horizontal line

System Security Management: MCSE 586

Summer 2022

Assignment on:-

**Risk Analysis and its Impact on Security**

Submitted by: Shied Shahriar Housaini; ID MCE 07905536

Submitted to:

Prof. Dr. Mohammad Mahfuzul Islam

# Introduction:

## What is a Risk Analysis-

Risk analysis is the phase where we’ll examine each identified risk and assign it a score using one of two types of the scoring system: quantitative or qualitative. These scores help we prioritize our risks so we know which ones to address first and the best ways to address them.

The COSO Enterprise Risk Management framework defines risk appetite as “the amount of risk, on a broad level, an organization is willing to accept in pursuit of stakeholder value.” Risk tolerance, the framework states, “reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achieve.”

## What is the Risk Analysis Process?

1. Identification and Quantification of Uncertainties.
2. Estimation of Their Potential Impact.
3. Development of a Risk Analysis Framework.
4. Formulation of Risk Management Actions.

## When to Use Risk Analysis

Risk analysis is useful in many situations:

* When we're planning projects, to help we to anticipate and neutralize possible problems.
* When we're deciding whether or not to move forward with a project.
* When we're improving safety and managing potential risks in the workplace.
* When we're preparing for events such as equipment or technology failure, theft, staff sickness, or natural disasters.
* When we're planning for changes in our environment, such as new competitors coming into the market, or changes to government policy.

## Identification: What’s involved?

we’ll need to use our imagination and envision worst-case scenarios for the risk identification phase, from natural disasters to economic ones.

What if a fire broke out in our building? What if someone stole our proprietary secrets? What if the economy crashed? What if ransomware locked our systems? What if a competitor undercuts our prices?

During the risk identification process, it’s essential to keep in mind that nobody can see into the future. New risks could emerge for which we have no plan (yet). Therefore, it’s also essential to keep our options open and our risk management process and program flexible. Plan to review our risk list regularly and establish contingency plans for new risks.

# Cyber Security Risk Analysis:

Risk analysis refers to the review of risks associated with a particular action or event. The risk analysis is applied to information technology, projects, security issues, and any other event where risks may be analyzed based on a quantitative and qualitative basis. Risks are part of every IT project and business organization. The analysis of risk should be occurred on a regular basis and be updated to identify new potential threats. The strategic risk analysis helps to minimize future risk probability and damage.

**Enterprise and organization used risk analysis:**

* To anticipate and reduce the effect of harmful results that occurred from adverse events.
* To plan for technology or equipment failure or loss from adverse events, both natural and human-caused.
* To evaluate whether the potential risks of a project are balanced in the decision process when evaluating to move forward with the project.
* To identify the impact of and prepare for changes in the enterprise environment.

### What Is the Difference Between Risk Analysis and Risk Assessment:

There is a critical distinction between risk assessment and risk analysis. Risk assessment is a larger process where all potential threats are considered. During the risk analysis process, the *level* of each risk is determined. Both fall under the broader umbrella of risk management tools.

An organization should conduct various risk assessments, to identify all potential hazards. A cybersecurity risk assessment is just one of those numerous assessments, and all of them include risk analysis as a crucial step.

## Steps in the risk analysis process:

The basic steps followed by a risk analysis process are-

**Conduct a risk assessment survey:** Getting input from management and department heads is critical to the risk assessment process. The risk assessment survey refers to begin documenting the specific risks or threats within each department.

**Identify the risks:** This step is used to evaluate an IT system or other aspects of an organization to identify the risk related to software, hardware, data, and IT employees. It identifies the possible adverse events that could occur in an organization such as human error, flooding, fire, or earthquakes.

**Analyze the risks:** Once the risks are evaluated and identified, the risk analysis process should analyse each risk that will occur, as well as determine the consequences linked with each risk. It also determines how they might affect the objectives of an IT project.

**Develop a risk management plan:**

After analysis of the Risk that provides an idea about which assets are valuable and which threats will probably affect the IT assets negatively, we would develop a plan for risk management to produce control recommendations that can be used to mitigate, transfer, accept or avoid the risk.

**Implement the risk management plan:** The primary goal of this step is to implement the measures to remove or reduce the analyses risks. We can remove or reduce the risk by starting with the highest priority and resolving or at least mitigating each risk so that it is no longer a threat.

**Monitor the risks:** This step is responsible for monitoring the security risk on a regular basis for identifying, treating and managing risks that should be an essential part of any risk analysis process.

### Types of Cyber Security Risk Analysis:

The essential number of distinct approaches related to risk analysis are:

#### **1. Qualitative Risk Analysis**

This method of analysis follows the probability and impact number. The chances of risk happening refers to probability while the significance of the risk refers to impact. It identifies the risk individually and then ranks them according to priority. This allows them to understand the probability of each risk and then filter them accordingly to determine risk exposure.

* The qualitative risk analysis process is a project management technique that prioritizes risk on the project by assigning the probability and impact number. Probability is something a risk event will occur whereas impact is the significance of the consequences of a risk event.
* The objective of qualitative risk analysis is to assess and evaluate the characteristics of individually identified risk and then prioritize them based on the agreed-upon characteristics.
* The assessing individual risk evaluates the probability that each risk will occur and effect on the project objectives. The categorizing risks will help in filtering them out.
* Qualitative analysis is used to determine the risk exposure of the project by multiplying the probability and impact.

### The Risk Impact/Probability Chart is based on the principle that a risk has two primary dimensions:

### Probability – A risk is an event that "may" occur. The probability of it occurring can range anywhere from just above 0 percent to just below 100 percent. (Note: It can't be exactly 100 percent, because then it would be a certainty, not a risk. And it can't be exactly 0 percent, or it wouldn't be a risk.)

### Impact – A risk, by its very nature, always has a negative impact. However, the size of the impact varies in terms of cost and impact on health, human life, or some other critical factor.

#### **2. Quantitative Risk Analysis**

This type of risk analysis follows numerical estimates of risk’s effect on project objectives. It is mainly useful for estimating contingency reserves and identifying time and cost. It is not compulsory in smaller projects but is efficient for identifying overall project risk.

* The objectives of performing quantitative risk analysis process provide a numerical estimate of the overall effect of risk on the project objectives.
* It is used to evaluate the likelihood of success in achieving the project objectives and to estimate contingency reserve, usually applicable for time and cost.
* Quantitative analysis is not mandatory, especially for smaller projects. Quantitative risk analysis helps in calculating estimates of overall project risk which is the main focus.

### 

Quantitative scoring assigns specific dollar amounts to the risk factors under consideration.

* What would be the cost to the organization if the risk were to happen? This is known as “single loss expectancy” (SLE).
* How often should we expect the risk to happen? Once per year assigns an annual rate of occurrence (ARO) of 1; once every 10 years, and ARO of 0.1.

To calculate the financial risk in a given year, multiply the SLE by the ARO.

Qualitative scoring is more subjective and uses a risk assessment matrix that typically involves four factors:

* **Likelihood:** What’s the probability of occurrence: the probability that the risk will happen?
* **Impact:** If the risk event occurred, what is the impact of the risk? How much would it harm our project, function, or enterprise?
* **Velocity:** How quickly would our project, function, or enterprise feel the impact?
* **Materialization:** What’s the potential severity of the impact? To measure this score, add the impact and velocity scores and divide by 2.

## How Do we Perform Risk Analysis:

Within the regulatory and industry frameworks are several best practices for performing a cyber risk assessment and analysis. These [steps for a cybersecurity risk assessment](https://reciprocity.com/6-steps-to-performing-a-cybersecurity-risk-assesment/) will help identify specific vulnerabilities based on our organizational needs and the common risks in our industry.

### Create a Risk Management Team

The first step in performing a security risk analysis is to create a cross-enterprise group that can deliver the necessary attention to the details of the risks to our data security and information technology (IT) systems. Team members should include:

* Senior management
* Chief information security officer (CISO)
* Privacy officer
* Legal
* Marketing
* Product management
* Human resources
* A manager from each operating business group

### 

### Identify and Map Systems and Assets

Document every IT asset on the network, including computers, tablets, routers, printers, servers, and phones. In addition, we must identify how they are used and interconnect with one another.

### Identify Vulnerabilities and Potential Threats

Management team must identify threats and vulnerabilities from all parts of our organization. Software-based vulnerability scanners can make it easier to locate vulnerable equipment, but our team’s expertise is necessary to determine flawed security policies, physical vulnerabilities, and other cyber threats hidden under our network and systems.

Other potential threats include:

* Unauthorized access to our network
* Misuse of information or data leaks
* Ransomware attacks
* Human error or negligence
* Process failures
* Data loss
* Data breaches
* Disruption of services

### Assess our Risks

Using our information asset catalog, examine the most significant risks for unauthorized access. Scrutinize every type of information, vendor, system, network, software, and device to determine its danger.

During this phase, our risk management team must use its combined knowledge and intuition to list worst-case situations, ranging from pandemics to natural disasters to economic calamities. The result is a list of all risks that can affect our organization.

Now, at last, we get to the crucial step: performing an analysis of those risks.

## Factors of Risk Analysis

A risk analysis, performed with the aid of a [risk register](https://reciprocity.com/resources/what-is-a-risk-register/) (that is, a formal list of our organization’s risks), considers two main factors:

* Probability: The likelihood of an attack
* Impact: The operational, reputational, or financial effect of the risk on our organization

These two elements will help we determine the severity of each potential risk in our register and improve decision-making so that we can develop strategies for each risk according to our security posture and tolerance. we can risk remediation in several ways: [accept, avoid, transfer or mitigate risk](https://reciprocity.com/blog/risk-avoidance-vs-risk-mitigation/).

### Set Cybersecurity Controls

To mitigate risks, we must develop cybersecurity controls to reduce our company’s risk exposure and prevent security incidents.

Cybersecurity controls are safeguards used to prevent, detect and mitigate cyber threats and attacks. These mechanisms can take a variety of forms depending on our unique threat landscape. Examples include physical controls, such as security cameras or guards. Technical controls might include firewalls or two-factor authentication.

Risk mitigation can also help our data protection efforts, compliance with regulations and requirements, and threat response.

### Monitor and Audit

we need to watch our IT systems over time to assure that cybersecurity measures are working as expected. Establish performance metrics for our security controls, and then monitor those controls to confirm that activity stays within our risk tolerance. (In addition, continuously monitor networks, systems, and devices for suspicious activity.) Also conduct annual audits of the efficiency of our cybersecurity program.

## Develop a Mitigation Plan to Reduce Potential Risks

Risk management is fundamentally about recognizing dangers and taking precautions to avoid them. It provides businesses with a strategy for deciding which risks are worthwhile and which are not, delivering better results for their bottom lines.

The [risk management process](https://reciprocity.com/blog/5-step-risk-management-process/) is a series of steps to identify, analyze, and respond to the potential harm of risk; to keep our business on track and meeting its objectives. Maintaining a risk management plan is essential because it reveals potential threats within the business before they can hurt our operations.

Risk management also generates several benefits, such as preventing data breaches and driving the need for a cybersecurity program. Cost/benefit analysis activities related to security, operational, business, and other metrics help develop risk perceptions and justify investments.

## Who Should Be Responsible for a Cybersecurity Risk Assessment?

Ideally, our organizations should have a specialized in-house team with risk analysts who conduct risk assessments (if resources allow). This team should include IT personnel who understand our digital and network architecture, and team members who understand the organizational structure, how information flows, and third-party interactions.

Small companies may lack the necessary personnel in-house to conduct a complete evaluation; in that case, we could hire an outside consultant. Companies also use various cybersecurity tools to automate security controls, monitor their cybersecurity score, prevent breaches, issue security questionnaires, and decrease third-party risk.

# 

# The Statistical Analysis of Measuring Cybersecurity Risk

Business organizations are more at risk of cyberattacks than ever before. Calculating that risk, however, is no easy task. In this post we will provide an overview of traditional calculation methods and a glimpse into what could be the future of measuring cybersecurity risk: statistical analysis.

The cost of a cyberattack can be painfully high and sometimes high enough to shut down business operations entirely. Research from 2020 suggests that $2.9 million is lost to cybercrime every minute, and the average cost of a data breach in 2021 was $4.24 million.

As cybersecurity threats continue to evolve, it is essential to understand how to predict cybersecurity risk adequately to create effective cybersecurity programs and safeguard our stakeholders.

## What Is a Cybersecurity Risk?

Cybersecurity, as defined by the Cybersecurity and Infrastructure Security Agency (CISA), is “the art of protecting networks, devices, and data from unauthorized access or criminal use, and the practice of ensuring confidentiality, integrity, and availability of information.”

These days, many service providers use cybersecurity frameworks, such as the [National Institute of Standards and Technology (NIST) framework](https://reciprocity.com/resource-center/complete-guide-to-nist-cybersecurity-framework-800-53-800-171/), to comply with regulatory requirements such as the General Data Protection Regulation (GDPR).

Cybersecurity risk is the likelihood that our organization will suffer from data, financial, or operational disruptions. This type of risk is most often associated with events that could ultimately result in a data breach. Breaches, ransomware, phishing, distributed denial of service (DDoS), and malware are the most common cybersecurity threats.

Many organizations turn to external advisers who can provide real-time risk metrics for their enterprises. A recent analysis of the “cybersecurity risk metrics” market shows that the rise of adversaries, boardroom pressures, and financial losses has led to an emerging force of underwriters, brokers, and consultants to help chief information security officers (CISOs) answer to concerns coming from the c-suite and the boardroom.

Keeping our data safe, however, is expensive. Many smaller organizations can’t afford to hire an outside company to measure risk for them.

Whether our organization hires someone to do that work for we, or uses our team of security professionals to measure cyber risk, our risk will likely be calculated using traditional “high-medium-low” categories.

Some security experts argue that using these qualitative methods leads to forecasting inconsistencies by as much as 20 percent. They suggest instead using statistical analysis to measure cybersecurity risk.

Regardless of the method we choose, we still need to measure risk somehow.

### Common Types of Cyber Threats

Despite cybersecurity professionals’ attempts to close security breaches, cybercriminals are always looking for new ways to escape detection, bypass security measures, and exploit emerging [vulnerabilities](https://reciprocity.com/why-vulnerability-management-is-important/) and information security weaknesses.

The most recent cybersecurity threats use work-from-home settings, remote management technologies, and new cloud services to reinvent well-known vulnerabilities. Cybersecurity programs work to protect against all forms of [corporate cybersecurity risks](https://reciprocity.com/resources/the-most-common-corporate-cybersecurity-risks/).

#### **Malware**

Malware is software installed by cybercriminals to harm a computer, server, system, or network. Malware comes in many forms, each with its own set of goals and consequences on the victim’s devices.

* **Ransomware.**
* **Trojan horse.**
* **Spyware.**
* **Adware.**

#### **Social Engineering**

#### **Man-in-the-Middle (MITM) Attacks**

#### **Advanced Persistent Threats (APT)**

#### **Distributed Denial-of-Service (DDoS) Attacks**

A distributed-denial-of-service assault attempts to overload and damage a system by flooding it with data, rendering it inoperable.

## Important Measuring Cybersecurity Risk

With the cost and frequency of cyber assaults on the rise, security executives must be able to demonstrate that the efforts they’re making to lower cybersecurity risk throughout their digital ecosystems are paying off. To do so, they must be able to analyze and explain risk in business-friendly terms.

Moreover, as managers are increasingly challenged to offer confidence that corporate assets are appropriately protected from the consequences of a future breach, assessing information security effectiveness has become a key performance indicator (KPI) for organizations.

### How Do We Measure Cybersecurity Risk:

The terms “vulnerability” and “cyber risk” are used interchangeably, but they are not the same. A vulnerability is a weakness that results in unauthorized network access when exploited. Cyber risk, in contrast, is the probability of a vulnerability being exploited.

To calculate cyber risk, many use this simple framework:

Cyber Risk = Threat x Vulnerability x Information Value

Usually, measurement of cybersecurity risk begins with a vulnerability assessment.

A [vulnerability assessment](https://reciprocity.com/the-difference-between-vulnerability-assessment-and-vulnerability-management/) is a systematic review of the security weaknesses in an information system. It evaluates whether or not our system is susceptible to any known vulnerabilities, assigns a severity level to them, and recommends remediation or mitigation.

The three factors that influence a risk vulnerability assessment are:

* What is the threat?
* How vulnerable is the system?
* What is the reputational or financial damage if the system is breached or unavailable?

After we conduct a vulnerability assessment to identify and prioritize our vulnerabilities, we can perform a [cyber risk assessment](https://reciprocity.com/resources/complete-guide-to-cyber-risk-assessments/) to measure the information value and threat components in the equation above.

The [NIST defines risk assessments](https://csrc.nist.gov/glossary/term/risk_assessment) as processes “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.”

A cyber risk assessment analyzes our cybersecurity risks to help inform stakeholders and decision-makers and support proper risk response. Cyber risk assessments also provide an executive summary to help stakeholders make informed security decisions.

Most standards and certification tests promote [cybersecurity risk analysis](https://reciprocity.com/resources/what-is-cybersecurity-risk-analysis/) as an ordinal scoring method. For example, the risk rating methodology on [OWASP.org](https://owasp.org/) states:

Once the tester has identified a potential risk and wants to figure out how serious it is, the first step is to estimate the likelihood. This is a rough measure of how likely an attacker could exploit a particular vulnerability. It is not necessary to be overly precise in this estimate. Identifying whether the likelihood is low, medium or high is sufficient.

Here are the steps that we would take to complete a thorough cyber risk assessment using the high-medium-low method to measure cybersecurity risk:

#### **Determine Information Value**

First, define a standard for determining the importance of an asset. If we don’t have an unlimited budget for information risk management, we should limit our scope to the most business-critical assets. Once the standard is incorporated into our organization’s information risk management policy, we should use it to classify each asset as critical, major, or minor.

#### **Identify and Prioritize Assets**

Next, identify our assets and determine the scope of the assessment. This will allow we to prioritize which assets we should assess. For example, we don’t need to evaluate every building, employee, trade secret, vehicle, or piece of office equipment.

#### **Identify Cyber Threats**

A [cyber threat](https://reciprocity.com/resources/what-are-cybersecurity-threats/) is a vulnerability that could be exploited, harming our organization or stealing data. Hackers, malware, and other IT security risks are apparent threats, including natural disasters, system failure, human error, and adversarial threats such as third-party vendors.

Threats that affect every organization include unauthorized access, misuse of information by authorized users, data leaks, loss of data, and service disruption. After identifying our organization’s threats, we also need to assess their impact.

#### **Identify Vulnerabilities**

Now that we’ve identified what might happen at a theoretical level, we need to address what actually could happen in reality: What are our vulnerabilities? A vulnerability is a weakness that a threat can exploit to breach security, harm our organization, or steal sensitive data.

Tools and methods to identify vulnerabilities include vulnerability analysis, audit reports, the NIST [cybersecurity vulnerability](https://reciprocity.com/blog/most-common-types-of-cybersecurity-vulnerabilities/) database, vendor data, incident response teams, and software security analysis. Examine both software-based and physical vulnerabilities during this step.

#### **Analyze and Implement New Controls**

Determine which controls are already in place to minimize or eliminate the probability of a threat or vulnerability. Classify controls as preventive or detective. Preventive controls attempt to stop attacks before they start, while detective controls work to discover an attack after it has occurred.

#### **Calculate the Likelihood and Impact of Various Scenarios Annually**

Now we have the information value, threats, vulnerabilities, and controls. Next, identify how likely it is that these cyber risks will happen and the harm that may occur if they do. Then we can use our findings to determine how much to allocate for mitigating each identified cyber risk.

#### **Prioritize Risks Based on the Cost of Prevention Versus Information Value**

Determine action for senior management or other stakeholders to mitigate risk, using risk level as a basis.

* High risk: corrective measures should be developed as soon as possible;
* Medium risk: corrective actions can be created within a reasonable period;
* Low risk: decide whether to accept the risk or mitigate it.

At this point, we have already determined the asset’s value and how much we should spend to protect it. Now we need to decide whether it makes sense to use a preventive control to protect that asset, especially if that preventative step costs more than the asset is worth. Remember to evaluate both the reputational and financial impact during this step.

#### **Document Results from Risk Assessment Reports**

Finally, develop a risk assessment report to support budget, policies, and procedures management decision-making. Describe each threat’s risk, vulnerabilities, asset value, potential impact, and likelihood of occurrence, along with control recommendations.

Although widely used, this high-medium-low qualitative method to calculate cybersecurity risk is still complex. For example, we must assign value to information as critical, major, or minor; calculate the likelihood and harm of various scenarios; and prioritize risks based on the cost of prevention versus information value.

Deciding which risks are the most critical and which risks can be put aside and dealt with later comes down to judgment calls that determine the probability that an attack will occur and the consequences that come with it.

## How to Use Statistical Analysis for Cybersecurity Risk Management

Statistical analysis is the science of collecting, exploring, and presenting large amounts of data to discover underlying patterns and trends. Although using statistical analysis to measure cyber risk may seem obvious, it’s not the traditional method of choice.

Richard Seiersen, a one-time general manager of cybersecurity and privacy at GE Healthcare and CISO at Twillo, is an advocate for simplifying cybersecurity risk measurement. In his recent book, “How to Measure Anything in Cybersecurity,” Seiersen and co-author Douglas Hubbard discuss using probabilistic programming and statistical analysis to measure cyber risk.

Using statistical analysis to measure other types of risk is nothing new; Seiersen notes that “risks have been measured in far more complex situations – flooding, droughts, military logistics, etc.” But when using statistical analysis to measure cybersecurity risk, the challenge seems to be how.

The first step is to convince skeptical security professionals that statistical analysis is viable for measuring cyber risk. Sieiersen’s research shows that statistical literacy plays a large part in any objections: Security professionals who don’t understand how to interpret statistics are most likely to doubt the untapped potential of statistical analysis.

Assigning probability – that is, determining the likelihood that certain risks will be exploited – sounds more complicated than it is.

For example, access to sensitive information makes a systems administrator more susceptible to a hack than someone who works as an intern. Of course, our organization shouldn’t discount the possibility that other accounts might be hacked; but statistical analysis shows that the most significant risk lies in the system administrator’s account.

Using a mathematical technique like statistical analysis, we could measure the risk in this scenario: “the probability that the system administrator’s account will be hacked is X percent.”

In their book, Seiersen and Hubbard provide several statistical theories, such as Bayesian statistics, that could be used instead of qualitative risk matrices.

Bayesian statistics is a theory where probability expresses a degree of belief in an event based on prior knowledge about the event, such as the results of previous experiments or personal beliefs about the event. Other methods the authors suggest are Monte Carlo simulations, simple “one-for-one substitutions,” loss exceedance curves, and the Rasch (Logodds) Model.

No matter which methods we use, Seiersen and Hubbard maintain that using statistical analysis to measure cybersecurity risk will provide more accurate predictions for our business.

Ultimately, the authors argue that organizations should stop using risk scores and risk matrices altogether and that standards organizations should stop promoting them. Instead, they suggest using simple probabilistic methods because those methods demonstrate a measurable improvement over unaided intuition and have already proven effective.

They also believe that decisions would be easier to support if risks and mitigation strategies are quantified more meaningfully using statistical analysis.

For those who believe that cybersecurity is too complex or lacks sufficient data for quantitative analysis, Hubbard and Seiersen remind us that “softer methods never alleviate a lack of data, complexity, rapidly changing environments or unpredictable human actors… they can only obscure it.”

Using statistical analysis is a more precise method to measure cybersecurity risk over traditional methods that are more qualitative. But it is still a complex and arduous process. Fortunately, software solutions can help our organization use statistical analysis to accurately calculate cybersecurity risk and report it to decision-makers in the boardroom.

**Cyber Security Risk Assessment Matrix**

## Prioritize Efforts With A Cyber Security Risk Assessment Matrix

As cyber threats continue to become more sophisticated and dangerous, third-party risk managers must find ways to maximize the impact of their limited risk management budgets. They are also under greater pressure to communicate the success of investments in cyber risk management to executive leadership and the board.

A cyber security risk assessment matrix can be a vital tool in accomplishing both objectives. By categorizing risks based on the importance of assets/vendors and the severity of the risk they pose to the organization, risk managers can get a clear sense of the areas of highest concentrated risk, enabling them to prioritize resources for remediation. Using a risk matrix in the boardroom provides a powerful and graphic representation of which areas of risk should be highest priority for the organization as a whole, while also suggesting [how to mitigate third party risk](https://www.bitsight.com/glossary/how-to-mitigate-third-party-risk) most effectively. This helps piece together the most important areas of our cybersecurity program so stakeholders don’t have to analyze overwhelming amounts of cybersecurity information.

As a leading provider of solutions for managing and mitigating risk, BitSight offers a cyber security risk assessment matrix that provides AI-driven risk prioritization to deliver greater insight into risk and strategies for remediation.

## How A Cyber Security Risk Assessment Matrix Works

A cyber security risk assessment matrix can be configured to represent risk in a variety of ways.

Before building a risk assessment matrix, security leaders must undertake a [security risk assessment](https://www.bitsight.com/glossary/security-risk-assessment) to identify the risks facing the organization, severity of those risks, and the importance of the assets or the vendors with which those risks are associated. Data from an [information technology risk assessment](https://www.bitsight.com/glossary/information-technology-risk-assessment) can then help security leaders to tier digital endpoints and third-party vendors into various categories.

Color-coding the categories of a cyber security risk assessment matrix when presenting data to business stakeholders or executives can help to make an immediate visual impact. For example, the category of non-critical assets that represent little risk can be colored green, as the potential adverse consequences of risk in this area is fairly light. Conversely, critical assets where the associated risk is severe may be colored red to indicate that this area should be prioritized for remediation.

## Questions we Should Have In our Vendor Assessment

## An AI-Driven Asset Risk Matrix

BitSight’s cyber security risk assessment matrix also includes an asset risk matrix that is the industry’s first AI-driven asset prioritization tool. Powered by BitSight’s advanced data collection and data science capabilities, this intelligent and configurable matrix factors a broad range of items into its prioritization schema, including measured system usage, user information submission, existence of specialized certificates, and other contributing factors that indicate criticality of assets.

By enabling rapid assessment of asset criticality and severity of issues affecting assets, BitSight helps organizations understand the most pressing issues facing their vendors and allows them to prioritize remediation efforts to mitigate risk. BitSight also provides rated vendors with contextual insights about the risks living on their network so they can drive action toward remediation.

## 

What is a cyber security risk assessment matrix?

A cyber security risk assessment matrix is a tool that provides a graphical depiction of areas of risk within an organization’s digital ecosystem or vendor network. A risk matrix can help define and categorize various risks that face the organization according to the importance of an asset and the severity of the risk associated with it.

What is the benefit of a cyber security risk assessment matrix?

A risk matrix can help organizations prioritize remediation of risk based on severity. It can also help prioritize which vendors should be more rigorously assessed based on their importance to the organization and the severity of the risk they represent.

What is a cybersecurity risk assessment checklist?

A [cyber security risk assessment checklist](https://www.bitsight.com/glossary/cyber-security-risk-assessment-checklist) is a set of information, questions and tasks that risk managers can use to perform due diligence during the vendor selection process. Checklists may include information to be obtained from the vendor through a [risk assessment questionnaire](https://www.bitsight.com/glossary/risk-assessment-questionnaire), for example, as well as data to be obtained independently from other sources. Risk assessment checklists are designed to provide a clear picture of the risk posed to the or ganization by prospective vendors.

How to Build a Cyber Risk Assessment Matrix

When conducting a cyber risk assessment, we need to quantify the risk levels of various scenarios taking place. An organization must first define and identify its assets, then prioritize those assets, and only then conduct an assessment.

There are various tools an organization can use to conduct a risk assessment, which can also aid with quantifying and visualizing the data.

One of those tools is a Risk Assessment Matrix that produces a risk score through the combination of two parameters:

1. The *impact* of this risk scenario taking place
2. The *probability* and frequency of this risk scenario occurring

An organization’s assets have inherent risks which are built-in risks just by the nature of how those assets function. Lowering those risks can be achieved by placing controls and safeguards in place to protect the organization from those risks materializing to their full capacity. The outcome of these actions will be a new score called Residual Risk.

The new residual risk score will be a function of how much we have lowered the impact and probability of that risk materializing, hence what is called the Control Effectiveness. This control effectiveness acts as a weight and will impact how low the residual risk is.

A more advanced approach can attribute the effectiveness to the impact or probability independently, which would help lead to a more accurate residual risk score, though this practice is often left for more mature security practices.

Visualizing the above is not a simple task. This is why we’ve spent years developing the Centraleyes platform dashboards with state-of-the-art heatmaps and reporting functions.

Below is an example of a heatmap in which we visualize a cyber risk assessment matrix. This allows users to interactively identify risks by intuitively clicking on various areas of the heatmap or on specific risks represented by a single point on the map. This tool is a very effective way for users to prioritize the highest risks in their organizations.

Other forms of the matrix data can be viewed in automated filters like the grouping below, where the risks are split automatically into 4 tiers: Critical, High, Medium and Low, further assisting in the prioritization and management process.

## Risk Matrix Frameworks

The [NIST SP 800-53 framework](https://www.centraleyes.com/standards-nist-800-53), alongside many other cyber risk frameworks, can be used as a set of best practices and controls to help the organization protect sensitive data, like PII (Personal identifiable Information) and PHI (Protected Health Information).

Using an assessment around these controls can help quantify the impact and probability of a data breach. These control sets also help create a baseline for what the readiness of an organization is for a cyber breach and how to prioritize remediation tasks of open gaps.

One of the advantages to having a cyber risk matrix as part of our organizational assessment is that we move from a tactical approach to a much more strategic one. An example of this will be around how we are able to create efficiencies on the following items:

See for ourself how the Centraleyes platform exceeds anything an old GRC

system does and eliminates the need for manual processes and spreadsheets

to give we immediate value and run a full risk assessment in less than 30 days

* Ability to benchmark and track progress overtime through self-assessment
* Cost savings – by prioritizing the most strategic and urgent items.
* Time saving – through a methodical approach we create efficiencies around assessing and collecting repetitive information.
* Identify weak points and threats faster, and lower our overall risk.
* Meeting compliance – as an ongoing and continuous risk assessment is now a requirement in many of the regulatory standards. This includes privacy acts, certifications and industry standards.
* Removing the subjective risk approach by creating a scientific and repeatable assessment methodology. This approach removes that gut feeling that is often used as a primary factor in our decision-making process. we now rely on data and trends, as well as information coming from outside the organization to help make smart decisions about where to focus new protection solutions or areas to remediate.

## The Sources of Data

The sources of data that feed the cyber risk matrix can come from a variety of places, both qualitative and quantitative. In cyber security in particular, it is important to try and create, independent and objective point of view on the validation of controls. To do so, we need to combine the following sources of data:

* Questionnaires and surveys
* Data feeds, logs from tools and network telemetry
* External sources of thread intelligence, vulnerability data

These sources of data, when combined together can provide a very unique point of view of our organizational risks. Collecting the data is one important step, by analyzing the data and creating insights is where all the magic happens. The cyber risk matrix is one of those tools that can help we create that very actionable and useful insight. Using the [Centraleyes platform](https://www.centraleyes.com/centraleyes-products), with its tens of pre-populated frameworks and standards, smart surveys and questionnaires, live data feeds and real-time intelligence from internal and external security sources, to visualize and build a cyber risk assessment matrix will help take our [cyber risk management program](https://www.centraleyes.com/post/why-a-cyber-risk-management-solution-may-be-right-for-you) to the next level and ensure our organization is always ahead of the game.

## Prioritizing our Risks

Once we’ve assigned scores to our risks, we can categorize them according to their priority. For example, many enterprises allocate rankings of “high priority,” “medium priority,” or “low priority.”

### High Priority

A ransomware attack, in which malicious actors use malware to lock we out of our systems and demand payment to restore our access, would fall under this category. So would a zero-day attack, in which hackers exploit a previously unknown vulnerability.

### Medium Priority

A medium-risk event might be a former employee stealing information after being terminated. Reviewing our organization’s employee-access policies would be a control against this risk’s materializing. A robust employee termination process coordinated between human resources and IT would help mitigate this risk.

### Low Priority

If our buildings are adequately secured, the probability might be low of someone’s breaking into our offices and stealing devices. If those devices don’t contain any information, the likelihood of a data loss may also be low or nil. Since there is no urgency associated with this risk, we might decide to review our device-risk-mitigation controls annually.

|  |  |  |
| --- | --- | --- |
|  |  |  |

# GRC 101: What is Cyber Risk?

Cyber risk is the fastest growing enterprise risk and organizational priority today. According to the [2019 Global Risk Perception Survey](https://www.marsh.com/us/insights/research/marsh-microsoft-cyber-survey-report-2019.html), cyber risk was ranked as a top 5 priority by 79% of global organizations.

The growth of cyber risk is in large part tied to the increasing use of technology as a value driver. Strategic initiatives—such as outsourcing, use of third-party vendors, cloud migration, mobile technologies, and remote access—are used to drive growth and improve efficiency, but also increase cyber risk exposure. Cyber risk has evolved from a technology issue to an organizational problem. In short, cyber risk is everyone’s problem.

A compounding factor here is over the last two decades, cyber crime has grown exponentially. According to the IC3, the FBI’s cyber crime reporting mechanism, [monetary damages from reported cyber crime](https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/) totaled $3.5 billion in 2019, while Cybersecurity Ventures project that the global costs of cybercrime will double to $6 trillion in 2021, up from $3 trillion in 2015.

## Definition of Cyber Risk

Cyber risk, or cybersecurity risk, is the potential exposure to loss or harm stemming from an organization’s information or communications systems. Cyber attacks, or data breaches, are two frequently reported examples of cyber risk. However, cybersecurity risk extends beyond damage and destruction of data or monetary loss and encompasses theft of intellectual property, productivity losses, and reputational harm.

## Examples of Cyber Risk

Cyber risk can be faced by any organization and can come from within the organization (internal risk) or from external parties (external risk). Both internal and external risks can be malicious or unintentional.

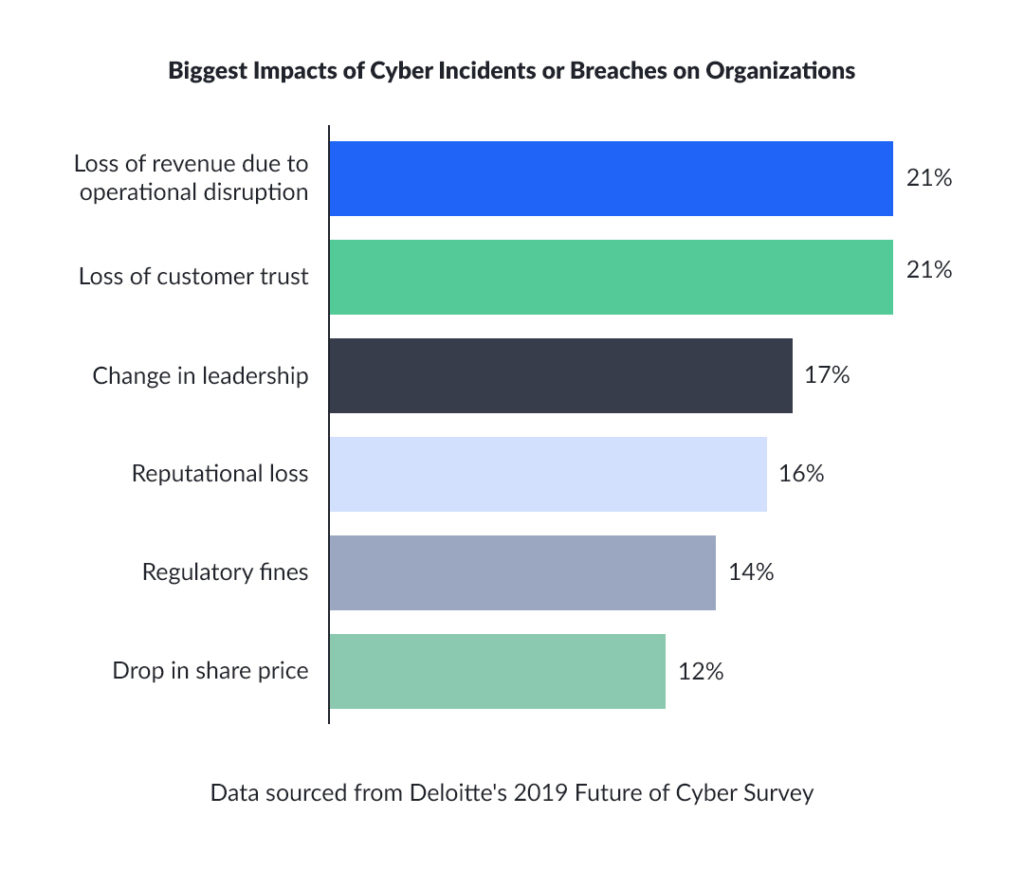
Internal risks stem from the actions of employees inside the organization. An example of malicious, internal cyber risk would be systems sabotage or data theft by a disgruntled employee. An example of unintended, internal risk would be an employee who failed to install a security patch on out-of-date software.

External risks stem from outside the organization and its stakeholders. An external, malicious attack could be a data breach by a third party, a denial-of-service attack, or the installation of a virus. An unintentional, external attack usually stems from partners or third parties who are outside yet related to the organization - a vendor whose systems outage results in an operational disruption to our own organization.

## Impact of Cyber Risk

According to Deloitte Advisory Cyber Risk Services, “Cyber risk is an issue that exists at the intersection of business risk, regulation, and technology.” In their [2019 Future of Cyber Survey](https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cyber-survey.html),

Deloitte found that the impact of security incidents varied from real monetary costs, including financial loss due to operational disruptions and regulatory fines, to intangible costs, including the loss of customer trust, reputational loss or a change in leadership.



Cybersecurity risks can result in both quantitative loss and qualitative impact. Realized costs may include lost revenue due to disruptions to productivity or operations, incident mitigation and remediation expenses, legal fees, or even fines. Less tangible impacts of cybersecurity incidents, which are difficult to quantify and generally take longer to rectify, include loss of goodwill, diminished brand reputation, or a weakened market position.

## Managing Cyber Risk

Cyber risk has the potential to affect every aspect of an organization, including its customers, employees, partners, vendors, assets, and reputation.

As such, an effective cyber risk management program involves the entire organization. Although IT or Infosec may ultimately own cybersecurity risk management, cyber risk is dispersed throughout the organization, requiring an integrated approach and cross-divisional collaboration to effectively manage and mitigate exposure.

Below are 4 key steps our organization can take to implement a robust cyber risk management strategy.

1. **Understand our Risk Profile**: Understanding our risk profile and potential exposure requires an enterprise-wide threat assessment.
   * Identify critical enterprise risks to determine the applications, systems, databases, and processes subject to cyber risk. Consider the array of external and internal threats, from unintentional user error to third-party access to malicious attacks.
   * Undertake risk assessments with all stakeholders to assess the likelihood and potential impact of cyber risk exposure, including cross-divisional and secondary effects and technology dependencies. Consider third-party exposure, as they have increasingly become vectors for cyber incidents, and the risk posed by the expanding technology perimeter due to work from home requirements.
   * Quantify risks including the potential financial, operational, reputational, and compliance impact of a cyber risk incident. A risk scoring framework can help provide a more holistic ranking of threats.
2. **Set a Firmwide Strategy**: Establish a firmwide strategic framework for cyber risk management
   * Prioritize risks by employing a shared risk measurement framework and reporting systems to effectively prioritize risks across the organization and enable informed resource allocation.
   * Consider industry-specific risk standards and incorporate any specific compliance requirements into our cyber risk management practice.
   * Set and communicate an enterprise-wide IT and cyber risk management strategy. Technology infrastructure and application use is critical throughout every organization. Therefore, cyber risk exposure can occur in any division, making it an organizational priority, rather than an IT one.
3. **Invest in Cyber Risk Management Infrastructure**
   * Assess system requirements to understand where organizational cyber threats originate and provide a guidepost to the types of systems required. A distributed, cloud-based organization will have different needs from a physical asset intensive organization. Consider how our company currently operates to ensure that a GRC platform will accommodate evolving needs.
   * Potential investment in GRC software or other cyber risk management tools should also consider risk reporting and incident management requirements, workflows, ease of use, flexibility, and future expansion capability.
4. **Establish a Dynamic Cyber Risk Management Process**
   * Establish robust oversight by maintaining an updated inventory of potential threats and dynamic quantification of the potential impact and mitigation costs of cyber incidents.
   * Communicate with third parties to ensure their security protocols align with organizational standards and practices.
   * Invest in Training - With rapid evolution of technology and related cybersecurity risks, cyber risk management is not a static, tick the box solution. Organizations can spend large sums on state of the art security infrastructure, but a truly effective cyber risk management program requires effective stakeholder training.

## What Is Cybersecurity Risk Management:

Cybersecurity risk management is a strategic approach to prioritizing threats. Organizations implement cybersecurity risk management in order to ensure the most critical threats are handled in a timely manner. This approach helps identify, analyze, evaluate, and address threats based on the potential impact each threat poses.

A risk management strategy acknowledges that organizations cannot entirely eliminate all system [vulnerabilities](https://www.imperva.com/learn/application-security/vulnerability-management/) or block all [cyber attacks](https://www.imperva.com/learn/application-security/cyber-warfare/). Establishing a [cybersecurity](https://www.imperva.com/learn/application-security/cyber-security/) risk management initiative helps organizations attend first to the most critical flaws, threat trends, and attacks.

Broadly speaking, the cybersecurity risk management process involves four stages:

* Identifying risk – evaluating the organization’s environment to identify current or potential risks that could affect business operations
* Assess risk – analyzing identified risks to see how likely they are to impact the organization, and what the impact could be
* Control risk – define methods, procedures, technologies, or other measures that can help the organization mitigate the risks.
* Review controls – evaluating, on an ongoing basis, how effective controls are at mitigating risks, and adding or adjusting controls as needed.

## What Are Cyber Threats?

The term [cyber threat](https://www.imperva.com/learn/application-security/cyber-security-threats/) generally applies to any vector that can be exploited in order to breach security, cause damage to the organization, or exfiltrate data.

Common threat categories facing modern organizations include:

* Adversarial threats—including third-party vendors, insider threats, trusted insiders, established hacker collectives, privileged insiders, ad hoc groups, suppliers, corporate espionage, and nation-states. This category also includes malicious software (malware) created by any of these entities. Large organizations mitigate these threats by establishing a security operations center (SOC) with trained security staff and specialized tooling.
* Natural disasters—hurricanes, floods, earthquakes, fire, and lightning can cause as much damage as a malicious cyber attacker. A natural disaster can result in loss of data, disruption of services, and the destruction of an organization’s physical or digital resources. The threat of natural disaster can be minimized by distributing an organization’s operations over multiple physical sites or using distributed cloud resources.
* System failure—when a system fails, it may cause data loss and also lead to a disruption in business continuity. Make sure that our most critical systems are running on high-quality equipment, have redundancy in place to ensure high availability, are backed up, and our providers offer timely support.
* Human error—any user may accidentally download [malware](https://www.imperva.com/learn/application-security/malware-detection-and-removal/) or get tricked by [social engineering](https://www.imperva.com/learn/application-security/social-engineering-attack/) schemes like phishing campaigns. A storage misconfiguration may expose [sensitive data](https://www.imperva.com/learn/data-security/sensitive-data/). To prevent and mitigate these threats, we should establish an employee training program and enforce strong security controls. For example, use password managers and monitor critical systems for misconfigurations.

Here are key threat vectors that affect the majority of organizations:

* Unauthorized access—may be the result of malicious attackers, malware, and employee error.
* Misuse of information by authorized users—an insider threat may misuse information by altering, deleting, or using data without authorization.
* Data leaks—threat actors or cloud misconfiguration may lead to leaks of [personally identifiable information](https://www.imperva.com/learn/data-security/personally-identifiable-information-pii/) (PII) and other types of sensitive data.
* Loss of data—poorly configured replication and backup processes may lead to data loss or accidental deletion.
* Service disruption—downtime may cause reputational damages and revenue losses. It may be accidental, or the result of a [denial of service](https://www.imperva.com/learn/ddos/denial-of-service/) (DoS) attack.

## Cyber Risk Management Frameworks

There are several cyber risk management frameworks, each of which provides standards organizations can use to identify and mitigate risks. Senior management and security leaders use these frameworks to assess and improve the security posture of the organization.

A cyber risk management framework can help organizations effectively assess, mitigate, and monitor risks; and define security processes and procedures to address them. Here are several commonly used cyber risk management frameworks.

### NIST CSF

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) is a popular framework. The NIST CSF framework provides a comprehensive set of best practices that standardize risk management. It defines a map of activities and outcomes related to the core functions of cybersecurity risk management—protect, detect, identify, respond, and recover.

### ISO 27001

The International Organization for Standardization (ISO) has created the ISO/IEC 270001 in partnership with the International Electrotechnical Commission (IEC). The ISO/IEC 270001 cybersecurity framework offers a certifiable set of standards defined to systematically manage risks posed by information systems. Organizations can also use the ISO 31000 standard, which provides guidelines for enterprise risk management.

### DoD RMF

The Department of Defense (DoD) Risk Management Framework (RMF) defines guidelines that DoD agencies use when assessing and managing cybersecurity risks. RMF splits the cyber risk management strategy into six key steps—categorize, select, implement, assess, authorize, and monitor.

### FAIR Framework

The Factor Analysis of Information Risk (FAIR) framework is defined for the purpose of helping enterprises measure, analyze, and understand information risks. The goal is to guide enterprises through the process of making well-informed decisions when creating cybersecurity best practices.

**Best Practices for Cybersecurity Risk Assessment:**

### Build Cybersecurity into the Enterprise Risk Management Framework

Fully incorporate our risk-based cybersecurity program into the enterprise risk management framework, which functions as the organizing principle for analyzing and classifying enterprise risks. The framework should not be used as a general guideline, but rather as the organizing principle. By framing cyber risk as a business risk, this approach makes cyber risk management more intelligible to businesses.

### Identify Value-Creating Workflows

Identify the workflows that generate the greatest business value and define their associated risks. It is important to consider the potential impact of crucial workflows because these can also pose a significant risk. For example, payment processes create value but present a business risk, as they are vulnerable to fraud and [data leakage](https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/).

Make sure the cybersecurity team knows which processes are regarded as valuable for our organization, and define the components (data assets, tools, teams) involved in each process. This allows we to apply the recommended controls. A collaborative approach involving both cybersecurity and business personnel is more effective than the one-sided maturity-based approach.

### Prioritize Cyber Risks

Determine risk level based on the cost of prevention and value of information to inform our risk management and mitigation procedures. High-level risks should be addressed as soon as possible, while low-level risks can be addressed down the line or accepted as a tolerated risks. If the cost of protecting an asset is higher than its value, the expense is not worthwhile unless the risk may impact our reputation.

### Implement Ongoing Risk Assessments

Perform continuous, adaptive, and actionable risk identification and assessment to keep up with evolving cybersecurity threats and solutions. Regularly review risk management processes to identify and remediate gaps. Cybersecurity teams rely on actionable insights from risk assessments to [secure digital environments and assets](https://www.imperva.com/learn/application-security/application-security/).

[Web Application Firewall](https://www.imperva.com/products/web-application-firewall-waf/) – Prevent attacks with world-class analysis of web traffic to our applications.

[Runtime Application Self-Protection (RASP)](https://www.imperva.com/products/runtime-application-self-protection-rasp/) – Real-time attack detection and prevention from our application runtime environment goes wherever our applications go. Stop external attacks and [injections](https://www.imperva.com/learn/application-security/prototype-pollution/) and reduce our vulnerability backlog.

[API Security](https://www.imperva.com/products/api-security/) – Automated API protection ensures our API endpoints are protected as they are published, shielding our applications from exploitation.

[Advanced Bot Protection](https://www.imperva.com/products/advanced-bot-protection-management/) – Prevent business logic attacks from all access points – websites, mobile apps and APIs. Gain seamless visibility and control over bot traffic to stop online fraud through account takeover or competitive price scraping.

[DDoS Protection](https://www.imperva.com/products/ddos-protection-solutions/) – Block attack traffic at the edge to ensure [business continuity](https://www.imperva.com/learn/availability/business-continuity-planning/) with guaranteed uptime and no performance impact. Secure our on premises or cloud-based assets – whether we’re hosted in AWS, Microsoft Azure, or Google Public Cloud.

[Attack Analytics](https://www.imperva.com/products/attack-analytics/) – Ensures complete visibility with machine learning and domain expertise across the application security stack to reveal patterns in the noise and detect application attacks, enabling we to isolate and prevent attack campaigns.

[Client-Side Protection](https://www.imperva.com/products/client-side-protection/) – Gain visibility and control over third-party JavaScript code to reduce the risk of supply chain fraud, prevent data [breaches](https://www.imperva.com/learn/data-security/data-breach/), and client-side attacks.

[Cloud Data Security](https://www.imperva.com/products/cloud-data-security/) – Simplify securing our cloud databases to catch up and keep up with [DevOps](https://www.imperva.com/learn/application-security/devsecops-devops-security/). Imperva’s solution enables cloud-managed services users to rapidly gain visibility and control of cloud data.

[Database Security](https://www.imperva.com/products/database-security/) – Imperva delivers analytics, protection and response across our data assets, on-premise and in the cloud – giving we the risk visibility to prevent data [breaches](https://www.imperva.com/learn/data-security/data-breach/) and avoid compliance incidents. Integrate with any database to gain instant visibility, implement universal policies, and speed time to value.

[Data Risk Analysis](https://www.imperva.com/products/data-risk-analytics/) – Automate the detection of non-compliant, risky, or malicious data access behavior across all of our databases enterprise-wide to accelerate remediation.

# Cyber Security Risk Analysis and Assessment:

Risk analysis is a process of reviewing risks that come with a particular asset or event. It is a crucial security process for any type of company. The risk analysis includes identifying the assets most vulnerable to cyberattack.

This may include equipment, customer data, intellectual property, etc. It follows risk estimation and evaluation and then takes measures to control the risk. The idea is to monitor the process continuously and detect any suspicion right on time.

The cyber risk analysis is for every company. The size and the industry doesn’t matter here. Any company operating with technology and consumers needs to perform this analysis. PSUs can majorly benefit from it by greater vigilance and methods of protection.

The cyber risk assessment should be carried out by in-house teams with trained professionals. The IT staff and executives should be in this team to understand digital and network infrastructure and proprietary organizational knowledge. The main element here is to maintain organizational transparency. For smaller companies, relying on cybersecurity software is the most economic option.

### Uses of Cyber Security Risk Assessment

1. To avoid adverse outcomes and anticipate them for minimum effect

2. To keep a plan ready for the resources which might be comprised

3. To recognize potential risk in a project

4. Identify the possibility and make amends for it

### Steps in the risk analysis process

#### 1. Determine information value

The account planning for every company is done at the start of the financial year. And a limited budget is put for information risk management as well. This becomes a limitation as now the company has to prioritize business-critical assets. This helps them save money and have a more well-planned analysis.

A few things to consider while making this list –

* Financial or legal penalties of information
* Value of information to a competitor
* Information recreation and time to do so
* Value of information in revenue or profitability
* Impact of information on business operations
* Reputational damage associated
* IT security policies
* IT security architecture
* Network topology
* Information storage protection
* Information flow
* Technical security controls
* Physical security controls
* Environmental security

#### 2. Identify cyber threats

The assessments are to identify the vulnerabilities of an organization. And looking at potential risks and previous breaches can allow experts to identify future situations as well. And now, threats are not just limited to hackers, malware, but much more than that. They are –

##### **a. Natural disasters**

These situations are something the management can look at according to geographic location and climate.

##### **b. System failure**

Sometimes the most important information is available on low-quality equipment which can lead to its corruption.

##### **c. Human error**

Lack of employee training can lead to frequent human eros and thus loos of data. This can also happen due to a lack of attention and management.

##### **d. Adversarial threats**

there are insiders, ethical hackers, suppliers, and sometimes even clients who can leak important information.

Some examples of cyber risks are –

* Ransomware
* Data leaks
* Phishing
* Malware
* Insider threats
* Cyberattacks

Some common threats that affect every organization include:

* Using different malware for unauthorized access
* Using information for personal gain by authorized users
* Leaking data for unethical reasons
* Losing data by some human error

#### 3. Identify vulnerabilities

After knowing what kind of threats we might face, we identify the weakness that a threat can exploit. If the data suggests a high number of human errors in history, we make our training more strong. If there are chances of software-based vulnerabilities then go for proper patch management.

#### 4. Analyze Controls

Having proper control can reduce the chances of a threat or vulnerability. This is possible by using encryption, detection mechanisms, authentication, automatic updates, etc. Other non-technical ways are following security policies and physical mechanisms.

Controls are either preventative or detective. Preventative controls are for stopping the attack by taking precautions. While detectives are to identify the threats by continuous security monitoring.

#### 5. Calculate the Impact

After knowing what is at risk, the next step is to find out what will be the impact. If we are presuming a natural disaster, then we know that our physical equipment is at risk. This can help we identify the budget we will need to overcome the situation.

#### 6. Prioritize Risks based on cost and value

Follow the data collected from information value and use risk level to mitigate the risk. If the risk is high, come up with measures as soon as possible. If the risk is medium then take a reasonable period of time. And in case of low risk, take a call to accept or mitigate.

Always remember that cost of controlling the threats should be less than the cost of assets at risk. But this being said, consider other things like –

* Organizational policies
* Reputational damage
* Feasibility
* Regulations
* Effectiveness of controls
* Safety
* Reliability
* Organizational attitude
* Tolerance for uncertainty

#### 7. Make Assessment Reports

The last and the most important step is to make a collective assessment report. This report becomes the basis for the team to take action and make decisions. The ending is usually the control recommendations that companies can refer to. This entire process helps to understand the company better and the scope of improvement.

### ISO 27001 and cyber risks

As we saw some of the important standards in previous articles, we are aware that ISO 27001 is an important standard to follow. It has guidelines for information security management systems, addressing people, processes, and technology.

Clause 6.1.2 of the standard says the following about the information security risk assessment process –

1. Organizations need to maintain information security risk criteria.

2. It is mandatory to have repeated risk assessments that are valid and comparable

3. Companies should the risk that comes with the loss of information

4. They should identify the owners of those risks

5. They must analyze and evaluate risks according to the criteria

6. They need to maintain documented information about the assessment process

7. And lastly, they must follow relevant steps for information security risk treatment process

## What is Cybersecurity Risk Analysis?

Foremostly, cybersecurity should be an [integral part of a business strategy](https://pestleanalysis.com/why-cybersecurity-should-be-part-of-your-business-strategy/), especially, if our business is involved in e-commerce. The cybersecurity risk analysis will help we analyze our business’s current situation. The analysis will help we identify, protect, and manage all our information data, systems, and resources. we can then determine the risks and create a suitable plan to secure and manage them.

### Why do we need it?

we may think that we have a small local business and question why would anyone target we. Well, know that according to a [Verizon Data Breach Investigations report](https://www.researchgate.net/publication/324455350_2018_Verizon_Data_Breach_Investigations_Report), 61% of the victims of cybercrime in 2017 were small to medium businesses. As the adage goes “one man’s garbage is another man’s treasure”, such is the case with data and information. we may not consider a data valuable but if a breach happens, it may land we and our business in hot waters and it can seriously damage our company’s image.

## How do we perform a Cybersecurity Risk Analysis:

Below is a short summary of how a cybernetwork security strategist may evaluate and analyze our company’s current security condition.

### Take a record of all the Network systems:

The analysis begins by collecting and tracing all the networks that our business connects with. This includes all our devices and the interaction of data between our vendors, our network provider, and our employees.

### Identify the Vulnerabilities:

The next step would be to identify the vulnerabilities in the data flow between software and hardware. The most commonly found susceptibility in institutions are mobile devices, gadgets, and other associated devices. Unauthorized emails are also a potential threat. Other major weaknesses include non-administrative access to network, open-source operating systems, and malwares.

### Limit the Cybersecurity Risks:

There is a plethora of ways to reduce network security risks but the most common course of action is to control data loss, network failures, backups, server breaches. But what requires the most attention are the business transactions and customer data. The encryption of these, along with the company’s personal data (such as employees’ identities, accounts, records) is of crucial importance.

### Develop Strong Security Protocols:

After we’ve fixed the internal security problems of the company, now comes the time to set up a strong defense against potential attacks. The stronger the protocols, the safer our business is. we can do this by setting up a firewall, dedicated networks, and strong passphrases. Furthermore, using [vendor risk management system](https://pestleanalysis.com/risk-management/) and multi-level authentication with encryption on data can prove to be a robust guard against data infiltrators.

### Why do we Need a Cyber Security Risk Assessment?

The primary purpose of cyber risk assessment or security risk analysis is to help inform decision-makers and support appropriate risk responses.

There are many reasons why a risk assessment is required:

* When it comes to quantitative risk assessment, they can help we save costs that may result from a security breach, hence creating a security incident. In addition, they can also minimize the qualitative costs such as reputational damage to the organization.
* An organization becomes aware of the risk and threats and how to tackle them on a repeated basis and carry out the risk assessment to uncover threats and vulnerabilities.
* It can help an organization avoid any compromise to assets and security breaches.

### How to Perform a Cyber Security Risk Assessment?

There are certain guidelines from NIST that can be followed:

#### **1. Upgrade and Update Software as Soon as the Patch is Available**

The organization should upgrade and patch the systems and software as soon as they are made available or released in the market. It is a good practice to automate the upgrading process as the manual procedure might get skipped sometimes, but it is scheduled to run as a part of the scope when it comes to automation. The bad guys keep looking at patches and possible exploits, and these can later become N-Day attacks. The updates are always signed and prove their integrity by securely being shared over the protected links.

#### **2. Access Controls and Privileges**

Any organization must use proper access controls and Privileged Access Management to manage the user accounts and their controls. The users should exactly be given the controls that they need, not less nor more. If given less, it will affect productivity, while if given more, it may open a path for exploit which could be disastrous. The elevated account must be controlled and monitored as they carry high privileges, and so, if they fall into bad hands, will be the impact of a compromise. All of the user’s accounts should be protected and monitored as well.

#### **3. Enforce Signed Software Execution Policies**

The software that is being used should agree to the integrity, i.e. it should not be altered or modified in any way; it should be properly signed. This can be easily checked by matching with hash functions like SHA256 or SHA 512 values. In addition, a list of reliable certificates should be maintained. If altered or unsigned software is used by any chance, it may have been designed to create vulnerabilities, and it should open up a door to expose our systems to hackers.

#### **4. Implementation of System Recovery Plan**

In times of adverse situations such as a disaster like floods and earthquakes, one should be ready with a recovery plan to take care of employees, assets, and mitigation and keep supporting the organization function from another place that is not affected by the disaster. Therefore, a recovery plan must be created, reviews, and exercised (tested) regularly.

#### **5. Actively Manage Systems and Configurations**

The organization should review software that is present in the user’s system and access controls that are enabled for users. The users should also be directed to raise requests to remove unnecessary software or privileges that are no longer required as a part of their role. By doing this, it will reduce the attack surface to a greater extent.

#### **6. Threat Hunting and Threat Intelligence for Network and Host Intrusion**

The endpoint protection solutions are often not fully capable of blocking, detecting, and removing the threat from the systems, especially if the attack is targeted and sophisticated. To detect such threats, we should employ [threat hunting](https://www.educba.com/threat-hunting/) and [threat intelligence solutions](https://www.educba.com/threat-intelligence/) that will correlate the organization’s environment from the threat indicators from across the globe, and if there are any matches, it will trigger an alert. A similar practice should be employed to network as well, where we can put IPS/IDS to filter through network packets to look for suspicious activities.

#### **7. Implementing Modern Hardware Security Features**

Today’s hardware comes with great security features such as Unified Extensible Firmware Interface (UEFI), Trusted Platform Modules (TPM), virtualization of hardware, disk encryption, port security which should be enabled to prevent any hardware security breaches which may finally takeover confidential data and breach security.

#### **8. Separate the Network using Application-aware Defense**

Separate critical networks and services. Deploy application-aware network security to block improperly formed according to traffic and restricted content, policy and legal authorities. Traditional intrusion detection based on known and signatures is effectively reduced due to encryption and offset techniques.

#### **9. Integrate Threat Reputation Services**

As pointed out earlier, the endpoint solutions are not fully capable of blocking, detecting and removing the threat from the systems, especially if the attack is targeted and sophisticated. In such cases, we can integrate global threat reputation services (GTRS) in our environment to get our files checked against the huge number of reputation services.

#### **10. Multi-Factor Authentication**

The multi-factor authentication just acts like a defense in a depth approach where we get a second layer of security. The hacker will find the greatest difficulty of his life cracking a device where multi-factor authentication is enabled; it cannot be unlocked unless physically accessed or attacked. So organizations should always deploy multi-factor authentication at all the places where it can be applied.

## Prioritizing our Risks

Once we’ve assigned scores to our risks, we can categorize them according to their priority. For example, many enterprises allocate rankings of “high priority,” “medium priority,” or “low priority.”

### High Priority

A ransomware attack, in which malicious actors use malware to lock we out of our systems and demand payment to restore our access, would fall under this category. So would a zero-day attack, in which hackers exploit a previously unknown vulnerability.

### Medium Priority

A medium-risk event might be a former employee stealing information after being terminated. Reviewing our organization’s employee-access policies would be a control against this risk’s materializing. A robust employee termination process coordinated between human resources and IT would help mitigate this risk.

### Low Priority

If our buildings are adequately secured, the probability might be low of someone’s breaking into our offices and stealing devices. If those devices don’t contain any information, the likelihood of a data loss may also be low or nil. Since there is no urgency associated with this risk, we might decide to review our device-risk-mitigation controls annually.

**To carry out a risk analysis, follow these steps:**

### 1. Identify Threats

The first step in Risk Analysis is to identify the existing and possible threats that we might face. These can come from many different sources. For instance, they could be:

* Human – Illness, death, injury, or other loss of a key individual.
* Operational – Disruption to supplies and operations, loss of access to essential assets, or failures in distribution.
* Reputational – Loss of customer or employee confidence, or damage to market reputation.
* Procedural – Failures of accountability, internal systems, or controls, or from fraud.
* Project – Going over budget, taking too long on key tasks, or experiencing issues with product or service quality.
* Financial – Business failure, stock market fluctuations, interest rate changes, or non-availability of funding.
* Technical – Advances in technology, or from technical failure.
* Natural – Weather, natural disasters, or disease.
* Political – Changes in tax, public opinion, government policy, or foreign influence.
* Structural – Dangerous chemicals, poor lighting, falling boxes, or any situation where staff, products, or technology can be harmed.

we can use a number of different approaches to carry out a thorough analysis:

* Run through a list such as the one above to see if any of these threats are relevant.
* Think about the systems, processes, or structures that we use, and analyze risks to any part of these. What vulnerabilities can we spot within them?
* Ask others who might have different perspectives. If we're leading a team, ask for input from our people, and consult others in our organization, or those who have run similar projects.

Tools such as [SWOT Analysis](https://www.mindtools.com/amtbj63/swot-analysis), [Failure Mode and Effects Analysis](https://www.mindtools.com/community/pages/article/newTMC_82.php), [PMESII-PT](https://www.mindtools.com/a27imvh/pmesii-pt), and [PEST Analysis](https://www.mindtools.com/aqa3q37/pest-analysis) can also help we uncover threats, while [Scenario Analysis](https://www.mindtools.com/al4u1y9/scenario-analysis) helps we to explore possible future threats.

### 2. Estimate Risk

Once we've identified the threats we're facing, we need to calculate both the likelihood of these threats being realized and their possible impact.

One way of doing this is to make our best estimate of the probability of the event occurring, and then to multiply this by the amount it will cost we to set things right if it happens. This gives we a value for the risk:

**Risk Value = Probability of Event x Cost of Event**

As a simple example, imagine that we've identified a risk that our rent may increase substantially.

we think that there's an 80 percent chance of this happening within the next year because our landlord has recently increased rents for other businesses. If this happens, it will cost our business an extra $500,000 over the next year.

So the risk value of the rent increase is:

**0.80 (Probability of Event) x $500,000 (Cost of Event) = $400,000 (Risk Value)**

we can also use a [Risk Impact/Probability Chart](https://www.mindtools.com/community/pages/article/newPPM_78.php) to assess risk. This will help we to identify which risks we need to focus on.

Gather as much information as we can so that we can accurately estimate the probability of an event occurring, and the associated costs. Use past data as a guide if we don't have an accurate means of forecasting.

# Impact of Risk Analysis on Security

Impact is how we measure the effect of exploiting a flaw in our security. It helps us understand what will happen; what systems, processes, and people are involved; and the effect this exploitation may have on our wider organization.

In security, we often start examining impact by looking at the effect on the confidentiality, integrity, and availability of operations, systems, or services. These effects can be on a system-by-system level or on an organization-wide level.

Let’s get familiar with each of these impacts.

#### **CONFIDENTIALITY:**

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.**\***

A confidentiality agreement is a system of rules controlling who is authorized to access or interact with our data or systems.

Imagine we’re in an office; we’re going to explore the difference between an implicit and an explicit confidentiality requirement.

A colleague wants to share something confidential with we. They whisper their secret to we. Now, what do we do at this point? How long do we keep it secret for? Who are we allowed to tell? Who are we not allowed to tell? Navigating this is called an implicit confidentiality agreement.

So what would we do? Who can we tell the secret to? How long do we need to keep this information secret for? And in what circumstances can we share it with other people?

#### **INTEGRITY:**

Integrity is interesting. We’re used to talking about integrity when it comes to people. For example, this person has really good integrity. I can trust them. Their character is good. However, that’s not the sort of integrity we’re talking about here. We’re talking about the integrity of the data in our systems and whether it can be trusted.

Integrity (or data integrity) in a system refers to maintaining the accuracy and completeness of data over its entire lifecycle. Integrity requires protection of system data from intentional or accidental unauthorized changes. The clearest example of systems that require good integrity are banks.

**AVAILABILITY:**

Availability in our systems means ensuring that the systems remain open for business as and when they are required to be, and that they remain accessible for all users. Security is about balance. It cannot come at the cost of availability.

Availability is incredibly valuable to our organizations. This means we can’t simply put in a security control to improve the safety of our data and our systems if it means the systems cannot be accessed anymore. A secure system allows people to use it 24 hours a day, seven days a week if that’s what they need, and it allows them to do what they need to do safely and securely. And that’s a difficult balance to achieve indeed.

### Risk Impact: Understanding the Cost:

While confidentiality, integrity, and availability are all important parts of how we examine the impact of a security event or risk, there is one last step we need to take. We need to translate these systems, or process-level impacts, into the overall effect that this event will have on our organization, data, or customers. This is a less technical, more business-focused assessment that is often used to communicate risk to senior leaders and directors. Should consider the following factors.

* Loss of revenue. our organization makes less money.
* Increased operating costs. It costs more to keep our business operating than it did before, which will impact its decisions about hiring and buying new things.

## Benefits of risk analysis

## Every organization needs to understand about the risks associated with their information systems to effectively and efficiently protect their IT assets. Risk analysis can help an organization to improve their security in many ways. These are:

## Concerning financial and organizational impacts, it identifies, rates and compares the overall impact of risks related to the organization.

## It helps to identify gaps in information security and determine the next steps to eliminate security risks.

## It can also enhance the communication and decision-making processes related to information security.

## It improves security policies and procedures as well as develop cost-effective methods for implementing information security policies and procedures.

### Other Benefits of Risk Analysis:

#### 1. Reduction in Costs - Long-Term Cost Reduction.

#### 2. Provides Assessment Framework - A Template for Future Assessments.

#### 3. Increases Organizational Knowledge - Organizational Awareness.

#### 4. Avoid and Prevent data breaches and Losses.

#### 5. Avoid regulatory issues - Avoid Regulatory Fines.

#### 6. Avoid Application Glitches and Malfunctions.

### Conclusion:

The risk analysis will ensure the long-term growth of any company. It can assure the smooth functioning of business and a more secure work environment. Following these simple steps can ensure the safety of any company from multiple cyber threats. Companies need to take it seriously and implement such a process at right time. The benefits of doing so are clear and can bring positive responses to the company. We have to make sure that be it any organization, having an analysis plan should be the priority.