INTRODUCTION TO CYBERSECURITY

Cybersecurity is the practice of protecting and recovering data, networks, devices, and programs from threats. Those threats can have digital, human, or physical components.

Digital security involves safeguarding your data and systems from digital threats. These threats range from malware attacks, such as viruses or ransomware, to hacking attempts designed to infiltrate systems and steal sensitive information. Some examples of digital security measures include firewalls and encryption software.

Human security involves protecting data against potential threats caused by human behavior or actions. These threats can be unintentional, such as an employee unknowingly downloading a malicious email attachment. Others are intentional, such as an employee intentionally leaking confidential data. Some examples of human security measures include employee security training and strong password policies.

Physical security involves protecting tangible assets against threats. These physical assets support digital infrastructure, such as workstations, server rooms, and data centers. And the threats to these assets can be intentional or unintentional, such as theft, tampering, or natural disasters. Some examples of physical security measures include surveillance systems, access control measures, and disaster recovery plans.

Effective cybersecurity delivers on three objectives: CIA triad (Confidentiality, Integrity, and Availability).

Confidentiality means keeping data secret; that is, only authorized people can access or disclose the data. For example, software companies typically keep their applications’ source code secret for competitive advantage. To reduce the chances of a source code leak, they restrict access to only the employees who need it. Confidentiality also covers people’s private data. One example is that your healthcare provider must ensure that data collected while treating you, such as diagnoses or prescriptions, stays private. With few exceptions, only you, your doctor, and authorized medical staff should have access to that data. In practice, confidentiality involves implementing safeguards that give the right level of access to the right set of users at the right times, using the right methods.

Integrity means ensuring that data is trustworthy and accurate by protecting it from unauthorized modification and destruction. Say you spend $10 on a pizza. You might not care whether that purchase is confidential. But what if something alters the transaction amount and you end up spending $10,000 instead? Note that the integrity of this transaction might have been compromised intentionally or unintentionally. Also, consider that although the cause of the error might be technical, it might be human, too. Maybe someone entered the wrong payment amount. To preserve integrity, you must also prevent unauthorized people from editing the data. In this sense, integrity and confidentiality overlap.

Availability means ensuring timely and reliable access to and use of the data. For example, you expect 24x7 online access to your bank account. To meet that expectation, your bank must implement and maintain sufficient resources to keep online banking available and functioning properly. But timely access does not always mean immediate or even continuous access. For example, when you request school transcripts, you might need to wait several days for school employees to locate, process, and send out the documents. And if the school provides transcripts electronically, it might limit the time frame in which recipients can access them. Regardless, the data is available within and for a reasonable amount of time.

The CIA triad helps guide cybersecurity-related policies in an organization. Depending on their operations and the scenarios that they encounter, different organizations might prioritize one objective over the others.

Confidentiality might be the most crucial objective for government intelligence agencies. These agencies handle sensitive data relevant to national security, ongoing investigations, intelligence reports, and other classified information. An unauthorized leak of this information might help criminals plan more successful illegal activities. It might even put lives in danger. Integrity might be the most crucial objective for banks. Financial transactions, central to banks’ business, rely heavily on data’s accuracy and consistency. Unauthorized modifications, deliberate or not, can lead to significant financial losses or legal repercussions. Availability might be the most crucial objective for an online retailer. As a customer, you probably expect to be able to shop for anything you want online, any time of day. Any downtime, lag, or disruption in services might lead you to take your business elsewhere. It might also reduce your trust in the company and damage the company’s reputation. Companies want to ensure that their website maintains constant uptime, loads quickly, and processes transactions without errors.

To meet each objective of the CIA triad, you need controls. In cybersecurity, controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical, tangible, or digital property.

Controls for confidentiality: Encryption converts your data into a form that only someone with the decryption key can understand. Access controls are measures designed to ensure that only the correct people can view, modify, or share data. If you use password protection, you’re using an access control. Access controls also include biometrics, such as fingerprints or retinal scans, that ensure that only authorized people can access the data. Patch management involves updating system software. Regularly updating system software fixes potential security weak points that attackers can exploit.

Controls for integrity: Checksums are mathematical algorithms that generate a unique value for a data set. If the data changes, the checksum will also change, alerting you to the alteration. Access controls and user permissions can limit who can change data and what changes they can make. Data backups can help restore data to its correct state if changes occur. Audit trails can track and record all changes made to data. They give you a clear record of who made a change and when they made it.

Controls for availability: Redundant systems and data backup procedures help protect against data loss or system failure. You might use multiple servers or store data in multiple locations. Antimalware software and firewalls protect systems from attacks that can disrupt services. Disaster recovery and business continuity plans lay out the steps needed to restore services quickly and efficiently in case a disruption occurs, minimizing downtime.

In cybersecurity, an asset is something valuable to its owner. Assets can be digital or physical. For example, a program or code is a physical asset, and a server is a physical asset. Sensitive information can also be called information assets. For example, information assets can include information contained in databases, research reports, or healthcare records. How would losing confidentiality, integrity, and availability impact you for each asset. 1. Low consequence: The loss would have no noticeable impact on your day-to-day life. 3. Medium consequence: The loss would have a minor impact, resulting in a couple of hours of lost time. 5. High consequence: The loss would have a life-changing, massive impact that might last months or years. The Highest rating will calculate automatically so you can compare how you value your assets and priorities.

You can secure information assets in many ways. Deciding on the best approach is important in cybersecurity.

Imagine you have an expensive painting that you need to protect. One option can be hiring security guards to stand by the painting and constantly watch it. Another option can be requiring all prospective visitors to your painting to make a monetary deposit or seek insurance confirmation. One more option can be installing laser trip wires, security cameras, and motion sensors to detect unknown people.

Each option has advantages and disadvantages; sometimes, relying on only one option might not be enough to protect valuable items. The same applies when trying to secure the information assets of an organization or person.

When thinking about cybersecurity, you should consider three key elements: Education, Process, Technology.

Education and awareness are among the most effective ways to improve an organization’s cybersecurity. You can hold regular training sessions to teach employees the importance of cybersecurity and their role in maintaining it. A culture of awareness around cybersecurity reduces the chances that employees engage in risky behavior and increases the chances of them reporting suspicious activity. In short, education and awareness build a human firewall that often catches threats that technology misses.

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

Imagine a process that makes users complete a 20-question survey whenever they wish to report suspicious activity. Many users, who can contribute useful information, might be deterred and give up on the process because of the lengthy survey.

Good processes have the following attributes:

They are clear and as easy as possible. During the process, what to do at every stage should be obvious. Processes should not use unnecessary jargon or be ambiguous.

They are accessible or well known. All users who can 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.

Technology is all your organization’s underlying infrastructure. Within cybersecurity, this infrastructure typically includes controls such as device encryption, network perimeter defences, and antimalware 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 software is often an essential tool for large organizations. If implemented correctly, then the technology is non-intrusive and users will be secured passively. If implemented poorly, then users might try to disable the software entirely.

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 response* |
| ***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 | Predictably repetitive | PasswordJan to then PasswordFeb |
| ***Encrypted emails*** | Attackers cannot read emails in transit | Additional configuration and complexity | Disable encryption feature |

Risks are part of everyday life and something that 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. For example, think of the insurance industry. An insurance company assesses the risk associated with insuring a person or entity. First, it determines the likelihood of an incident and the probability of someone making a claim if the incident occurs. Then, it sets premiums accordingly. It absorbs the potential financial risk from its clients in return for these regular premium payments.

All risks are not equally important. Some risks require urgent attention, while others can be ignored. More significant risks are known as high risks. You can use this basic equation to calculate the value of a risk: [ *Risk value = Consequence × Likelihood* ]. Consequence is the impact and associated damages. Likelihood is how often the risk impact occurs.

The risk value equation quantifies the significance of a risk. It’s the product of the potential consequence of a risk occurring and the probability of its occurrence. This high risk would require immediate attention and mitigation. A risk with a low consequence or likelihood wouldn’t require such immediate attention.

An example of the risk value equation applied to the previous flat tire scenario might be as follows. Someone might lose a day’s productivity because they got a flat tire on the way to work. The consequence of this risk is the loss of one day of work. Though this consequence is annoying, remember that the likelihood of the risk is low: one in 10 cars a year. Thus, you might assess the overall risk value to be low.

In cybersecurity, likelihood is hard to measure directly because of the constant evolution of technology and the involvement of outside attackers. Generally, the likelihood of an organization experiencing an attack depends partly on three attributes: [ *Likelihood = Adversary capability × Adversary motivation × Vulnerability severity* ].

Adversary is a general term for an entity that wishes to compromise an information system. Adversary capability includes the attacker’s resources, technology access, and expertise. High adversary capability indicates that the attacker has the tools, means, and proficiency to exploit vulnerabilities, thus posing a greater risk. Conversely, an attacker with low capability might not be able to exploit complex vulnerabilities, thus posing a lesser risk. Adversary motivation is the incentive or reason that drives an adversary to attempt a cyberattack. This motivation can come in various forms, such as financial gain, desire for information, political influence, or simply the thrill of disruption. Vulnerabilities are potential weaknesses within a system that someone can exploit to compromise it. For example, a vulnerability can be a login process that does not authenticate a user accurately.

Let’s consider an example to demonstrate how the equation for likelihood works. Imagine that a recently formed hacking group targets a bank. The malicious group is interested in stealing users’ banking login details and passwords. You might assess the adversary capability as low because their organization is new and might not have the latest technology or resources to develop their own tools, if required. You might assess their motivation as high because they can attempt multiple attacks over a period of time. You might assess an identified vulnerability as high because it is comparatively easy to exploit. For example, some vulnerabilities have published descriptions online, enabling attackers to mirror attacks easily.

Using the rating terms low, medium, and high is an example of qualitative risk analysis. In an ideal world, you would use exact numbers or percentages. However, finding them can be challenging, so estimates are often all you have.

Which question is relevant for determining the value of this risk?

Risk 1: Outdated operating system. The clinic’s computers run on an outdated operating system (OS). The vendor of the OS no longer supports it and doesn’t provide security updates for it. *What negative impact can this outdated OS have on system and data security?* Outdated operating systems are more likely to have known vulnerabilities, increasing the likelihood of an attacker exploiting the system. And the greater the potential consequences of someone exploiting this weakness, the higher the risk value.

Risk 2: Single-factor authentication for email accounts. The clinic’s email system uses single-factor authentication. Users need only one form of authentication, a password, for access. The current industry standard for authentication is multifactor authentication, which is when a login requires at least two types of credentials. For example, logging into your bank account from a new device might require a password and the answer to a security question. *How can single-factor authentication compromise the clinic’s email security?* To determine the risk value of single-factor authentication, you must know its vulnerabilities and understand how someone might exploit it to compromise security. The easier the vulnerabilities are to exploit, the more likely attackers might be to exploit them, increasing the risk value.

Risk 3: Antimalware software isn’t updated regularly. The organization’s antimalware software isn’t updated regularly. The software isn’t configured to update automatically, and the system administrator, Heidi, updates the software manually on an irregular basis. *What is the probability of a virus or other malware attacking this system?* The probability, or likelihood, of a risk impact occurring is a key component of risk value. In this scenario, the greater the chances of malware attacking the clinic’s system, the greater the risk value.

Risk 4: Important files aren’t backed up. The organization has no regular backup routine for important data files. *What damages can result from losing patients’ data?* Losing patients’ data is one potential consequence of not backing up data regularly. For example, if a hardware failure or cyberattack occurs, the clinic might lose critical patient records and have no way of restoring them. The resulting harm might include disrupted patient care and reputational damage to the clinic. It might even include fines and penalties for failing to comply with relevant laws and regulations protecting the data, such as the US Health Insurance Portability and Accountability Act (HIPAA).

Risk 5: Old hardware. The clinic relies on old hardware. Some computers are quite old and don’t support the latest updates or software. Employees use these computers only for basic tasks that don’t require high processing power, and the computers don’t hold sensitive data. *Are the old computers accessible through the clinic’s network?* The consequence, or impact, of a risk occurring is a key component of risk value. In this scenario, the outdated computers don’t contain sensitive data. So, some might assume that a compromise of this hardware has little consequence from a security standpoint. But if the computers are connected to the network, then attackers might use them as easily exploitable entry points. From there, attackers can attack devices that contain sensitive data.

After an organization assesses all its risks, it starts risk management or response. Generally, organizations can choose from the following four responses to a risk.

Acceptance: The organization accepts the risk in its current form. It acknowledges the potential consequences of the risk and is prepared to deal with them if they occur. A senior person within the organization, referred to as a risk owner, makes the decision to accept a risk.

Reduction: The organization decides a risk is too large to accept and aims to reduce it in some fashion. To reduce the risk, the organization can reduce either its likelihood or consequence. It does so by implementing security controls or patching system vulnerabilities.

Transference: The organization chooses to transfer the risk. It can have a third party accept part or all of the risk instead of accepting the risk itself. Transfer typically occurs through insurance or outsourcing. Though the risk remains, another entity manages its impact, reducing the direct threat to the organization.

Rejection: The organization decides a risk is too high and rejects it, meaning that the organization withdraws from being affected by it. Rejecting the risk can significantly change business operations. For example, rejection might involve shutting down sites, avoiding markets, or avoiding activities that lead to the risk.

Imagine that you are considering starting an at-home bakery business. One risk in any bakery is a fire, which can cause extensive damage. Consider the following responses to this risk. Acceptance: You examine the risk and, with faith in your baking skills, 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 prefer not to put your kitchen and oven at a high level of risk, and you decide to reduce the risk. You can reduce the likelihood of fire-related incidents by installing a smoke detector to provide early warning. You can reduce the consequence of a fire by having a fire suppression system installed. Both options will incur a small cost, but you believe that they are worth it. Transference: You go to your insurance company and upgrade your insurance to cover home cooking-related fires. The company performs its own assessment of the risk. Together, you agree on a cost to pay the company to cover the risk. Should your oven catch fire, the company 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 can change recipes to make cakes without using an oven or not start your business in the first place.

Risk management is a full-time job in many companies and guides a lot of both strategic and tactical decision-making.

A risk appetite is the level of risk that an organization is willing to accept. An organization has a high risk appetite if it is willing to accept a high level of risk. An organization has a low risk appetite if it does not like accepting risk.

Organizations with a high risk appetite might take bold initiatives, using the latest technologies and potentially vulnerable systems, to pursue significant competitive advantages. They accept the risk of potential cyberattacks, but also have robust contingencies for when breaches occur. Conversely, organizations with a low risk appetite are more cautious in their approach to cybersecurity. They might prioritize stability and reliability over competitive advantage, focusing more on protective measures such as firewalls, encryption, and regular system updates. These organizations aim to minimize the risk of cyberattacks as much as possible, even if doing so means missing out on certain opportunities.

Note that neither approach is better. An organization’s level of risk appetite should align with its overall strategic goals and resources. It should also vary by the potential impact of cyberattacks on its operations and reputation.

Most cybersecurity roles rely on IT in part or entirely. But not all the roles firmly depend on that background. Because cybersecurity covers so much, employers search for talent in many areas. Skills range from people management and communication to mathematics and data science. Having diverse experiences and skills also helps teams approach problems in new ways, which is valuable.

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 to hijack their operations. Today, thousands of computer hackers are employed in a variety of IT roles and contribute toward the legal understanding of IT systems as part of many businesses. Their curiosity and drive are invaluable in ensuring that organizations build IT systems safely and securely.

Because of the constantly evolving areas in cybersecurity and its vast scope, the field offers 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. Note that a lot of education and training is available for anyone wanting to advance in this field.

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 examine problems with both fresh and experienced perspectives. With such a diverse team, you get a range of ideas and solutions instead of narrow, one-sided views of problems.

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 or travel to. Some governments have written their laws to be more prohibitive than others so that a legal action in one might be illegal in another. If you are in doubt, seek legal advice.

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 forcing access to a person’s account is banned. These laws can catch people for circumventing broken controls such as authentication. An example is placing a fake login 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 the 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. An example is 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 way of helping others is by writing malicious software, commonly known as malware. The intent behind these laws is to help with breaking up criminal gangs. An example is producing a program in which an attacker can access another person’s machine remotely without the owner’s awareness.

Unauthorized data alteration: Laws exist to prevent unauthorized alteration, deletion, or blocking of personal data. Unauthorized alteration includes altering data in a way that can harm a person or an organization. An example is an attacker hacking into a financial institution’s database and changing account balances. This act leads to unauthorized data alteration and causes significant financial harm to the organization and its clients.

Prohibited software: Laws are in place against creating, using, or distributing software designed for committing cybercrimes. Such software includes malware, such as viruses, and hacking tools. An example is an attacker sending an email with a seemingly harmless file attached, such as a PDF file. But when the recipient opens the file, a virus within it runs, infecting the recipient’s device. Laws prohibit distributing malware through means such as email.

Cyberstalking and harassment: Cyberstalking and harassment laws curb harmful or threatening behavior online. Common examples of this behavior include stalking, bullying, or intimidating others on the internet. A typical example of cyberstalking or harassment is someone continuously sending threatening messages to another person through social media platforms, email, or other online communication tools. Cyberstalking and harassment laws apply if the threats escalate to a point where the recipient feels unsafe or fearful. Such actions can result in serious legal consequences, so people must exercise respect and discretion in online interactions.

Some cybercrime offenses, such as unauthorized data alteration, overlap with data protection laws and traditional property laws. Should a cybercrime result in the theft of intellectual property, the crime might be examined as a case of theft. In IT security, the golden rule before experimenting on a device is to get the required permissions or level of access from the owner. You should also know exactly what you are doing and how you will do it to avoid unintentional side effects.

As the laws vary across the world, so do ethics. Lively debate continues about many aspects of ethics within cybersecurity.

Retaliation: Ethical dilemmas exist around using techniques from the security industry to target criminals. Can an act of retaliation be justifiable or defensible? Rigorous debate surrounds hack back or active defense. This concept refers to the measures that a cyberattack victim can take to find the perpetrators and potentially disrupt their operations. Though some argue that such measures are needed to protect assets and deter future attacks, others raise concerns about the potential for escalation.

Artificial Intelligence: The ethical implications of artificial intelligence (AI) in cybersecurity have also come under the spotlight. As AI becomes increasingly prevalent in cybersecurity tools and practices, so do questions about accountability, transparency, and potential misuse. Should an AI system make a mistake, who is responsible? How much trust should people put in these systems, and how can people ensure that they are used responsibly?

Government Use: Many nations have established cyberwarfare units to safeguard national security. These units protect critical infrastructure, conduct surveillance, and launch cyberattacks. The laws and regulations governing these units vary considerably and can be ambiguous. Whether laws of traditional warfare should apply to the cyber realm is a contentious issue, and no worldwide consensus exists yet. The same concerns apply to other government agencies and their operations. Though many governments have implemented laws to safeguard their citizens’ data privacy, debate continues about the extent to which government surveillance is ethical. Governments must balance national security concerns and individual privacy rights.

To illustrate the complexity of the laws and ethics of cybersecurity, check out the following examples of how the areas of legality and ethics overlap.

|  |  |  |
| --- | --- | --- |
| ***Legal*** | ***Ethical*** | ***Legal and ethical*** |
| * Collecting excessive data on a product or user * Collating public posts or online information without consent * Posting deceptive content online | * Performing certain scam-baiting activities * Hunting down attackers using active defense * Placing booby traps for prospective attackers * Performing certain whistleblowing activities | * Conducting normal IT system testing * Reviewing open-source code * Following responsible disclosure policies for vulnerabilities |

Cybersecurity is the practice of protecting and recovering data, networks, devices, and programs from threats. Cybersecurity can have one or more of the following three components: digital, human, or physical. Effective cybersecurity delivers on the three objectives of the CIA triad: confidentiality, integrity, and availability. In cybersecurity, controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical, tangible, or digital property. To secure information assets, organizations should focus on three key elements of cybersecurity: education, process, and technology. Risk value is the product of the potential consequence of a risk occurring and the probability of its occurrence. Organizations can choose one of four responses to a risk: acceptance, reduction, transference, and rejection. Key skills for cybersecurity jobs can range from strategic analysis and anticipating the evolving landscape of IT businesses to vigilance and patience in system monitoring roles. A wide-ranging set of international laws govern the use of computing technologies and the protection of the information residing within them. Some of the most important ethical debates in cybersecurity revolve around retaliation, artificial intelligence, and government use.