

**Cybersecurity reference guide**

**User manual**

# Cybersecurity reference guide

## Table of Contents

---

<b>Introduction</b> .....	3
Definition of cybersecurity .....	3
Organization types .....	3
<b>Terminology</b> .....	4
Risk .....	4
Assets .....	5
Threats .....	6
Vulnerability .....	7
Policy .....	7
Security controls .....	7
<b>Protective measures for common threats</b> .....	9
Deliberate or accidental misuse of the system .....	9
Physical tampering and sabotage .....	9
Exploitation of known software vulnerabilities .....	10
Supply chain attack .....	10

# Cybersecurity reference guide

## Introduction

---

### Introduction

The purpose of this guide is to provide a common baseline, and serve as a reference for cybersecurity-related materials produced by Axis. These are simplified descriptions, models and structures based on NIST, SANS, ISO and RSA conferences, as well as materials from various organizations within the cybersecurity community.

Links to other materials from Axis:

- [axis.com/about-axis/cybersecurity](https://axis.com/about-axis/cybersecurity)
- [help.axis.com/cybersecurity-qna](https://help.axis.com/cybersecurity-qna)
- [axis.com/support/cybersecurity/resources](https://axis.com/support/cybersecurity/resources)
- [help.axis.com/axis-security-development-model](https://help.axis.com/axis-security-development-model)
- [axis.com/support/cybersecurity/vulnerability-management](https://axis.com/support/cybersecurity/vulnerability-management)

### Definition of cybersecurity

Based in part on the definition from NIST:

Cybersecurity is the protection of computer systems and services from cyberthreats. Cybersecurity practices include processes for preventing damage and restoring computers, electronic communications systems and services, wire and electronic communications, and stored information to ensure their availability, integrity, safety, authenticity, confidentiality, and nonrepudiation.

### Organization types

Different organizations have different assets, resources, exposure, and cyber maturity. When following recommended practice, *The CIS Controls (formerly known as Critical Security Controls)* defines three organizational profiles.

- **SANS Implementation Group 1 (IG1)**  
In most cases, an IG1 enterprise is typically small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel.
- **SANS Implementation Group 2 (IG2)**  
An IG2 enterprise employs individuals who are responsible for managing and protecting IT infrastructure. These enterprises typically support multiple departments with differing risk profiles based on job function and mission. Small enterprise units may have regulatory compliance burdens.
- **SANS Implementation Group 3 (IG3)**  
An IG3 enterprise commonly employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight.

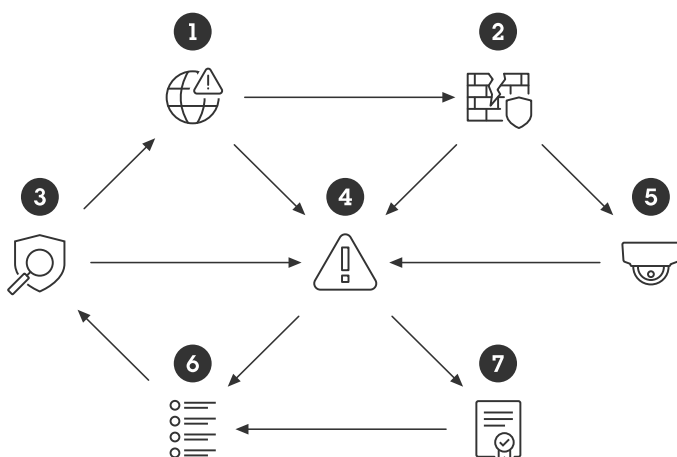
# Cybersecurity reference guide

## Terminology

---

### Terminology

The terminology map shows the relationships of specific cybersecurity key terms that are discussed in this document.



- (1) Threats exploit (2) vulnerabilities exposing (5) assets and increasing (4) risks
- (4) Risks influence (7) policy and indicates (6) requirements
- (6) Requirements are addressed in (3) security controls , which constantly face (1) threats while mitigating (4) risks

### Risk

Cybersecurity is about managing risks over time. Risks can never be eliminated, only mitigated. Sometimes people confuse the terms: risk, asset, threat, vulnerability, or negative impact

RFC 4949 Internet Security Glossary defines risk as an expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

A shorthand version commonly used is **Risk = Probability x Impact**

This formula is used to prioritize risks. The RFC definition includes the term "particular" for threat, vulnerability, and harmful result. Each threat should be looked at individually, starting with the one that is most plausible and having the highest negative impact.

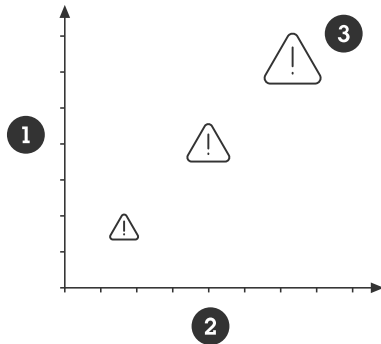
A challenge when discussing risk is the probability factor. Things may happen or they may not. The probability of an adversary exploiting a vulnerability is often determined by how easy the vulnerability is to exploit (exposure) and the potential benefit for the adversary to exploit it.

It is possible to plot risks with these two dimensions: use the probability that a risk will occur as one axis and the impact of the risk, if it occurs, on the other. This gives a clear view of the potential impact and priority that you need to give to each risk.

# Cybersecurity reference guide

## Terminology

---



- 1 **Probability** from low to high
- 2 **Negative impact** from low to high
- 3 **Risk levels** from low to high

$\text{Attack value} = \text{Attack benefits} - \text{Attack cost}$

Adding protection will increase the attack cost and thus reduce the probability. The attack cost relates to how much time, resources, skills, and sophistication are needed for the attack to be successful. The risk of getting caught or other negative consequences is also part of the attack cost.

Risk assessment, which is the process for analyzing risk in cyberspace, is the same as for physical protection. The questions to consider are as follows:

1. What do you want to protect?
2. Who do you want to protect it from?
3. What is the probability of a negative impact?
4. How bad are the consequences if you fail?
5. What strategies should you implement to mitigate the risks?

Implementing any type of protective or security control measure results in incurring some type of cost. All organizations have limited fiscal resources. If you do not know what the risks are, it is difficult to estimate the budget for your protection. You will always need to accept risks, but that decision needs to be a deliberate risk-based decision.

Estimating the potential negative impact on each asset type is hard and complex. In many cases, the estimations are subjective, and the impact analysis is often underestimated. Using the ISO 27000 impact model and designation types – i.e., Limited, Serious, Severe or Catastrophic – can help you get a quick overview to help you prioritize. It provides a simple way to establish a more exacting value by basing the estimation on the amount of time it would take to recover from a negative impact, namely:

- **Limited** = from hours to days
- **Serious** = from days to weeks
- **Severe** = from weeks to months
- **Catastrophic** = from months to years, if at all

## Assets

While physical protection is focused on protecting people and physical objects, cybersecurity protection is focused on protecting data assets and computer resources. There are three main areas:

- **Confidentiality:** disclosure of information or resource

# Cybersecurity reference guide

## Terminology

---

- **Integrity:** destruction or altering of information or resource
- **Availability:** accessibility to information and resources

These areas are also referred to as the CIA triad. Operation Technology (OT) will often prioritize usability, while those working with Information Technology (IT) will often prioritize security. Finding the right balance between confidentiality, integrity and availability is often challenging.

Assets and resources need to be classified in order to determine adequate protection levels. Not all data assets and computer resources are equal in terms of the negative impact. They are often classified as follows:

- **Public:** the asset is targeting a public consumer. Or, the negative impact is limited if disclosed to the public.
- **Private:** the asset is privileged to a specific/selected group. Typically, the negative impact is limited to within a specific organization such as a company or family.
- **Restricted:** the asset is privileged to selected individuals within an organization.

Live video in a video system could be classified as public, which refers to both the general public as well as the public within an organization. But in most cases, live video is classified as private, which means it is only accessible to a specific organizational unit. Meanwhile, recorded video, in most cases, is classified as restricted as there may be scenes that could be very sensitive. Credentials and configurations are also data that should be classified as restricted.

## Threats

A threat can be defined as anything that can compromise or cause harm to your assets or resource. In general, people tend to associate cyberthreats with malicious hackers and malware. In reality, negative impact often occurs due to accidents, unintentional misuse or hardware failure.

Attacks do not arise from nowhere. There is always some motivation to compromise a system and its assets. Attacks can either be categorized as opportunistic or targeted. In cybersecurity, attackers are also referred to as adversaries that may have malicious intent.

The majority of attacks today are opportunistic: attacks that occur just because there is a window of opportunity. In many cases, an external opportunistic attacker does not even know who the victim is. These attackers will use low-cost attack vectors such as phishing and probing. In these cases, they do not have the determination to spend time and resources on a failed attack; they quickly move along to their next attempt. Applying a standard level of protection will mitigate most risks related to opportunistic attacks. It is harder to protect against targeted attacks –those attackers who target a specific system with a specific goal. Targeted attacks use the same low-cost attack vectors as opportunistic attackers. However, if the initial attacks fail, they are more determined and are willing to spend time and resources to use more sophisticated methods to achieve their goals. For them, it is largely about how much value is at stake.

Common adversaries (threat actors)

- **Near and dear:** people who may want to pry into your personal life
- **Employees:** or people who have legitimately accessed the system, either by accident or deliberate misuse
- **Pranksters:** people who find interfering with computer systems an enjoyable challenge
- **Hacktivists:** people who wish to attack organizations for political or ideological motives
- **Cybercriminals:** people interested in making money through fraud or from the sale of valuable information
- **Industrial competitors:** entities interested in gaining an economic advantage for their companies or organizations
- **Cyber terrorists:** people or entities that carry out an attack designed to cause alarm or panic, often for ideological or political reasons
- **Nation states:** foreign intelligence service agents acting to either gain economic and political mileage or to inflict damage to critical information systems

# Cybersecurity reference guide

## Terminology

---

- **Individuals:** a specific person or group acting on their own where motivation may differ from the ones listed above. This could be an investigating journalist, white hat hacker or similar. White hat hackers (aka ethical hackers) may pose a threat if you prioritize hiding the flaws rather than fixing them.

### Vulnerability

All systems have vulnerabilities. Vulnerabilities provide opportunities for adversaries to attack or gain access to a system. They can result from flaws, exposure, features, or human errors. Malicious attackers may look to exploit any known vulnerabilities, often combining one or more. The majority of successful breaches are due to human errors, poorly configured systems, or poorly maintained systems – often due to lack of adequate policies, undefined responsibilities, and low organizational awareness.

#### Software vulnerabilities

A device API (Application Programming Interface) and software services may have flaws or features that can be exploited in an attack. No vendor can ever guarantee that products have no flaws. If the flaws are known, the risks may be mitigated through compensating security control measures. On the other hand, if an attacker discovers a new unknown flaw, the risk for successful zero-day exploits is increased as the victim has not had any time to protect the system.

Common Vulnerability Scoring System (CVSS) is one way to classify severity of a software vulnerability. It's a formula that looks at how easy it is to exploit and what the negative impact may be. The score is a value between 0-10, with 10 representing the greatest severity. You will often find a CVSS number in published Common Vulnerabilities and Exposures (CVE) reports.

Axis uses CVSS as one of the measures to determine how critical an identified vulnerability in the software/product may be

### Policy

It is important to define clear system policies and processes in order to achieve adequate risk reduction over the long term. A recommended approach is to work according to a well-defined IT protection framework, such as ISO 27001, NIST or similar. While this task may be overwhelming for smaller organizations, having even minimal policy and process documentation is far better than having nothing at all.

### Security controls

Security controls are safeguards or countermeasures employed to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems or other assets. The processes of deploying security controls are often referred to as hardening.

Compensating security controls are alternative safeguards that can be used when it may not be possible to apply the preferred security control, or when the preferred control may not be available or may be too costly.

Security controls need to be continuously monitored and updated as threats, value, vulnerabilities, and exposure changes over time. This requires defining and following policies and processes.

SANS Institute has published a *list of CIS controls*, which is a recommended set of prioritized cyber defense best practices. To show the diversity of the security controls, here's the list in its entirety.

- CIS Control #1: Inventory and Control of Enterprise Assets
- CIS Control #2: Inventory and Control of Software Assets
- CIS Control #3: Data Protection
- CIS Control #4: Secure Configuration of Enterprise Assets and Software
- CIS Control #5: Account Management
- CIS Control #6: Access Control Management
- CIS Control #7: Continuous Vulnerability Management
- CIS Control #8: Audit Log Management

# Cybersecurity reference guide

## Terminology

---

- CIS Control #9: Email and Web Browser Protections
- CIS Control #10: Malware Defenses
- CIS Control #11: Data Recovery
- CIS Control #12: Network Infrastructure Management
- CIS Control #13: Network Monitoring and Defense
- CIS Control #14: Security Awareness and Skills Training
- CIS Control #15: Service Provider Management
- CIS Control #16: Application Software Security
- CIS Control #17: Incident Response Management
- CIS Control #18: Penetration Testing

*AXIS OS Hardening Guide* is based on CIS.



# Cybersecurity reference guide

## Protective measures for common threats

---

### Protective measures for common threats

By understanding and countering the common threats, you can mitigate the majority of risks.

#### Deliberate or accidental misuse of the system

The balance between a system's usability and security is hard. Many systems are hardened from a convenience perspective, not security. This provides opportunities for deliberate or accidental misuse. People who have legitimate access to a system is the most common threat to any system.

Examples of common threats:

- Individuals may access services (e.g. live or recorded video) that they are not authorized to
- Individuals make mistakes
- Individuals may try to fix things that result in reduced system performance
- Disgruntled individuals may cause deliberate harm to the system
- Individuals are susceptible to social engineering
- Individuals steal
- Individuals may lose or misplace critical components (access cards, phones, laptops, documentation, etc)
- Individuals' computers may be compromised and unintentionally infect a system with malware

Common recommended protective measures are:

- Defined user account policy and process
- Sufficient access authentication scheme
- Tools to manage user accounts and privileges over time
- Reduce exposure
- Cyber awareness training

How Axis helps counter this threat:

- *AXIS OS Hardening Guide* describes common security controls for common threats to a device
- *AXIS Camera Station Hardening Guide* describes common security controls for video systems
- *AXIS Device Manager* and *AXIS Device Manager Extend* help manage common security controls

#### Physical tampering and sabotage

Physical protection for IT systems is very important from a cybersecurity perspective.

Examples of common threats:

- Physically exposed gear may be tampered with
- Physically exposed gear may be stolen
- Physically exposed cables may be disconnected, redirected, or cut

Common recommended protective measures:

# Cybersecurity reference guide

## Protective measures for common threats

---

- Place network gear (e.g. servers and switches) in locked areas
- Mount cameras so they are hard to reach
- Use protective casing when physically exposed
- Protect cables in walls or conduits

How Axis helps counter this threat:

- Encrypted SD card to prevent playback of video if an unauthorized user is able to eject the SD card
- Detection of camera view tampering
- Open casing detection

## Exploitation of known software vulnerabilities

All software-based products have vulnerabilities that could be exploited. These can be categorized as either known and unknown. All unknown vulnerabilities will eventually be known; it is just a matter of time. Most vulnerabilities have a low risk, meaning either they are very difficult to exploit or the negative impact is limited. Occasionally, vulnerabilities are discovered that may be exploitable and may cause substantial negative impact. MITRE hosts a large database of CVE (Common Vulnerabilities and Exposures) to help people mitigate risks.

Common recommended protective measures:

- A continuous patching process helps minimize the number of known vulnerabilities in a system.
- Minimize network exposure to make it harder to probe and exploit known vulnerabilities.
- Work with trusted sub-suppliers that work according to policies and processes that minimize flaws, have processes to provide patches, and make disclosures when critical vulnerabilities are discovered.

How Axis helps:

- *Axis Security Development Model* is a framework that defines the processes and tools Axis uses to reduce the risk of releasing products with software vulnerabilities.
- *Axis vulnerability management policy* involves identifying, remediating, and disclosing vulnerabilities that customers need to be aware of in order to take appropriate actions. Since April 2021, Axis has been approved as a Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA) for Axis products, allowing us to adapt our processes to MITRE Corporation's industry standard process. This, in turn, helps us to support our customers in a better way.
- *Axis hardening guides*, such as the *AXIS OS Hardening Guide*, provide recommendations on how to reduce exposure and add compensating controls to reduce the risk of software flaw exploitation.
- LTS (long-term support) firmware versions enable customers to patch the operating system of Axis devices while minimizing risks of incompatibility issues with third-party video management systems.

## Supply chain attack

A supply chain attack is a cyberattack that seeks to damage an organization by targeting less secure elements in the supply chain. It is mainly used when other attack vectors (e.g. social engineering, phishing attacks and interface probing) fail due to high levels of system protection. The attack is achieved by compromising software/firmware/products and luring an administrator to install it in their system. A product may be compromised during shipment to the system owner. To successfully pull off a supply chain attack requires skills, time, and resources.

Common recommended protective measures are:

- Have a policy to only install software from trusted and verified sources.
- Verify software integrity by comparing the software checksum (digest) with vendor's checksum before installation.

# Cybersecurity reference guide

## Protective measures for common threats

---

- Upon delivery, check the package or product for signs of tampering.

### How Axis helps counter this threat:

- Axis software is published with a checksum, enabling administrators to validate the integrity of the software before installing it.
- Signed firmware in an Axis device ensures that the installed AXIS OS is genuinely from Axis and that any new firmware to be downloaded and installed on the device is also signed by Axis.
- Secure boot in an Axis device enables the device to check that the firmware has an Axis signature. If the firmware is unauthorized or has been altered, the boot process is aborted.
- The IEEE 802.1AR-compliant Axis device ID is a device-unique Axis vendor certificate that provides a way for the system to verify that the hardware inside the casing comes from Axis.
- SD card encryption and filesystem encryption prevent the extraction of stored data when the card or device is stolen.

