**CYBER RISK IDENTIFICATION**

As mentioned in the section on the [cyber risk management process](https://cyberwatching.eu/demystifying-cyber-risk-management-process), there are four essential steps involved:

* [Identify risks](https://cyberwatching.eu/cyber-risk-identification)
* [Assess risks](https://cyberwatching.eu/cyber-risk-assessment)
* [Identify possible mitigation measures](https://cyberwatching.eu/risk-mitigation)
* [Decide what to do about the residual risk](https://cyberwatching.eu/residual-risk)

One of the biggest challenges is in the very first step: *identification* of the risks. Cybersecurity is a constantly evolving field, making risk identification a moving target. Nevertheless, a basic approach has evolved over time that all risk identification methodologies tend to follow:

* Identify your **assets**;
* Identify the **threats** to those assets:
* Identify your **vulnerabilities** to those threats.

**Identifying assets**

In order to determine your cyber risk exposure, you need to first decide what your assets are. This is not as easy as it may seem: you can’t protect everything, so you need to identify the assets that must be protected, and their priorities.

A series of questions can help to clarify the situation:

* What kind of data do you store in your organization?
* Whose data is it? Yours? Somebody else’s?
* What would be the consequences if something happened to this data?

That last question leads us into the CIA – no, not the Central Intelligence Agency (although they happen to care about such things, too), but rather the fundamental triangle of cybersecurity: *Confidentiality*, *Integrity*, and *Availability*.

A blue triangle with white text

Description automatically generated

The CIA triangle guides you in asking these fundamental security-related questions about your data assets:

* What would happen if the data were revealed or became public (*confidentiality*)?
* What would happen if the data were incorrect or falsified (*integrity*)?
* What would happen if the data could no longer be accessed (*availability*)?

Some examples:

* You are a credit card company, and the numbers and personal identification codes of your customers are hacked and published (*confidentiality*);
* You are a bank, and a hacker adds a zero to the amounts in bank transfers (*integrity*);
* You are a hospital, and a ransomware attack makes it impossible to access your medical records (*availability*).

The CIA triangle helps you to identify the assets you need to protect, by understanding the kind of damage that could occur if they are compromised. But: compromised by whom? Or what? That leads to the next topic.

**Identifying Threats**

Threat analysis involves the identification of potential sources of harm to the assets (information, data) that you need to protect.

The world is full of threats, and the boundaries between what constitute relevant “cyber threats” and other kinds of threats will always be unclear. For example, although **hacking** is clearly a cyber threat, **environmental factors** such as flooding and fire could also threaten your data. You will have to decide how relevant they are to your situation.

Business-related threats constitute an even grayer area regarding their relevance to cybersecurity. Equipment failure like broken disks could threaten your data. An emerging source of much preoccupation is **supply-chain security**: can you be sure that your suppliers are not delivering malware to you, intentionally or otherwise? **Insider** threats, e.g. from disgruntled or idealistic employees (or former employees) who decide to steal or publish your data constitute another growing cause for concern.

Some of these types of threats may not always seem related to cybersecurity, but the connection can be subtle. As always, experience is the key to recognizing threats and correctly prioritizing them.

Even when threats are clearly related to cybersecurity, you will need to refine your identification of the threats. For example, hacking by a remote malicious user is obviously a cybersecurity threat. But what *kind* of hacking? A “denial of service” hack will block access to your data (making it unavailable). A ransomware attack will do the same (and make you pay in the process). A malware attack might install a program to read what you type and steal your confidential information. Here, too, the experience of professional analysts is key to successful identification.

**Identifying Vulnerabilities**

Once threats have been identified, your next task is to identify weaknesses in your overall cybersecurity environment that could make you **vulnerable** to those threats.

It may not always be simple to identify weaknesses and their sources and remedies. For example, how might you be vulnerable to insider threats? Certainly, by firing or losing an employee who was in charge of sensitive data. But you might also be vulnerable because of insufficient employee cybersecurity awareness: perhaps your employees innocently choose weak passwords (recall that this is how the famous Enigma code was broken in World War II), or are not sufficiently aware of the dangers of opening attachments to electronic mail messages.

**The Asset – Threat – Vulnerability Identification Cycle**

As mentioned at the beginning, identifying the cyber risk exposure of your organization is one of the biggest challenges in the overall risk management process. This has to do with the fact that cybersecurity is constantly evolving.

For this reason, it is essential to participate in a **cybersecurity community** where incidents and responses are continuously recorded and shared with others. This is the purpose of the many global and national initiatives to establish well-known centers of expertise and repositories to which organizations can refer for new information, and to which they can contribute their own experience. One example is the **NIS Directive** in Europe, which mandated the establishment of the *Computer Security Incident Response Teams* (CSIRTs) in the Member States. These CSIRTs help organizations to become aware of new threats as they appear, and to take appropriate steps. That is only one example of the many initiatives and centers available to you, and one mission of cyberwatching.eu is to inform you about the overall landscape of cyber information sources.

In summary, it is difficult to go it alone in the identification of the cyber risks facing you. But you don’t have to – *and should not* – go it alone. The cyber risk landscape has become too complex to manage alone; it can only be done within a community. And you need the benefit of the experience of others to be able to identify your assets in need of protection; to identify the many, ever-changing ways in which they could be threatened; and to become aware of the vulnerabilities of your organization to those threats.