Acronis

WHITE PAPER

Data security: Protecting your information from cyberthreats

Table of contents

Executive summary

This white paper explains the different types of cyberthreats and their corresponding impacts on data security. It outlines several best practices for data security and discusses the legal and ethical steps to take when a data breach occurs. Businesses and IT professionals will learn what operational steps are required to protect their organization's data from cyberthreats, thereby maintaining clients' trust and preventing reputational damage.

Introduction

The cyberspace continues to grow at an unprecedented rate, fostering inter- and intra-business collaborations at scale. Data sits at the forefront of this growth, as it is now more shared and used than ever before. However, along with this growth in data, there is also a corresponding expansion of the cyberthreat landscape. While this growth is remarkable, it also presents a challenge. According to a 2022 IBM report, the average cost of a data breach hit a record high of $4.35 million in 2022, a figure expected to snowball into $5 million in 2023.

Cyberthreats manifest in several forms; these can include hacking, ransomware attacks, phishing attacks, malware infections and social engineering. Although all forms of cyberthreats differ in approach and target, they have one common denominator: they target data shared between an organization's various components.

Securing data is thus critical to business operations, and organizations must take a holistic approach to doing so.

What is data security?

Data security protects sensitive data from unauthorized access, misuse, disruption, destruction or modification. It entails cybersecurity measures such as access restriction, data encryption and others.

Data breaches can result in significant financial loss, legal consequences, loss of public trust and long-term viability. The primary aim of data security is to therefore prevent data breaches.

Understanding cyberthreats

A cyberthreat or cyberattack is any potential danger that can harm internet use on computers or other electronic devices. Cybercriminals orchestrate cyberattacks by exploiting vulnerabilities in software or hardware, accessing and stealing personal or financial data, installing viruses or spyware, or launching attacks to bring down websites.

Types of cyberthreats

Although cyberthreats can come in many forms, we will discuss six of the most common ones below.

Malware

Malware is software developed to harm, disrupt or damage computer systems. It infects a system as a virus, worm, Trojan horse, ransomware, spyware or adware to steal sensitive data, delete files or cause a system crash. Malware spreads from one computer to another via shared files on a network or email attachments. As with other types of cyberthreats, it can significantly reduce data integrity.

Phishing

Cybercriminals often pose as trustworthy entities to obtain usernames, passwords, credit card details and other personal data. This is called phishing. Phishing emails typically contain a link that, when clicked, leads victims to a fake website resembling a legitimate website, tricking them into giving away their sensitive information. Phishing attacks that target businesses can lead to the loss of intellectual property, trade secrets and other sensitive company information.

Ransomware

Ransomware infects a system and prevents an organization from being able to access its data until a ransom is paid. If the victim decides not to pay, data may be lost permanently, which can cause irreparable damage to a business.

Insider threats

These threats originate from inside an organization and involve any employees, contractors or vendors with access to sensitive data, systems or facilities. Such threats can result from accidental negligence and misuse of data or systems; however, they also can be due to deliberate actions of employees or other insiders who have decided to steal or tamper with sensitive data.

Insider threats are difficult to detect since individuals with authorized access are the ones carrying them out. With access to critical systems, insiders can easily escalate their privileges and access more sensitive data, enabling them to cause severe damage that may be difficult to recover from.

DDoS attacks

In a distributed denial of service (DDoS) attack, a hacker deliberately floods a server or website with traffic from multiple systems. Servers, computers, internet-of-things (IoT) devices, and more can be compromised to send a large volume of traffic to the target system. This renders it incapable of handling legitimate traffic and results in the target system being unable to respond to requests.

When a server or website is hit with a DDoS attack, any data processed by its server is rendered inaccessible. The damage can be even more severe if the DDoS attack is used as a smokescreen to distract security from a secondary attack.

Social engineering

This cyberattack technique seeks to obtain personally identifiable information (PII) from a social security number to bank account data, via several possible methods, such as pretexting and phishing. It is mostly orchestrated via fake emails, social media messages, or even phone calls.

Social engineering attacks do not depend on technological weaknesses but rather on exploiting human vulnerabilities, making them a particularly effective form of cyberthreat.

Data security best practices

The following are effective data security best practices every business and IT professional should implement.

Strong passwords and password managers

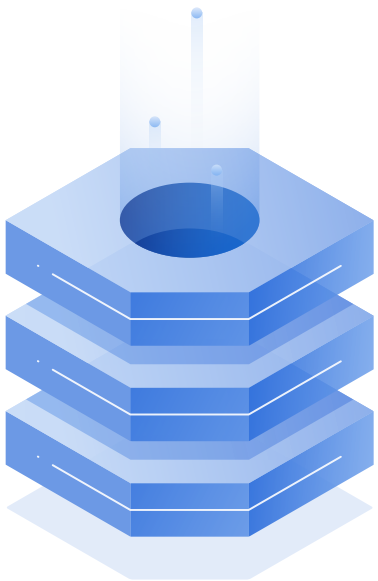
Strong passwords are critical to preventing cyberthreats. Using unique, complex and lengthy passwords that include letters, numbers and special characters is one of the easiest ways to make your SMB accounts more secure. Also, avoid using generic passwords like "123456" or the same password for multiple accounts. Passwords that are too simple or commonly used only serve as an invitation to hackers.

Password managers let you keep all of your passwords secure and easily accessible in one place. This allows you to avoid common password security mistakes, such as trying to memorize multiple passwords, reusing them, or writing them down.

Enabling multifactor authentication (MFA)

MFA provides extra protection since it requires users to verify their identity by providing two or more authentication factors. In addition to the traditional username and password, an MFA-layered system may require a fingerprint, facial recognition or a security code sent to a registered mobile device before granting access.

Without an MFA enabled, your password is your only line of defense. This means that once an attacker gains access to it, they can easily compromise your business accounts. You will also be more vulnerable to phishing attacks.



Regular backup

Data loss can be sudden and occurs due to a variety of factors from human error to natural disasters — not just an external cyberthreat. Regularly backing up important data helps ensure that vital information can be recovered no matter the circumstances.

Losing data can cause considerable financial loss to your business, and it can take much time and effort to recover or recreate that data.

Encryption of sensitive data

Encryption entails converting plain-text data into complex code that only individuals with the encryption key can access. Failure to encrypt sensitive data can lead to the exposure of confidential information, resulting in financial liabilities, reputational damage and a loss of client trust.

For example, if a company stores client credit card information in plain text, a hacker can gain access to the database and easily steal it. Not implementing encryption could also result in legal and regulatory penalties, lawsuits and fines. Many countries and industries have legal and regulatory requirements for data protection, which usually include the encryption of sensitive data.

Software and OS updates

Outdated software is a target of cybercriminals because they contain known security flaws. In some cases, cyberattacks happen so quickly that they may escape the notice of cybersecurity techniques. Effective patch management can often be the last line of defense that will nip the attack in the bud.

Email and web filters

Email and web filters help detect and filter potentially harmful content, such as malware, phishing emails and suspicious links. They reduce the likelihood of accessing malicious websites or downloading malware through emails. These filters are considered basic security requirements, and failure to use them can lead to legal and regulatory penalties.

Virtual private network (VPN)

A VPN is a secure connection that enables confidential data to be transmitted between users on a public

network over the internet. Using one is an essential data security best practice, as it provides a secure, encrypted connection for remote workers, allowing them to access company resources while ensuring that the data transmitted is protected from unauthorized access.

Without a secure VPN, sensitive data can be compromised when employees work remotely, travel, or use unsecured public Wi-Fi networks. Business organizations should therefore ensure that they have a robust VPN security protocol in place to prevent data breaches and protect sensitive information.

Compliance frameworks and standards

Compliance frameworks and standards such as the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) provide guidelines and recommendations to help organizations establish an effective data security program.

NIST is a nonregulatory agency of the United States Department of Commerce. ISO is a nongovernmental organization that has developed several security standards, such as ISO 27001; these provide a blueprint for building and maintaining a secure information security management system (ISMS).

These frameworks and standards provide a comprehensive roadmap for data security, enabling organizations to implement effective security programs.

Cybersecurity training

Cybersecurity training is critical for your employees to know how to effectively protect sensitive data. Employees who are properly educated in cybersecurity techniques are better equipped to avoid and detect phishing scams, malware attacks and social engineering tactics that can lead to data breaches. Additionally, organizations may not be able to meet legal and regulatory requirements for data protection if they do not provide cybersecurity training.

For instance, data protection laws such as GDPR demand that organizations continually educate employees on secure data management practices. Failure to follow these guidelines can result in regulatory violations and, in turn, significant legal and financial penalties from regulatory bodies.

Implementing a cybersecurity incident response plan (CIRP)

A CIRP outlines the steps an organization must take to detect, respond to and recover from cyberthreats. It is a prerequisite for effective cybersecurity management, enabling organizations to minimize the damage from cyberattacks and maintain business continuity. Delayed response to a cybersecurity incident can result in prolonged downtime, lost productivity and financial loss.

Not having a CIRP is perceived as a management failure. Any organization without a CIRP is regarded as unprepared and unprofessional, leading to a possible loss of client trust and decline in market share.

Conducting a security audit

Security audits help organizations assess their current security posture, identify weaknesses that can be exploited by cyberattackers, and establish a roadmap for strengthening their security protocols.

A security audit is essential for ensuring compliance with relevant regulations, standards and best practices in cybersecurity. Regulatory frameworks such as GDPR, HIPAA, and PCI DSS require that organizations conduct regular audits and penetration testing to ensure compliance and the protection of sensitive data.

Tips for protecting your online privacy

To bolster the security of your organization's data, consider asking your employees to implement the following tips to protect themselves (and your business) from cyberthreats.

Use privacy-enhancing browser extensions

Privacy-enhancing browser extensions block third-party cookies, ad trackers and other activity monitoring tools. They offer a layer of security by helping you stay anonymous while browsing the internet; this prevents websites from tracking your activity and blocks ads that may be collecting your information.

Avoid public Wi-Fi networks

Although public Wi-Fi networks are convenient when you're on the go, they make you cybervulnerable.

Cybercriminals use them to install malware, track user activity or steal sensitive information. If you need to connect to public Wi-Fi, use a virtual private network (VPN) and only use encrypted websites.

Disable location tracking

Mobile apps track user locations to provide location-based services such as maps, weather forecasts and personalized content. However, this can pose a privacy risk, as such information can be used to predict a user's movements and location. Review app permissions and disable location tracking on apps that are not location bound.

Limit sharing of personal information

Sharing personal information, such as your name, address, phone number and date of birth, can increase the chances of identity theft, fraud and social engineering attacks. Be strategic about what personal information you share and with whom.

Start by reviewing your social media and other online accounts. Delete any unnecessary information, such as your full birthdate, home address or email. Only connect with people you know, and never share login credentials with untrustworthy individuals or services.

Always remember: less is more when sharing personal data online.

Responding to a data breach

Any unauthorized access to confidential, sensitive or protected data, as well as the theft or release of such data, constitutes a data breach. It can be orchestrated through any of the cyberattack methods explained earlier.

A data breach is a confusing and overwhelming situation, but can be managed by following these six steps.

1. Containment

Once a breach is detected, the first step is to stop the leak and contain the damage as much as possible. This involves cutting off access to the network, disabling compromised accounts and disconnecting affected systems.

2. Assessment

It's important to quickly determine the extent and nature of the breach, what data was compromised, and how it occurred. This may involve forensic analysis, vulnerability testing or reviewing logs and records.

3. Notification

If personal data has been exposed or stolen, affected parties should be notified promptly and accurately. Depending on the organization and scope of the breach, it may also be necessary to notify regulatory authorities or law enforcement officials.

4. Remediation

Once the breach is identified and assessed, remediation steps should be taken. These can include patching vulnerabilities, improving access controls, updating software, reviewing policies and procedures, and providing quick security tips to users or employees.

5. Communication

Communication is key during and after a data breach. All stakeholders must be kept in the loop, including affected individuals, business partners, regulators and the public.

6. Evaluation

After the breach is resolved, it's critical to thoroughly evaluate the incident, the response and the outcome. This can help identify areas for improvement, best practices and lessons learned. It can also inform future security strategies and investments.

Data privacy and security regulations

Besides simply being a good business practice, data security is also regulated by certain regional and international laws. These regulations police the entire process and establish protocols and data security baselines organizations must adhere to. We will briefly cover the four major data security regulations today.

1. General Data Protection Regulation (GDPR)

The GDPR is a comprehensive E.U. regulation aimed at safeguarding the privacy rights of E.U. citizens. It requires all companies that collect, store, and use the personal data of E.U. citizens to comply with certain data privacy and security standards.

For instance, the GDPR requires companies to provide clear and transparent notices to individuals about their data collection and privacy practices. They must obtain explicit consent before collecting and processing anyone's data; limit data usage to specific purposes; and implement appropriate data security measures to protect personal data from unauthorized access, deletion or disclosure.

2. Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA is a Canadian law that applies to all private-sector organizations operating in Canada and governs the collection, use and disclosure of PII. It requires organizations to obtain explicit consent from individuals before collecting such data; limit the collection, use and disclosure of personal data; implement appropriate data security measures to protect said data; and provide individuals with access to their data at all times.

3. Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a U.S. federal law that governs the privacy and security of protected health information (PHI) collected and stored by healthcare providers, health plans and their business associates.

HIPAA requires these organizations to implement appropriate administrative, physical and technical safeguards to protect PHI and limit the use and disclosure of PHI to specific purposes. They must also obtain explicit consent before using or disclosing PHI and promptly notify individuals and the Department of Health and Human Services (HHS) in the event of a data breach.

4. Payment Card Industry Data Security Standard (PCI DSS)

To better protect cardholder data, major credit card companies came up with PCI DSS. It requires companies that handle credit card information to adhere to certain security standards and practices. These include maintaining a secure network, enforcing a proper information security policy, and regularly monitoring and testing their security systems.

Conclusion

As cyberthreats continue to grow in sophistication, organizations must continuously evaluate how to effectively secure their data. Data security tools such as Acronis Cyber Protect sit at the core of any proactive efforts to rigorously protect data. Acronis Cyber Protect is a comprehensive cybersecurity suite that provides a unified approach to data protection and backup, making it possible to secure your data against both known and unknown cyberthreats.

With features such as AI-powered malware protection, URL filtering, vulnerability assessments, and backup and recovery capabilities, Acronis Cyber Protect is the ultimate solution for data security today.

About Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions powered by AI.

Founded in Singapore and headquartered in Switzerland, Acronis now has over 2,000 employees and offices in 34 locations worldwide. Learn more at acronis.com.

Acronis

Learn more at
www.acronis.com