

A background image showing two IT professionals in a server room. One man is pointing at a laptop screen while the other looks on. They are both wearing blue lanyards. The room is filled with server racks and has a blue tint. Three red diagonal bars are on the left side of the image.

# A comprehensive guide to Assessing & Improving Cybersecurity

 **EXIGENT**

# A comprehensive guide to Assessing & Improving **Cybersecurity**

## 10 Steps to Assessing and Improving Cybersecurity

In today's digital world, cyber threats are a constant reality. From data breaches and ransomware attacks to business disruptions and reputational damage, the consequences of cyberattacks can be devastating. To protect your organization, **it's crucial to have a robust cybersecurity posture**. This ebook offers 10 steps for examining your cybersecurity.

### Step 1: Identifying High-Value Assets

Not all assets are created equal. The first step in securing your organization is identifying highvalue assets – those critical to your business operations and most attractive to attackers. These could include:

- **Servers:** *Housing sensitive data and applications, servers are prime targets for cybercriminals.*
- **Client information:** *Customer data, financial records, and intellectual property are essential for your business and valuable to attackers.*
- **Intellectual property:** *Trade secrets, patents, and proprietary information are crucial for your competitive advantage and vulnerable to theft.*
- **Domains:** *Your website and online presence are your digital storefront, and losing control of your domain can cripple operations.*
- **Financial records:** *Bank accounts, payment systems, and other financial data are essential for business operations and lucrative to cybercriminals.*

Once you've identified high-value assets, consider the potential consequences of a cyberattack on each asset and prioritize efforts accordingly. By focusing on protecting your most critical data and systems, you can significantly reduce overall risk.

### Step 2: Understanding Potential Threats and Risks

Cybersecurity threats come in various forms, each posing unique risks to your organization. Understanding these threats is crucial for developing effective defenses.

- **Cybercrime:** *Hackers may attempt to steal data, disrupt operations, or extort money from your organization. These attacks can come in various forms, from phishing scams and malware to ransomware and zero-day exploits.*
- **Human error:** *Unintentional mistakes by employees, such as clicking on phishing links or falling victim to social engineering scams, can compromise your security.*
- **System vulnerabilities:** *Outdated software, unpatched security holes, and misconfigured systems can provide attackers with easy access to your network.*
- **Physical threats:** *Natural disasters, power outages, and physical attacks on your infrastructure can compromise your data and systems.*

By understanding the different types of threats and the potential targets and impact of each, you can make informed decisions about cybersecurity investments and prioritize risk mitigation efforts.



68% of organizations have experienced one or more attacks that successfully compromised data and/or their IT infrastructure.

# A comprehensive guide to Assessing & Improving **Cybersecurity**

## Step 3: Identifying and Addressing Common Vulnerabilities

While a comprehensive professional security assessment is essential, your organization can address some common vulnerabilities quickly and effectively:

- **Lack of multi-factor authentication (MFA):** MFA adds an extra layer of security by requiring a second identification confirmation, such as a code from your phone, to access sensitive data. Implementing MFA can significantly reduce the risk of unauthorized access.
- **Outdated technology:** Using obsolete software and operating systems leaves systems vulnerable to known exploits and exposes them to security risks. Regularly update software and hardware to stay ahead of attackers.
- **Lazy patching:** Patching known vulnerabilities promptly is crucial for closing security holes. Develop a patching strategy to ensure timely updates to all systems.
- **Employee-created vulnerabilities:** Unsecured devices, weak passwords, and poor security hygiene by employees can compromise your network. Implement security awareness training and enforce strong security policies to educate and empower employees.

Addressing these basic vulnerabilities can significantly improve your security posture before diving into a deeper assessment.

Keep reading to learn about **risk evaluation**, developing a **risk management plan**, and implementing a comprehensive **cybersecurity strategy**.



In 2022, intrusion attempts by cyber criminals increased 19% to **6.3 trillion**.

## Step 4: Evaluating Risks and Prioritizing Action

Once you've identified the threats and vulnerabilities facing your organization, it's time to assess the risks they pose. This involves considering two key factors:

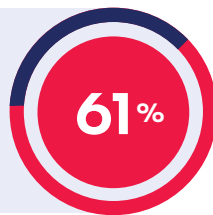
- **Likelihood:** How probable is it that a specific threat will occur? Analyze past breaches, industry trends, and your specific vulnerabilities to estimate the likelihood of each threat manifesting.
- **Impact:** What are the potential consequences of a successful attack? Consider the financial losses, operational disruptions, reputational damage, and legal ramifications to quantify the potential impact of each risk.

By combining these factors, you can prioritize your risk mitigation efforts. Focus on addressing the most likely and impactful threats first, allocating resources for effective implementation of security measures.



# A comprehensive guide to Assessing & Improving Cybersecurity

61% of organizations have suffered outages that cost their organization more than \$100,000.



## Step 5: Building Robust Risk Management Plan

Risk assessment helps us understand the dangers, but risk management translates that understanding into action. Developing a comprehensive risk management plan is crucial for proactively addressing potential threats. Key elements of a strong plan include:

- **Clearly defined objectives:** Outline desired outcomes in terms of risk reduction and improved security posture.
- **Specific control measures:** Identify specific actions to mitigate identified risks, such as implementing MFA, patching systems, or conducting security awareness training.
- **Resource allocation:** Determine the resources (personnel, budget, tools) needed to implement control measures effectively.
- **Timeline and milestones:** Establish a clear timeline for implementing the plan and set milestones to track progress.
- **Monitoring and review:** Continuously monitor the effectiveness of controls and update the plan as needed to adapt to evolving threats and vulnerabilities.

A well-developed risk management plan provides a roadmap for proactive cybersecurity, ensuring your organization stays ahead of emerging threats.

## Step 6 : Craft a Comprehensive Cybersecurity Strategy

Risk management focuses on specific threats, but a comprehensive cybersecurity strategy encompasses your overall approach to securing your organization. This strategy goes beyond technical measures and address all aspects of security, an approach referred to as “cyber resiliency.”

- **Security awareness training:** Educating employees on cybersecurity best practices, such as phishing awareness and password hygiene, is crucial for strengthening your security posture.
- **Access control:** Implement granular access controls to restrict access to sensitive data and systems based on the principle of least privilege. Don't overlook the physical access control that can be required by compliance standards.
- **Data security:** Encrypt sensitive data at rest and in transit and implement data loss prevention (DLP) solutions to limit unauthorized data access and exfiltration. Consider a zero-trust approach that assumes any internal or external access could be a bad actor.
- **Incident response:** Develop a well-defined incident response plan to manage cyberattacks effectively, minimizing damage and ensuring a swift recovery.
- **Business continuity:** Prepare for unforeseen events like natural disasters or power outages with a plan to ensure continued business operations and data availability.

By addressing these critical areas, your cybersecurity strategy creates a holistic framework for safeguarding your organization against diverse threats.

Continue to the next chapters, where we'll explore essential **cybersecurity policies**, **cyber insurance** considerations, and the importance of **eliminating legacy technology**.



# Step 7: Establishing Essential Cybersecurity Policies

While technology plays a vital role in cybersecurity, clear and comprehensive policies set the ground rules for behavior and expectations. Implementing these essential policies empowers employees and strengthens your overall security posture:



## Acceptable Use Policy (AUP)

Defines acceptable and prohibited uses of technology resources such as company computers, emails, and the internet. Clarifies expectations regarding downloading software, sharing information, and online communication. Helps prevent employee misconduct and misuse of technology that could compromise security.



## Data Management/Classification

Categorizes data based on sensitivity (e.g., confidential, proprietary, public) and outlines handling procedures for each category. Specifies access controls, storage requirements, and retention periods for distinct types of data. Ensures consistent data management practices and minimizes the risk of accidental exposure or unauthorized access.



## Access Control Policy

Defines who has access to sensitive data and systems, based on the principle of least privilege. Outlines the process for requesting and granting access and establishes review procedures to ensure continued appropriateness. Prevents unauthorized access and minimizes the number of individuals with access to sensitive information.



## Password Creation/Management

Establishes minimum password complexity requirements (length, character types, etc.) and update frequency. Prohibits the use of weak passwords and common phrases and encourages the use of password managers. Reduces the risk of successful brute-force attacks and unauthorized access via stolen credentials.



## Remote Access Policy

Defines the rules and procedures for accessing company resources remotely, including approved devices, VPN usage, and data security practices. Minimizes the risks associated with remote work and ensures consistent security measures when accessing sensitive information outside the office network.



## Incident Response Policy

Outlines the steps to take in case of a data breach or security incident, including notification procedures, containment measures, and remediation actions. Ensures a coordinated and effective response to minimize damage and restore operations quickly. Helps mitigate legal and reputational risks associated with security incidents.



## Business Continuity

Define procedures for maintaining business operations and data availability in the event of natural disasters, power outages, or other disruptions. Identify critical systems and data, designate backup locations, and outline recovery processes. Ensure your organization can bounce back quickly from unforeseen events and minimize downtime.



## Regular Maintenance

Regularly reviewing and updating these policies, coupled with comprehensive training for all employees, forms the foundation for a strong security culture within your organization.

# A comprehensive guide to Assessing & Improving **Cybersecurity**

## Step 8: Securing Cyber Insurance for Extra Protection

While robust security measures go a long way, cyber insurance provides an additional layer of financial protection in case of a cyberattack. It can help cover costs associated with:

- *Data recovery and remediation*
- *Legal fees and regulatory fines*
- *Public relations and reputation management*
- *Business interruption and lost revenue*

However, securing the right cyber insurance requires careful evaluation:

- **Assess your cyber risk profile:** *Understand your vulnerabilities and the potential impact of an attack to determine the level of coverage you need.*
- **Compare different policies:** *Look for comprehensive coverage with clear terms and conditions, including exclusions and limitations.*
- **Choose a reputable insurer:** *Select an experienced and financially stable provider with expertise in cyber risks.*
- **Prepare your environment:** *Take the time to work through a comprehensive cyber insurance prep checklist before applying for coverage can help improve your ability to secure coverage.*

Remember, cyber insurance is not a substitute for strong cybersecurity practices. It's essential to prioritize proactive risk mitigation and maintain robust security measures to minimize the likelihood of an attack in the first place.



**2 out of 3 small to midsize businesses will have a breach of some sort in the next 12 months.**

# A comprehensive guide to Assessing & Improving **Cybersecurity**

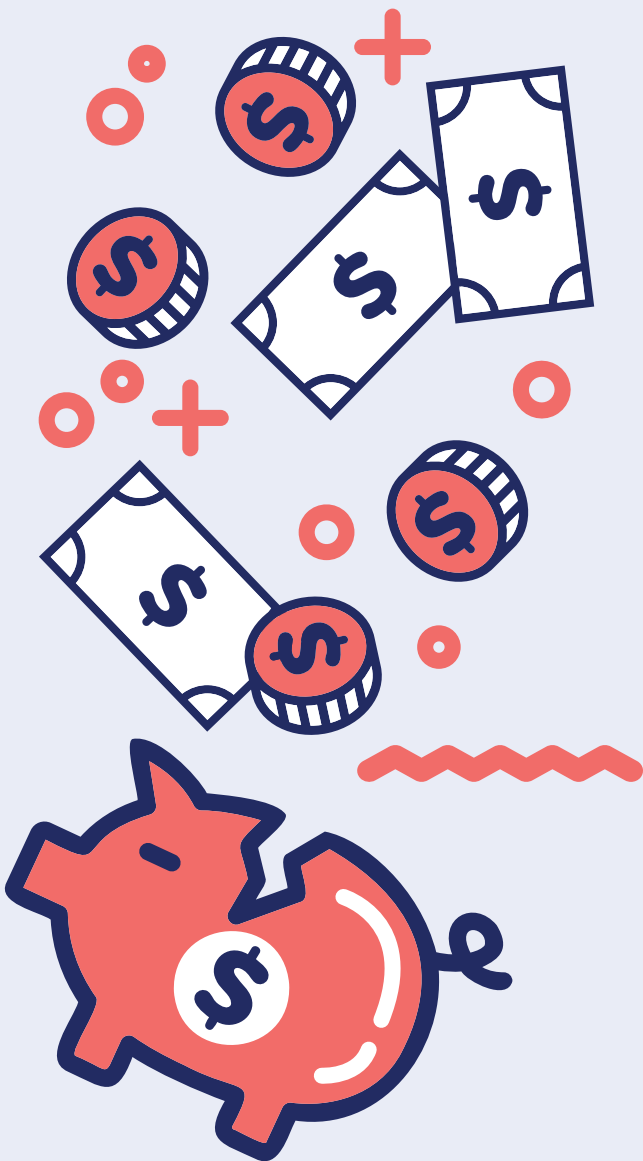
## Chapter 9: Migrate Away from Legacy Tech

Outdated technology poses a significant threat to your cybersecurity posture. Legacy systems often lack vendor support, making them vulnerable to unpatched vulnerabilities and incompatible with modern security solutions.

Consider these challenges:

- **Vulnerability to Attack:** *Unpatched systems provide easy entry points for hackers, leaving your data exposed to cyberattacks.*
- **Compatibility Issues:** *Integrating obsolete technology with newer solutions can be difficult, creating security gaps and hindering your ability to implement essential security tools.*
- **Maintenance Expenses:** *Keeping legacy hardware and software operational can be costly, requiring specialized technicians and consuming more resources than modern alternatives.*
- **Compliance Challenges:** *End-of-life technology often doesn't meet industry compliance standards, exposing your organization to legal and regulatory risks.*

Migrating away from legacy technology involves careful planning and execution. Evaluate your systems, prioritize replacements based on criticality and vulnerability, and choose modern solutions that offer improved security, efficiency, and scalability. While the initial investment may seem significant, the long-term benefits of enhanced security, improved productivity, and reduced maintenance costs often outweigh the cost of maintaining outdated technology.



**\$9.4 million** was the average cost of a 2022 breach in the United States.



# A comprehensive guide to Assessing & Improving **Cybersecurity**

## Step 10: Monitor and Adapt is Key to Sustained Security

Cybersecurity is not a one-time fix, but an ongoing journey of vigilance and adaptation. The threat landscape is constantly evolving, with new vulnerabilities emerging and attackers using increasingly sophisticated tactics. To maintain a robust security posture, continuous monitoring, and robust adaptation are crucial.

Here are top practices for ongoing security vigilance:

- **Proactive threat intelligence:** *Stay informed about emerging threats, vulnerabilities, and attack trends. Partner with a trusted managed IT services partner that provides valuable insights and expert guidance.*
- **Regular system scans and vulnerability assessments:** *Conduct regular scans of your systems and networks to identify potential vulnerabilities and misconfigurations. Prioritize patching or mitigating newly discovered vulnerabilities promptly.*
- **Security monitoring and event log analysis:** *Implement security monitoring tools and analyze event logs to detect suspicious activity and potential breaches. Investigate anomalies and implement appropriate responses to contain and remediate potential incidents.*
- **Security awareness training and phishing simulations:** *Educate your employees on cybersecurity best practices through regular training sessions. Conduct phishing simulations to assess their awareness and build resilience against social engineering attacks.*
- **Incident response plan testing:** *Regularly evaluate and refine your incident response plan to ensure it is effective in handling security incidents.*

- **Data backups and disaster recovery drills:** *Maintain regular backups of critical data, routinely test those backup processes, and conduct disaster recovery drills to confirm you can restore operations quickly and minimize downtime in case of an incident.*
- **Embrace a security culture:** *Fostering a culture of security within your organization is key. Encourage employees to report suspicious activity, prioritize security awareness in onboarding and training, and promote open communication about cybersecurity risks and best practices.*

By continuously monitoring, adapting, and improving your security measures, you can build a resilient defense against ever-evolving threats and safeguard your organization's valuable assets.

## Summary: Securing Your Digital Future

In today's digital landscape, cybersecurity is no longer just an IT concern; it's a business imperative. Protecting your valuable assets, data, and reputation from cyber threats requires a proactive and comprehensive approach. This ebook has provided you with a roadmap for achieving just that – 10 essential steps to assess and improve your cybersecurity posture.

Partnering with a managed IT services provider that understands the constantly shifting threat landscape and can guide your organization toward cyber resiliency can provide the highest level of reassurance and protection.

Learn more about how Exigent Technologies leverages nearly 30 years of cybersecurity experience to protect clients at [www.exigent.net](http://www.exigent.net).