

Partners in protection



INSIGHTS & INSPIRATION FROM
THE WORLD OF CYBERSECURITY

[Enter >](#)

INTRODUCTION

A robust framework for protection

As you probably know, there's no single solution to the challenges of cybersecurity and no such thing as iron-clad cybersecurity that comes built-in to any product. Rather, cybersecurity is a question of trusted partnerships where everyone, sub-supplier to manufacturer and from installers and integrators to end users, each has an important role to play. It's also a question of ongoing processes, rather than of one-time achievement.

As part of being a responsible cybersecurity partner, we've put this collection of articles, tips, and inspiration. We think they might be helpful to you in your efforts to stay up to date and to protect yourself, and we hope you will find them useful.

But before turning the page, we would like to take a moment to tell you a little about the National Institute of Standards and Technology's risk management framework (NIST). Because cybersecurity is essentially a question of managing risk, a good starting point is to evaluate potential risks to your business or organization in terms of their probability, and their potential level of harm using a risk management framework – of which there are many.

At Axis, we've chosen to align our cybersecurity approach with the NIST framework. The NIST guidelines are used globally and are appropriate not just for large businesses and organizations but for small and medium ones as well. Even if your organization uses a different framework, chances are it's compatible with the NIST framework.

The NIST framework revolves around five pillars: Identify, Protect, Detect, Respond, and Recover. You can learn more about each pillar, our role as your cybersecurity partner, and your own roles on our website at www.axis.com/cybersecurity.

In the meantime, we hope you enjoy the magazine!

CONTENTS

1 COMMON CYBER THREATS

2 10 TIPS FOR A HEALTHY NETWORK

3 LIFECYCLE MANAGEMENT

4 ZERO TRUST NETWORKS

5 AI AND CYBER

6 COLLABORATION

7 TRUSTED EDGE

8 COMPLIANCE

9 SECURITY SUPPLY CHAIN

10 WHY AXIS?

What cybersecurity can learn from physical security

For most people, it is easy to understand physical security risks. An unlocked door increases the risk of unauthorized people entering. Valuable goods that are visible could be easily taken. Mistakes and accidents may cause harm to people, property, and things.

Physical security and cybersecurity are tackled in generally the same way. Whether you are responsible for your organization's physical security or cybersecurity, you need to apply the same principles:

- Identify and classify your assets and resources (what to protect)
- Identify plausible threats (who to protect it from)
- Identify plausible vulnerabilities that threats may exploit (the likelihood)
- Identify the expected cost if bad things happen (the consequences)

Risk is often defined as the probability of a threat multiplied by the harmful result. Once you have determined this, you must ask yourself what you are willing to do to prevent a negative impact.

Be aware of your assets and resources

As far as video systems are concerned, the obvious resource that needs protection is the video feed from the cameras. The asset is the video recordings in the video management system (VMS). Access is typically controlled according to user privileges. Other assets to consider are user accounts and passwords, configurations, operating system, firmware and software, and devices with network connectivity.

[Read more >](#)

What threats should you look out for?

Step number one on the way to protecting yourself from cyberthreats is knowing which ones you face. Confidentiality, integrity, and availability are considered the key elements to protect in an IT system. Anything that negatively impacts any of them is a cybersecurity incident. So let's have a look at the most common threats to cybersecurity and the vulnerabilities they exploit.

The three most common cyberthreats for video surveillance

1

Unintentional human naivety and error

2

Deliberate misuse of the system

3

Physical tampering and sabotage

[Read more >](#)

1

Unintentional human naivety and error

No matter how great the technology is that you add to protect your network, if an attacker can get just one person to click on a dodgy link in an email, that attacker is in. So for cybercriminals, this is the easiest – and thus the preferred – means of attack. Types of human error that open the door to cyberattack include:

- **Social engineering:** When a user is tricked by psychological manipulation into making security mistakes or giving away sensitive information. Phishing and scareware are examples of social engineering
- **Password misuse:** Including failing to use strong passwords or failing to protect and/or update passwords appropriately.
- **Mismanagement of critical components:** Losing or misplacing something that allows access to the system. Access cards, phones, laptops, and documentation are some examples.
- **Poor system management:** Failure to install system updates and security patches.
- **Unsuccessful improvements:** Individuals trying to fix something, which results in reduced system performance.



Vulnerabilities and human error

Some of the most common vulnerabilities caused by human error are lack of cyber awareness and lack of policies and long-term processes for managing risk. To mitigate the threat of human error, everyone in an organization must be educated about cybersecurity best practices. You should also limit access to video and restrict critical permissions to a few trusted individuals via your VMS.

[Read more >](#)

Deliberate misuse of the system

2

Another all-too-common cyberthreat is the deliberate misuse of your video system by people with legitimate access to it. Types of intentional misuse include:

**Unauthorized
access and
manipulation of
system services
and resources**

**Stealing
data**

**Causing
deliberate
harm to the
system.**

Vulnerabilities and intentional misuse

It is important to implement policies and long-term processes to help manage vulnerabilities and mitigate the threat of intentional misuse of the system. Proper vetting of individuals with permissions that allow them access to sensitive data is important as is limiting the number of individuals with such permissions. Devices should have separate accounts for administration and for daily operation clients (the VMS) and should use a temporary account for maintenance and troubleshooting. If all three of these accounts were to share the same account, the password could easily become known within the organization, creating an opportunity for deliberate or accidental misuse.

[Read more >](#)

3

Physical tampering or sabotage

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

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

Vulnerabilities and physical threats

Cameras themselves are not just susceptible to tampering; they may also expose network cables. This can provide an opportunity to breach the network. Other common vulnerabilities that may provide opportunities for threats that can be exploited include network gear such as servers and switches that are not placed in locked areas, cameras that are easily reached and not shielded by protective housing, and cables that are not protected by walls or conduits.

Be aware of the negative impact

Video systems do not process financial transactions or hold customer data. This means an attack on a video system may be hard to monetize and thus have limited value to organized cybercriminals. But a compromised system may become a threat to other systems. So estimating costs is hard. Unfortunately, in many cases, organizations learn the hard way. Protection is like quality, you get what you pay for. And if you buy cheap, it may end up costing you much more in the long run.

Maintaining good cyber hygiene

Good cyber hygiene refers to the practices and steps that system and device users take to maintain system health and improve online security. Often part of overall internal processes, good cyber hygiene helps ensure the safety of identity and other information that could be stolen or corrupted. Like physical hygiene, cyber hygiene should be performed regularly to help eliminate natural deterioration and common threats.

Benefits of good cyber hygiene

Having routine cyber hygiene procedures for your devices and software benefits maintenance and security.

- Maintenance ensures devices and software run at peak efficiency. Fragmented files and outdated programs increase the risk of vulnerabilities. Maintenance procedures help identify these issues early on and can prevent serious issues from occurring. Well-maintained systems are less likely to be vulnerable to cybersecurity risks.
- From hackers and identity thieves to viruses and intelligent malware, organizations are constantly at risk. By predicting threats and implementing good cyber hygiene practices, it's possible to facilitate early detection, and prepare or prevent risks from becoming a reality.

Like physical hygiene, cyber hygiene should be performed regularly

[Read more >](#)

Use strong, unique passwords

This might sound obvious, but the most common way cybercriminals gain unauthorized access to your system is through the use of weak passwords. Most IP-based devices are shipped with default passwords and settings. It's therefore vital that these are immediately changed following IT or company policy. Organizations need to ensure good password management using strong, unique passwords (with a minimum of 8 characters), they should be regularly changed, and passwords should never be shared between sites. Password policies can't be enforced by computer systems. Organizations must ensure their employees are trained and understand the organization's best practices for passwords. It's also recommended to use certificates to encrypt passwords and usernames.

Deploy and install devices following IT or security network policy

You should never leave unused services enabled when deploying a device. This is an easy way for cybercriminals to attack and install malicious applications. Disabling unused services and only installing trusted applications reduces the chances that a would-be attacker could exploit a system vulnerability. It's also essential that devices follow proper physical installation, and that network ports and SD card ports are never accessible to the public.

A password that is just a single common word or name can be cracked within seconds regardless of length.

[Read more >](#)

Define clear roles and ownership

Clear rules and procedures need to be established to ensure employees have the correct access rights for their area of responsibility. Organizations should follow the principle of "least privileged accounts", meaning users only have access to the resources they need to perform their job. Default accounts should never be used. If you use temporary accounts for maintenance purposes, ensure they are removed when the task is completed.

You should never rely on any device's default settings, especially the password. Default administrative account IDs and passwords for common devices are easily discoverable through a simple Google search, making it all too easy for hackers to get in. Be sure to enable and configure the device protection services and only use default settings for demonstration purposes.

61%

of workers mix personal and work tasks in their devices

80%

of employees admit to using non-approved software-as-a-service (SaaS) applications in their jobs

75%

of network intrusions exploited weak or stolen credentials

[Read more >](#)

Use the latest applicable firmware

Are your devices updated with the latest firmware available? Bugs or flaws in systems and devices leave organizations vulnerable to attack and can allow hackers to steal server private keys or user passwords. It's important to have a well-documented software/firmware update management plan, and always ensure network devices are updated with the latest firmware and security updates.

Perform a risk analysis

How much should your organization spend on asset protection? By analyzing the potential internal and external threats, and the implications if your key assets are damaged or lost, you can prioritize your efforts to protect them. There are also risk management frameworks, such as the NIST (National Institute of Standards and Technology) Cybersecurity Framework, which can help provide processes and guidelines to manage risks.

The number of breaches recorded jumped significantly in 2019 with over

8.5 billion records

exposed – more than 3 times greater than 2018 year-over-year.*

*IBM X-Force Threat Intelligence Index 2020 Gain knowledge on system protection and possible threats

[Read more >](#)

How secure

is your supply

chain?

By working closely with your entire supply chain, you can better understand the possible threats to both your network and connected devices. Today, many IT manufacturers offer documented best practices or guides for hardening their devices on your network, as well as secure supply chain documentation. If this isn't available, it's important to start that conversation with your manufacturer or source other user-generated documentation. Devices should comply with your IT policy – both as individual devices and the system as a whole.

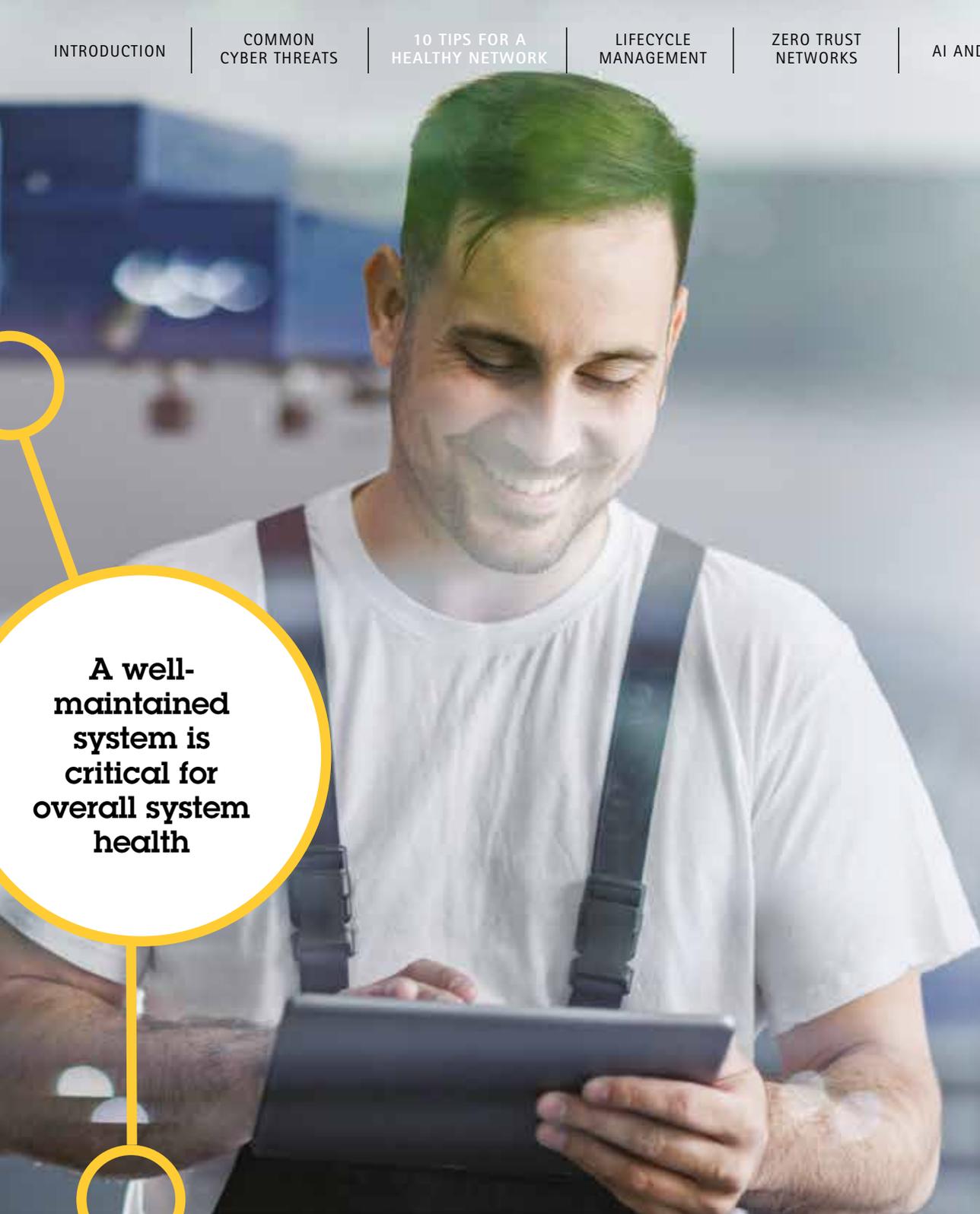
Always use encrypted connections

Regardless of your industry, all data needs secure encryption. Encrypted connections should also be used on all networks, even local or 'internal' ones. Authentication protocols ensure information is encrypted before being sent across the network and effectively reduces the chance of an attack, where malicious code "listens" for unencrypted transmissions.

Secure protocols

- HTTP Digest (access) authentication is one of the agreed-upon methods a web server can use to confirm credentials and a user's identity, such as username or password.
- HTTPS (HyperText Transfer Protocol Secure) is the most common data encryption protocol. HTTPS is identical to HTTP, except the data transferred is further encrypted using Secure Sockets Layer (SSL) or Transport Layer Security (TLS).
- SRTP (Secure Real-Time Transport Protocol) encrypts the video stream for added protection on the video itself. If using a VMS or SD cards for local storage of video, ensure that these are encrypted as well.

[Read more >](#)



A well-maintained system is critical for overall system health

Secure the network perimeter

Do you understand your firewalls and filters? By securing your network from the backbone you can better support other efforts to implement cybersecurity best practices. Using network segmentation such as VLANs (Virtual Local Area Networks) on physical security devices helps decrease the risk of snooping for sensitive information and attacks on individual servers and network devices. Additionally, ACLs (Access Control Lists) can help control malicious movement on the network. Before investing in new devices, ask your vendor for a network port list to ensure the solution will work across the entire network.

Maintain your systems and processes

A well-maintained system is critical for overall system health. Devices and system logs should be regularly monitored to detect any attempts at unauthorized access. In today's fast-paced world of technology, new updates, features, and best practices are created all the time, so you should document maintenance procedures to ensure everyone understands the processes.

Device management software, such as AXIS Device Manager, can help organizations quickly gather a full real-time inventory of all devices and software connected to the network. It scans the entire network and captures all the key information including model number, IP and MAC addresses, firmware version, and certificate status.

Why it's critical to implement effective lifecycle management

As the saying goes, a network is only as secure as the devices connected to it. And, while organizations are active in implementing layered protection practices to secure their networks, they also need an effective way to manage the lifecycle of their physical assets. But organizations often neglect to update the software even when new firmware is readily available. This is usually because they lack a full overview of all the technologies on their network.

One device – two lifetimes

There are two types of lifecycles associated with software-based devices.

1

The device's functional lifetime – or how long a device can realistically operate and function. For instance, a network camera typically has a functional lifetime of 10 -15 years

2

The device's economic lifecycle – how long until the device starts costing more to maintain than adopting new, more efficient technology? Because while an IP camera might function for 15 years, its actual lifespan will be shorter due to rapid changes in the cybersecurity landscape.

Proactively manage your assets

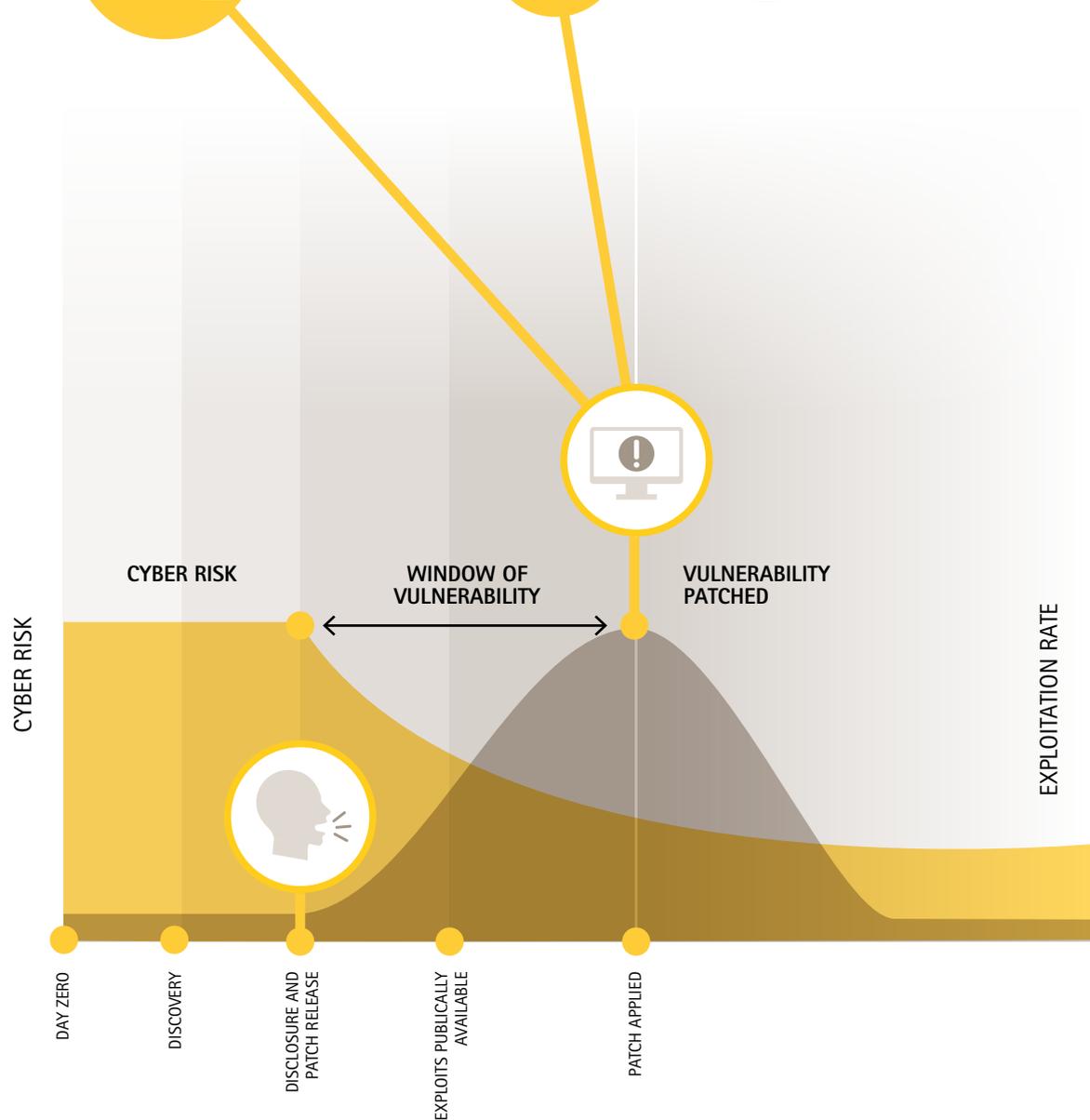
Lifecycle management is the effective management of both the functional and economic lifecycle of physical assets. Organizations need a clear overview of all the technologies deployed on the network, so they can keep a close eye on their networks and critical data, and ensure they are safe from threats and vulnerabilities.

According to the UK's Information Commissioner's Office (ICO)

“60% of breaches involved vulnerabilities for which a patch was available but not applied.”

[Read more >](#)

Hope is not a plan



At some point, all technological devices – from network cameras to VMSs – need to be updated and patched to prevent attackers from exploiting known vulnerabilities and undermining existing protections.

Updates and patches are the best way to improve cybersecurity, but they are not always available for older technologies. This is because they may no longer be supported by the manufacturer. And, from a cybersecurity perspective, older, unpatched technologies pose the greatest risk. It's vital that organizations stay on top of developing threats and ensure they always follow the latest cybersecurity best practices. Any overlooked device could easily become an entry point for attackers.

Keeping pace with threats

Effective lifecycle management can help organizations keep their business secure. And, it helps them to better prepare for the future. It requires knowing where risks lie and keeping up to date on areas that might be exploited. This is especially important for security systems, because if a network surveillance camera goes down, the consequences could be dire.

Physical devices also need updating

Manufacturers regularly release firmware updates and security patches that address vulnerabilities, fix bugs, and resolve other performance issues to help ensure a stable and secure system. While organizations understand the importance of patching operating systems and applications, they often fail to update the firmware that hardware runs on. This leaves these devices vulnerable to cyberattacks and can result in anything from loss of valuable customer data to large fines from regulators for non-compliance.

[Read more >](#)

Streamlined lifecycle management

A structured lifecycle management program helps organizations adequately plan for the future. It uses the most appropriate and advanced technologies to minimize security threats and vulnerabilities. Device management software, such as AXIS Device Manager, can help organizations automate this task so they can effectively manage their assets.

How it works?

Device management software can quickly gather a full real-time inventory of all the cameras, encoders, access control, audio, and other devices connected to the network. It can scan the entire network and when a new or updated device is found, it captures all the key information including model number, IP and MAC addresses, firmware version, and certificate status.

The full overview

With a highly detailed overview of the entire network ecosystem, it's easier to implement consistent lifecycle management policies and practices across all devices and securely manage all major installation, deployment, configuration, security, and maintenance tasks.

Save time and effort

Device management software helps organizations save a lot of time and stress when it comes to managing cybersecurity risk. This type of software can be used to maintain the system by allowing you to:

- Push out system changes, firmware updates, and new certificates to all appropriate devices simultaneously.
- Easily create or reconfigure security settings and apply them across your entire network to ensure all devices comply with the most current security policies and practices.
- Verify that all devices are running the latest and most secure firmware version.
- Manage user privilege levels across the network and configure modifications.

[Read more >](#)

Gain real-time insights

Device management tools offer organizations real-time insights into the state of their ecosystem. For instance, you can see which devices are up to date with the latest patches, firmware updates, and certificates. And, you'll know if a device has been flagged for removal if the manufacturer no longer supports it. This valuable information can help you to determine if malware could potentially infect your devices. You'll have access to all the information you need to resolve a host of other vulnerability issues before they compromise your network.

Proactive ecosystem security

Automating device management processes helps protect networks from threats and vulnerabilities. But organizations should also ensure they follow meaningful cybersecurity policies and best practices. For instance, does your organization have policies around password strength and how often do users need to change their passwords? Is it best practice to turn off unused services to reduce surface area for potential attacks? How frequently are devices scanned for vulnerabilities? And do you have procedures in place for accessing risk levels when a manufacturer posts known exploitations? These are some of questions to ask so you can identify and implement measures to proactively protect your network ecosystem.

5 benefits of automated lifecycle management

1

Stay focused on the critical technology in your environment

2

Know in advance when technologies will reach end of life

3

Avoid needing to suddenly replace a major system component

4

Adequately plan for replacement of devices

5

Budget for a predictable percentage of devices each year

What are zero-trust networks?

Networks are increasingly vulnerable. They are threatened by both more and more sophisticated and numerous cyberattacks and the exponential growth in connected devices – each of which creates another network endpoint open to attack. As a result, the concept of “zero trust” has emerged, and with it zero-trust networks and architectures. For hardware manufacturers, Axis included, it is essential to prepare for the zero-trust future. It will be here sooner than we think.

Trust nobody and nothing in the network

As the name suggests, the default position in a zero-trust network is that no entity connecting to and within the network – whether apparently human or machine – can be trusted. This is regardless of where they are, and how they may be connecting. Rather, the overriding philosophy of zero trust networks is, “never trust, always verify”.

Stick to the minimum access required

This demands that the identity of any entity accessing or within the network is verified multiple times in different ways, depending on behavior and the sensitivity of the specific data being accessed in the network. In essence, entities are granted the minimum amount of access required to complete their task.

The default position in a zero-trust network is that no entity connecting to and within the network can be trusted.

[Read more >](#)

3 reasons a firewall isn't enough

Historically, organizations have relied on ensuring that the corporate firewall is as robust as possible, but this approach is increasingly problematic for a number of reasons.

1 The potential for damage is high

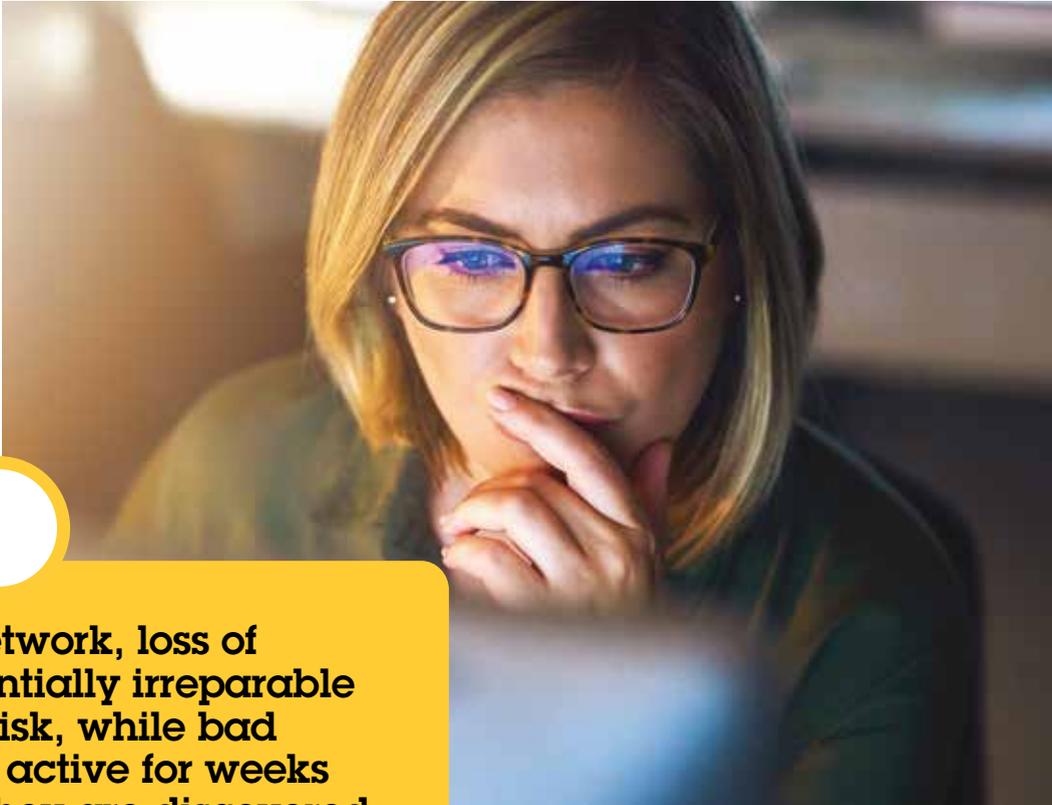
While relying on a firewall appears to ensure security for network access, should anyone be able to breach the firewall they are then able to move about fairly freely within the network.

2 A firewall is no longer sufficient

The sheer number of devices connected to the network mean protecting the network perimeter with a single solution is no longer feasible.

3 More “permeable” networks offer benefits

The use of cloud-based services beyond the network and the benefits of systems of customers and suppliers who are seamlessly connected have changed the nature of network security.



“ Once inside the network, loss of data causing potentially irreparable damage is a real risk, while bad actors can remain active for weeks or months before they are discovered (if they are at all).

Wayne Dorris, Regional Architecture & Engineering
Manager for Axis Communications

[Read more >](#)



How zero trust works

Zero trust employs techniques such as granular network perimeter security and network micro-segmentation. The former is based on users and devices. It uses their physical locations and other identifying data to determine whether their credentials can be trusted to access the network. The latter involves applying varying levels of security to specific parts of the network where more critical data resides.

An additional layer of security

Giving individuals access only to parts of the network and the data required to undertake their role brings obvious security benefits. But flagging anomalies in the behavior associated with these identities adds an additional level of security. For instance, a network administrator may have extensive network access for maintenance of R&D or finance servers.

A security red flag

It would be a security red flag if the credentials of that same network administrator were used to download specific critical files or data in the middle of the night and send them outside the network. In a zero-trust network, either additional authentications can be used, or the anomalous activity could be flagged in real-time and brought to the attention of the security operations center for investigation.

Anomalies in behavior could point to security credentials having been stolen, a disgruntled employee, or someone looking to gain through corporate espionage.

[Read more >](#)

Enter the policy engine...

At the heart of every zero-trust network is a policy engine: software that lets an organization create, monitor, and enforce rules about how data and network resources can be accessed. Policy engines use a combination of network analytics and programmed rules to grant role-based permission based on a number of factors.

Yea or nay to every request

Put simply, the policy engine compares every request for network access and its context to policy and informs the enforcer whether the request will be permitted or not. In a zero-trust network, the policy engine defines and enforces data security and access policies across hosting models, locations, users, and devices.

Defining and applying rules

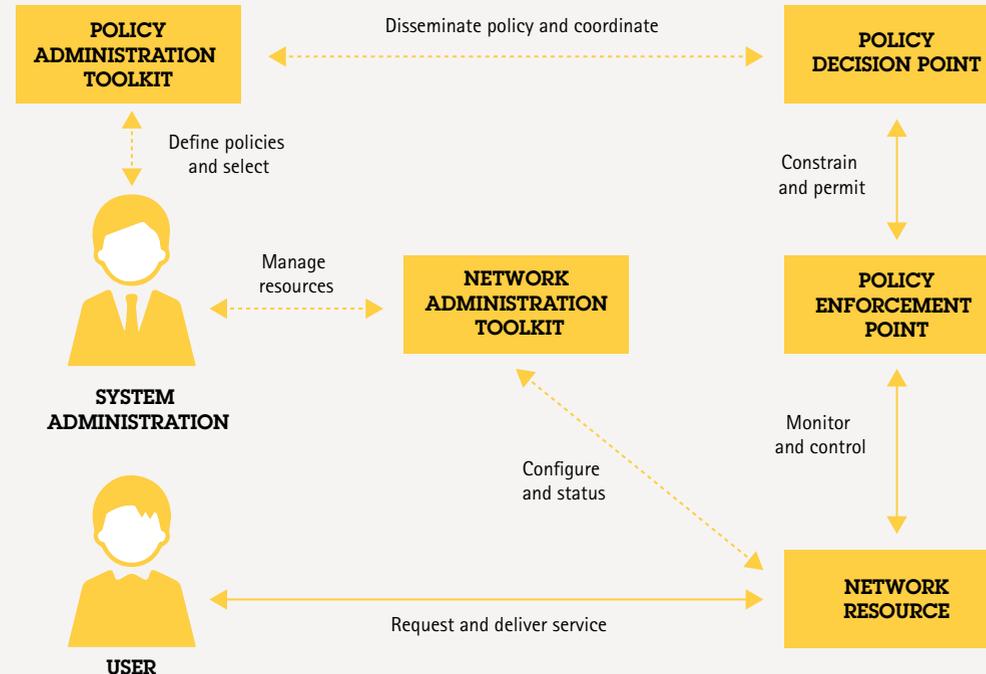
For a policy engine to work, organizations must carefully define rules and policies within key security controls such as next-generation firewalls (NGFWs), email and cloud security gateways, and data loss prevention (DLP) software. Together, these controls combine to enforce network micro-segmentations beyond hosting models and locations.

How can data and network resources be accessed?

Policy engines let you:

- Create rules
- Monitor rules
- Enforce rules

Policy engines – an overview



Policy engines today and tomorrow

Currently, it may be necessary to set policies in each solution's management console, but increasingly integrated consoles can automatically define and update policies across products.

Identity and Access Management (IAM), multi-factor authentication, push notifications, file permissions, encryption, and security orchestration all play a role in the design of zero-trust network architectures.

[Read more >](#)

Zero trust networks and video surveillance

Entities connecting to a network include people, of course, but today the most numerous network connections come from devices. This includes network surveillance cameras and associated network-connected devices. As organizations move toward zero-trust network architectures, it will be essential that network devices adhere to the principles of "never trust, always verify".

Oh, the irony!

Wouldn't it be ironic if a surveillance camera designed to keep the organization physically secure led to a cybersecurity vulnerability? Again, traditional forms of device security are no longer sufficient. In the same way that bad actors can steal the access credentials of an employee, they can also compromise the security certificate of devices. In a zero-trust network, new approaches are needed for devices to prove their trustworthiness to the network.

A somewhat surprising solution

One technology that can provide an immutable root of trust for connected hardware devices is blockchain technology. To many, blockchain is associated with cryptocurrencies, which has given it a bit of a bad reputation. But in itself, blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. Organizations can employ private blockchains for the use of hardware roots of trust and thereby establish immutable trust keys within devices.

Forecasts suggest there will be more than

75
billion

IoT devices in
use by 2025



Why blockchain technology works

Because of the construction of the blockchain, no data transaction in the chain can be changed without agreement from the consensus nodes of all preceding transactions, which are all cryptographically linked. So if trust keys for the identifiable parts of a hardware device are built into the blockchain, it creates immutable credentials for the device itself.

The AI arms race is on – in cyberspace

With any advancement in technology, you can bet that bad actors will quickly be examining its potential for supporting their criminal goals. When cybercriminals plan ransomware attacks or the theft of financial information – or when nation-states look to disrupt the critical infrastructure of adversaries (if not worse) – new technology has the potential to strengthen their armory.

These organizations are as well-funded as any legitimate business. They can innovate in their use of new technologies, such as artificial intelligence (AI), machine learning (ML), and deep learning (DL). And they're unencumbered by any national or international regulations or laws, morals, or ethical norms.

They will simply look at the opportunity these technologies give them to achieve their criminal objectives.

New technology – including AI – will always find its way into the hands of criminals. **Fortunately, it can also be used as defense by organizations being targeted.**

[Read more >](#)



Hidden in plain sight

Increasingly, network intruders are using artificial intelligence to improve the sophistication of their attacks. Large-scale Distributed Denial of Service (DDoS) attacks often make the headlines – because they disable high-profile websites and online services. How are they possible?

Remaining undetected for as long as possible is the primary aim of most cybercriminals. They act, essentially, like house burglars. Moving from room to room, carefully staying clear of cameras and alarms, they search for valuables, then leave as stealthily as they entered. In the same way, cybercriminals seek to penetrate, move around, and exit a network without being detected.

1

One way of doing this is to appear as much as possible like a legitimate user of the network, whether human or a device. And, this is where AI and ML becomes an invaluable new weapon. It allows cybercriminals to learn the network behaviors of people and devices, rapidly develop new malware and phishing strategies, and deploy these on a huge scale.

2

But the simplest way to access any network is still to somehow compel a legitimate user to click on a link and open the door. And a fake email from the boss – virtually indistinguishable in tone and style from the real thing – can often be the most effective key.

Artificial intelligence (AI) is a set of algorithms that allow a computer to store and analyze the outcome of an operation. It can then adjust that operation accordingly the next time it encounters a similar request. During hundreds and thousands of such requests, it gradually optimizes its own responses and actions.

[Read more >](#)

Roads leading to Rome

Cybercriminals use a multitude of AI tools through the attack lifecycle – ranging from "chatbots", which engage employees through fake social media profiles, to the use of neural networks to identify the most valuable data for extraction.

Lateral movement in the network, once access has been gained, is one such technique. This is essential, as the network entry point – which may be an unsecured device in a remote location – is rarely the desired final location.

Ultimately, the intruder will be moving toward far more sensitive areas of the network, harvesting user credentials along the way, and particularly those of privileged users such as network administrators, which will give them a primary key to network access.

[Read more >](#)

IT

OT

The dangerous link between IT and OT

With the world exploding with connected devices and the so-called Internet of Things (IoT), the risks rapidly increase – as the Information Technology (IT) network becomes more tightly integrated with the Operational Technology (OT) environment.

Put simply, the IT network manages the flow of digital information. By contrast, the OT manages the operation of physical processes, machinery, and physical assets of a business or specific location. For those bad actors whose aim is disruption and destruction rather than theft, access to the OT is essential. It takes no imagination at all to understand the potential damage that could be caused through access to the machinery within a power station, oil refinery, or hospital.

[Read more >](#)

Enter the detectives

The potential use of AI by cybercriminals paints a fairly chilling picture. However, these same technologies are, of course, available to those aiming to protect networks from penetration. And in many ways, the advantage is in the hands of the defenders over the attackers.



DARKTRACE

Darktrace is recognized as one of the leading global companies focused on AI in cybersecurity. As you'd expect, they're also experts at understanding the increasing use of AI by the criminal fraternity. Darktrace is continually innovating in AI and ML to stay a step ahead of the criminals.

In many ways, the advantage is in the hands of the defenders over the attackers.

[Read more >](#)

AI as a tool for defense as well as attack

Over the next few pages, we will be talking to Jeff Cornelius, Executive Vice President at Darktrace, to learn more about how his company uses AI and ML to stay ahead of cyber criminals.



How bad are things?

Q

"First of all – despite the impression you may get from the media – developing AI and ML isn't easy! And while we have a powerful adversary in the criminal fraternity and nation-states looking to perpetrate cyberattacks, there are a number of aspects in our favor.

"Primary among these is that – given the access provided by our customers – we can see the entirety of the network activity. We use this to create an understanding of the behavior of every device and user. By contrast, bad actors will only ever be able to rely on a limited view of the activity. Every action they take from an initial foothold is partially a blind step into an environment that we understand, and they do not.

"Ultimately, their goals include activities that the business does not normally perform. Our primary objective is to identify and address such anomalies in network behavior. Our scope needs to be wide since we don't know when or where an adversary might appear or what their specific new methods or goals may be."

[Read more >](#)

An intriguing analogy

Q

Could you clarify?

"To draw an analogy, someone who studies my daily movements from outside my house will build up a fairly detailed view of my habits: what time I generally leave the house each day, which route I take to work, where I grab my lunch, and so on. They could probably do a decent job of mimicking those parts of my life.

"But without having a view inside my house, if they tried to mimic my tastes at breakfast, they'd almost certainly make a mistake that would easily be spotted as an anomaly by a close family member. There is usually decent information available on the internet to target an individual with a clever spear-phishing email, but once inside they are sitting at our table."



Interview with Jeff Cornelius, Darktrace

[Read more >](#)

Supervised machine learning...



Q

Tell us more about machine learning.

"There's an important distinction to be made between supervised and unsupervised ML. In the former, computers are trained against a set of known data. They constantly refer back to these data to check if the outcome recorded is the expected one.

"From a cybersecurity perspective, the models for learning are based on known malware. And this is where the real race between criminals and cybersecurity lies: bad actors are using ML to create new versions of malware – we're seeing exponential growth in these. And cybersecurity companies are trying to keep pace by writing new models for supervised ML defenses. It's a bit like a spellcheck trying to keep pace with a world where new words and even languages are being created daily. And it's becoming increasingly difficult, if not impossible, to keep pace.

[Read more >](#)

...vs. unsupervised machine learning'

A white question mark icon inside a yellow circle, connected by a yellow line to a larger yellow circle containing the text 'But is there another way?'. This circle is further connected by a yellow line to a large yellow circle containing a quote.

**But is
there another
way?**

"Yes. By contrast, instead of relying on knowledge of past threats, unsupervised ML algorithms independently classify data and detect compelling patterns. They analyze network data at scale and make billions of probability-based calculations based only on the evidence that they see. From this, they form an understanding of 'normal' behaviors across the specific network, pertaining to devices, users, or groups of either entity. They can then detect deviations from this evolving 'pattern of life' that may point to a developing threat. This early warning system will allow us to stay a step ahead of the cybercriminals and bad actors."



DARKTRACE



Interview with Jeff Cornelius, Darktrace

Joining forces to mitigate cybersecurity threats

Protecting companies, organizations, our critical infrastructure, and our cities is not a one-man job. There's no magic bullet – no single solution. Rather, successfully maintaining acceptable levels of cybersecurity must be a collaborative effort between a long list of committed stakeholders – including end users.



Building a culture for cybersecurity

Here too, it's all about joining forces. You should look at every individual in your organization as a member of your cybersecurity team. Consider:

- Investing in employee cybersecurity training
- Educating new employees as they onboard
- Encouraging senior leaders to enforce cybersecurity policies
- Continuously learning and communicating about cyber threats as they emerge
- Examining cybersecurity as a requirement when choosing new network equipment
- Implementing a bring-your-own-device (BYOD) policy
- Creating and applying a cybersecurity incident response strategy

By getting your entire organization on board with your cybersecurity plans, you're in a much better position to ensure the security of your network and devices.

[Read more >](#)

A shared responsibility

Cybersecurity is about products, people, technology, and ongoing processes. And it's clear that we need to join forces to ensure that every link of the cybersecurity chain is as strong as possible. Cybersecurity is a shared responsibility that requires the following stakeholders – including end users to work together:

Integrators and installers

They need to ensure that all installed equipment is patched with the latest updates and runs a sophisticated virus scanner. It is also a joint effort with stakeholders to ensure a solid strategy is in place for passwords, management of remote access, and maintenance of software and connected devices over time.

Distributors

For distributors, who do not directly touch the products they handle, cybersecurity becomes relatively simple. Value-add distributors, however, need to consider the same aspects as integrators and installers, especially when they buy equipment from a manufacturer and relabel it under another (or their own) brand. Transparency is key. The origin of the equipment must be clear.

Consultants

They help specify systems and should also help specify proper lifetime maintenance, and they must be transparent about potential associated costs. The challenges of using OEM/ODM equipment, where cybersecurity responsibilities often are unclear, should also be a part of the overall discussion about cybersecurity.

Device manufacturers

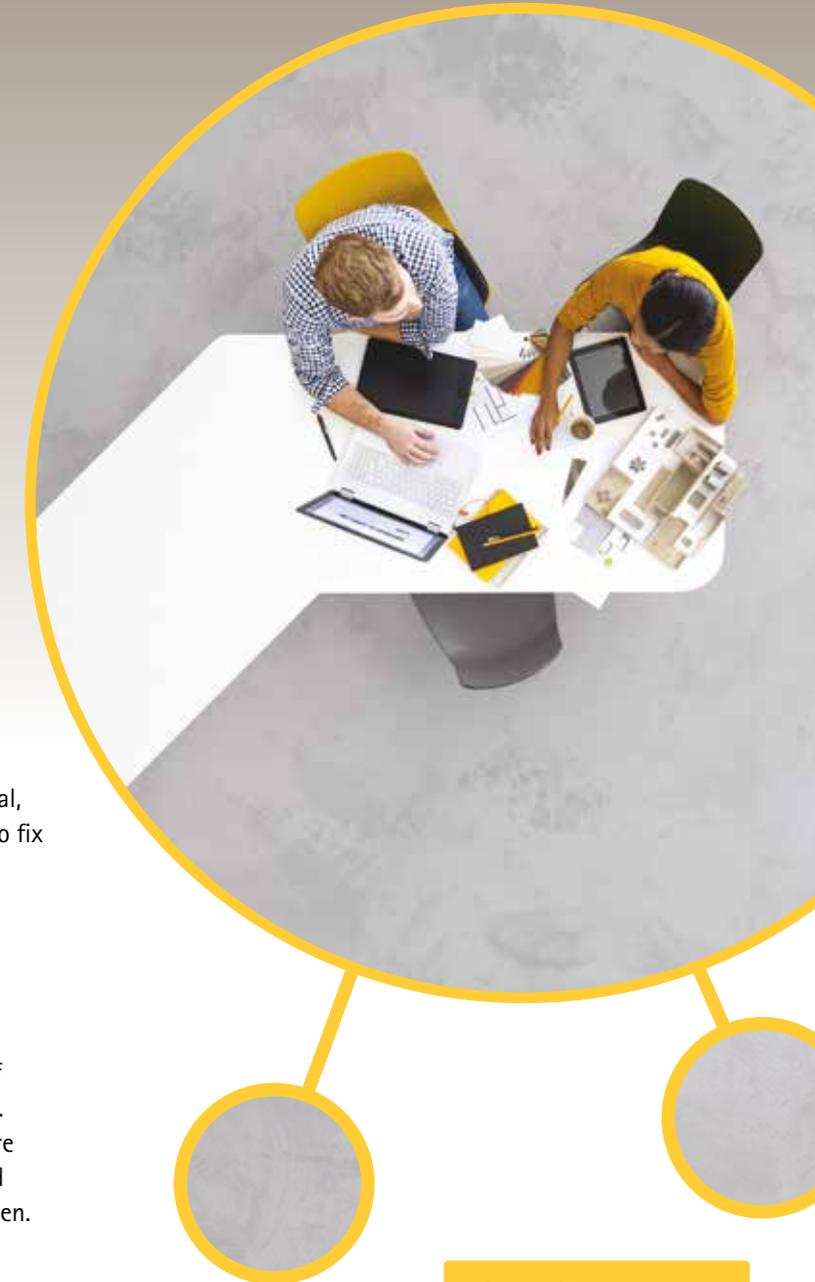
This is where cybersecurity starts. Manufacturers should apply cybersecurity best practices in design, development, and testing to minimize the risk of flaws. Built-in security features, in-house developed chips, and careful control of their own supply chain are also important. As is supplying tools for affordable, automated device management and informing channels and partners about known vulnerabilities.

Researchers

They often discover device vulnerabilities. If the vulnerability is not intentional, the researcher typically informs the manufacturer and gives them a chance to fix it before publishing it. However, if a critical vulnerability has an intentional character, they often approach the public to raise awareness among users.

End users

As each organization has specific and unique cybersecurity needs, there is no universal cybersecurity configuration. Instead, it is important to have a set of information security policies in place to define the scope of security required. Removing default accounts, establishing unique – strong – passwords that are stored safely and changed regularly, assigning differentiated permissions, and always installing patches and updates are just a few steps that should be taken.



[Read more >](#)

Partners in protection

Only by working together can we ensure that we are better prepared to address the constantly evolving cybersecurity threat and remain capable of reacting fast if the threat materializes. All stakeholders have a role to play in ensuring that every aspect of implementing cybersecure solutions is carried out correctly – from device manufacture, system design and installation, to maintenance and device management. This is how we stay vigilant.

**All
stakeholders
have a role
to play**

How cybersecurity increases trust on the edge

The world on the edge

As we head into 2021, we are seeing growing momentum toward computing at the "edge" of the network. The fact that billions of so-called **IoT** devices are already connected to the network, and that this number is **rapidly accelerating**, isn't news in itself. But the nature and demands of those devices do have some serious implications for cybersecurity.

IoT

IoT (Internet of Things) refers to a network of devices that are connected to the internet and can "communicate" with each other. They include tech gadgets such as smartphones and wearables, smart home devices such as smart meters, and industrial devices like smart machines. IoT devices make use of sensors and processors to collect and analyze data acquired from their environments and create actions accordingly.

Rapid growth

By 2025, forecasts suggest that there will be more than 75 billion connected Internet of Things (IoT) devices in use. This would be a nearly threefold increase from the IoT installed base in 2019.

[Read more >](#)

The world on the edge

Put simply, more of the “things” that are connected to the network require or would benefit from the ability to instantly sense what is happening, decide what to do, and take action.

Autonomous vehicles are an obvious example

Whether in relation to communications with the external environment (for example, with traffic signals) or through sensors detecting risks (for example, an object suddenly appearing in front of the car), decisions must be processed in a split second. The latency of data being sent from the car across the network for processing and analyzing in a data center before being returned with a decision on the action to be taken is unacceptably long.

It's the same with video surveillance

If we are to move toward the proactive rather than reactive – to prevention of incidents rather than response after the fact – more processing of data and analysis needs to take place within the camera itself. But with the increasing number of devices at the edge, and with those devices playing a more critical role in safety and security, comes a number of consequences, which we will explore on the following pages.

“ There is a trend toward more processing of data and analysis taking place within the camera itself.

[Read more >](#)

Proprietary power in dedicated devices

Dedicated and optimized hardware and software – designed for the specific application – is essential with the move toward greater levels of edge computing. Connected devices will need increased computing power and to be designed and manufactured to purpose from the silicon up with cybersecurity front of mind.

This is where proprietary integrated processing chips become important. For example, devices from Axis make use of an in-house designed "system-on-a-chip" that protects devices from cyber attacks – such as unauthorized malevolent "firmware" upgrades that would create a "backdoor." In its latest iteration, the ARTPEC-7 processor is designed specifically for the video surveillance needs of today, and of the future, with a security-first mindset.

Specifically designed for video surveillance, the latest Axis ARTPEC-7 chip has more than 50 times the performance of the original. Controlling the design and manufacture of its own chip means that Axis can create the products best optimized for customer needs, while addressing the evolution of external factors, such as threats to cybersecurity.

“ ARTPEC-7 allows us to provide network cameras with extremely high image quality, as well as delivering high performance, good bandwidth efficiency, and the ability to run analytics at the edge.

Stefan Lundberg, Expert Engineer, Axis Communications

Read more >

Toward the trusted edge

Trust takes many forms:

- Trust that organizations will collect and use our data responsibly
- Trust that devices and data are secure from cybercriminals
- Trust that the data itself is accurate and that the technology itself will work as designed

The edge will be the point at which this trust will be created or destroyed.

Trust throughout the entire supply chain will be vital. While embedding spying chips on the hardware itself is a relatively distant possibility, it would be relatively easy to install a spying "backdoor" into a device through a subsequent firmware upgrade than at the point of manufacture.

[Read more >](#)

Toward the trusted edge

Issues around personal privacy will continue to be debated around the world. While technologies such as dynamic anonymization and masking can be used on the edge to protect privacy, attitudes and regulation are inconsistent across regions and countries. The need to navigate the international legal framework will be ongoing for companies in the surveillance sector.

Cybersecurity is more critical than ever

With more processing and analysis of data taking place in the device itself, cybersecurity will become ever more critical. Even when faced with increasingly numerous and sophisticated cyberattacks, many organizations are still failing to undertake even the most basic firmware upgrades. Fundamental to a secure system is the need both for individual device management and for comprehensive lifecycle management of the entire surveillance solution, through clear hardware, software, and user policies.



The threat of non-compliance

In recent years, organizations like British Airways and Marriott International have received hefty fines for failure to comply with regulations. The threat of penalties has sent shockwaves through the business community and is now impacting how organizations spend their cybersecurity budget.

Organizations are also under threat of other targeted attacks, such as ransomware, malware, and phishing. This can result in system shutdowns, lost data, operational disruption, negative publicity, loss of customers, and revenue dips.

What is compliance?

It's often assumed that compliance refers to conforming to governmental regulations and international standards. However, this is only part of the story. Organizations also need to implement and follow internal controls and best practices, while ensuring the partners that they deal with are also compliant.

Organizations now have the responsibility to ensure that their customer data is adequately protected.

There are three areas to consider:

1

Regulatory Compliance

Government regulations such as GDPR and international standards and frameworks such as ISO or NIST

2

Internal Compliance

Internal company policies and best practices

3

External Compliance

Compliance within the supply chain

[Read more >](#)

Our obligation to obey the law

Data protection laws such as the EU General Data Protection Regulation (GDPR) are designed to control how consumers' personal information is used by organizations, businesses, or governments. When it comes to cybersecurity, such laws are often closely related to the security solutions an organization has in place.

While GDPR is a European law, most global organizations need to deal with this in some way. For instance, U.S. companies that store data in the EU need to comply with GDPR. Similarly, if an organization has a contract with a third party that uses data processing, these parties will also need to be GDPR compliant. Over in the U.S., all 50 states have separate regulations for data protection which makes it difficult and time-consuming to manage cross-state work.

Internal governance is more costly

Hackers don't hack standards - they look at a company and determine what their specific vulnerabilities are and where they are exposed. Organizations could easily spend their entire budget on cybersecurity. However, the goal should be to provide enough protection but not impede innovation. This is a balance and depends on the organization's appetite for risk. Some organizations implement even more vigorous controls than dictated by law. Because if there's a cybersecurity breach, organizations need to demonstrate that they took the right steps to protect the business.

Compliance within the supply chain

Organizations with complex supply chains will also have other compliance requirements. For instance, European based organizations doing business with the U.S. government need to comply with standards such as the Cybersecurity Maturity Model Certification which requires audit certification based on internal management of cybersecurity procedures. In the worst-case scenario, third parties (such as suppliers) can also be partly liable for non-compliance and therefore incur a percentage of the fines.



While external obligations are important, it is recommended that the organization's internal policies exceed these rules. Because at the end of the day, it is the organization's responsibility to ensure compliance and guarantee that data is protected against any and every breach.

[Read more >](#)

Which regulations apply to you?

Staying on top of compliance requires constant work. The cybersecurity and data management regulations that apply to your organization are usually dependent on the industry that you are in. However, several regulations span multiple industries and countries.

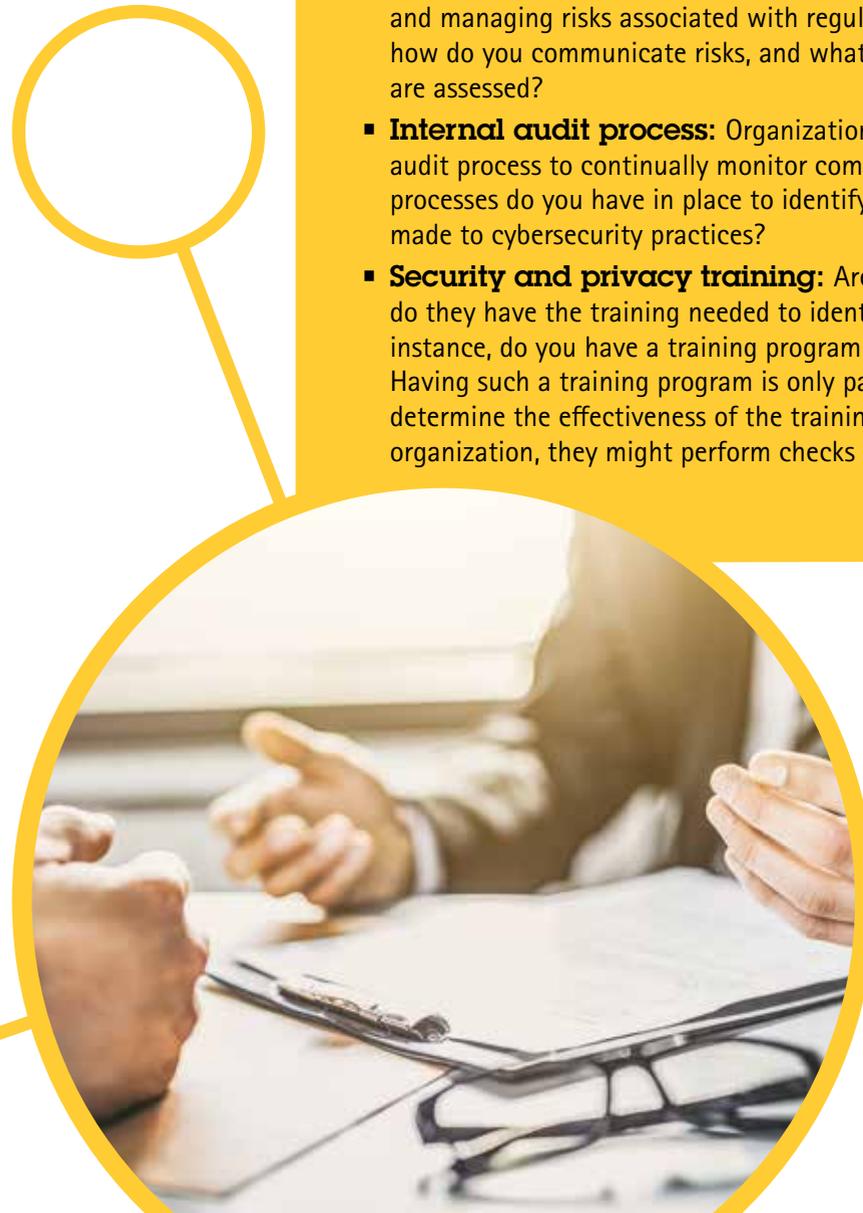
Organizations need to constantly review upcoming guidelines and changes that could be made into law. By examining current threats and attacks and understanding which compliance laws and regulations are being rolled out, organizations can determine what changes they need to make to ensure they pass new compliance checks.

Cybersecurity audits

Once you've identified which regulations your organization must adhere to, you need to assess the state of your overall compliance. By conducting an internal cybersecurity audit, you can evaluate your organization's IT security governance processes. In general, organizations need to conduct a cybersecurity audit annually. However, it is recommended that all controls are continuously monitored to help ensure timely redress of any gaps in your controls. It is also recommended that organizations regularly document this ongoing evaluation of security controls. This can then be used in future audits.

Some of the things to consider during a cybersecurity audit:

- **Risk management:** What is your organization's process for identifying and managing risks associated with regulatory compliance? For instance, how do you communicate risks, and what are the processes to ensure risks are assessed?
- **Internal audit process:** Organizations need to establish an internal audit process to continually monitor compliance. For instance, what processes do you have in place to identify, evaluate, and control changes made to cybersecurity practices?
- **Security and privacy training:** Are your employees empowered and do they have the training needed to identify gaps in IT security needs? For instance, do you have a training program for how to handle email phishing? Having such a training program is only part of the story. Internal controls will determine the effectiveness of the training. If an area is a high risk for an organization, they might perform checks quarterly instead of annually.



[Read more >](#)

Compliance monitoring

The outcome of an internal audit can be used to create a compliance monitoring plan. This plan can be used to continually assess an organization's overall compliance efforts and address all risks identified during the audit. Risks that pose the greatest threat to your organization should be prioritized. By evaluating the compliance controls your organization has in place, you can identify any regulatory gaps within your cybersecurity controls.

When determining who is responsible for monitoring cybersecurity risks, roles should be assigned based on the expertise required. It's possible to optimize allocation by asking yourself, which employees have the skill sets required and which risk monitoring activities can be combined.

Are you up to date?

Manufacturers typically send out regular firmware updates to address vulnerabilities and whenever new legislation is adopted. However, it's also important to have a clear overview of all devices and the status of their lifecycle so you're always prepared for when a product is no longer supported. Device management tools like AXIS Device Manager help ensure products are updated and compliant. These tools send notifications about license subscription renewals, maintenance times, or approvals to help guarantee that organizations meet compliance requirements and are always kept up to date. Plus, if needed for audits, these tools can also provide the required documentation.

Demonstrate your compliance

Device manufacturers are often asked by customers to complete surveys about their level of cybersecurity. Organizations need to answer questions about their continuity plans, how they will implement certifications, and how they protect data on the network. By ensuring all this information is ready to share, organizations can help put their customer's minds at ease by quickly demonstrating how they performed due diligence.

Since 2008, U.S.
banks have been fined

**\$243
billion**

Since 2008,
compliance related
operating costs have
increased

60%

Cost of regulatory
risk amounts to

\$10K
Per employee

“ The cost of non-compliance is great. If you think compliance is expensive, try non-compliance. ”

Former U.S. Deputy Attorney General Paul McNulty
<https://youattest.com/>

Read more >

Document, document, document

Documentation is crucial to ensure you can demonstrate adherence with regulations. Your internal policies could include explanations such as:

- Why and what are you recording?
- Do you display signs informing the public that they are being monitored?
- Does your surveillance show individuals? This impacts their privacy and must be considered and documented. Who has access to the footage?
- How is data stored and for how long? Is data storage secure both physically and from a cybersecurity perspective? How do you ensure older footage is deleted?

You should also include documentation on certain specific scenarios. For instance, if you have an intruder, how should it be handled – who is responsible for controlling the data and what processes are in place? Furthermore, it is also recommended that regulatory boards are kept informed of any failings identified during internal audits and the efforts your organization is taking to eliminate the gaps.

Compliance is a moving target

Laws and regulations are constantly evolving and it's important to recognize that even the most stringent compliance monitoring plans will not fully protect you from regulatory fines. Organizations must continuously monitor their adherence and be able to confidently demonstrate compliance.

The time to act is now

There is no doubt that compliance is a key component in cybersecurity and compliance concerns are here to stay. Organizations and consumers are sitting up and taking notice of the threat, realizing that their systems and data are vulnerable to attack if they don't act fast. While organizations want to pursue innovation and growth with confidence, they also need to minimize the risks posed by cybercrime. On the other hand, consumers want their data kept safe and expect the organizations they deal with to figure out how to do this. Governmental regulations are an issue that can only be met by a collaborative approach where vendors, manufacturers, and end-users all take responsibility for cybersecurity effectiveness. This will ultimately minimize the risk of a damaging breach.

There is no doubt that compliance is a key component in cybersecurity and compliance concerns are here to stay.



What do you need to know about your surveillance supplier – and your supplier's suppliers?

Security threats are always present. New threats arise, and their nature might change at any point in time. Organizations need to know that their system supplier continuously assesses and counters these risks – not only within their own premises but also those of their sub-suppliers.

It's common for organizations to only focus on how their suppliers help in terms of cybersecurity. But what about the supplier's supplier? How do suppliers control and maintain their entire supply chain and ensure all products have a safe journey from component level to finished product?

Is your supplier focused on minimizing security risks?

- Do they design and manufacture secure products with built-in protection?
- Do they share knowledge and tools for putting safeguards in place?
- Do they provide speedy response and free upgrades in case of newly discovered vulnerabilities?
- Do they control the entire supply chain from component level to finished product?

“How do suppliers control and maintain their entire supply chain?”

[Read more >](#)

Finding the right partner

Supply chain security begins with choosing the right supply chain partners through a rigorous evaluation process. The evaluation process should include an analysis of each company's quality and sustainability management process. As a minimum, it should be certified by a third party according to ISO 9001 or IATF 16949.

Evaluating sub-suppliers

Your supplier also needs to evaluate its sub-suppliers' processes for risk management, as well as their production facilities and processes. Site visits should be made and followed up with onsite audits to assess if the company meets the requirements and standards set for approved vendor qualification. As part of the evaluation of a potential new supply chain partner, suppliers should conduct an in-depth analysis of the organization's financial position and ownership structure.

Strategic sub-suppliers

When it comes to suppliers of critical components and manufacturing partners, relationships with these parties tend to be particularly close and long-term. They are strategic sub-suppliers, with whom your supplier drives joint projects and development, sets targets, and makes long-term mutual commitments and plans. Collaboration and communication are therefore close and occur daily, with frequent onsite visits.

All critical components in your supplier's products should be procured directly from strategic sub-suppliers and stored in-house. Non-critical components can be procured by manufacturing partners, but only from suppliers on the established approved-vendor list.

How secure is your supplier's production?

- Do they define and monitor the manufacturing processes?
- Are they developing and producing critical production equipment?
- Does your supplier provide a system for testing components, modules, and products during production, along with software, testing computers, and other IT hardware infrastructure?
- Does your supplier gather production data 24/7 to enable real-time data analysis, assess any potential security risks, and implement mitigation plans?

[Read more >](#)

Auditing your supplier

The best way for your supplier to assure sub-supplier compliance to the specified requirements is to conduct regular onsite audits, yearly or bi-yearly.

Audits should cover a range of important aspects:

- Process compliance, including documentation
- Facility security
- Physical in-plant handling
- Inventory handling
- Production equipment
- Quality control
- Traceability records

Quarterly business reviews are also a good way of following up on performance against expectations. For strategic sub-suppliers, it is recommended that these reviews are conducted at the top management level.

Physical security

Every site within the supply chain, from the component supplier to the distribution center, must meet high requirements for facility security:

- Entrances and exits must be continuously guarded and access controls and visitor registration must be logged and stored. Some areas may require continuous surveillance, even using guards to secure the facility and surroundings.
- Scanning equipment should be used for detecting undesirable objects or materials.
- Transportation should only be arranged with recognized, well-known forwarders who maintain rigorous security regulations and controls. Chauffeurs and trucks should be subject to safety regulations at pick-up and drop-off.
- All air-freight cargo should be x-rayed. It's also common to seal each shipment at the origin, preventing intrusion without detection.
- Incoming and outgoing goods are often surveilled and documented using CCTV cameras.

[Read more >](#)

Data transfer and information security

Data transfer in the supply chain network must be protected by security protocols, utilizing encryption methods and authentication. Sub-suppliers and partners need to maintain a high level of information security to mitigate risks of any gaps in the supply chain.

Your supplier should take a systematic approach to identifying and managing sensitive company information. This system should include people, processes, IT systems, and physical locations, and should comply with ISO 27001 and the EU General Data Protection Regulation (GDPR). This will improve awareness and enable effective risk management.

Personnel security

Knowing who you're hiring is critical, not only from an educational, competence, and work experience perspective but also from a security perspective. For instance, at Axis, quality and security in the recruitment process are key, and approaches include identity verification, requesting references, and making security background checks before employment. New employees and consultants are required to sign a non-disclosure agreement (NDA) protecting intellectual property and other sensitive information, both during employment and after departure.

Empower your employees and reduce risks

At Axis, we ensure employees maintain a high level of information security awareness. We believe that empowered employees have the necessary information to know what needs to be done and which risks exist. Every Axis employee is part of the commitment to real security and trust, and all employees get education and training on information security awareness and are called on to exercise caution and stay alert. Access to information, systems, and resources is restricted and only granted to those employees who need it to perform their tasks. Similarly, employees at suppliers and manufacturing partners share information, systems, and resources with Axis.

[Read more >](#)

Product integrity

Just like all products, surveillance products must function as designed and intended, with maintained integrity. This can be achieved if the product's hardware and firmware are successfully protected from unauthorized change or manipulation during the product's journey through the supply chain.

Quality controls

Together with our suppliers and manufacturing partners, Axis applies a multitude of quality controls to maintain and protect the integrity of our products. Components are always sourced from a supplier on the Approved Vendor List, according to the bill of materials in the Axis specification. The supplier may not make any changes to the specification, work instruction, or quality inspection documents, without permission from Axis. Any approved changes must be documented and logged.

Traceability

A material handling process always ensures the status of materials, revealing any deviations that could compromise quality. Suppliers and manufacturing partners are required to maintain a traceability system to ensure traceability of produced batches from incoming material to the finished component. During production, the physical component will undergo multiple tests, verifying conformance and highlighting any deviations.

Detect counterfeit components

An Automatic Optical Inspection (AOI) contributes to verifying that there are no counterfeit components mounted. At Axis, we develop and produce our critical production equipment, as well as the system for testing the components, modules, and products at the different levels during production. This process limits the risk of tampering. As an additional security control, all test data is shared with Axis 24/7 so unauthorized modifications are immediately identified.



Why Axis?

Solutions for a smarter, safer world

Quality in everything we do: All our products go through extensive testing to give our customers peace of mind.

Innovative technology: We combine technology and human imagination to enhance both performance and usability. Built on open industry standards, it's flexible, scalable, and easy to integrate.

Sustainability at every level: Axis has an ongoing and recognized commitment to environmentally responsible development with the use of sustainable materials. For example, 80% of Axis cameras and encoders are PVC-free.

Driving cybersecurity: We continuously monitor threats and consequences and take quick, decisive action. Even after installation, we continue to harden the devices' cybersecurity with upgrades, updates, and installations.

Global presence with local expertise: Axis has the world's largest installed base of network video products and employees in more than 50 countries. We share insights and experiences and stay up to date on the latest developments.

The power of partnerships: Our commitment to partnership has made Axis the most integrated camera brand on the market.



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, intercom and audio systems. Axis has more than 3,800 dedicated employees in over 50 countries and collaborates with partners worldwide to deliver customer solutions. Axis was founded in 1984 and has its headquarters in Lund, Sweden.

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