White paper

How to perform a cyber security risk assessment

VULCAN.

Table of contents

Introduction 03

Understanding cyber security risk assessment 04

The process of cyber security risk assessment 05

12 steps to perform a cyber security risk assessment 06

Parting thoughts 12

About Vulcan Cyber 12

Introduction

Cyber risk, a term barely in our lexicon a few decades ago, has now firmly planted its roots in our present reality. Today, the digital era exposes organizations globally to a myriad of security threats. However, these cyber threats do not merely exist outside our walls. Rather, they lurk within our very systems, seeking opportunities to exploit unnoticed vulnerabilities. The consequences? They're not trivial: substantial financial loss, reputational erosion, operational upheaval, and severe legal implications.

According to a report from Cybersecurity Ventures and sponsored by eSentire

Recognizing cyber risk extends beyond spotting threats. It requires a deep understanding of your organization's frailties, the valuable assets at stake, and the catastrophic aftermath if these assets are compromised.

This is where cyber security risk assessment comes into play. A cyber security risk assessment is a methodical procedure that revolves around detecting, scrutinizing, and estimating cyber risks. It's a critical component of any organization's cyber security strategy, providing the insights needed to manage risks effectively and protect valuable information assets.

Through this definitive guide, we chart a course to effectively conduct a cyber security risk assessment. We will steer you through identifying your most valuable assets, understanding their worth, and establishing an iterative risk management strategy. We emphasize a structured method, underscoring the invaluable role of established cyber security frameworks and standards.

Understanding cyber security risk assessment

Cyber security risk assessment methodically guides organizations to identify, analyze, and evaluate vulnerabilities within their information systems. It's an essential cog in the machinery of cyber security strategy, arming you with the necessary insights to devise robust defenses for your information assets.

It is a pivotal process that unveils numerous advantages:

Threat identification: Pinpoint the potential dangers that could disrupt your information security and gauge the possibility of such breaches.

Vulnerability risk prioritization: Uncover the weak points in your systems and comprehend the business impact of these vulnerabilities being exploited.

Informed decision-making: It guides you in making calculated choices about risk management strategies such as mitigation, transfer, acceptance, or avoidance.

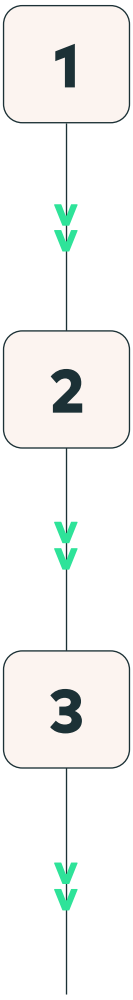
However, remember that a cyber security risk assessment isn't a one-and-done activity. It's a continuous cycle, an ever-attentive watchdog adapting to the incessant evolution of your organization's systems, operations, and the outside threat environment. It learns and adjusts to the progression of new technologies, emerging threats, and shifting business objectives.

But who stands to benefit from conducting a cyber security risk assessment? In the grand scheme of things, any entity is entwined with information systems and data. From the small business owner safeguarding customer data on a solitary server to sprawling corporations managing complex IT infrastructure—cyber security risk assessment is indispensable. No matter the size or sector, this assessment plays a critical role in steering clear of cyber risks and ensuring the safety of your invaluable information assets.

The process of cyber security risk assessment

A structured approach is critical when conducting a cyber security risk assessment. It ensures that the process is exhaustive and efficient. It helps organizations identify all potential risks, analyze and evaluate these risks appropriately, and decide on the best risk treatment options. It also ensures that the results of the risk assessment are documented properly, supporting decision-making and risk management activities.

Throughout this process, the organization should refer to established cyber security frameworks and standards. These provide best practices and guidelines for conducting a risk assessment, ensuring that the process is comprehensive, consistent, and effective. Examples of such frameworks and standards include the ISO 27001[1] standard for information security management, the NIST Cybersecurity Framework[2], and the CIS Critical Security Controls.



Understanding the business context

The process begins with a clear understanding of the organization's business context including its mission, objectives, stakeholders, and the regulations under which it functions. This understanding forms the foundation for the risk assessment, providing the context in which risks will be identified, analyzed, and evaluated.

Identifying information assets

The organization needs to identify its information assets and their value. This could include data, software, hardware, systems, and even people. The value of these assets is not just their financial worth, but also their importance to the organization's operations and the potential impact of a security incident.

Identifying threats and vulnerabilities

Once the assets have been identified, the organization needs to identify the threats that could potentially impact these assets. These could be anything from natural disasters and system failures to cyber attacks and insider threats. The organization also needs to identify the vulnerabilities that could be exploited by these threats, using techniques such as vulnerability assessments, threat intelligence and penetration testing.

[1] ISO/IEC 27001 Requirements
[2] NIST Cybersecurity Framework

4

Evaluating and prioritizing risks

The identified risks are then analyzed to determine their likelihood and potential impact. This involves taking factors such as the nature of the threat, the efficacy of the current preventive measures, and the plausible aftermath of a security mishap into account. The risks are then appraised to ascertain their acceptability or to decide if additional measures are needed.

5

Deciding on risk treatment options

Based on the evaluation, the organization can then decide on the appropriate risk treatment options. These could include implementing new controls to reduce the risk, transferring the risk through insurance, accepting the risk if it is within the organization's risk appetite, or avoiding the risk by changing business processes.

6

Documenting the results

The next step is documenting the results of the risk assessment in a risk assessment report. This report provides a record of the risk assessment process and its findings, supporting decision-making and risk management activities.

7

Reviewing and updating the assessment

Finally, the risk assessment process is not an isolated event. It demands continuous re-evaluation and modification to ensure that it carries weight in the face of changing business circumstances and evolving threats.

12 steps to perform a cyber security risk assessment

Performing a cyber security risk assessment involves a series of steps that help organizations identify, analyze, and manage their cyber risks. Here's a detailed look at these steps:

1. Determine information value

The first step in a cyber security risk assessment is understanding the value of the information your organization holds. It's not only about fiscal value but also about the possible ramifications of an information breach.

In 2022, the United States experienced 1,802 data breaches[3], affecting more than 422 million people. These compromises included data breaches, leakage, and exposure, all of which resulted in sensitive data being accessed by an unauthorized threat actor. Sectors like financial services, medical and healthcare, and those involved with manufacturing were hit the hardest.

The potential impact of such breaches is not just financial but can also lead to legal penalties, competitive disadvantages, and reputational damage. To that end, this step is crucial, as it helps prioritize efforts in the later stages of the risk assessment.

2. Identify and prioritize assets

Once you've determined the value of your information, the next step is to identify all the assets in your organization. These assets include:

- **Hardware:** Servers, computers, mobile devices, and any other physical devices used in your organization.
- **Software:** Applications, operating systems, and databases that store and process your information.
- **Data:** Both the data you store and the data you process. This includes customer data, employee data, intellectual property, and any other sensitive information.
- **People:** This includes your workforce, contractors, and anybody who can access your systems.
- **Systems:** These are your networks, the IT infrastructure, IoT devices, cloud services, and physical security systems like surveillance cameras and similar that help your organization operate efficiently.

After recognizing your assets, prioritize them according to their significance and value to your institution. This will guide your risk assessment efforts in the most vital areas.

3. Identify cyber threats

With a clear understanding of your valuable assets, the next step is to identify the threats that could potentially harm those assets. Threats can come from various sources:

- **Natural disasters:** Events like floods, fires, or earthquakes that could damage your physical infrastructure.
- **System failures:** This could be hardware malfunctions, software glitches, or network downtime.
- **Human errors:** Mistakes made by your employees or contractors, such as accidentally deleting important data or falling for phishing scams.
- **Adversarial threats:** These include hackers, cyber criminals, or even state-sponsored attackers who are actively trying to breach your security and gain unauthorized access to your systems or data.

[3] Annual number of data compromises and individuals impacted in the United States from 2005 to 2022

A White & Case LLP report[4] states that even the most cautious company can be a victim of a cyber security incident, such as the theft of client or company information, or a ransomware attack.

These incidents can lead to significant reputational damage, which can erode customer trust and lead to loss of business. In addition, companies may face legal implications, including fines, breach of contract claims, and litigation. The report emphasizes the importance of having an effective data breach response program and managing cyber security risks proactively.

For example, in case of non-compliance the General Data Protection Regulation (GDPR) in the European Union can impose fines of up to €20 million[5], or 4% of the global annual revenue from the previous financial year, whichever is higher. This means that companies that do not comply with the GDPR could be fined significantly.

Identifying these threats gives you a clear picture of the potential risks your organization faces, setting the stage for the next steps in the risk assessment process.

4. Identify vulnerabilities

After you have identified the potential threats, the next phase involves identifying vulnerabilities within your organization that could be exploited by these threats. Vulnerabilities can exist in various forms:

- **Software vulnerabilities:** These can include outdated software, unpatched systems, or insecure configurations.
- **Hardware vulnerabilities:** Physical security is just as important as digital security. Unsecured servers, lack of backup power supplies, or inadequate cooling systems can all be considered hardware vulnerabilities.
- **Operational vulnerabilities:** These can include inadequate security policies, lack of employee training, or ineffective incident response procedures.

Various tools and techniques can be used to identify these vulnerabilities, including vulnerability scanners, penetration testing, and security audits. It's also beneficial to refer to resources like the National Vulnerability Database (NVD) or vendor security advisories for information on known vulnerabilities.

5. Analyze controls and implement new controls

Once you've identified your vulnerabilities, the next step is to analyze the controls you currently have in place to mitigate these vulnerabilities. Controls can be:

- **Technical:** These include firewalls, intrusion detection systems, encryption, and other security software and hardware.

[4] Cybersecurity: Legal Implications and Risk Management

[5] The Biggest GDPR Fines of 2022

- **Administrative:** These include security policies, procedures, and training that help reduce human error and guarantee everyone across the organization understand their part in upholding security.
- **Physical:** These include locks, access cards, and other physical security measures.

After analyzing your existing controls, you may find that you need to implement new controls to address uncovered vulnerabilities. The type of control you implement will depend on the specific vulnerability you're trying to mitigate.

6. Calculate the likelihood and impact of each threat

The next step is to calculate the likelihood of each identified threat exploiting a vulnerability and the potential impact of such an event. This phase is essential as it enables you to comprehend the possible threat to your organization.

Factors to consider when calculating likelihood include the capability of the threat actor, the nature of the vulnerability, and the effectiveness of existing controls. When calculating impact, consider factors like the sensitivity of the affected data, the criticality of the affected system, and the potential operational and reputational damage.

It's important to note that in 2022, the healthcare, financial services, and manufacturing sectors were most vulnerable to data breaches[6]. The annual number of data compromises and individuals impacted in the United States from 2005 to 2022, indicates a high likelihood of threat actors targeting them. The impact of these breaches was significant, given the sensitive nature of data in these sectors and the potential operational disruption and reputational damage that could result.

7. Take into account the value of the information and the attack prevention cost

After calculating the likelihood and impact of various scenarios, the next step is to prioritize the risks. This requires you to balance the expense of risk prevention against the worth of the data at stake. Here are some factors you need to consider when prioritizing risks:

- **The potential impact of the risk:** Risks that could cause significant damage to your organization should be given higher priority.
- **The likelihood of the risk:** Risks that are more likely to occur should also be given higher priority.
- **The cost of mitigation:** Consider the cost of implementing preventive measures to reduce each risk. If the cost of mitigation is higher than the potential loss, it might be more cost effective to accept the risk or consider other risk treatment options.

[6] Annual number of data compromises and individuals impacted in the United States from 2005 to 2022to 2022

8. Document results from risk assessment reports

Once you've identified and prioritized your risks, it's important to document your findings. A risk assessment report should ideally include:

- A description of the identified risks, including their potential impact and likelihood
- A description of the existing controls and their effectiveness
- Recommendations for additional controls or other risk treatment options

This report will provide a clear record of your risk assessment process and support decision-making for risk management. In light of the increasing number of data compromises, such documentation is crucial for demonstrating due diligence and compliance with data protection regulations, as well as for informing strategic decisions about cyber security investments and initiatives.

9. Develop a robust risk management plan

Based on the findings of your risk assessment, you can now work toward creating a risk management plan. You will first have to consolidate all your cyber security information. You'll want to spotlight risk hotspots—things like weak firewall defenses, out-of-date access permissions, and gaps in team knowledge about malware, phishing, hacking, and other typical cyber security hazards. Don't forget to earmark your most precious data assets, such as proprietary information and software.

Next, you need to correlate the potential damages each risk area could cause to your business processes and calculate the cost of remediation. This also includes any reporting responsibilities that are necessary for your business to keep up with industry regulations.

After identifying and assessing the risks, you need to enrich your understanding of them. This means scoring them based on the potential fallout and the expense of fixing them. Keep a log of the flagged risk areas and form dedicated security teams responsible for rolling out security guidelines for each risk.

10. Implement the risk management strategy

Once your risk management strategy has been developed, the next step is to implement it. This could involve making changes to your IT infrastructure, updating your security policies, or rolling out a new training program. Make sure to notify all parties involved about these updates and offer the needed support for smooth execution.

Prioritization is key at this stage. Assemble a security team to translate your research into a clear risk profile of your company. This team will also lead in educating staff on network security and updating everyone on the latest cyber security risks. Plus, it's crucial to orchestrate your efforts to ensure that all actions are coordinated and efficient. This involves automating the communication and collaboration remediation tasks to streamline risk mitigation.

Next, you'll have to focus on collaboration. It ensures everyone is on the same page about the risks and consequences of weak spots, and organizes remediation efforts across teams and systems. This will help foster a security-conscious culture across the organization.

The final step is reporting. Generate and share reports that give a rundown of the identified vulnerabilities, the progress of resolution efforts, and how well those efforts are working.

The security team will also lead in educating staff on network security and updating everyone on the latest cyber security risks, such as new ransomware, social engineering schemes, and other threats that may fit your risk profile.

11. Monitor and review

After implementing your risk management strategy, it's crucial to monitor its effectiveness and review it regularly. This involves:

- **Regular audits:** Conduct regular security audits to ensure that your controls are working properly and to identify any new vulnerabilities.
- **Regular reviews:** Review your risk management strategy periodically so that it is always up to date. This should factor in any modifications in your business operations, technological environment, or the external threat landscape.
- **Incident tracking:** Keep track of any security incidents that occur. This can offer precious insights into the efficiency of your preventive measures and help you detect areas that can be improved.

12. Continuous improvement

Cyber security is an ongoing effort and far from a static endeavor. The threat landscape is evolving continuously, and your risk management plan needs to keep up with these changes:

- **Updating controls:** As new threats emerge and old ones evolve, you may need to update your controls to ensure they remain effective.
- **Updating policies and procedures:** As your business grows and changes, you may need to update your security policies and procedures to reflect these changes.
- **Training:** Provide continual training to your employees to ensure they stay abreast with the latest security procedures and understand their role in maintaining security.

By following these steps, you can ensure that your cyber security risk assessment is thorough, effective, and aligned with your organization's needs. It's a continuous process of improvement that helps you stay one step ahead of the threats and protect your valuable information assets.

LEARN FROM THE EXPERTS WITH THESE CYBER SECURITY TIPS AND BEST PRACTICES >>

Parting thoughts

Cyber security incidents can have far-reaching implications beyond the immediate financial impact. As we've seen, performing a cyber security risk evaluation is not a one-off job but a cyclic process. It's a crucial part of any organization's cyber security strategy, helping to identify, analyze, and manage cyber risks. By following the steps outlined in this guide, you can ensure that your risk assessment process is thorough, effective, and aligned with your organization's needs.

About Vulcan Cyber

Vulcan Cyber enables security teams to effectively manage and reduce vulnerability risk across IT and cloud-native surfaces. The platform consolidates vulnerability scan and threat intelligence data from all attack surfaces and provides asset risk context, recommendations for the best fixes, and automated remediation workflows to streamline tedious mitigation tasks. Our commitment to innovation has earned recognition as a Forrester Wave Leader in the Q3 2023 Vulnerability Risk Management, a 2019 Gartner Cool Vendor and as a 2020 RSA Conference Innovation Sandbox finalist. Prominent security teams, such as those at Mandiant, Deloitte, and Skechers, trust Vulcan Cyber to help them own their risk.

TRY VULCAN FREE >>

READ OUR BLOG >>

Start owning your risk today

SEE VULCAN CYBER IN ACTION