White paper

Cybersecurity reference guide

Terminology and concepts

September 2018

AXIS® COMMUNICATIONS

Table of contents

This document describes common cybersecurity terms and concepts. It is intended to serve as a reference for all cybersecurity related documents and literature produced by Axis Communications. The purpose of this is to provide individuals and organizations that want to understand the fundamentals of cybersecurity, with a focus on physical security systems. The content is based on simplified descriptions, models and structures.

PART ONE: TERMINOLOGY

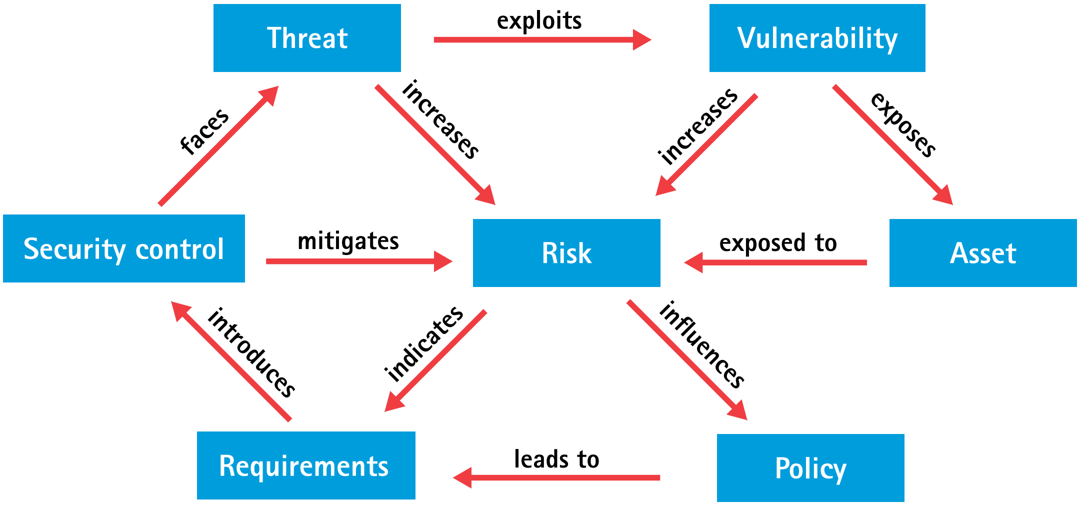
1. Definition of Cybersecurity

There are several definitions of cybersecurity. Wikipedia's description refers to Computer Security:

> *Computer security, also known as cybersecurity or IT security, is the protection of computer systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide.*

2. Terminology map

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



3. Risk

Cybersecurity is about managing risks over a longer period of time. While risks can be mitigated, it is very rare that they can be completely eliminated. Sometimes people confuse the terms: risk, threat, vulnerability, negative impact or asset.

RFC 2828 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.*

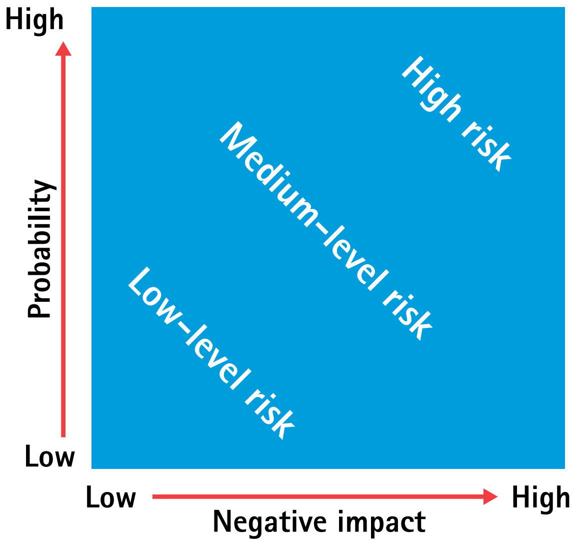
A shorthand version to determine risk is:

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 a 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 lets. This gives a clear view of the potential impact and priority that you need to give to each risk.



Attack value = Attack benefits – Attack cost

Applying protection measures will increase the attack cost and thus reduce the probability. The attack cost relates to how much time, resources, skill 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.

4. Assets and resources

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

> **Confidentiality:** disclosure of information or resource
> **Integrity:** destruction or altering of information or resource
> **Availability:** accessibility to information and resources

These areas are also referred to as the CIA triad. While those working with Operation Technology (OT) will often prioritize availability, their Information Technology (IT) colleagues will often prioritize confidentiality. Finding the right balance between these two 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. But 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 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. In most cases, recorded video is classified as restricted as there may be scenes that could be very sensitive. Credentials and device or system configurations should always be classified as restricted.

Estimating the potential negative impact on each asset types is 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 to base 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

5. Threat

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

IBM's 2014 Cyber security Intelligence Index concluded that more than 95% of all successful breaches could be attributed to three factors:

> Human errors
> Poorly configured systems
> Poorly maintained systems

These factors typically result from of a lack of adequate policies, undefined responsibilities and limited organizational awareness.

6. Vulnerability

Vulnerabilities provide opportunities for adversaries to attack or gain access to a system. They can result from flaws, features or human errors. Malicious attackers may look to exploit any known vulnerabilities, often combining one or more.

You need to consider both probability and potential negative impact in order to determine the risk of a vulnerability. The risk of vulnerability may be classified low if there is a low probability and/or have limited negative impact.

Example: The risk of a vulnerability in a web server may be classified as severe on a public web server for an enterprise business portal. The risk of the same vulnerability may be classified as limited for a camera deployed on a local protected network due to the reduced exposure.

A device Application Programming Interface (API) and software services may have flaws 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 though compensating security control measures. If an attacker discovers unknown flaws, on the other hand, zero-day exploits may occur, not giving the victim any time to protect the system.

In cybersecurity, the 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 CVSS number in published Common Vulnerability and Exposure (CVE) reports.

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

7. 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 is 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 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.

8. Policy

It is important to define clear 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 standard, 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.

9. Other common terminologies

There are many other terms and concepts used in cybersecurity. The items below are common things brought up and discussed within the Axis ecosystem.

9.1 Vulnerability scanning

Vulnerability scanning is audit of a software or product which can be either automated or manual. Several tools on the market are available for performing vulnerability scanning. This audit attempts to identify if the product has services that may have known vulnerabilities associated with a specific software or service version. Vulnerability scanning can only help to identify known vulnerabilities. It is not a good measure to determine how secure a product is. A new critical vulnerability may be discovered tomorrow. The result from a vulnerability scanning needs to be assessed.

9.2 Penetration testing

Penetration testing is an authorized attack on a device/system to identify vulnerabilities and assess what type of negative impact a successful exploit may have.

9.3 Common Vulnerability and Exposure (CVE)

A simplified description of CVE is a database maintained by the Mitre Corporation. This database includes known vulnerabilities in software-based products and components. When someone discovers a vulnerability (typical security researchers), they will submit their discovery to the CVE database. In most cases they will also contact the vendor with a request to fix the vulnerability. This database helps others asses and mitigate risks. Vulnerability scanning tools will often use the CVE database to identify potential vulnerabilities. Most vulnerabilities in the CVE database have already been patched in later versions, so it does not indicate how secure a product actually is.
Common Vulnerability Scoring System (CVSS) is one way to classify the severity of a software vulnerability. It uses a formula that looks at how easily the vulnerability can be exploited and what the negative impact may be. The score is a value between 0 and 10, 10 being the most severe. You will often find the CVSS number in a published Common Vulnerability and Exposure (CVE) report. Axis uses CVSS as one of several measures to estimate how critical an identified vulnerability in the software/product may be.

Exposure also plays a role in determining the risk of a vulnerability. How easy is it for an attacker to exploit the vulnerability? This depends on the infrastructure, service exposure and daily operation.
Example: The risk of a vulnerability may be classified as severe on a public web server serving an enterprise business portal. The same vulnerability could be classified as limited when used in cameras on a local protected network.

PART TWO: CONCEPTS

10. Threat modeling

Threats 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 intents — or cause harm to assets unintentionally or by accident.

The majority of cyber 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:

> Scanning open networks, services and ports
> Trying to expose default or common credentials
> Finding unpatched services
> Sending phishing emails

Opportunistic attackers will normally 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.

Target attackers will often start with social engineering and spear phishing (a well-crafted email targeting a specific recipient) to gain access to the system. If those tactics fail and the value of a successful attack remains high, these attackers often further analyze the system, software or processes to find alternative exploitable vulnerabilities.

11. Common adversaries

Attempting to better understand the actors whom are most likely to cause harm helps you gain insights into their motives, skills and level of determination. This help prioritize which counter measures you may need to apply. Ask questions like:

> "What assets are they targeting?"
> "How much time and resources they are willing to spend?"
> "How skilled are they?"
> "What vulnerabilities will the try to exploit?"
> "Which attack vectors will most likely be used?"

The range of various types of actors typically includes the following:

- **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
- **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 rather spend your resources on hiding your flaws and vulnerabilities than fixing them.

12. Common organization types

The range of threats, risks and potential adversaries vary between different types of organization.

12.1 Small organizations

Small organizations typically include consumers, family businesses and non-profit organizations. Compared to other organizations, the value for an attacker is limited and the negative impact is typically on an individual level. Adversaries typically have limited skills, determination and sophistication. The common threat actors include near and dear, pranksters and opportunistic cyber criminals.

A video system may be exploited to pry on other individuals or pranksters posting video clips on social media. These organizations will often want to view video of their family, house and business from a remote location over the Internet. Internet-exposed devices add risk if not implemented with additional security controls.

12.2 Local business organizations

Local business organizations are companies, industries or institutions with a small- or medium-sized organization. They will typically outsource physical protection and IT. The cyber threats to their business include lost money, operational downtime and trust. Compared to small organizations, local businesses will have additional adversaries such as employees and hacktivists. They may also attract targeted cyber criminals.

12.3 Global business organizations (enterprises)

The difference between local and global business organization is the size, exposure and value. The potential negative impact also includes loss pf competitive advantage and intellectual property. The list of potential adversaries is extended to inlcude organized cyber criminals with increased levels of skill, sophistication and determination.

12.4 Critical infrastructure organizations

Sectors such as energy, water, transportation, telecom, public health, education, police and military are all examples of critical infrastructure organizations. The negative impact of a cyber attack on critical infrastructure organizations is on a public level, which includes disrupting the flow of supplies and services essential to everyday life as well as causing general public safety concerns or panic.

Large enterprise/business companies may also be classified as a critical infrastructure organizations if an attack they suffer could impact the general public. The list of potential adversaries for critical infrastructure organizations also encompasses nation-states, hacking and cyber terrorists.

13. Risk assessment

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. How likely is it that you will need to protect it?
4. How bad are the consequences if you fail?
5. How much trouble are you willing to go through in order to try to prevent those consequences?

Implementing any type of protection 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 very hard 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.

14. Asset assessment

The main purpose of cybersecurity is to protect data assets and network resources. You cannot protect everything. An assessment to determine which assets to prioritize for protection is required.

Some examples of assets and resources that can be protected in a camera are:

> Video
> Operating system
> Network connectivity
> Passwords
> Interfaces
> Device configuration

Each of these assets and resources need to be classified. It is important to understand how critical a role each of these elements has to the security of the system and what negative impact may occur if an element is compromised.

15. Policies and processes

Hardening the system during deployment is a good start. Maintaining a limited risk level throughout the life-cycle of the system requires policies and process.

It is important to define clear policies and processes that govern usage and privileges in order to achieve adequate risk reduction for the system over the long term. A recommended approach is to work according to a well-defined IT protection standard, 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. This could include simple things like defining:

- Roles, responsibilities and privileges
- Protection levels for the system and its elements/components
- System maintenance intervals
- Common dos and don't s based on best practices and common sense

16. Common risk reduction controls

16.1 Device inventory

A video system may have a large number of cameras. If you do not have control over the device inventory you may face challenges with device monitoring and maintenance. AXIS Device Manager is an on-premise tool that delivers an easy, cost-effective and secure way to perform device management. It lets you manage all major installation, security and maintenance tasks in batches, instead of one device at a time manually. Its device inventory makes it easy to gain an overview of and document all AXIS Devices on your network. And let you automatically identify, list and sort them based on your own criteria.

16.2 User account management

"Use a strong password" is a commonly repeated phrase. Yes, using strong passwords are important. However, a common challenge with device passwords is that they tend to spread within the organization. For example, during device maintenance someone new requests the password in order adjust something. A couple days or weeks later, someone new also has the same request. Within short many new (or temporary) users now know the password to all your devices. And you lose control over who may access them. The strength of password makes no difference in this typical scenario.

Managing devices should have multiple accounts (role-based) and temporary accounts should be created for occasional maintenance/troubleshooting. AXIS Device Manager helps you easily and efficiently manage multiple accounts and passwords for AXIS Devices. AXIS Devices belong to three different privileges levels: viewer, operator and administrator.

16.3 Keeping software/firmware up to date

All software-based products can potentially be released by it manufacturer with unknown vulnerabilities that may one day be discovered. In most cases these vulnerabilities will pose limited risk as they may be either very hard to exploit or the impact may be limited. Occasionally, however, a critical vulnerability can be discovered that escalate risk levels.

Axis development teams, process and dedicated personnel aim to reduce the risk of critical vulnerabilities in products, applications and services. Axis vulnerability management processes also includes patching and announcement of identified vulnerabilities.

Running devices with up-to-date firmware versions will mitigate common risks for devices. That is because latest firmware versions will include patches for known vulnerabilities that attackers may try to exploit. AXIS Device Manager shows you if new firmware versions are available to AXIS Devices connected to your network and efficiently deploy firmware upgrades.

16.4 Limit Internet exposure (Internet-facing)

Exposing computers or devices for public Internet access is risky. Internet-facing means that the device IP address (or port) is accessible by clients on the Internet. Any camera or other network device that is placed behind a firewall is not Internet-facing but is still able to access services on Internet, just like a computer.

The sheer volume of malicious computers on the Internet that continuously probe public IP addresses to find known, exploitable vulnerabilities is enormous. They get help from web-crawler search engines like www.shodan.io to find potential victims. Shodan probes every public IP address and provides a database of which devices or services are available on Internet. This means that all external IP addresses will eventually be indexed and the service/interface behind the address will be identified.

The most common mistake made by a small organization is to expose a camera as a public web server. These organizations will often want to view video from their business, house or store over the Internet. A common, insecure solution is to configure the router to port-forward in order to forward external requests to the camera (poking a hole in the firewall). Risk increase when an Internet-facing device is combined with a weak (or default) passwords. This combination is what hacker groups will exploit when building botnets such as Mirai.

Axis recommends small organizations to use Axis Companion for secure remote video access. Larger organizations that require remote video should use some proxy solution that does not expose the camera, just the video service. A recommendation is to always consult with your Video Management System (VMS) vendor or IT security specialist.

16.5 Limit Local Area Network (LAN) exposure

Devices on a local network are protected by a firewall that reduces risk of threats from public Internet. Reducing the exposure on a LAN will help mitigate risks from adversaries on the inside. Reducing LAN exposure will help mitigate risks related to compromised passwords, unpatched devices and brute-force-login attacks. The following common security controls can be applied based on infrastructure and budget factors.

16.5.1 Network isolation (network segmentation)

Network isolation is a way to separate critical network resources from each other in order to reduce the risk of each of them having a negative impact on each other. This is an especially relevant tactic if different resources do not need to interact with each other — or should not. Network segmentation can be virtual (VLAN) and requires an infrastructure of managed switches, or the networks can be separated with different cabling and network gear. The decision on which type of segmentation to use depends on cost, infrastructure and policies.

16.5.2 IP filtering (IP Tables)

IP filtering acts like a local firewall in the camera. The VMS is the center of the system in a professional video system. Video clients will access live and recorded video from the VMS, never accessing a camera directly. This means that the only computer or server that should be accessing cameras during normal operations is the VMS server. The cameras can be configured with an IP filter to only respond to whitelisted IP addresses, typically the VMS server and administration clients. IP filtering helps mitigate risks if the camera password is compromised, from unpatched cameras and for brute-force attacks.

17. Network encryption

Network encryption should be used when traffic is transferred over unsecure networks where there is a probability of Man-In-The-Middle (MITM) attacks, such as network sniffing and network spoofing (see below). Internet is one such network. However, a LAN may also be classified as unsecure if it lacks control over which devices are present on it.

Network encryption does not necessarily increase the protection for the camera, VMS or clients. Rather, it protects communication between the client, VMS and the camera. It does this by preventing information from being extracted by network traffic sniffing and by preventing data being altered during transfer.

17.1 Network sniffing (HTTPS)

All network packages sent on the network may be collected by other computers on the same network. If the payload in the packages is sent in clear text the data can be easily compromised. Never use plain-text passwords with unencrypted connections.

Axis cameras support Hyper Text Transfer Protocol Secure (HTTPS. i.e. HTTP over a secure SSL/TLS tunnel) which provides network encryption. The client also needs to support HTTPS. HTTPS will encrypt all administrative traffic (normal HTTP traffic) but not video as this is transferred over RTP/RTSP (Real-Time Protocol/Real-Time Streaming Protocol). Encrypting video requires that the VMS also supports requesting RTP tunneled over HTTPS. A recommendation is to always consult with your VMS vendor as not all systems supports. Before HTTPS can be established the camera needs to have a certificate (self-signed or CA-signed) and HTTPS policy needs to be set. Axis products comes with self-signed certificates enabling HTTPS out-of-the-box.

17.2 Network spoofing (HTTPS + CA-signed certificates)

Self-signed certificates provide the necessity to create an encrypted HTTPS connection. There is no difference in the encryption level between self-signed or CA-signed certificates. The difference is that self-signed certificates do not protect against network spoofing, which refers to when an attacking computer tries to impersonate a legitimate server, computer or network device.

A Certificate Authority (CA) is a service that issues (sign) server certificates and needs to be installed in cameras. The VMS uses the certificate to validate the identity of the camera.

A publicly trusted CA such as Comodo and Symantec is typically used for public services, such as public web and email servers. Public trusted CA root certificates are pre-installed on clients, such as Windows, Linux, Mac and mobile devices.

A private CA is a trust point for private network services and issues certificates for private servers. The private CA root certificate needs to be installed in clients that need to validate the signed certificates in cameras. To meet demands for end-to-end encryption, the VMS also needs to have a server certificate so that video clients can validate it is accessing a legitimate VMS.

AXIS Device Manager has a built-in CA service that can cost-efficiently issue and deploy server certificates to the cameras.

18. IEEE 802.1X Network Access Control

Referred to as 802.1X, this standard prevents unauthorized network devices from accessing the local network. Before a device is allowed access to the network (and its resources) it needs to authenticate itself. There are different authentication methods that can be used such as MAC address (MAC filtering), user/password or client certificate.

Operating an 802.1X infrastructure is an investment. It requires managed switches and additional servers, typically RADIUS. An 802.1X infrastructure needs personnel to maintain and monitor the infrastructure.

Axis devices only support 802.1X EAP-TLS with certificates. When using client certificates, there must be a CA (private or public) that can issue the client certificates. AXIS Device Manager enables you to efficiently manage certificates by:

- Issuing CA-signed certificates when no other CA is available
- Distributing IEEE 802.1X certificates
- Deploying HTTPS certificates
- Monitoring certificate expiration dates
- Renewing certificates prior to expiration

About Axis Communications

Axis enables a smarter and safer world by creating network solutions that provide insights for improving security and new ways of doing business. As the industry leader in network video, Axis offers products and services for video surveillance and analytics, access control, and audio systems. Axis has more than 3,000 dedicated employees in over 50 countries and collaborates with partners worldwide to deliver customer solutions. Founded in 1984, Axis is a Sweden-based company listed on the NASDAQ Stockholm under the ticker AXIS.

For more information about Axis, please visit our website www.axis.com.

©2018 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ETRAX, ARTPEC and VAPIX are registered trademarks or trademark applications of Axis AB in various jurisdictions. All other company names and products are trademarks or registered trademarks of their respective companies. We reserve the right to introduce modifications without notice.