**Cybersecurity risk mitigation** involves the use of security policies and processes to **reduce the overall risk or impact of a cybersecurity threat**. In the context of cybersecurity, risk mitigation can be separated into three key elements:

1. **Prevention**: Implementing measures to prevent cyber threats from occurring in the first place. This includes deploying firewalls, intrusion detection systems, access controls, and secure coding practices.
2. **Detection**: Establishing mechanisms to detect and identify potential threats or breaches promptly. This involves monitoring network traffic, analyzing logs, and using threat intelligence tools.
3. **Remediation**: Taking corrective actions when a threat is detected. Remediation includes incident response, patch management, and recovery procedures to minimize the impact of successful attacks.

**What is cyber risk mitigation?**

Cyber risk mitigation is the application of policies, technologies and procedures to reduce the likelihood and impact of a successful cyber attack. It is a critical practice to help guide decision-making around risk control and mitigation and allows your organization to stay protected and achieve its business goals.

A cyber risk mitigation practice allows your organization to answer the following questions:

* Do we have a [complete inventory of all our assets](https://www.balbix.com/insights/what-is-asset-inventory-management/)?
* Do we know which assets are the most critical?
* Do we have real-time visibility into our entire [attack surface](https://www.balbix.com/insights/attack-surface-management/)?
* Can we prioritize our [vulnerabilities](https://www.balbix.com/insights/what-is-a-vulnerability/) based on business criticality and risk?
* How comprehensive and effective are our cyber security controls?
* How vulnerable are we to potential breaches and attacks?
* What policies, technologies and procedures should we deploy to maintain [cyber resilience](https://www.balbix.com/insights/what-is-cyber-resilience/)?

**What are the challenges of cyber risk mitigation?**

Cyber risk mitigation can be challenging as many organizations lack real-time visibility of their cybersecurity posture in light of the rapid evolution of networks and changing threat landscape. They often don’t know what assets they need to protect, where and how they could be breached and whether adequate [security controls](https://www.balbix.com/blog/the-reason-you-need-to-have-complete-visibility-of-all-your-assets-and-security-controls/) are in place. Even if controls are in place, security teams aren’t always confident that they’ll be effective against different types of threats.

Speed is another challenge. In most instances, security teams aren’t able to identify and respond to threats in a timely manner as many risk identification and mitigation processes are still manual. Lack of resources can be another reason why organizations might have difficulty mitigating cyber risk efficiently.

**What are the benefits of cyber risk mitigation?**

There are many benefits of cyber risk mitigation, some of which include:

Timely identification and mitigation of cyber risks

Cyber risk mitigation efforts by your security teams help identify risks in a timely manner. Doing so aids with determining where the threats are in your network and ensuring that your critical systems stay safe. These efforts involve monitoring your systems for suspicious activity and assessing vulnerabilities to pinpoint security gaps and determine remediation steps.

Fewer vulnerabilities

Cyber risk mitigation efforts help identify threats early so your organization has time to eliminate vulnerabilities before they can be exploited by cyber criminals. For example, by undertaking a [cyber risk assessment](https://www.balbix.com/insights/how-to-perform-a-cyber-risk-assessment/), security teams can identify all types of threats – internal and external – and understand security gaps in order to strengthen its controls and mitigate vulnerabilities faster.

Better security compliance

Cyber risk mitigation efforts help your organization implement the right security procedures, policies and technologies to make it easier to meet regulatory standards and comply with security requirements. Taking such measures allows you to avoid costly penalties and fines and improve your organization’s [security posture](https://www.balbix.com/insights/what-is-cyber-security-posture/).

Improved brand reputation

Another vital benefit of cyber risk mitigation is that it protects your organization’s reputation. By implementing risk mitigation policies, procedures and technologies, you can keep your data protected, thereby gaining trust and increasing loyalty from your customers.

Increased revenue

Cyber risk mitigation efforts can identify vulnerabilities and other issues to help your organization avoid downtown and prevent the loss of revenue from compromised data and systems.

Understanding risk mitigation in cyber security requires a grasp of its key elements.

These include risk identification, risk assessment, risk prioritisation, and risk control.

### Risk identification

The first step in risk mitigation is [identifying potential risks](https://www.institutedata.com/blog/9-types-of-cybersecurity-threats/).

In the fourth quarter of 2022, the Anti-Phishing Working Group (APWG) recorded a total of 1,350,037 phishing attacks, marking an increase from the previous quarter’s 1,270,833.

Throughout the year 2022, APWG documented approximately [4.7 million phishing attacks](https://www.stationx.net/phishing-statistics/#:~:text=In%20Q4%202022%2C%20The%20Anti,by%20more%20than%20150%25%20yearly.), reflecting a significant annual surge of over 150%.

These attacks encompass a spectrum of threats, ranging from conventional phishing attacks to more intricate and sophisticated forms, such as advanced persistent threats (APTs).

Tools such as threat intelligence platforms can aid in risk identification, providing insights into emerging threats and helping organisations stay one step ahead of cybercriminals.

### Risk assessment

Once risks have been identified, the next step is to assess them.

This involves evaluating the potential impact of each risk and the likelihood of it occurring.

This step is crucial in understanding the level of threat each risk presents to the organisation.

Risk assessment tools can help in this process, providing a quantitative analysis of risks and helping organisations prioritise their mitigation efforts.

### Risk prioritisation

Not all risks are equal, and organisations need to prioritise their mitigation efforts.

This involves ranking risks based on their potential impact and the likelihood of them occurring.

By doing so, organisations can focus their resources on the most significant threats.

Risk prioritisation is often a complex process that requires a deep understanding of the organisation’s operations and the potential impact of each risk.

### Risk control

The final step for risk mitigation in cyber security is controlling the risks.

This involves implementing measures to reduce the likelihood of risks occurring or to minimise their impact if they do occur.

This could include anything from implementing robust security measures to providing staff training on cyber security best practices.

Risk control is an ongoing process that requires regular review and adjustment as the cyber security landscape evolves.