



What is cybersecurity

What we protect, what we protect it from, and why you are the first link in the chain

Gianluca Bonomo · www.gianlu.it · info@gianlu.it



Contents

How to use this handout 3

1. A Monday morning with no files 3

1.1 What is at stake in an office 4

2. The three properties to protect 5

2.1 Confidentiality: who can see 6

2.2 Integrity: what has been changed 6

2.3 Availability: there when you need it 7

3. What we defend against: technical and human threats 8

3.1 Technical threats 9

3.2 Human threats 9

3.3 Often the two families meet 9

4. Human error: where incidents really start 10

4.1 First case: the «director's» email 10

4.2 Second case: the supplier's USB stick 11

4.3 Why we make mistakes, and how to get out of it 12

5. Why training is the most effective defence 13

5.1 What being trained means 13

5.2 What we will cover in the course 14

5.3 What a well-protected day looks like 14

5.4 An honest limit 16

Exercise: the map of your data 17

Questions that come up in class 18

Glossary 18

Further reading 19

How to use this handout

This handout gathers, in written and ordered form, everything covered in the lesson. You do not need to memorise it: it is there so you can find things again calmly, later, when the lesson is over and a question is left hanging.

> **GOAL**
>
> Understand what cybersecurity really means: the three properties of information to protect, technical and human threats, the weight of human error, and what is at stake when you work with other people's data.

What you will be able to do

- Explain confidentiality, integrity and availability in your own words, with one example each.
- Tell a technical threat from a human one.
- Recognise the work situations where a small mistake can become an incident.
- Identify which personal data of other people passes through your computer every day.
- Explain why training is the most effective defence.

1. A Monday morning with no files

Picture switching on your computer on Monday morning and finding that the list of enrolled students will not open.

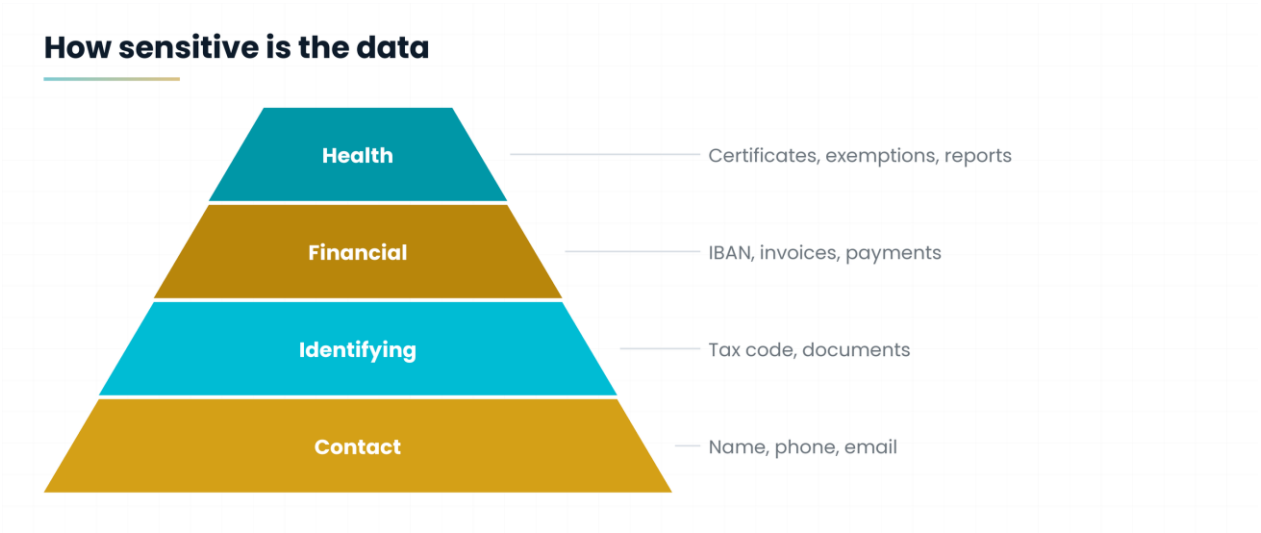
In the office of a small music school, Marta (a made-up name) opens the enrolment folder. The files are there, but they have a strange extension and no program can read them. On the desktop there is a message she has never seen before.

At the same moment, in another office, a colleague notices that the amount on an invoice has changed. Nobody knows who edited it. In a third office, an email with the list of parents has gone by mistake to an outside address.

Three different episodes, one theme: **cybersecurity**. It is the set of rules, habits and tools that protect information and the computers that hold it. It is not a subject for technicians only: it concerns anyone who uses a computer at work.

1.1 What is at stake in an office

An office computer holds data about people: names, addresses, phone numbers, tax codes (the code that identifies every Italian citizen for tax purposes, the *codice fiscale*), sometimes health or financial documents. It is information that someone has entrusted to you.



People's data in an office, from the most common to the most sensitive

Protecting it is a legal duty, but first of all it is a matter of trust. A family enrolling a child at school, a client leaving documents with a small firm, a patient booking a visit: they all expect that data to stay safe.



Protecting data means safeguarding people's trust.

THE IDEA IN ONE LINE

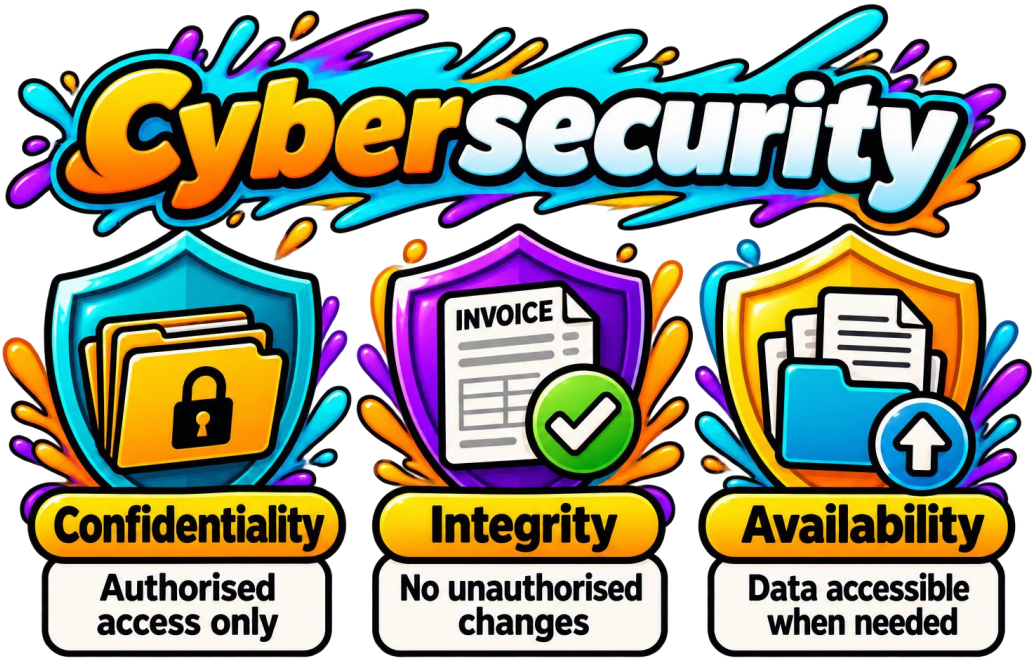
Cybersecurity means making sure the right information is available to the right people, and only to them, with no hidden changes.

2. The three properties to protect

Experts say that cybersecurity protects three things, called the three properties of information. The names sound technical, but the ideas are ones you already know.

Property	It means	Example in an office
Confidentiality	Only those who have the right can see the data.	The list of enrolled students does not reach a stranger.
Integrity	Data is not altered without authorisation.	Nobody quietly changes the amount on an invoice.
Availability	Data is accessible when it is needed.	On Monday morning the files are still there, even after a breakdown.

The three properties of information, with an everyday example for each.



Cybersecurity

2.1 Confidentiality: who can see

This is the most intuitive property. A student's record should be readable by the person who handles it, not by the visitor waiting in the corridor who can see the screen.

Confidentiality is lost in many ways: an email sent to the wrong person, a sheet forgotten on the printer, a password lent to a colleague because «he is trustworthy anyway».



Confidentiality: data is visible only to authorised people.

2.2 Integrity: what has been changed

A piece of data can stay confidential and still become unreliable if someone changes it. Think of an IBAN (the code that identifies a bank account) altered in a payment request: the invoice looks the same, but the money goes elsewhere.

Changes are not always malicious. A file overwritten by distraction, or a program that crashes while saving, can leave wrong data that nobody notices right away.



Integrity: protecting data from hidden changes.

2.3 Availability: there when you need it

Data can be perfectly confidential and correct, yet useless if you cannot open it. A failed disk, a virus that encrypts your documents, an account locked on the day of a deadline: all of these are losses of availability.

This is the property defended by safety copies (**backups**), which we cover in a dedicated lesson.

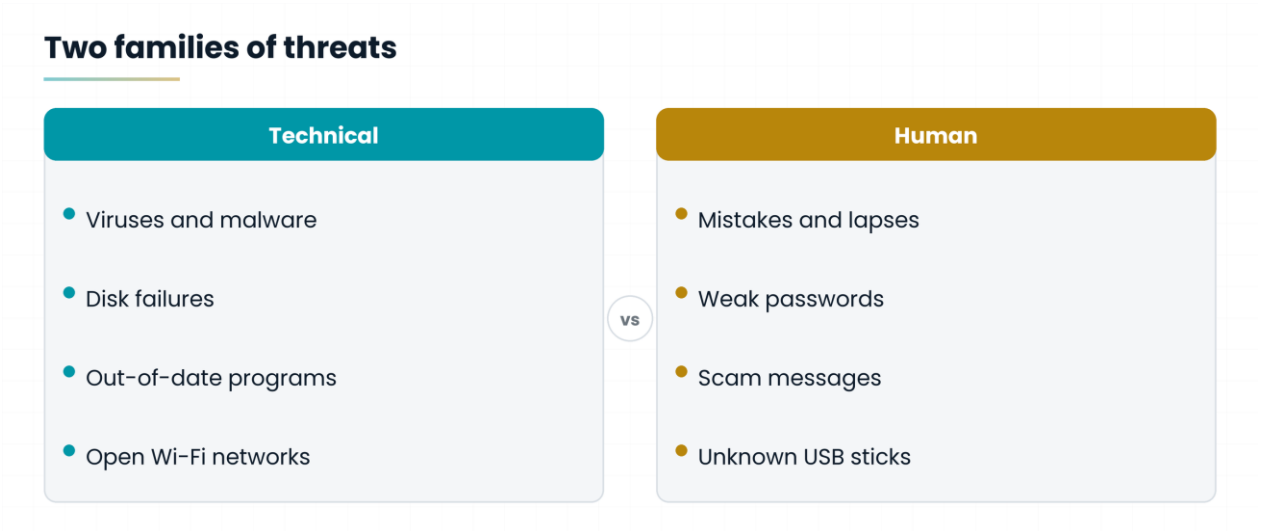


Availability: getting your data back when you need it.

> **ONE CASE, THREE PROPERTIES**
>
> A made-up accounting firm, «Studio Esempio», keeps the payslips of a client's employees.
>
> **Confidentiality:** only two people in the firm can open them. **Integrity:** nobody can change an amount without leaving a trace. **Availability:** on payment day the files must open, even if the computer broke the evening before.

3. What we defend against: technical and human threats

Threats are anything that can make you lose one of the three properties. We split them into two big families, and it helps to keep them apart because they are fought in different ways.



Two families of threats, two ways of defending

3.1 Technical threats

These come from machines and software. A virus, meaning a harmful program, is the best-known example. But there are also a disk failure, an out-of-date program with a known flaw, and an unprotected public Wi-Fi network.

Against these threats you need tools: updates, antivirus, backups. We will go through them one by one in the next lessons.

3.2 Human threats

These pass through people: a mistake, a distraction, or a deception. A fraudster does not need to break into the computer if he can convince you to open the door yourself.

- **the mistake:** an email sent to the wrong recipient, a file deleted by distraction;
- **the lapse:** a computer left on and unlocked, a password written on a sticky note;
- **the deception:** a message pretending to come from the bank, the courier or the director;
- **the carelessness:** a USB stick found in the car park and plugged in «just to see what is on it».

3.3 Often the two families meet

A successful attack usually combines both. The fraudster uses a human trick (a convincing email) to launch a technical threat (a harmful program). That is why a good antivirus is not enough: you also need to know what not to click.



Technical and human threats often meet.

> **WARNING**
>
> No technical tool stops a person who willingly hands over their password to a stranger who claims to be technical support.

4. Human error: where incidents really start

In real life, most incidents start with human error.

A wrong click, a weak password, a lost USB stick. It is not a fault to pin on anyone: it is the normal result of working in a hurry, among a thousand other things, with email arriving in waves.

Attackers know this well. That is why scam messages are written to create urgency, fear or curiosity: these are the emotions that make us click before we think.

4.1 First case: the «director's» email

Giulia (a made-up name) works in the office of a small organisation. On a Thursday afternoon she receives a message that looks like it comes from the director: «I am in a meeting and cannot call. Make a bank transfer to this supplier right away, I will explain later.» The name is right, the tone is the usual one.

If Giulia goes ahead, the money is gone. If she stops and reads the sender's address, she notices that the domain (the part of the address after the @ sign) is slightly different from the organisation's. If she phones the director on the number she already knows, she discovers the deception in a few seconds.



An urgent request for money deserves a check.

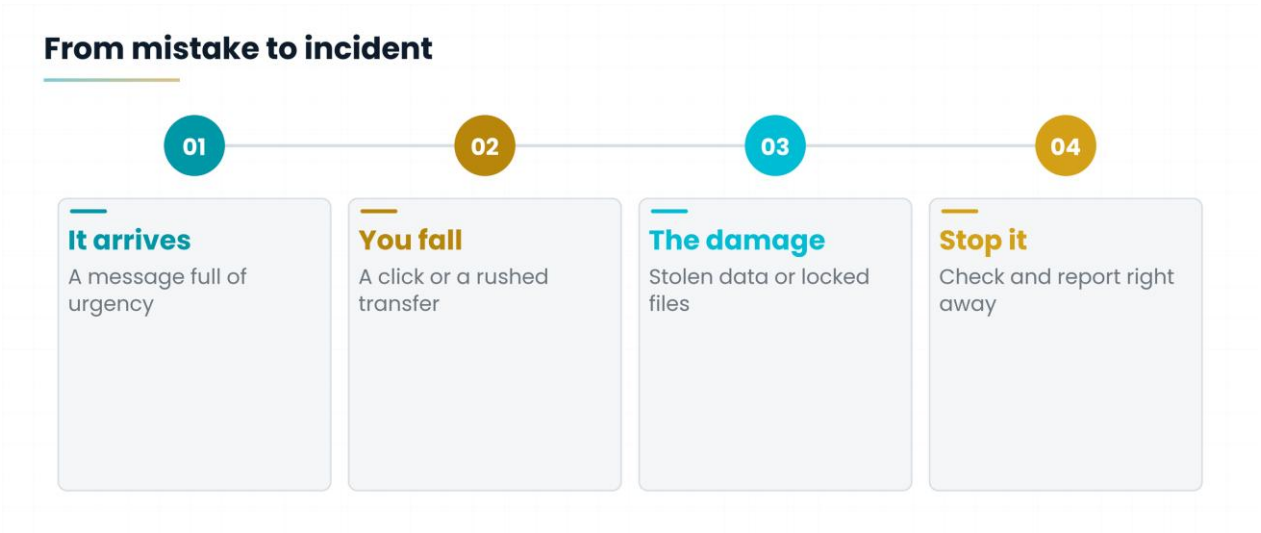
4.2 Second case: the supplier's USB stick

In a made-up shop, a sales rep leaves a USB stick with «the updated price list». The shop assistant plugs it into the till computer to print it. If the stick contains a harmful program, it is now on the computer that handles the takings and the customers' data.



Even a well-meant gesture can introduce a risk.

The gesture was in good faith. But good faith is not enough: you need a simple rule that everyone knows, for example **nothing is plugged into a work computer unless the IT contact has checked it**.



How a small mistake becomes an incident, and where it can be stopped

4.3 Why we make mistakes, and how to get out of it

What makes us slip	What helps
Hurry and deadlines	A moment of pause before clicking or making a payment.
Habit («I have always done it this way»)	Written rules that are simple and the same for everyone.

What makes us slip	What helps
Trust in the sender's name	Check the address and, if in doubt, call back on a known number.
Embarrassment at asking	An environment where you can say «I am not sure, can you check with me?».

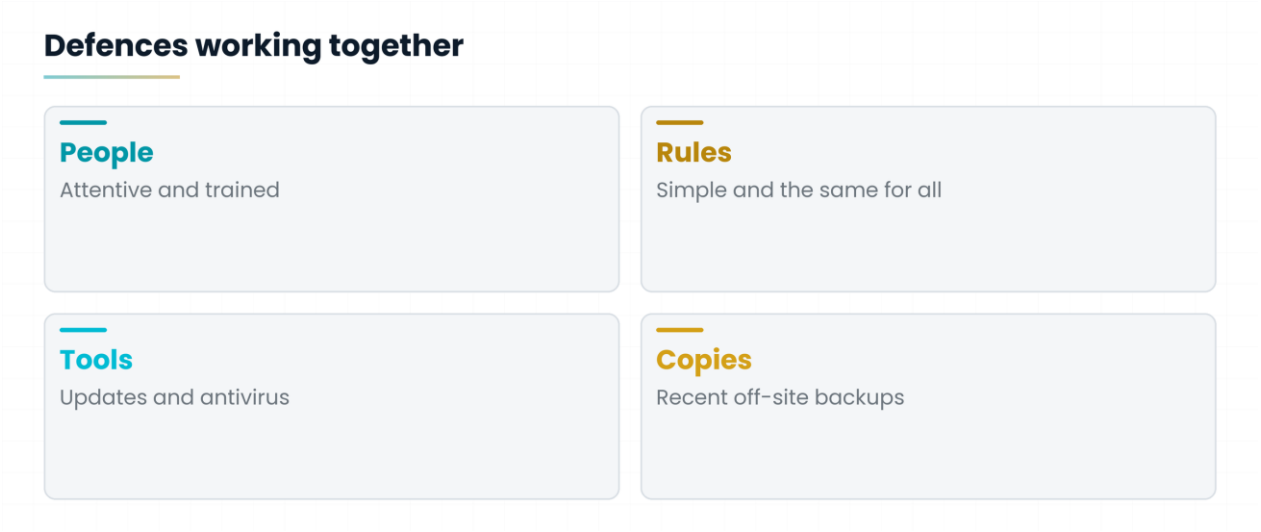
The most common causes of error and the countermeasure that works.

> **THE IDEA IN ONE LINE**
>
> A mistake does not become a serious incident if you report it right away. Silence, on the other hand, makes it worse.

5. Why training is the most effective defence

If most incidents pass through people, the most effective defence passes through people too. A good antivirus protects you from what it already knows. An attentive person protects you even from what no program has yet seen.

That does not mean tools are useless. It means they work together: tools stop the bulk, people stop the rest.



Defences work together: none is enough alone

5.1 What being trained means

- **knowing** what is at risk and why other people's data must be handled with care;
- **recognising** the signs of a deception before clicking;
- **knowing** a few simple rules and applying them always, even when in a hurry;

- **knowing who to tell** if something goes wrong, and doing it right away.

5.2 What we will cover in the course

This lesson is the map. In the next ones we will look at malware and ransomware, phishing and its variants, fake sites and social engineering, passwords and two-step verification, protecting devices and networks, backup, privacy, and what to do when it happens.

Each lesson starts from a real problem and ends with a short exercise you can do with what you already have on your computer.



Which personal data passes through your work? Who should be able to see it?

5.3 What a well-protected day looks like

It is not a heroic day: it is an ordinary day with a few extra gestures. You switch on the computer and unlock it with your password, which nobody else knows. When you leave your desk, you lock the screen. An email that puts you under pressure gets a calm second read and, if it involves money, you phone whoever is supposed to have written it.

At the end of the day, your important documents are also in a safe copy. None of these gestures needs technical skill. They need a habit, and habits can be built: that is exactly what we will do, lesson after lesson.



Lock, reread, verify and keep a copy: small everyday gestures.

There is also an effect you notice over time: people who work where these habits are shared feel less alone in front of a doubt. They know who to ask and they know that asking is not a weakness.



Stop, check, report. Asking for help is part of security.

5.4 An honest limit

No defence gives absolute security. The goal is not never to make a mistake, but to greatly reduce the chances of error and limit the damage when one happens. An office that has recent backups and people used to reporting problems is already far safer than one that trusts luck.

> **WARNING**
>
> The rules in this course are common-sense basics. If you work for an organisation or a company, also follow its internal procedures and the guidance of your IT contact: they come first.

Exercise: the map of your data

A short exercise with pen and paper and the computer you normally use. Nothing to install.

1. List which personal data of other people passes through your work in a normal week: names, addresses, phone numbers, tax codes, documents, photos.
2. For each type of data, write where it lives: on the computer, in a shared folder, in an email, on paper, on a USB stick.
3. For three of them answer these questions: who should be able to see it (confidentiality)? What would happen if someone changed it (integrity)? What would happen if on Monday morning it were no longer available (availability)?
4. Find one habit of yours or of your colleagues that puts one of the three properties at risk, for example a shared password or a sheet left in view.
5. Write the first small rule you would adopt to fix it.

> **CHECK YOUR RESULT**
>
> Did you find at least five types of data and where they are kept?
>
> Did you answer all three questions for each piece of data you analysed?
>
> Is the rule you wrote simple enough to apply even on busy days?

Questions that come up in class

I am just an office assistant: why would anyone attack me?

Because most of the time they are not after you in particular. They send the same message to a huge number of people and see who falls for it. Besides, an office computer is attractive precisely because it holds personal data and has access to email, payments and archives.

Is a good antivirus enough to be safe?

No. Antivirus is an important part, but it does not stop a fraudster who convinces you to hand over a password or make a bank transfer. You need tools, rules and attentive people together.

If I made a mistake and clicked, will I get a telling-off?

It depends on the organisation, but the right message is this: reporting right away is far better than staying silent. A wrong click reported immediately can often be fixed; the same click hidden can become serious damage.

What is the difference between cybersecurity and privacy?

Cybersecurity protects information and systems from loss, alteration and unauthorised access. Privacy concerns people's right to have their personal data used properly. They overlap: without security there is no privacy. We devote a separate lesson to privacy.

Does anything change when working from home or from a smartphone?

The principles are the same. The places change: a home or café Wi-Fi network, a phone that gets lost. That is why personal devices used for work need the same care, and you should always ask your organisation what its rules are.

Glossary

Term	What it means
Availability	The property whereby data is accessible when it is needed.
Backup	A safety copy of data, kept so that it can be restored if the originals are lost.
Confidentiality	The property whereby only those entitled to it can see the data.
Cybersecurity	The set of rules, habits and tools that protect information and the devices that hold it.
Domain	The name of a website or email address, for example ente-esempio.it.

Term	What it means
Integrity	The property whereby data is not altered without authorisation.
Malware	From «malicious software»: a program created to damage a computer or steal data.
Personal data	Any information relating to an identified or identifiable person: name, address, email, tax code, photo.
Threat	Any event, technical or human, that can cause a loss of confidentiality, integrity or availability.

Further reading

Regulation (EU) 2016/679 (GDPR) - official text on EUR-Lex

Agenzia per la cybersicurezza nazionale (ACN), Italy's National Cybersecurity Agency - information material for citizens and businesses, acn.gov.it

Garante per la protezione dei dati personali, the Italian Data Protection Authority - guides on data security, garanteprivacy.it

> **WATCH OUT**
>
> Information up to date as of October 2026. Names of people, firms and domains in the examples are made up. Italian bodies are explained in brackets: the Garante is Italy's data protection authority. The general rules in this course do not replace your organisation's own procedures.