal sensitive information or disrupt operations.

Organizations may not be aware that the following standard IoT devices are vulnerable to attacks:

- ✓ Security cameras and systems
- ✓ Voice assistant devices (e.g., Alexa)
- ✓ Wireless printers
- ✓ Routers
- ✓ Smart lighting systems
- ✓ Smart doorbells
- ✓ Wireless speakers
- ✓ Smart HVAC systems

TOP IOT THREATS

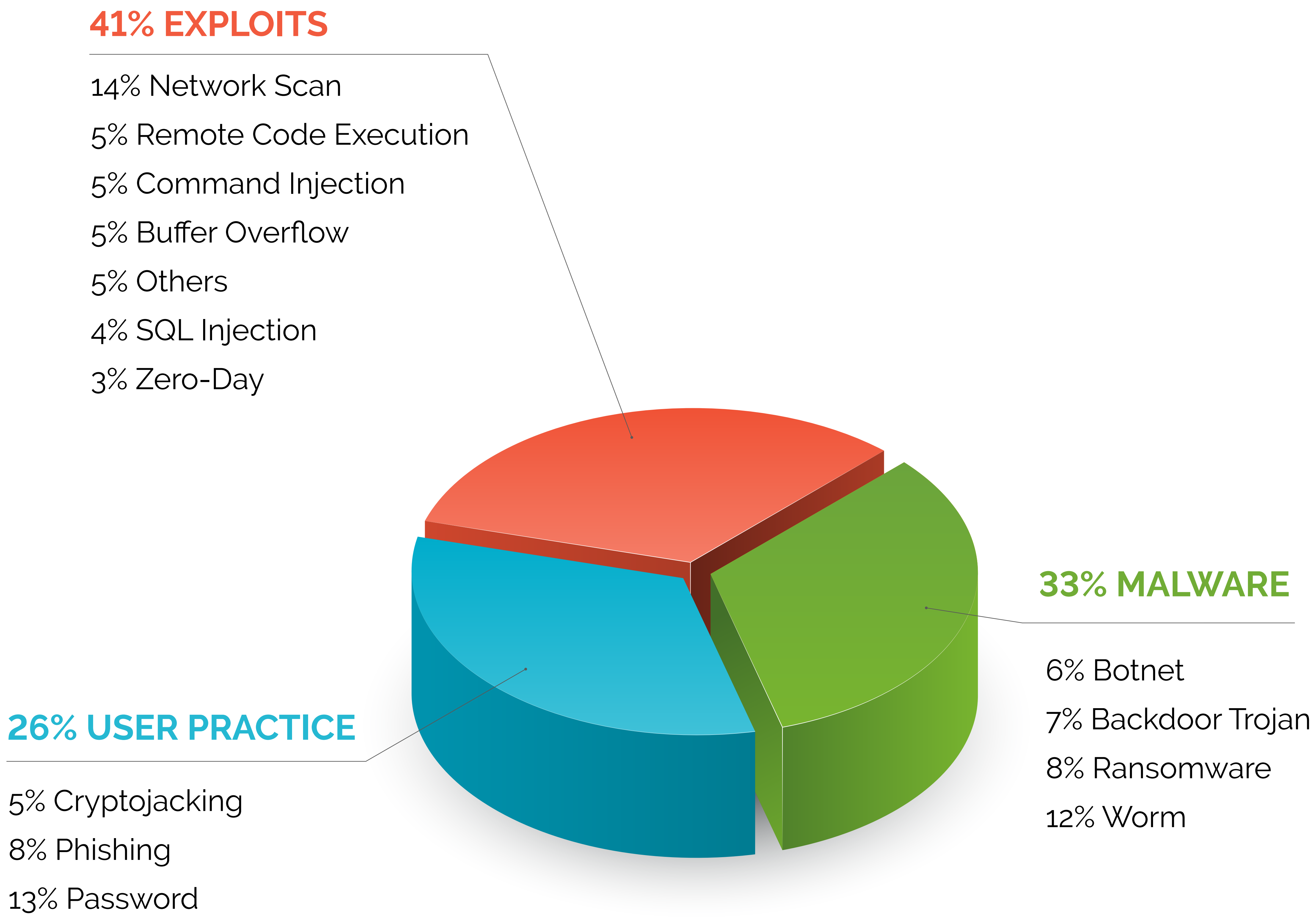
Hackers are continuously finding new ways to attack IoT devices, including using peer-to-peer command and control communications and worm-like features for self-propagation, as well as exploiting weak device and network security.

✓ 57% of IoT devices are vulnerable to medium- or high-severity attacks. This makes them an attractive target for attackers.

✓ 41% of attacks exploit focus on exploiting vulnerabilities in devices, with IT-borne attacks specifically targeting known weaknesses by scanning through network-connected devices.

IoT devices are frequently used for attackers to move laterally within a network, and password-related attacks remain common due to weak manufacturer-set passwords and poor security practices. However, the implementation of California's SB-327 law in 2020, which prohibits the use of default credentials, may lead to a change in this trend.

There has been a shift in the primary motivation of attackers away from using IoT devices to run botnets and conduct DDoS attacks towards using them to spread malware across networks using worm-like features to carry out new attacks.



To protect against cyber attacks, organizations can take the following steps to secure their IoT devices:

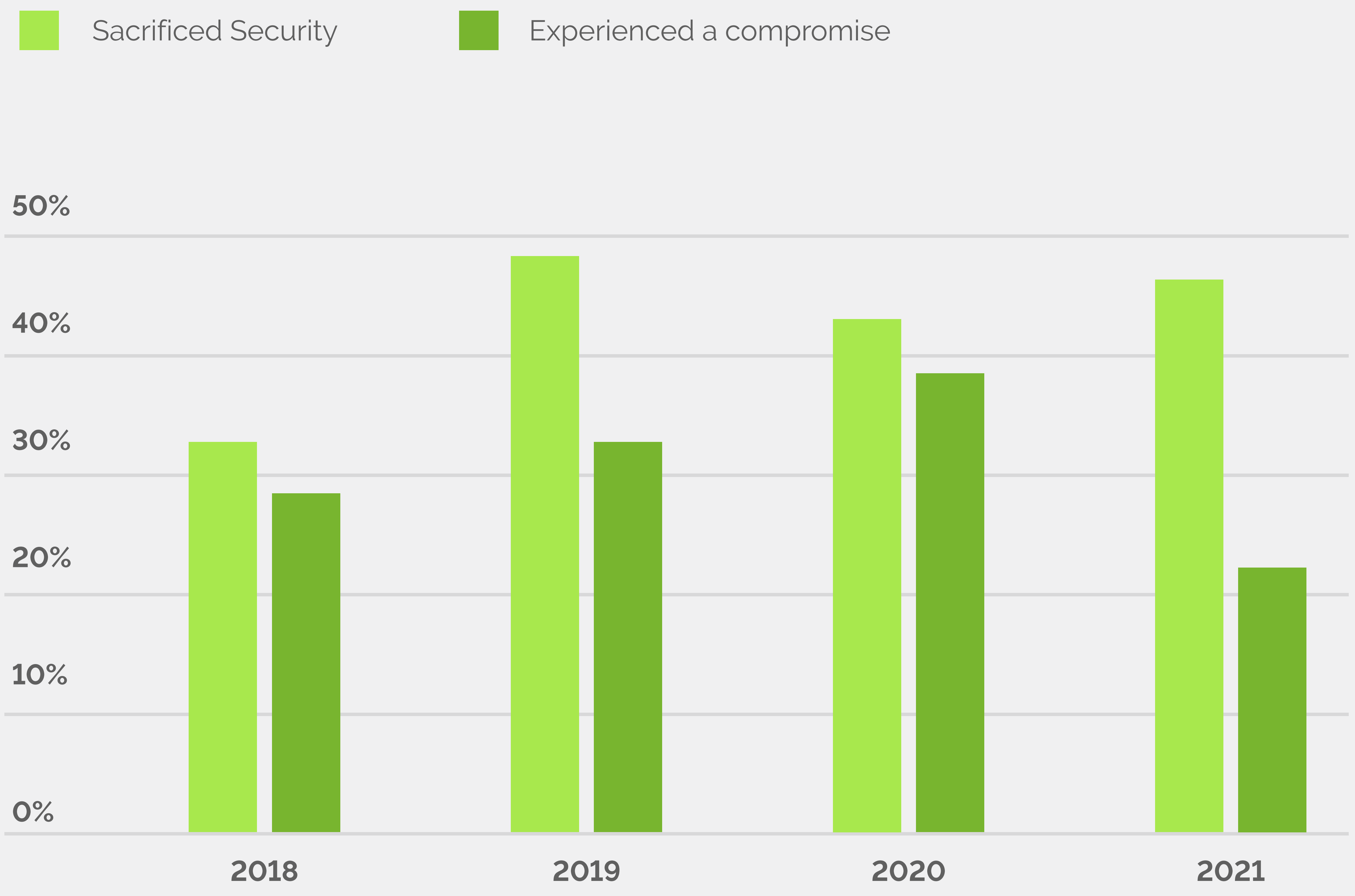
- ✓ Change any default device settings, including the name of the device, any privacy and security settings, and especially any default passwords.
- ✓ Disconnect IoT devices when they are not in use, and learn about the features of each device and which ones need to be connected to the Internet to function properly.
- ✓ Use strong, unique passwords for each device.
- ✓ Keep all software and firmware up to date to fix vulnerabilities and reduce the risk of cyber attacks on devices.
- ✓ Segment the network using a firewall to isolate all IoT devices into their own virtual network, preventing them from having any access to corporate systems.

4 USER MISTAKES INCREASE THE RISK OF MOBILE DEVICE ATTACKS

As mobile devices become more prevalent for work and personal use, they are increasingly at risk for data security breaches if proper precautions are not taken. Mobile devices often store large amounts of sensitive, personal information, including social media use, digital wallets, and data related to remote work. Cybercriminals are taking advantage of these opportunities, and the potential consequences of a mobile device cyberattack are numerous.

Here are some common mobile device vulnerabilities that organizations should be aware of:

- ✓ Open Wi-Fi
- ✓ Spyware
- ✓ Malicious apps
- ✓ Apps with weak security
- ✓ Weak passwords
- ✓ Outdated devices
- ✓ Outdated software



According to recent reports, only 14% of organizations have implemented basic mobile cybersecurity practices, and 32% of professionals have stated that their organization sacrifices some security measures to complete tasks. Organizations that do not prioritize mobile cybersecurity are more than twice as likely to experience an attack or data breach.

To ensure mobile device security, organizations should take steps to implement additional layers of protection, educate employees on security measures, and stay informed about emerging mobile device cybersecurity trends. There are many different approaches to securing mobile devices, here are a few that organizations should consider:

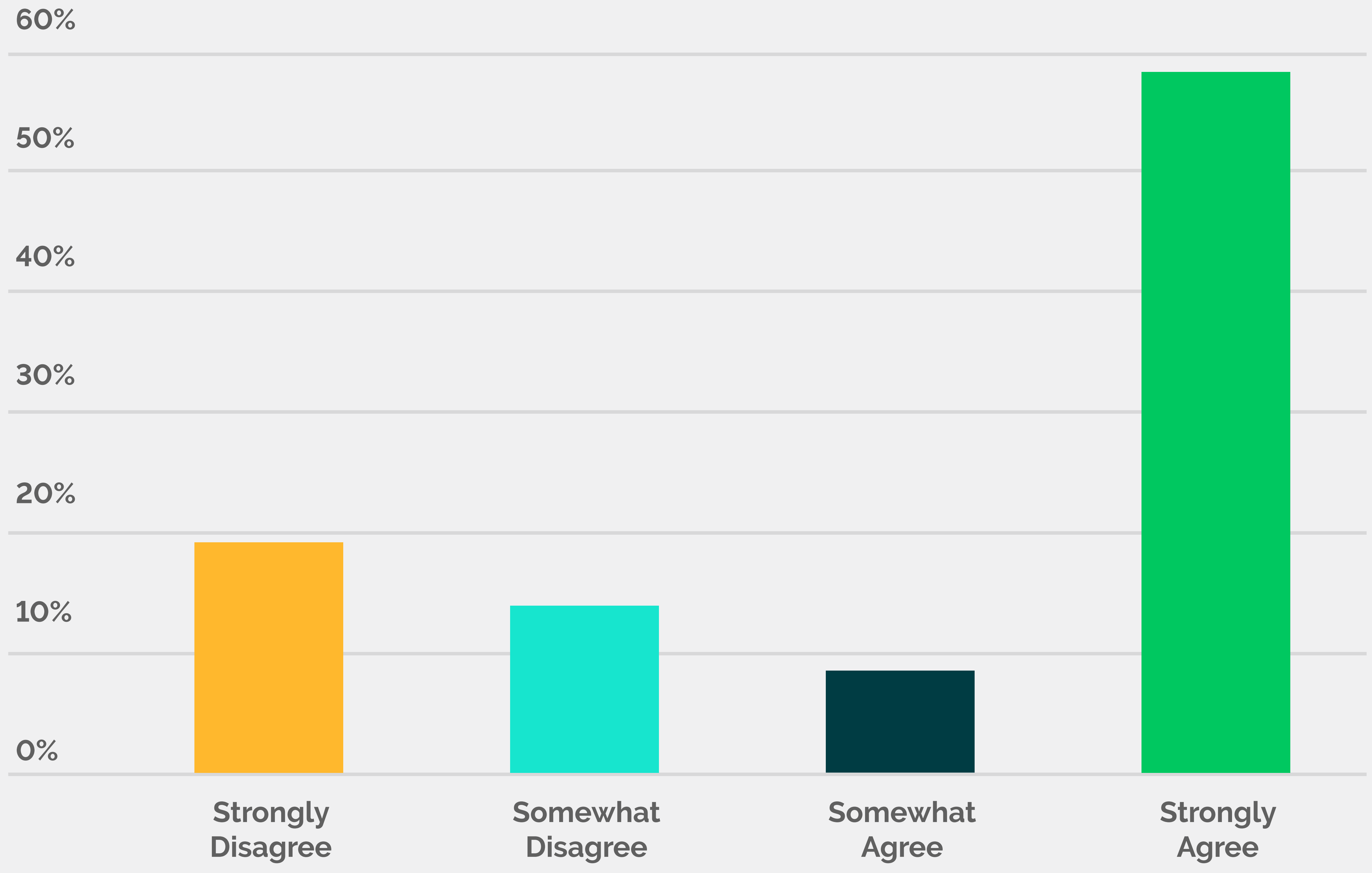
- ✓ Regularly review, update, and enforce mobile device security policies.
- ✓ Train employees on the safe use and handling of mobile devices and phishing awareness.
- ✓ Use mobile device management solutions to monitor, manage, and secure corporate data and apps on mobile devices.
- ✓ Implement mobile threat defense solutions to detect and prevent malicious activities.
- ✓ Implement secure authentication methods such as biometrics and multi-factor authentication to secure access to corporate data and apps.
- ✓ Regularly back up data on mobile devices.
- ✓ Use anti-malware and anti-virus software.
- ✓ Regularly patch and update all mobile operating systems and apps.

5 REMOTE WORK CYBERSECURITY CHALLENGES

The rapid shift to remote work has introduced new cyber threats and is a significant trend to consider. Cyber threats within the workplace are no longer confined to company-owned devices or company networks/premises. Many remote employees use their personal devices to access company software, two-factor authentication, company data, and apps to communicate with coworkers and clients. This blurring of the line between work and home presents several challenges for cybersecurity:

- ✓ It may be more difficult for company data security teams to ensure that company protection is up to par since they do not have access to employees' personal devices.
- ✓ With employees working from home and using personal devices for work, there is no guarantee that every employee will utilize protective measures.
- ✓ BYOD, or Bring Your Own Device, is a trend where employees use their own personal devices, like smartphones, laptops, and tablets, to access company data and applications. This can present significant risks for organizations, such as device insecurity, data leakage, compliance problems, and network vulnerabilities.

Figure 7: **How frequently do you transmit confidential files or company information to colleagues using your personal apps (like iMessage, Gmail, or personal Box or Dropbox accounts)?**



According to a research, 75% of employees use their personal cell phones for work-related activities. This trend has contributed to a 238% increase in global cyberattacks since the start of the pandemic, as the growth of remote work has created new opportunities for cybercriminals.

The sudden shift to remote work left many businesses and workers little time to implement adaptable security systems for remote or hybrid work environments. While more organizations, teams, and employees are becoming aware of the increased cybersecurity threats, it is not always a given that every employee is taking necessary precautions while accessing company data.

To reduce the risk of cyberattacks on remote work devices, organizations can assess the potential risks associated with remote work and implement appropriate security measures. This can include ensuring that all security software on devices and work-related platforms is up to date and providing training to remote workers on company data security policies and protocols. By taking proactive steps to address potential risks, businesses can significantly reduce their risk of falling victim to a cyberattack. Here are some crucial recommendations for organizations to ensure a secure remote work environment:

- ☑ Disallow BYOD and implement strict security protocols.
- ☑ Use a virtual operating environment like Azure Virtual Desktop.
- ☑ Regular security training for employees.
- ☑ Implement multi-factor authentication.
- ☑ Have an incident response plan in place.

6 THE INCREASING DIFFICULTY OF CLOUD SECURITY

The shift to remote work has also led to an increase in demand for cloud solutions. As companies rapidly adopted cloud infrastructures in recent years, many struggled to implement adequate security measures. The rapid adoption of cloud technologies and lack of security resources left many organizations vulnerable to cyber threats to the data stored on these solutions. Additionally, many cloud solutions do not offer secure authentication or audit logging, making them attractive targets for cybercriminals and increasing the risk of a data breach.

Cloud security issues such as data privacy, unauthorized access, and compliance are major organizational concerns. In 2021, 79% of companies experienced at least one cloud data breach, highlighting the importance of addressing these security challenges.

Cloud Security Statistics

Phishing is the most common **cloud security** threat, followed by account compromise and ransomware.

29% of **cloud security** threats were targeted attacks on **cloud infrastructure.**

Misconfiguration and **unauthorized access** are the biggest causes of **cloud security** problems.

An effective cloud-based security strategy is crucial for protecting against cyberattacks on the cloud. To safeguard against these threats, organizations that utilize cloud-based systems should consider implementing protective measures such as strong authentication, encryption of data in transit, and the use of intrusion detection and protection systems. By taking these steps, businesses can significantly reduce their risk of a data breach and protect sensitive information stored on cloud platforms.

To ensure the security of their cloud-based assets, organizations should stay informed about the latest developments in cloud infrastructure security. By keeping up with these advancements, businesses can access the necessary tools and frameworks to protect against cyberattacks on the cloud. Regular updates and assessments of cloud security measures are essential for maintaining the safety of sensitive data and systems.

Cloud-based security infrastructure consists of various components that help to protect against cyber threats and ensure the security of data stored on the cloud. These include:

- ✓ **Access Control:** To prevent unauthorized access, businesses should have robust cloud security infrastructure in place to manage and control access to their data and systems.
- ✓ **Data Protection:** Organizations should implement proper solutions and policies to secure data stored on the cloud just as one would for on-site data storage. Data retention and backup policies can help minimize the amount of data at risk and minimize the impact of disruptions.
- ✓ **Attack Prevention:** To protect against cyberattacks, companies need a proactive strategy that enables them to detect, identify, and mitigate security threats quickly, such as Managed Detection and Response (MDR). This involves constant security vigilance and monitoring of the cloud environment.

7 MANAGED DETECTION AND RESPONSE: PROACTIVE AND CONTINUOUS MONITORING FOR ENHANCED CYBERSECURITY

Managed Detection and Response (MDR) is a specialized cybersecurity service that leverages advanced technology and human expertise to detect, monitor, and respond to potential threats. With MDR, organizations can proactively identify and mitigate the impact of potential threats in real time, enhancing the organization's overall security posture, significantly reducing the probability and the impact of cyber-attacks.

(MDR) services offer organizations a comprehensive and streamlined approach to cybersecurity, enabling them to outsource the management of threats to a team of experts. This rapidly growing area of cybersecurity is increasingly being adopted by organizations seeking to benefit from modern, turnkey solutions that provide continuous protection around the clock. According to a Gartner analysis, MDR services are expected to be used by 50% of organizations by 2025.

To reduce the risk of cyberattacks on remote work devices, organizations can assess the potential risks associated with remote work and implement appropriate security measures. This can include ensuring that all security software on devices and work-related platforms is up to date and providing training to remote workers on company data security policies and protocols. By taking proactive steps to address potential risks, businesses can significantly reduce their risk of falling victim to a cyberattack. Here are some crucial recommendations for organizations to ensure a secure remote work environment:

- ✓ The provider's ability to customize their services to meet the organization's specific needs.
- ✓ Compatibility with or enhancement of the organization's existing security stack.
- ✓ The ability to configure logs to include relevant data and detail.
- ✓ Support for incident response activities.
- ✓ Transparency and open communication.
- ✓ A team of experienced professionals who use the latest security tools.
- ✓ A holistic MDR that covers all critical business systems, including at least all endpoints, cloud applications, email, and access control.

CONCLUSION

Given the ongoing increase in cyber risk and the evolution of technology and cyber threats, it is essential for organizations to prioritize protection and prevention. This can be achieved through a range of measures, such as conducting a cybersecurity audit, maintaining necessary security measures, and enlisting the services of professionals for proactive monitoring and defense.

At Greenlight, we understand cybersecurity's critical role in protecting organizations from threats and risks. Our team of experts offers tailored, sophisticated solutions to help organizations identify and mitigate these challenges.

TRUSTED CYBER PROTECTION.
RELIABLE IT SERVICES.

For over a decade, Greenlight has been a trusted provider of top-quality cybersecurity services for small to midsize businesses. Our team of innovative cyber experts is experienced in the unique challenges facing organizations in today's rapidly evolving digital landscape. We are equipped to deliver cutting-edge technology and cybersecurity solutions that empower organizations to thrive while safeguarding them against the most advanced cyber threats, allowing them to operate with complete peace of mind.

If this article was informative and valuable to you, we highly recommend scheduling a consultation with a cybersecurity expert at Greenlight to gain further insights and guidance on this important topic. Our full range of services includes cybersecurity assessments, cloud security, Managed Detection and Response, Microsoft zero-trust security, and penetration testing, all designed to provide the protection your organization requires. We offer tailored solutions to fit the unique needs of your business and help you protect all systems and data.

CONTACT US

www.greenlight-is.com
15375 Barranca Pkwy., A212 Irvine, CA 92618