MOSSADAMS

Cybersecurity Guide

PROTECT THE VALUE OF YOUR COMPANY

Updated October 2023

AN OVERVIEW

Cybersecurity, at its core, is about protecting what's valuable to you as an organization. For some, that might mean protecting valuable customer data—credit card information, Social Security numbers, or patient health care records. For others, intellectual property, the contents of an agreement, and personal finance and tax records may be the most valued asset.

In today's world, those assets are constantly under attack, as bad actors and cybercriminals attempt to compromise the networks and systems that handle sensitive and business critical data using evolving tools and techniques that make securing data one of the most challenging business concerns.

An Increasingly Costly Threat

For many organizations, it's no longer a question of whether a system will be compromised, but when a system will be compromised. The United States had the highest data breach costs, according to the Cost of a Data Breach Report 2023 by the Ponemon Institute. The average data breach costs a company $4.45 million.

That's a frightening perspective with a huge cost attached to it—and things aren't going to get better anytime soon.

INFLUENCING FACTORS

There are several factors influencing cybercriminals to increase the amount and scale of attacks.

Emerging Technology

The rise of artificial intelligence (AI) is a significant technological evolution that's expected to transform the way companies operate and enhance the capabilities of the workforce.

This rise of AI has also played well in the hands of cybercriminals who are leveraging AI for nefarious purposes, like crafting more realistic, natural-sounding phishing emails, accelerating and automating the development of malicious code, and spreading false information as a precursor to social engineering attacks.

Global Instability

Tension and conflict between countries can create a backdrop for an increase in cyberattacks.

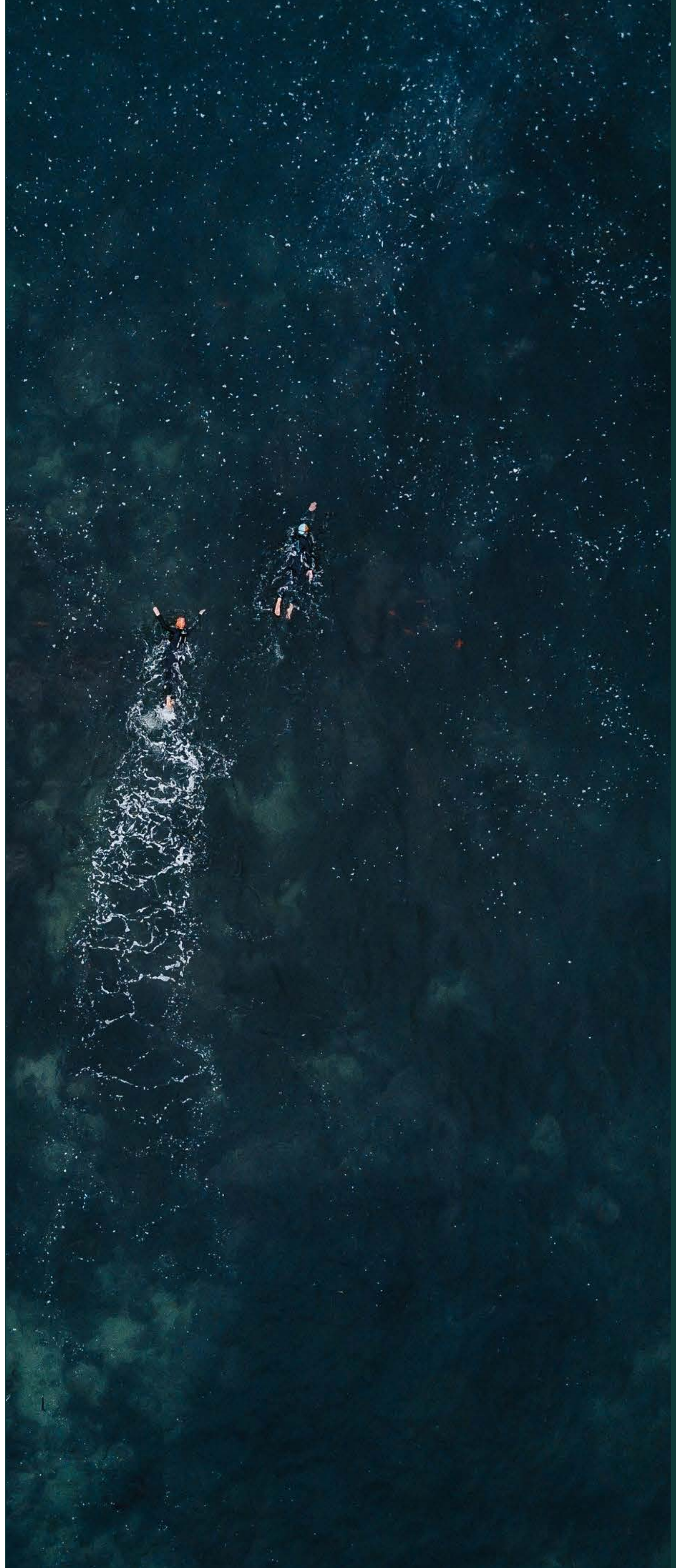
Consequently, cyberattacks backed by and perpetrated by nation states has been on an upswing, which has led to an increase in attacks on critical infrastructure entities.

Low Barrier to Entry for Would-Be Cybercriminals

The dark web is filled with services that cater to aspiring cybercriminals. The proliferation of Ransomware-as-a-Service and Crimeware-as-a-Service providers and the relative ease of engaging these services has increased the threat of attacks by novice and expert alike. Many of these criminal entities provide their service for a percentage of the stolen funds or exfiltrated data.

Social Engineering Attacks

Even with stronger technical security defenses, organizations are still at a disadvantage in the fight against hackers. Why? Because cyberattacks are increasingly aimed at individuals rather than systems—and the human factor is much harder to manage. Social engineering and the human continue to provide cybercriminals a path of least resistance and an effective attack vector for compromising a system, and the attacks are getting more sophisticated with AI-based tools. People, however, are also the first line of defense—with proper training.



CYBERATTACKS & INCIDENTS

In recent years, a variety of industries have fallen victim to cyberattacks and incidents, proving none are immune to the whims of bad actors who see opportunities for data theft and big payouts from victims of ransomware.

HEALTH CARE

A New York-based molecular diagnostics company suffered a ransomware attack that potentially exposed the clinical test information and Social Security numbers (SSN) of nearly 2.5 million individuals. Since 2020, health care data breaches have increased by more than double.

GOVERNMENT

A state's Department of Motor Vehicles was hit with a cyberattack that exploited a flaw in the commercial file transfer service that was used to store driver's license holders' information such as driver names, addresses, and the last four digits of their SSN.

BIOTECHNOLOGY AND LIFE SCIENCE

A large pharmaceutical company exposed sensitive patient data for more than a year after a list of login credentials was exposed online due to user error. The login credentials were to an internal server on a well-known code sharing site.

BANKING AND FINANCIAL SERVICES

A nationwide banking and financial services company settled a class action lawsuit stemming from a cyber incident in 2019 that impacted approximately 106 million US and Canadian customers that exposed information typically collected in credit applications, including SSNs, contact information, and credit scores.

FOOD PROCESSING

A ransomware attack shut down the operations of a large, multinational meat processing company, effectively disrupting the worldwide food supply chain. The company eventually paid the ransom amount of $11 million.

ACCOUNTABILITY

High-profile enterprise hacking leads to the painful loss of precious data, customer confidence, and hundreds of millions of dollars in legal fees, notification costs, and technology remediation.

It's no wonder C-level executives are now paying more attention to their organizations' vulnerabilities when it comes to cybersecurity. Other individuals also demand results.

Investors and boards of directors are increasingly holding senior management accountable for cybersecurity.

Customers and partners demand adequate cybersecurity controls are in place before conducting business.

US states, regulators, and regulatory bodies are legally mandating cybersecurity compliance.

Standards and Guidelines

Below are cybersecurity standards and guidelines companies are embracing.

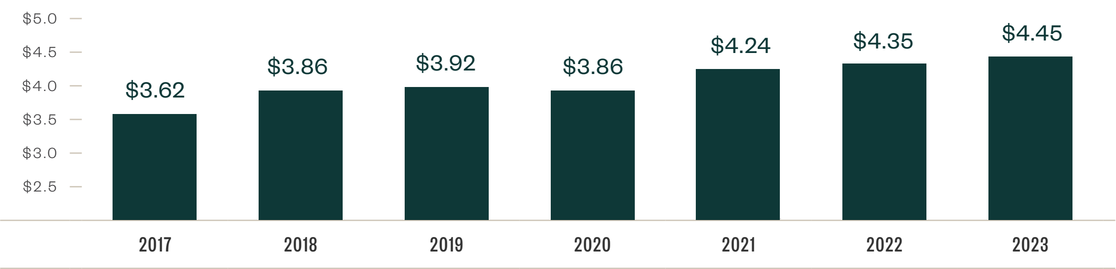
- **National Institute of Standards and Technology (NIST)**
  - NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF)
  - NIST Special Publication 800-53, Revision 5 (NIST SP 800-53r5)
  - NIST Special Publication 800-171
- **International Standards Organization**
  - ISO 27000 series
- **HITRUST Common Security Framework (CSF)**
- **Center for Internet Security (CIS) Critical Security Controls**

TOTAL COST OF A BREACH

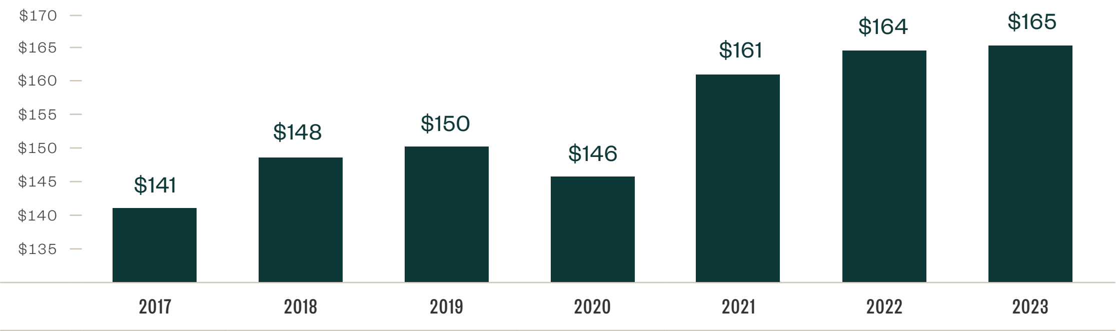
Year on year, the costs of a data breach are consistent. IBM, in conjunction with the Ponemon Institute, studied 553 organizations impacted by data breaches and documented their findings in the Cost of a Data Breach Report.

The report presents insights to help IT and security teams manage risk and limit losses by providing an analysis of how the breach occurred, how it was identified, and costs associated with the breach.

TOTAL COST
OF A DATA BREACH (USD MILLIONS)



PER-RECORD COST
OF A DATA BREACH (USD)



Source: Ponemon Institute, 2023

THE STATE OF CYBERSECURITY

Some interesting statistics to come from the Cost of a Data Breach report include the following.

Most companies discovered the data breach through their own security teams, highlighting a need for better monitoring and detection.

When attackers disclosed a breach, it costs organizations as much **as $1 million or more** compared to internal detection.

Organizations that didn't involve law enforcement in a ransomware attack spent **nearly half a million more dollars in additional costs**—and these organization experienced a longer breach lifecycle.

The time to identify and contain breaches—known as the breach lifecycle—makes a difference in the costs. Breaches with longer identification and containment times **cost organizations as much as a million dollars more** than those with a shorter breach lifecycle.

Most breaches involve data stored in the cloud.

> It's no longer a question of whether a network will be compromised, but *when* a network will be compromised.

Attack Types

Attackers are increasingly sophisticated and have more access points to networks, particularly with the ubiquity of cloud-based technologies, mobile phone devices, and the use of system hosting providers.

Consequently, the borders of an organization's network are increasingly blurred and more challenging to protect. Bad actors intent on compromising an organization's systems and data or who are looking for a quick payout have a multitude of vectors to attack and exploit.

Common Cyberattack Approaches

Phishing

Phishing is a common email-based social engineering technique used by bad actors to trick an individual into providing sensitive information and has been used for years.

Whaling

When the target is C-level executives, it's known as whaling. C-level email fraud takes place when a hacker requests that members of an organization's finance function disburse or wire funds to a third-party in an email that looks like it comes from senior management.

Smishing

Like phishing, smishing uses social engineering to trick individuals into providing sensitive information. Rather than using email, smishing uses SMS-based messaging platforms. The bad actor will attempt to build rapport with the target before fooling them into giving them the information they want.

Business Email Compromise (BEC)

This attack targets employees working in the finance and accounting functions of a business by sending them fake invoices for goods or services that appear to come from a legitimate source, but in reality, is sent by a bad actor who provides wiring instructions for payments that are deposited into their own bank accounts.

Cloud Misconfiguration

As businesses increasingly leverage cloud-based services to host production IT systems, cloud misconfiguration has opened more opportunities for bad actors to steal data or gain unauthorized access to data.

Cloud misconfiguration attacks occur when a bad actor exploits a cloud-based service, such as a data storage repository service, that doesn't sufficiently restrict access, still uses default settings, or whose systems haven't been patched with security updates.

Third-Party Attacks

Attacks on third-party providers in an organization's supply chain have been on an uptick in recent years. This attack targets a service provider such as HVAC service providers, IT support services, and software companies, among others. A prime example was the December 2020 attack on network and system monitoring software provider, SolarWinds, which impacted thousands of their customers worldwide due to vulnerabilities inherent in one of their popular products.

Internet of Things (IoT)

IoT devices have been increasingly invading our business and personal lives with always on, always-connected, nontraditional computing technologies being used in the workplace and at home. Devices such a smart videoconferencing systems, vehicle entertainment systems, and smart lighting and environmental systems, along with the multitude of consumer IoT devices, provide no shortage of potential attack vectors for bad actors.

PHISHING & WHALING

Sophisticated attacks usually begin here. A social engineering attack preys on the psychological willingness of employees to divulge a company's confidential digital information.

These attacks involve an email from a hacker who appears to be an individual or business you know. The target tends to be an unaware or untrained employee who may be willing to give up desirable information—their system password or company account details, for example.

Defense Strategy

There isn't an all-encompassing solution to combat these types of attacks, but there are steps you can take to try and prevent them. Prior to an attack, the following defenses should be in place.

End-User Security Training

People are your first line of defense. Keeping them informed and educated about current cyber threats and attack types will help them recognize attempts by bad actors to steal data or gain unauthorized access to systems. Annual security awareness training for all employees along with regularly scheduled social engineering exercises and testing will help to reinforce the roles and responsibilities the workforce has in ensuring the safekeeping of data.

Technical Controls

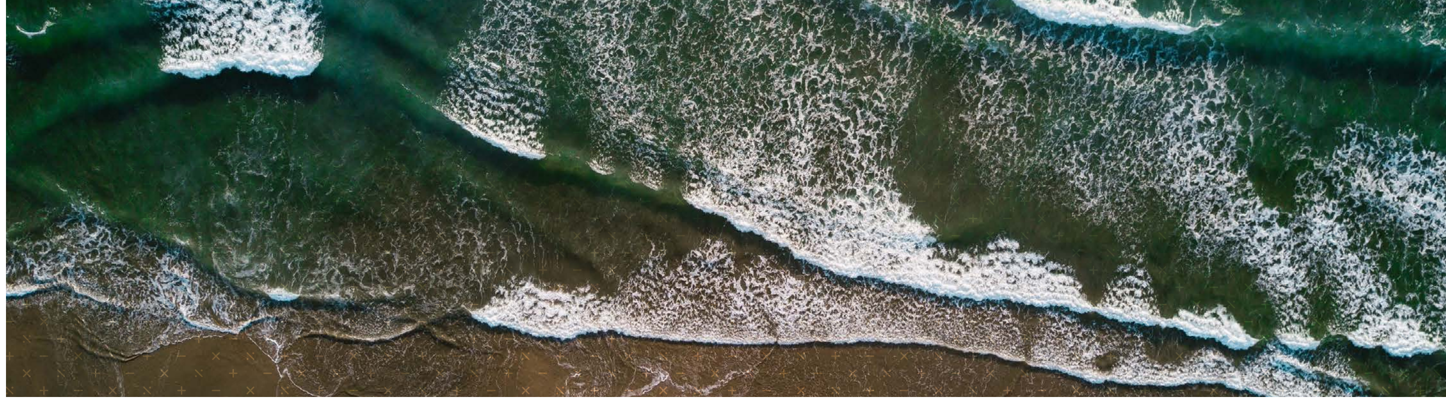
This includes email system security measures, including antispam, URL scanning, and attachment stripping. As a common avenue of attack, it's imperative that solid email system security controls are in place, such as:

- Domain-based message authentication, reporting, and conformance (DMARC)
- Sender policy framework (SPF)
- Domain keys identified mail (DKIM)

These help to protect against email spoofing attacks and confirm legitimacy of the sender.

Internal Process Controls

Have at least two sets of eyes and approval for requests that meet a certain threshold, particularly when the email is requesting an immediate transfer of funds or when a vendor request is received requesting a change in wire transfer or bank routing information.



SMISHING

With personal cell phones often being used for work purposes, bad actors take advantage of the ease of sending text messages—and spoofing their phone number at the same time—as a social engineering attack to obtain sensitive information, steal money, or gain unauthorized access to a device or system.

After building rapport with the target individual by impersonating someone they know either personally or as a business associate, the bad actor tricks the individual into clicking a link in a text message that diverts them to a seemingly legitimate-looking login page to a commercial website. The individual then enters login credentials, bank information, account details, or other sensitive information—unknowingly providing it to the bad actor.

Defense Strategy

Smishing is difficult to defend against, largely because it's difficult to regulate and control employee-owned mobile phones and devices. There are a few things that can be done to minimize the risk of becoming a victim of a successful smishing campaign.

End-User Security Training

As with educating employees on the threat of phishing attacks, the same should be done with smishing attacks. Employees should know not to click on links in text messages from individuals they don't personally know. They should also be wary about text messages asking for personal or sensitive information, and they should report smishing attacks to their IT security staff if the texts are of a business nature.

Technical Controls

To prevent smishing attacks, organizations should implement technical safeguards, such as:

- Using multifactor authentication (MFA) with SMS verification
- Implementing anti-spam filters
- Maintaining a whitelist of approved senders
- Scanning URLs to analyze links within SMS messages for potential threats

In addition, implementing an enterprise mobile device management (MDM) system, regularly updating and patching systems, using encryption, and network monitoring will help mitigate smishing risks. Many commercial, off-the-shelf MDM solutions provide protections against smishing attacks.

CLOUD MISCONFIGURATION

Attacks on a misconfigured or insufficiently secured cloud environment are becoming more common as an attack vector for bad actors and cybercriminals. With critical business systems and services moving off-premises to cloud infrastructure providers, such as Amazon Web Services and Microsoft Azure, the risk of implementing insecure systems has increased.

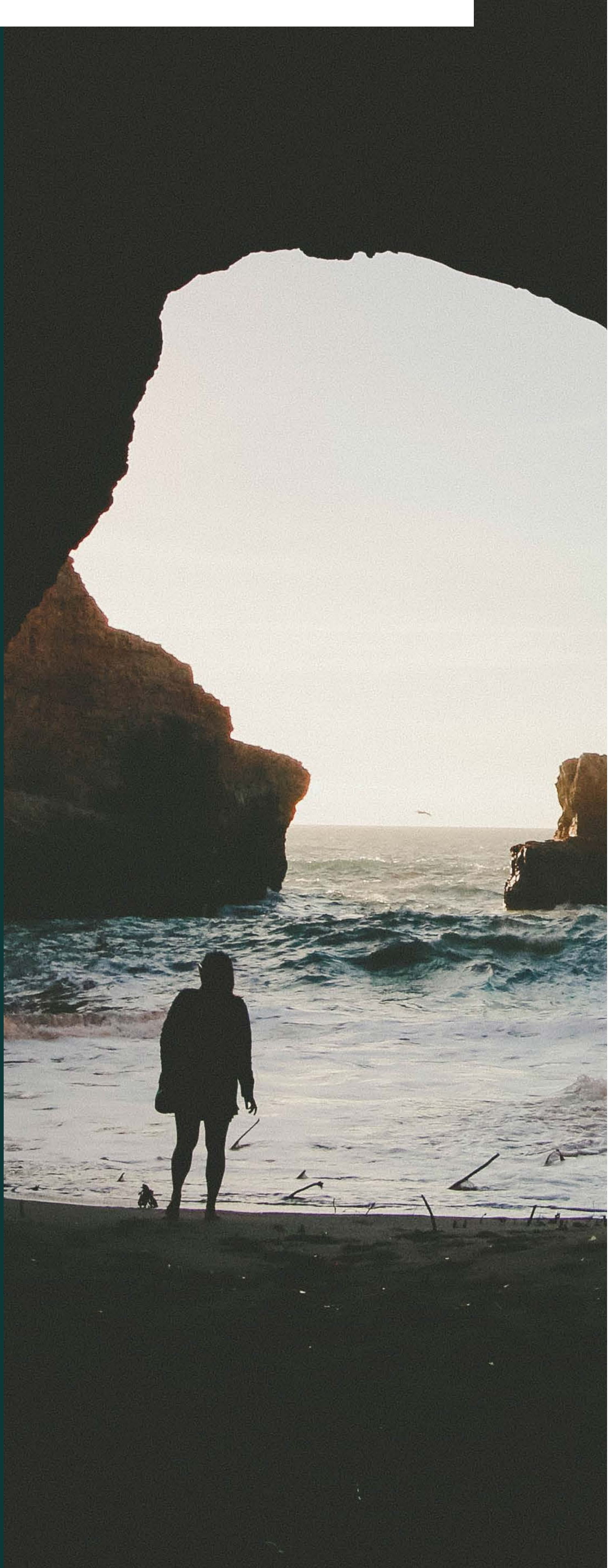
Defense Strategy

Preventing cloud misconfiguration attacks can largely be done through strong technical controls.

Technical Controls

Controlling access to cloud infrastructures is critical to maintaining the confidentiality, integrity, and availability of the systems and data hosted in these environments. An effective technical control to have in place is using a cloud access security broker (CASB) service. A CASB is a service that helps to control and monitor access to an organization's cloud-based systems. It also helps to identify cloud misconfigurations.

Other technical controls include regularly conducting vulnerability assessment scans to identify weaknesses in the systems and implementing MFA to ensure only authorized employees can access the cloud-based systems.



THIRD-PARTY ATTACKS

Attacks on service providers within an organization's supply chain are difficult to defend against and respond to since the organization isn't in direct control over the service provider's operating environment.

Defense Strategy

Below are strategies to help minimize the risk of being a victim of a cyberattack due to the mistakes of a service provider.

Administrative Controls

Conduct due diligence on third-party service providers prior to engaging them. Requesting and reviewing the results of a recent third-party attestation of controls report, such as one from a Systems and Organizational Controls SOC 2® examinations, also known as SOC 2 audit, can provide valuable insight on a service provider's IT security controls, hiring practices, and operations that may influence your decision to do business with them.

Be sure their cybersecurity measures are in line with any data security regulatory requirements to which your organization adheres. Also, include a right to audit clause in your agreement with the service provider, as that will help to ensure they're keeping their environment secure and your data safe.

Technical Controls

The technical controls to protect against third-party attacks are largely the basics. That is, to implement strong user authentication controls, such as the following:

- Use MFA, along with strong passwords on systems
- Regularly scan your systems for vulnerabilities
- Use a web application firewall (WAF), especially for applications exposed to the internet
- Monitor trusted sources for emerging threats and vulnerabilities impacting systems that are in use
- Have an incident response plan in place so you can quickly and effectively respond to a cybersecurity event impacting a third-party provider that directly affects your organization

INTERNET OF THINGS

Another entry point for hackers is the IoT. These devices—a wireless HVAC controller, smart watch, or even a drug-infusion pump that dispenses medication based on a patient's physiological alerts—are particularly vulnerable because vendors are rushing to push products to market without considering the design of security elements.

Security and privacy are also hindered by the fact that a myriad of manufacturers have too many different types of devices, which typically have low processing power, are designed to perform a single function, and aren't secured with universally accepted security standards.

A 2020 forecast estimated there are 40.9 billion devices in use—double the number from 2014. Additionally, it's estimated IoT solutions will grow to $7.1 trillion in the worldwide market—a significant jump from $1.9 trillion in 2013.

Defense Strategy

Strategies to protect your business from IoT-related attacks include:

- Know where IoT devices are in the environment
- Develop a policy for governing the use of IoT devices in the environment
- Have governance and risk assessment processes in place when new IoT devices are considered
- Use a separate wireless network to separate devices from the corporate network
- Use encryption while data is in transit, especially for sensitive information, if possible

OTHER EXAMPLES OF IOT DEVICES

- AVL sensor in a public transportation card
- Smart video conferencing systems
- Radio frequency identification (RFID) systems used for inventory
- Vending machines
- Fitbits

RANSOMWARE

Also known as scareware, this software allows hackers to access an employee's computer, encrypt sensitive data, and then demand some form of payment to decrypt it. Often beginning with a spear-phishing attack, it infects the system and can propagate from there.

Defense Strategy

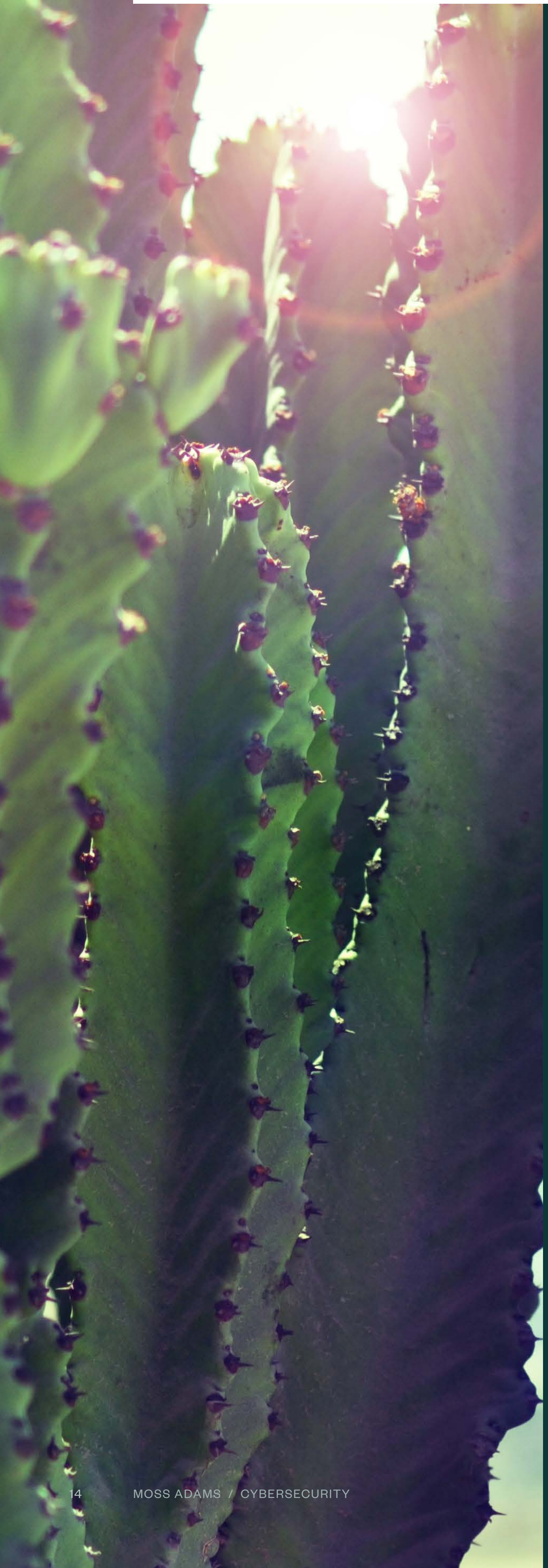
There are administrative and technical controls to employ in this situation.

Administrative Controls

- End-user security awareness training
- Internal process controls
- Disaster recovery and business continuity plans
- Contact information for local law enforcement, the FBI, and service providers

Technical Controls

- Frequent backups and snapshots of databases
- Test backups for key systems
- Network segmentation
- Up-to-date antivirus and system software through frequent patching
- Near real-time monitoring services, such as firewall information networks

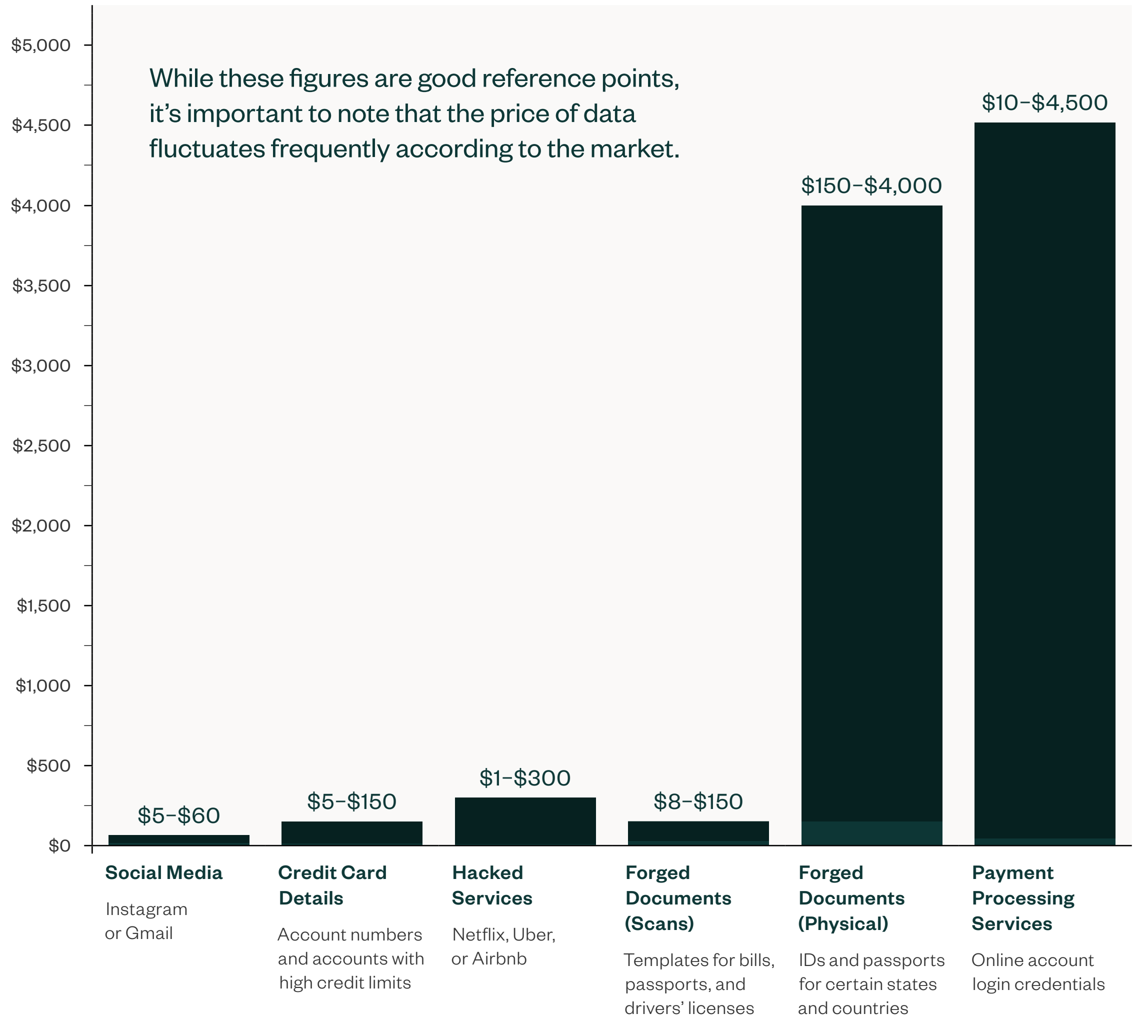


The Going Price of Data

The biggest motivation for attackers to steal data is for financial gain, whether that's through identify theft or selling the information. Holding data for ransom is one way for them to profit, but stealing other information, such as passwords, personal information, bank or credit card details, or medical information and selling that data on the dark web is another.

The cost of data fluctuates from year to year, but there are consistent trends. Following are details on the types of data stolen and the estimated value of that data to an attacker.

COST OF DATA ON THE DARK WEB



While these figures are good reference points, it's important to note that the price of data fluctuates frequently according to the market.

Assessing Your Vulnerabilities

Assessing your vulnerabilities is critical when deciding what prevention methods are right for your organization. That starts with determining your organization's security weaknesses.

COMMON WEAKNESSES

A cybersecurity attack is often adapted for a particular company or industry. Here are five common problems that make organizations especially vulnerable to cyberattacks.

EXCESSIVE ADMINISTRATOR-LEVEL ACCESS TO NETWORKS AND SYSTEMS

Often vendors, consultants, and outside contractors retain access long after engagements with organizations are completed.

NOT SECURING CLOUD-BASED SYSTEMS PROPERLY

As more organizations have systems and data residing in private, public, or hybrid cloud environments, attackers have focused on the insecurities within these systems. Security system misconfigurations and insecure access controls are some of the main reasons these systems get breached. Vulnerability identification and management are critical for these systems, but often get overlooked by administrators.

LACK OF CYBERSECURITY AWARENESS AMONG EXECUTIVES AND EMPLOYEES

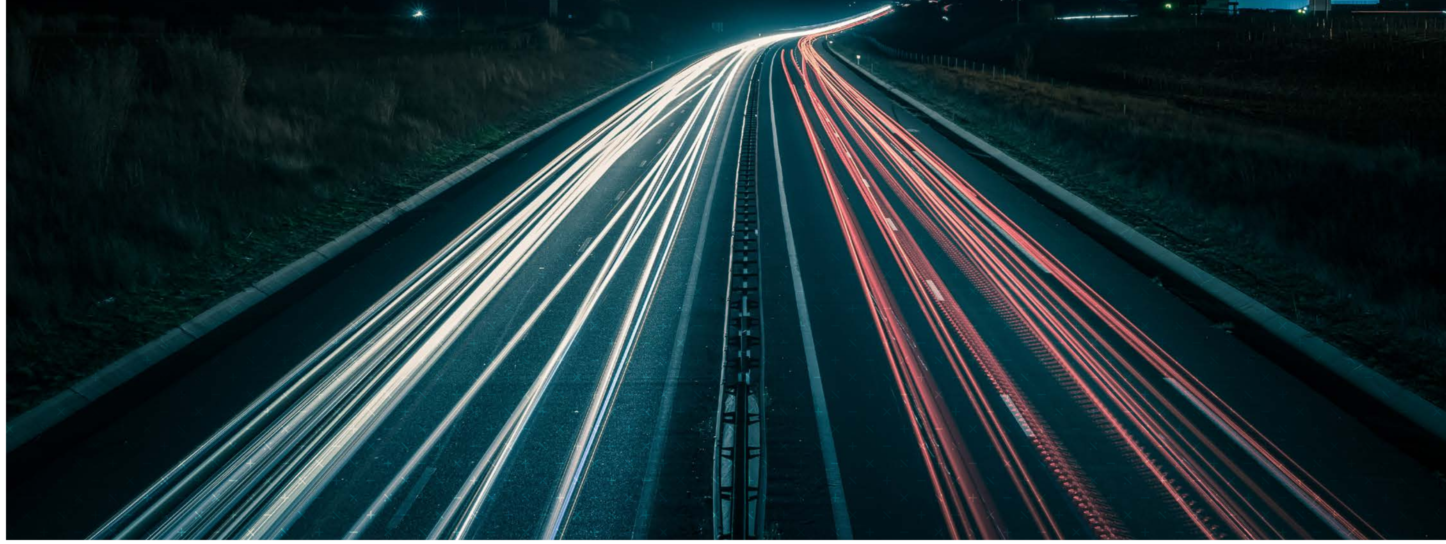
Training is essential so staff at all levels are aware of cybersecurity risks and how to recognize and avoid them. This training should be included in a mandatory HR best practices portfolio and conducted at least annually with regular communications about updates and practices.

INADEQUATE INCIDENT RESPONSE OR DISASTER RECOVERY PLAN

An incident response plan provides steps for personnel to follow before, during, and after a security incident, while a disaster recovery plan provides steps to restore systems quickly and minimize downtime. A proper plan should include steps to deal with various incident types, destructive data loss, or a security breach. Many companies are ill-prepared to cope with this type of crisis, and the ensuing damage and recovery time can be exponential.

PRIORITIZING CONVENIENCE

Too many organizations, especially smaller ones, choose convenience over high-level cybersecurity. For example, they have one flat network that doesn't contribute to a layered defense rather than a segmented structure. This prevents a company from containing a security breach in one isolated part of the network.



RISK ASSESSMENT & ANALYSIS

There are many ways to infiltrate a company. Often, a company's biggest weakness is not knowing how exposed it is to a cyberattack. An IT security risk assessment and analysis can help identify and assess the holes in your operation—a good step toward protecting your organization.

A risk assessment can help answer several key questions:

- What systems are most at risk?
- Who has access to the most significant organizational data?
- How was mission-critical data acquired?
- What vital data is being processed, by whom, and how?
- What essential data is being stored, and how?
- What valuable data is being transmitted, and how?

A cybersecurity risk assessment and analysis needs to be conducted annually and should focus on internal and external cybersecurity controls. It's important to know what cybersecurity controls are implemented as well as if those controls are working and up to date.

Examine these cybersecurity controls on a regular basis.

Administrative Security

Policies and procedures related to IT security, incident response plans, and disaster recovery plans

Technology

Networks, servers, mobile devices, and workstations

Physical

Access rights to your data center and server rooms

Operational

Approval processes for access requests and system changes

Social Engineering

Confront the newest forms of people-driven cyberattacks through security awareness training

PENETRATION TESTING

In addition to conducting a cybersecurity risk assessment and analysis and focusing on cybersecurity controls, prudent cybersecurity management also requires vulnerability scanning and penetration testing.

Penetration testing allows highly skilled and experienced security consultants to identify vulnerabilities by assessing your systems from a bad actor's perspective. Put another way, penetration testing is ethical hacking. Among other things, penetration testing helps identify:

- Holes and flaws in IT systems
- Patches that weren't installed to fix issues
- Incorrect or inadequate configurations
- Updates and upgrades that have and haven't been performed

THIRD-PARTY RISK MANAGEMENT

If you use cloud-based systems or third-party providers that help manage an aspect of your technology environment, such as firewall management or data backup, you should ascertain the protections and security measures the vendor has in place to protect your sensitive data.

Third-party risk management is a continuous process for management of the provider throughout the lifecycle of use.

The third-party risk management process involves:

- Identifying critical vendors and screening new vendors
- Assessing vendor risks and any risk mitigation and remediation activities
- Evaluating contracts and monitoring service level agreements
- Ongoing monitoring of the vendor's risk posture through audits or review of attestations attained, such as SOC 2 Type 2 reports, ISO 27001 certification, or HITRUST certification
- Create offboarding processes for the vendor as a whole or for vendor personnel that have access to systems when no longer required

Recovering from an Attack

If your organization experiences a data breach, there are immediate steps that should be taken to stem the damage and minimize the impact as well as to stay compliant with regulatory requirements.

01 Exercise Your Security Incident Response Plan

When a breach occurs, time is of the essence. Having an incident response plan is instrumental in alleviating the pressure of making decisions.

A typical plan should include:

- Roles and responsibilities
- Trigger incidents
- Technology environment overview, including a network diagram, containment procedures, and eradication and cleanup procedures
- Communications protocols
- A call list, including key vendors the organization is dependent on for technology support and law enforcement agencies

02 Bring In a Fresh Set of Eyes

This perspective often comes from a third-party that specializes in computer forensics or postattack analysis; the FBI has a division that investigates cybersecurity breaches, for example. The objective is to reveal clues or leads and offer external assistance when IT staff, who are often too close to the situation, might get weary-eyed and lose focus.

03 Know Your Notification Responsibilities

Federal and state-specific regulations mandate that affected parties be notified of any data breach that involves their personal information. It's important to know what your organization's obligations are from a compliance standpoint to avoid potential monetary penalties, fines, and lawsuits.

04 Call Your Insurance Carrier

Contact your insurance agent immediately upon stabilizing the situation. Determine what's covered, which may include fees related to legal, public relations, communications, notifications to external parties, forensics activities, and the overall response effort. Also, determine if theft of proprietary information is covered, particularly if you have intellectual property.

05 Develop Remediation Plans

After the situation has stabilized, many organizations fail to learn from their mistakes and don't implement the controls or protections necessary to prevent a future attack or at least minimize the risk of a successful attack. Developing a remediation plan to address the risk and implement stronger controls and protections is essential to prevent a similar attack in the future.

06 Include Security Protocol and Controls in Your Business Processes

Practice securing data throughout its life cycle. This means considering protections and security controls that should be in place once the data is acquired, when it goes through processing, where it gets stored, and when it's transmitted or moved.

The risk of a security incident or breach will always be present, but staying one step ahead and being aware of evolving cybersecurity threats will go a long way toward enhancing your organization's cybersecurity posture.

If you'd like to learn more, contact your Moss Adams professional or visit us online.

mossadams.com/cybersecurity

CYBERSECURITY SOLUTIONS

- IT security and risk assessments
- Network vulnerability assessments and penetration testing
- Web application penetration testing
- IT infrastructure and network security consulting
- Wireless network assessments
- Social engineering testing
- Incident response, disaster recovery, and business continuity planning
- Security policy and procedure development and review
- Technology strategic planning

PROFESSIONAL AFFILIATIONS

Our professionals are members of a number of information security associations, including:

- Information Systems Audit and Control Association
- Information Systems Security Association
- International Information Systems Security Certification Consortium
- Institute of Internal Auditors
- Cloud Security Alliance

The material appearing in this communication is for informational purposes only and should not be construed as legal, accounting, tax, or investment advice or opinion provided by Moss Adams LLP or its affiliates. This information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although these materials have been prepared by professionals, the user should not substitute these materials for professional services, and should seek advice from an independent advisor before acting on any information presented. Moss Adams LLP and its affiliates assume no obligation to provide notification of changes in tax laws or other factors that could affect the information provided.

ABOUT MOSS ADAMS

At Moss Adams, we believe in the power of possible. A business and personal advisory firm with more than 100 years of experience and 4,400 professionals across 30 markets, we work with clients to rise above challenges and seize emerging opportunities. Discover how we can help you go where you want to be next. Upward.

mossadams.com

Assurance, tax, and consulting offered through Moss Adams LLP. ISO/IEC 27001 services offered through Moss Adams Certifications LLC. Investment advisory offered through Moss Adams Wealth Advisors LLC.

MOSSADAMS