CYE

A Step-By-Step Guide to Cyber Risk Assessment

How to strengthen your security posture and optimize security investments by assessing and prioritizing cyber risks

Why Conduct a Cyber Risk Assessment?

Today, IT security leaders are faced with an almost overwhelming array of threats, from ransomware and phishing, to attacks on infrastructure, to the theft of intellectual property and customer data, to unsecure supply chain partners, to malicious actions by insiders. They must anticipate risks related to cloud computing, remote work, mobile devices, and other innovations. They are also under pressure to cut expenses and invest wisely.

For these reasons and others, CIOs and CISOs need to make optimum use of the limited resources available to defend their organizations. One of the most effective tools available to them is a cyber risk assessment.

A cyber risk assessment enables security leaders to:

- Achieve consensus on the threats most relevant to their organization
- Identify vulnerabilities in existing defenses
- Assess the maturity of their IT and OT security programs
- Better communicate risks to non-technical executives
- Prioritize investments in security controls
- Develop a roadmap to improve their security program

Cyber risk assessments also create the basis for cyber risk quantification, which CIOs and CISOs can use to justify security investments and fine-tune their risk management strategies.

This ebook outlines three approaches to cyber risk assessment and presents a step-by-step process for conducting an assessment that produces powerful insights and recommendations for security leaders.

> [Cyber] risk assessments are used to identify, estimate, and prioritize risk to organizational operations… organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems.
>
> NIST Guide for Conducting Risk Assessments
> (SP 800-30, Revision 1)

Three Approaches to Cyber Risk Assessment

Three leading approaches to conducting a cyber risk assessment are compliance-driven, threat modeling, and attack route analysis. All three approaches involve the same activities: understanding the organization's security posture and compliance requirements, collecting data on threats, vulnerabilities, and assets, modeling potential attacks, and prioritizing mitigation actions. However, there are important differences in emphasis and in results.

Approach 1: Compliance-driven

The compliance-driven approach to cyber risk assessment focuses on comparing an organization's security controls with requirements specified in cybersecurity and regulatory frameworks, such as those published by the National Institute of Standards and Technology (NIST), ISO/IEC, the Payment Card Industry Security Standards Council, or the European Union. Some of these organizations even provide guidance on how to conduct a cyber risk assessment (for example, NIST SP 800-30 and ISO/IEC 27005).

These frameworks are well established and very credible as guidelines for compliance activities and basic security practices. However, they provide mostly high-level, "one size fits all" recommendations and typically lack detail on (or ignore) important areas such as cloud security and secure coding practices. Sometimes they lead to a "check-the-box" mentality where security teams are incentivized to fix many vulnerabilities quickly even when they pose no significant risk to the organization.

	Compliance-Driven	
Focus	Pros	Cons
Compare controls with requirements of NIST, ISO/IEC, PCI, GDPR or other cybersecurity and regulatory frameworks	• Uses established, credible frameworks • Ensures regulatory compliance	• Emphasizes generic requirements rather than specific needs of the organization • Can encourage a "check-the-box" mentality

Approach 2: Threat modeling

Another approach to assessment starts with compiling comprehensive lists of the threats facing the organization, vulnerabilities in systems and networks, and infrastructure and information assets. This information is acquired through questionnaires and interviews with IT and business managers, together with vulnerability scanning. The data is used to model the impact of possible security events based on factors such as the probability of attacks, the severity of vulnerabilities, the weaknesses of existing controls, the value of assets, and the consequences of outcomes such as data breaches and business interruptions. The security team can then select remediation actions that most reduce risk.

A cyber risk assessment based on extensive threat modeling generates valuable, detailed insights into potential threats and gaps in existing controls. The results identify the greatest risks to the organization and help prioritize remediation actions.

However, this approach requires a large investment of staff time compiling lists, completing questionnaires, holding interviews, collecting data, estimating probabilities, and modeling long catalogs of threats and vulnerabilities. It may take weeks or months before the analysis is complete and ready to be applied, by which time much of the analysis may be obsolete.

	Threat Modeling	
Focus	Pros	Cons
Compile comprehensive lists of threats, vulnerabilities, and assets and model probability and impact of possible security events	• Generates detailed insights into potential threats and gaps in existing controls	• Large investment of staff time • Long wait for results

Approach 3: Attack route analysis

Another leading approach to cyber risk assessment is attack route analysis. It starts with gathering information about likely threats and key assets. But instead of relying primarily on checklists, questionnaires, and interviews, it utilizes the techniques and thought processes of real attackers: discovering and exploiting existing vulnerabilities, exploring the organization's environment, and deciding on a sequence of tactics to reach critical business assets.

The information gathered from this activity enables the security team to build a graph of attack routes between the likely threats and the key assets. These routes are the paths threat actors could take to reach the critical assets, including systems, networks, and cloud platforms with vulnerabilities. Routes also include security controls that can block attacks.

Security teams can use the graph of attack routes to focus on modeling those attacks that pose a real danger to the organization. They can deprioritize the vast majority of vulnerabilities which either (1) are not on an attack route leading to a critical asset, or (2) are on an attack route that is blocked by an existing control.

The graph also helps identify the most effective remediation options. An attack route can be eliminated by removing any of the vulnerabilities in the path or by deploying a security control. With a little analysis, and sometimes merely by viewing the graph, security teams can quickly determine the most cost-effective mitigation action to protect a specific asset.

The attack route analysis approach also simplifies communication with non-technical managers. The graph shows them how threats operate to reach critical assets and how the threats can be neutralized by removing vulnerabilities or adding controls. However, to achieve maximum benefits, the assessment must be revisited periodically so the organization can address emerging threats and medium-priority vulnerabilities not covered in the first round of modeling.

	Attack Route Analysis	
Focus	Pros	Cons
Map attack routes between probable threats and high-value assets, deprioritize low-risk vulnerabilities, and model the most critical threats	• Quickly prioritizes critical vulnerabilities and threats • Identifies cost-effective remediation actions • Simplifies communication with non-technical managers	• Requires ongoing use to achieve maximum benefits

A Plan for Conducting a Cyber Risk Assessment

Let's look at a step-by-step plan for conducting a cyber risk assessment. This plan will work for all three of the approaches discussed above, but it elaborates on some activities specific to attack route analysis.

Step 1:

Understand the Organization's Security Posture and Compliance Requirements

The first step in a cyber risk assessment is to gain a broad understanding of the organization's security posture and compliance requirements. This includes compiling information on the organization's:

- Business operations, objectives, and major challenges
- Compliance requirements and security policies
- Structure and use of information systems
- Existing cybersecurity controls, processes, tools, and governance
- Business critical assets and technological "crown jewels," including applications, confidential data, intellectual property, employee and customer credentials, networks, data center and cloud servers and services, and end user devices

Typically, this information is gathered through questionnaires, interviews with IT and business managers, and existing documentation.

To avoid bogging down in excessive detail, the methods used in this step should be to "go broad, but not deep." In other words, the assessment team should obtain a complete high-level picture of the organization's critical business and IT processes, but not, for example, attempt to inventory every data center server or information asset.

After gaining a broad understanding of the organization's security posture, the team may decide to target its initial assessment at one critical business unit, geographic region, or security domain.

Step 2:
Identify Threats

After the assessment team has surveyed the organization's business operations, information systems, security controls, and business-critical assets, the next step is to identify threats and estimate the probability that they will affect the organization.

The team should capture all the threat actors likely to attack the organization, their motivations, and their targets. These might include, for example:

- Cybercriminals seeking credit card information they can resell on the dark web
- Ransomware gangs that encrypt databases to extort payments
- Competitors attempting to steal intellectual property or confidential research results
- Disgruntled employees aiming to tarnish the organization's brand or abscond with customer lists
- Equipment suppliers providing systems with vulnerabilities that expose the organization to data breaches
- State-sponsored hackers intending to deface a website or shut down a factory in the event of an international conflict

When gathering information on threats, the assessment team should work with security and business managers to estimate the probability of each type striking the organization.

Obviously, the relevant threats and probabilities will vary widely depending on the organization's industry, geographical locations, business model, and many other factors. For that reason, the assessment team should approach this task with open minds, solicit input from a range of sources, and not rely heavily on "one size fits all" templates or playbooks.

Step 3:
Identify Vulnerabilities and Map Attack Routes

Once the threats most likely to affect the organization have been identified, the assessment team can collect information on vulnerabilities and map attack routes leading to high-value assets.

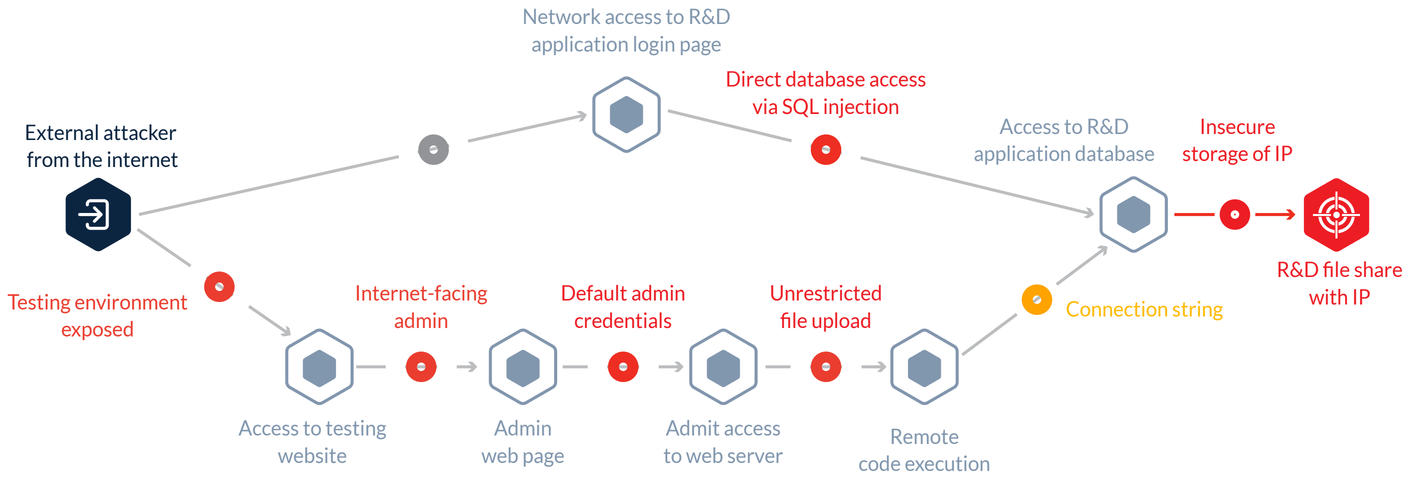
Identify vulnerabilities

In this context, “vulnerabilities” comprise all types of weaknesses in cybersecurity that attackers can exploit, including software and hardware with security flaws, misconfigured systems, faulty security processes, and untrained employees. Finding them requires a combination of:

- Interviews with IT security and support staffs
- Automated network and endpoint scanners
- Red teaming and penetration tests

Map attack routes

The assessment team can then start with the most critical threats and the highest-value assets and map the attack routes between them (see example below). As mentioned earlier, attack routes are the paths across systems, networks, and platforms with vulnerabilities that threat actors could take to reach high-value assets. A graph of the attack routes can also show existing security controls that block attacks.


Network access to R&D application login page
Direct database access via SQL injection
External attacker from the internet
Access to R&D application database
Insecure storage of IP
R&D file share with IP
Testing environment exposed
Internet-facing admin
Default admin credentials
Unrestricted file upload
Connection string
Access to testing website
Admin web page
Admit access to web server
Remote code execution

Simplified example of a section of an attack route graph

The mapping process is essentially combining knowledge of the attackers' TTPs (tactics, techniques, and procedures) with the structure of the organization's information systems, identified vulnerabilities, and security controls, to show which assets are exposed to loss or damage.

A graph of attack routes enables the assessment team to:

- Deprioritize vulnerabilities not on an attack route to a critical asset
- Deprioritize attack routes blocked by existing controls
- Document the combination of vulnerabilities and attack actions that could affect specific assets
- Highlight sensitive and high-risk areas and focus incident detection tools on them
- "Connect the dots" from technical vulnerabilities to specific business risks and likely consequences

Organizations that want to use the attack route analysis approach to assessment will want to use an attack route mapping solution (such as the one created by CYE) to streamline the process.

Step 4:
Model the Consequences of Attacks

After vulnerabilities have been identified and attack routes mapped, the assessment team can focus on modeling the consequences of the most likely attacks that have open attack routes to high-value assets. The analysis should document for each attack type:

- The assets (applications, systems, and data) at risk
- The exposure of the assets (open to the internet, in a restricted area, on a public web platform, etc.)
- The degree of difficulty of attacks (amount of expertise required, scripts and tools available on the dark web, etc.)
- Likely consequences, such as:
  - Lost revenue
  - Lost productivity
  - Lost intellectual property
  - Failure to meet contractual obligations
  - Data breach notification costs
  - Regulatory fines related to violation of security and privacy rules
  - Remediation costs
  - Damage to the organization’s reputation and market position

This modeling will also help refine and add depth to other aspects of the assessment, such as the probabilities of attacks and gaps in controls.

Step 5:
Prioritize Mitigation Options

With a clear picture of risks, attack routes, and consequences, the assessment team is now in a position to prioritize mitigation options. Mitigation methods include:

- Patching or upgrading vulnerable software and hardware
- Fixing misconfigurations and hardening devices
- Segmenting networks and restricting access to assets
- Adding security controls (firewalls, intrusion prevention systems, endpoint detection and response, data encryption, etc.)
- Implementing stronger security policies and increased training for employees and IT staffs

Mitigation is most important for highly probable attacks that have attack routes to high-value assets and are not protected by effective security controls.

An additional objective is to identify the mitigation option for each attack route that involves the lowest cost and the least effort. For example, fixing a misconfiguration on one server or tightening up access to a database might produce the same reduction in risk as reconfiguring a network or investing in an expensive data monitoring product.

Assessment teams can use an attack route graph to visualize the chain of vulnerabilities used in an attack and select the one that is easiest to eliminate or mitigate with a control.

Ongoing Assessment and Cyber Risk Quantification

The assessment journey

Cyber risk assessment is a journey. The first cycle of information gathering and analysis is likely to yield more high-priority mitigation recommendations than can be implemented in a short period. The assessment team should group the recommendations into phases and create a roadmap showing how the organization's security posture will be strengthened in stages. The team can then track, measure, and quantify cybersecurity performance and increased resilience over time.

In addition, the assessment should be revisited periodically to address:

- Emerging threats
- Changes to the business
- Changes in the organization's technologies, IT architecture, and security controls

> Risk assessment and risk management are not single shots but rather are continuous processes repeated as a cycle of identifying risks, creating plans to address those risks, acting on those plans, and monitoring the results of the actions.
>
> SANS Institute white paper: Security Program Management and Risk

Cyber risk quantification

Cyber risk assessments create the basis for cyber risk quantification, a powerful tool CIOs and CISOs can use to justify security investments and fine-tune risk management strategies.

Cyber risk *assessment* helps organizations identify important threats, high-value assets, attack routes, gaps in security, and high-priority remediation options. Cyber risk *quantification* builds on assessment by enabling the organizations to estimate specific monetary values for the consequences of attacks and for mitigation options. This helps CIOs and CISOs:

- Justify security investments by calculating a monetary savings or ROI
- Fine-tune the priorities and sequence of mitigation options
- Evaluate alternatives to mitigation, such as accepting risks, transferring risks to other parties, or paying for cyber insurance
- Quantify improvements in the organization's security posture over time in terms CEOs and boards of directors can understand

How CYE Can Help

CYE is the leading provider of technology and services for cyber risk assessment and cyber risk quantification featuring attack route analysis. With the help of experienced red teams performing real attacks, we map attack routes to business assets across all environments to deliver a detailed contextual assessment of organizational security. As a result, you receive full visibility into true cyber risk, the business assets that are impacted, and the effectiveness of security protection and detection solutions.

References and Additional Information

NIST Special Publication 800-30, *Guide for Conducting Risk Assessments, rev. 1*

SANS white paper: *An Overview of Threat and Risk Assessment*

ISO/IEC 27005:2018, *Information security risk management*

CYE Blog: *Cyber Risk Assessment Services in the Financial Industry: 5 Key Tactics*

CYE Blog: *What Should a Cyber Risk Quantification Strategy Entail?*

CYE Guide: *The Guide to Choosing a Cyber Risk Quantification Strategy*

About CYE

CYE's cybersecurity optimization platform enables businesses to assess, quantify, and mitigate cyber risk so they can make better security decisions and invest in effective remediation. CYE combines this with dedicated professional guidance and advice provided by established cybersecurity experts. The company serves Fortune 500 and mid-market companies in multiple industries around the world. With headquarters in Israel and offices in New York and London, CYE is funded by EQT Private Equity and 83North. Visit us at cyesec.com.

Would you like to learn more about how CYE can help protect your company from cyber threats?

Contact us

© 2022 CYE, All rights reserved. www.cyesec.com | info@cyesec.com