Cybersecurity Fundamentals

Overview of Cybersecurity

What is cybersecurity?

15 Minutes

Module Overview

This module focuses on some fundamentals about cybersecurity to get you started within the course. You will learn about these topics:

- What is information security and cybersecurity?
- Objectives of information security, using the CIA triad
- Key elements of cybersecurity
- Risk and the methods to manage risk
- Common misconceptions about the cybersecurity industry
- Importance of laws and ethical considerations for the cybersecurity industry

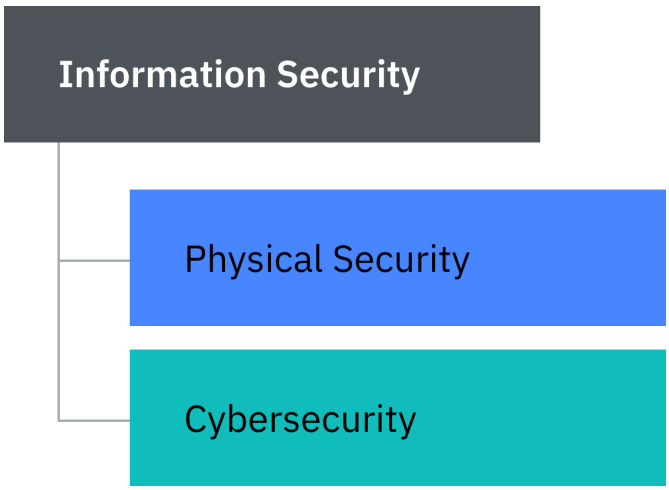
Information security

Let's start by thinking about what cybersecurity is and what we are trying to accomplish. Most definitions of cybersecurity tend to focus on **technology**, so a typical definition might include the "security of digital systems" or "security of communications". These definitions tend to get blurry, very quickly. For instance:

- What if a fraudster sends an email to a person claiming to be from their bank and asking for their personal identification number (PIN). Is that a cybersecurity concern?
- What if a private investigator calls an employee of a company to ask him to print some confidential files and leave the papers in the mail room them to collect. Is that a cybersecurity concern?

In the real world, most attacks typically have some **digital elements** as well as some **human factors** and occasionally a **physical element** too. Please keep this in mind. We should not just focus on digital elements because this limits our thought process and gives potential attackers greater flexibility.

Let's consider a new concept called **information security**. Information security focuses on the **value of the information we are trying to protect** rather than how we protect it. The following diagram shows that under information security are the physical elements and digital elements.



- **Physical security** is the practice of physically protecting assets like buildings, security cameras, equipment, and property from physical threats such as theft, vandalism, fire, and natural disasters.
- **Cybersecurity** is the practice of protecting and recovering networks, devices, and programs from any type of malicious cyber attack.
- Good security cannot have one without the other and both must work towards the same objectives.

EXAMPLE

Let's consider this from a customer's perspective. Imagine that you go to a travel company and share your passport details to book a trip abroad. What if an employee of the company accidentally emails your passport details to the wrong address or drops printed papers with your passport details from a briefcase on a train? The result is the same. Your private information has been compromised. In information security, the **emphasis is on the outcome** rather than the exact method.

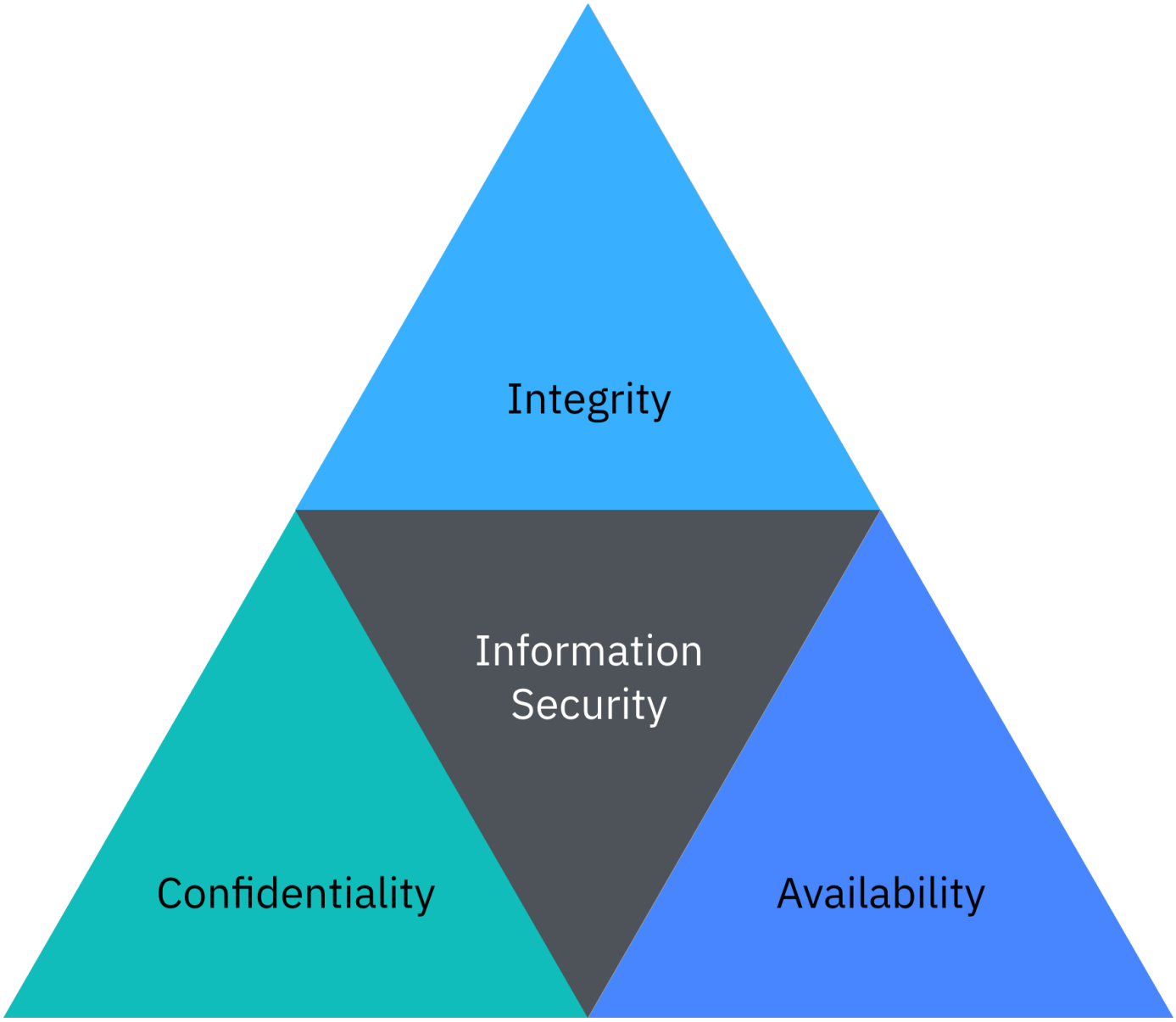
What are cybersecurity professionals trying to accomplish?

According to the **National Institute of Standards and Technology (NIST) (https://csrc.nist.gov/glossary/term/information_security)**, **information security** is: "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."

So, information security's **objectives** are often defined using the **CIA triad** as a good starting point. CIA is a mnemonic for the three objectives: **Confidentiality**, **Integrity**, and **Availability**.

Confidentiality *Information is private*	Confidentiality means preventing information from falling into the hands of people who do not have authorization to access the information.
Integrity *Information has not been altered*	Integrity means making sure the information stays accurate and consistent, and ensuring that unauthorized people cannot makes any changes to the information.
Availability *Information can be accessed when required*	Availability means timely and reliable access to and use of the information when required.

The CIA triad is a model to help guide policies for information security within an organization.



Different organizations and scenarios may mean that one objective is prioritized over the others.

EXAMPLE

Let's look at some examples to put the information security objectives into context for you.

- **Confidentiality** may be the most important objective for government intelligence agencies. Think about the lengths they go to in order to keep information private, such as using bespoke encryption or even lead-lined brief cases that sink if thrown into a body of water.
- **Integrity** may be the most important objective for banks. Think about if you spent USD $10 on a pizza. You would not be particularly concerned about this transaction being confidential. However, if the transaction is altered and you end up spending USD $10,000 instead, then you would be in serious financial trouble. Should this happen at scale for your bank, it could cease operating as a result of a loss of trust.
- **Availability** may be the most important objective for a website. Think about if you have a blog. You would not be particularly concerned if it was confidential or an editor helps correct your spelling. You want it to be there and available to you any time you want to update and publish it.

What do you think?

Let's look at how the information security objectives could relate to your day-to-day life by evaluating assets that you likely value. In cybersecurity, an **asset** is defined as something that has a value to its owner. Assets can be digital, such as a program, or physical, such as a server. Sensitive information such as databases, research, or records can also be called **information assets**.

Consider your personal bank account, photo library, social media account, and mobile phone. **How would a loss of Confidentiality, Integrity, and Availability impact you for each asset?** Use this provided scale of 1 to 5 to type your rating in the provided fields.

1) Low consequence: You would have no noticeable impact to day-to-day life.

3) Medium consequence: You would have minor impact resulting in a couple of hours of lost time.

5) High consequence: You would have a life changing, massive impact that could last for months or years.

The **Highest value** will calculate automatically so you can compare how you value your assets and priorities.

> EXAMPLE
>
> There is one example already displaying for you: an online debate submission. In this example:
>
> - A loss of **Confidentiality** is considered annoying, but will have only a minor impact and is given a rating of **2**.
> - A loss of **Integrity** from another person editing the submission could start an argument, which could lead to wasted time making updates. Integrity is therefore given a rating of **3**.
> - Finally, should the online comment disappear entirely, or become inaccessible, there are virtually no impacts, so a loss of **Availability** is given a rating of **1**.

Now, using the rating system above, try and complete your evaluations.

	Confidentiality	Integrity	Availability	Highest value
Online debate submission	2	3	1	**3**
Bank account				
Photo library				
Social media account				
Mobile phone				

When you are finished, you can see that certain assets matter more to you than others. This should correspond with the **Highest values** you see. Do any of your evaluations of value surprise you?

From a security perspective, it is sensible to prioritize your protections around the assets which matter most to you. For instance, the password for your password manager may be 20+ characters long and kept private whereas a home wifi password may occasionally be shared with friends and family!

In cybersecurity, organizations make these decisions all of the time.

Key elements of cybersecurity

10 Minutes

There are many ways to secure information assets and deciding on the best approach is an important consideration in cybersecurity.

> EXAMPLE
> Imagine you have an expensive painting that you need to protect. One option could be to hire some security guards to stand by the painting and constantly watch it. Another option could be that you require all prospective visitors to your painting to place a monetary deposit down or seek insurance confirmation. Finally, you could opt for laser trip wires, security cameras, and motion sensors to detect unknown people. Each of these options has various advantages and disadvantages. Like all great heist movies, relying on only one option may not be enough.

There are three key elements of cybersecurity to consider:

These are the areas where an attacker could attack and where organizations should focus cybersecurity efforts. Let's examine them further in this lesson.

People

As counter intuitive as it might be for a highly digital industry, people are the most important part of cybersecurity. First, people are the end users of digital systems and second, people are often those responsible for the design and maintenance of digital systems. Human action is by far the leading cause of cybersecurity incidents. When organizations design a secure system, they must design with people in mind.

A common example of this going wrong is the case of alert fatigue. If people receive too many notifications or alarms, then they eventually become desensitized to it. Good systems will be designed to anticipate and make allowances for human behavior.

Process

In business, most activities follow a clearly defined set of steps. These processes can aid cybersecurity by considering security at each step or hinder cybersecurity by being frustrating for the end user.

Imagine a process which makes a user complete a 20-question survey whenever they wish to report suspicious activity. Many users, who could contribute useful information, might be deterred and give up the process.

Good processes have the following attributes:

- They are **clear and as easy as possible**. During the process, it should be obvious what to do at every stage. Processes should not use unnecessary jargon or be written in an ambiguous fashion.
- They are **accessible or well known**. All users who could follow a process at any stage, should know how to access the process. A good example of this commonly being done well is with fire evacuations in buildings. Most people know where the nearest evacuation points are because of good signage.
- They are **consistent**. Processes should not contradict each other, if possible. If a process has a lot of exceptions or deviations, it increases complexity. Later, you will learn about how cyber attackers can exploit this during their attacks.

Technology

Technology is all of the underlying infrastructure.

Within cybersecurity, this commonly covers elements such as device encryption, network perimeter defenses, and anti-malware technologies.

Within business, good uses of technology solve problems without creating new ones for their users.

An example of good technical security is device management software, which can track software patch statuses and apply updates. This is often an essential tool for large organizations. If this is done correctly, then the technology is non-intrusive and users will be secured in a passive manner. If this is done poorly, then users might try to disable the software entirely. As users of devices, you encounter this too.

The following table shows some technological leaps for security, their perceived drawbacks, and some downsides to their introduction from the user perspective.

Technological leap	**Business benefit**	**Perceived drawback**	**Undesirable user responses**
Automated patch management	All software is up-to-date	Interruptions to use of device	User does not power down devices
High complexity mandatory passwords	Harder for attackers to guess passwords	Tedious to use	P@ssw0rd!
Mandatory passwords expire after 30 days	Passwords cannot be compromised for long periods of time	Predictably repetitive	PasswordJan to then PasswordFeb
Encrypted emails	Attackers cannot read emails in transit	Additional configuration and complexity	Disable encryption feature

You can see it is important for organizations to educate users as to why exactly the technology has been introduced and why perceived drawbacks might be necessary.

What do you think?

Here are some questions to think about. Please type your answer to each question in the boxes. Reflecting and typing an answer is a good way to process your thoughts. Your answers are just for you and are only saved in this course for you. Be sure to click **Save Text**.

Think of a time when you have examined your own personal digital security for your computer and/or devices.

1. In terms of **people**, did you attempt to educate yourself to improve your security posture?

Save Text Save Text Save Text Save Text

2. In terms of **process**, did you start any new processes, such as enabling two-factor authentication for each login?

Save Text

3. In terms of **technology**, did you purchase or use a new technology to help improve your personal security?

Save Text

Risk management

10 Minutes

Risks are part of everyday life and something we are all instinctively familiar with. A **risk** is the possibility of something happening with a negative consequence. Managing risk is at the heart of most businesses and the core of many industries, such as the insurance industry. Good businesses understand and manage risks effectively to give them a competitive advantage.

In this lesson, we'll explore some key concepts about risk and how they apply to cybersecurity.

Risk valuation

All risks are not equally important. Certain risks may require urgent attention whereas others may be ignored. Risks that are more significant, are known as **high risks**. Here is a basic equation to calculate the value of a risk:

Risk value = Consequence x Likelihood

Consequence is the impact and associated damages.

Likelihood is how often the risk impact occurs.

Ideally, for mathematical reasons, it would be great if we had good statistical information for every risk. If, for instance, we know on a given year that 1 in 10 cars will experience a flat tire, then the associated risk value can be easily worked out.

> EXAMPLE
>
> An example of the risk value equation applied to the the previous flat tire scenario could be as follows. An individual may lose a day's productivity as a result of getting a flat tire on the way to work. The *consequence* of this risk would be the loss of one day of work. While this consequence is annoying, remember the *likelihood* of the risk is low - 1 in 10 cars in a given year. This means we may assess the overall risk value to be low.

Within cybersecurity, likelihood is hard to directly measure due to the constant evolution of technology and involvement of outside attackers. As a good rule of thumb, the likelihood of an organization being attacked depends partly on three attributes as follows:

Likelihood = Adversary capability x Adversary motivation x Vulnerability severity

An **adversary** is a general term used to describe an entity who wishes to compromise an information system. Later in this course, you will learn more about how adversaries can be categorized. This will enable you to assign values for their capabilities and motivations.

Vulnerabilities are potential weaknesses within a system that could be exploited to compromise it. For instance, a vulnerability could be a webpage that does not authenticate a user correctly.

> EXAMPLE
>
> An example of this second equation could be as follows. Let's imagine a bank is being targeted by a criminal gang who is interested in stealing users' banking login details and passwords.
>
> - The **adversary capability** could be assessed as *medium* because the criminals could use a range of tools and develop their own tools if required.
> - Their **motivation** could be assessed as *high* because they could attempt multiple attacks over a period of time.
> - An identified **vulnerability** could be assessed as *high* because it is comparatively easy to exploit. For example, certain vulnerabilities have published descriptions online which enable attackers to mirror attacks easily.
>
> **Note**: Using the rating terms of "low", "medium", and "high" is an example of qualitative analysis of risk. In an ideal world, we would use exact numbers or percentages; however these can be hard to find so estimates are often all we have.

Risk response

Once an organization has assessed all of its risks, the emphasis is then placed upon risk management, or response. In general, there are four responses to a risk that an organization could choose. The following table describes them.

Accept	The organization accepts the risk in its current form. This is a decision that will be made by a senior individual within the organization, referred to as a “risk owner”.
Reduce	The organization could decide a risk is too large to accept and aim to have it reduced in some fashion. This could either be through reducing the likelihood or consequence.

Transfer	The organization may want a third party to accept the risk, or part of it, instead of accepting it themselves. This is done via insurance.
Reject	The organization could decide a risk is too high and may withdraw from being affected by it. This will have significant business impacts such as shutting down sites or avoiding markets.

EXAMPLE

Let's illustrate these four responses to a risk. Imagine that you are considering starting a cake baking business at home. There is a risk that your kitchen could be damaged if you set your oven on fire during the baking process. Here are several responses to this risk.

- **Acceptance**: You could look at the risk and with faith in your baking, take the chance that it is unlikely anything will go wrong. Should your baking go wrong, you can repair your kitchen and are prepared to do so.
- **Reduction**: You decide that you would prefer your kitchen and oven are not put at a high level of risk and you decide to reduce the risk. You could reduce the likelihood of fire-related incidents by installing a smoke detector to provide early warning. You could reduce the consequence of a fire by having a fire suppression system installed. Both options will incur a small cost, but you believe they are worth it.
- **Transference**: You go to your insurance company and upgrade your insurance to cover home cooking related fires. They perform their own assessment of the risk. Together you agree on a cost to pay them to cover the risk. Should your oven catch fire, they will cover the costs. This arrangement incurs a cost initially, but limits your liability.
- **Rejection**: You decide that the oven-related fire risk is too high. You could change recipes to make cakes without using an oven or not start your business in the first place.

As you can see from this example, there are many things to consider in even a simple example. Businesses with rapidly changing IT technology face many continually evolving risks. Risk management is a full time occupation in many companies and guides a lot of both strategic and tactical decision making.

Risk appetite

A **risk appetite** is the level of risk an organization is willing to accept.

- An organization is said to have a *high* risk appetite if it is willing to accept a high level of risk.
- An organization is said to have a *low* risk appetite if it does not like accepting risk.

What do you think?

Here is a question to think about. Please type your answer in the box. Reflecting and typing an answer is a good way to process your thoughts. Your answer is just for you and is only saved in this course for you. Be sure to click **Save Text**.

Think of a risk that you have recently encountered in your life.

What was the risk and your response? Did you accept, reduce, transfer, or reject it?

Your text has been saved. Click "X" to continue. ✖

Common misconceptions

5 Minutes

There are a lot of misconceptions about cybersecurity in the world today. They range from unrealistic Hollywood clichés about the process of attacking a computer system to outdated stereotypes of people who work in the industry. Let's examine a few common misconceptions and provide some clarity for you.

Expand each misconception to debunk it.

Everyone who works in cybersecurity comes from an IT background.

While most roles within cybersecurity rely on IT either in part or entirely, the roles don't all have a firm dependence on that background. As you should already have noticed, since cybersecurity covers so much, there is demand for talent in lots of areas. Skills range from people management and communication to mathematics and data science. Having a diverse set of experiences and skills also helps teams approach problems in new ways and this is very valuable.

All hackers are criminals.

The term hacker historically refers to someone who enjoys adapting things and discovering how they work. This definition got mixed up with people who illegally tried to gain access to computer systems with the intent of hijacking their operations. Today, there are thousands of computer hackers who are employed in a variety of IT roles and contribute toward understanding IT systems in a legal fashion as part of many businesses. Their curiosity and drive are invaluable in ensuring IT systems are built in a safe and secure manner.

Cybersecurity is something I can't do.

Due to the constantly evolving areas in cybersecurity and vast scope, there is something for everyone. The diversity of roles requires a great diversity of skills. Those skills can range from strategic analysis and anticipating the evolving landscape of IT businesses to vigilance and patience in system monitoring roles. Keep in mind that there is a lot of education and training available.

I'm too old or too young to work in this industry.

A good litmus test for the diversity of a team is to check how many decades are covered by the team's composition. A good team will have a diverse range of experiences and life views. Cybersecurity needs to look at problems with both a fresh set of eyes and an experienced view. Whether you think approaches are great or bad, you've probably got half of the solution and a great voice to add to the dialogue.

What do you think?

Here is a question to think about. Please type your answer in the box. Reflecting and typing an answer is a good way to process your thoughts. Your answer is just for you and is only saved in this course for you. Be sure to click **Save Text**.

At this point in your learning, what assumption do you have about the cybersecurity industry? At the end of the course, you can revisit this section to see if you still have this assumption.

Your text has been saved. Click "X" to continue. ✖

Laws and ethics

10 Minutes

Cyber crime is quite a new concept, having only developed within the last 30 years. Before that, people who used computers maliciously had to be prosecuted using a combination of theft and telegraphy acts, which were not that applicable.

Today, a wide-ranging set of international laws have been created to govern the use of computing technologies and protection of the information residing within them. Everyone is affected by these laws and it is important that all cybersecurity professionals have a basic understanding of them.

This lesson will provide a quick overview of common types of laws and the importance of considering ethics.

Important Note

Laws are not the same across the world. They can vary greatly by country. You should check and abide by the relevant laws for the country you live in and/or travel to. Some governments have written their laws to be more prohibitive than others so that a legal action in one may be illegal in another.

If you are in doubt, seek legal advice.

Common types of computer misuse laws

Let's review some common features or concepts that are mirrored around the world in computer misuse laws.

Unapproved use or control of a computer device

- Many laws prohibit unauthorized or unapproved access or use of a computing device.
- This catch-all barrier means that hijacking computers through technical material or by forcing access to a person's account is banned.
- These laws can catch people for circumventing broken controls such as authentication.

EXAMPLE

Placing a fake log-in screen on a website to steal a set of user passwords and using them to spy on someone's account.

Preventing others from legitimate use

- These laws attempt to cover attacks on availability of computer resources, such as networking capabilities.
- Actions that degrade the quality of service for others, or prevent it entirely, will usually be covered within these laws.

EXAMPLE

Overloading a server or networking switch by sending it too many packets of information to process.

Aiding other criminals or designing malware

- These laws refer to helping others commit computer misuse offenses, such as being an accomplice.
- One such manner of helping others could be by writing malicious software, commonly known as malware.
- These laws are intended to be used to help with breaking up criminal gangs.

EXAMPLE

Producing a program which allows remote access to a machine without the owner's awareness.

In addition to the laws concerning computer misuse, you will find that a couple of cyber crime offenses overlap with data protection laws and traditional property laws. Should a cyber crime result in theft of intellectual property, this may be examined as a case of theft.

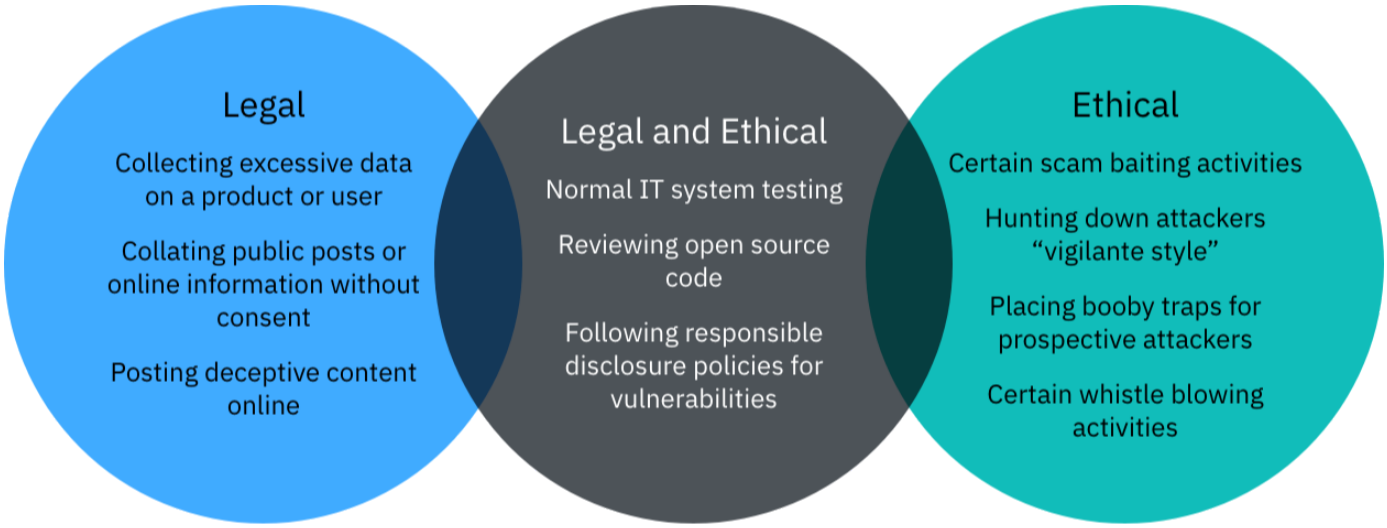
The golden rule before trying anything in IT security is to get the correct permissions in place from the owner before experimenting on a device. It is also important to know exactly what you are doing to avoid unintentional side effects.

Discussion on ethics

As the laws vary across the world, ethics do too. There is a lively debate about many aspects of ethics within cybersecurity. For instance, is it permissible for organizations to leave booby-trapped files within their infrastructure awaiting an attacker to trigger one? Many could argue that this is ethically sound, although under most legal frameworks, it would be argued that such an action is illegal since the trapped files would be considered malware. Then there are the ethical dilemmas around using techniques from the security industry to target criminals. Could a retaliation be justifiable or defensible? What about the rules for military action or governments?

You can see there are ethical dilemmas and they have been going on for as long as the industry has existed. These debates are a good sign of a healthy industry reaching maturity and its participants displaying integrity by considering these important issues.

To illustrate the complexity of the laws and ethics of cybersecurity, this diagram shows how the areas of legality and ethics could be seen to *overlap*.



Activity

Do a quick internet search for computer laws in your country. Are there computer laws to abide by? If so, what are they?

Please type your answer in the box. Your answer is just for you and is only saved in this course for you. Be sure to click **Save Text**.

Your text has been saved. Click "X" to continue. ✖