How to Improve Your **Cyber Health**

Cybersecurity
Ten Best Practices
For a Healthy Network

AXIS COMMUNICATIONS

Introduction

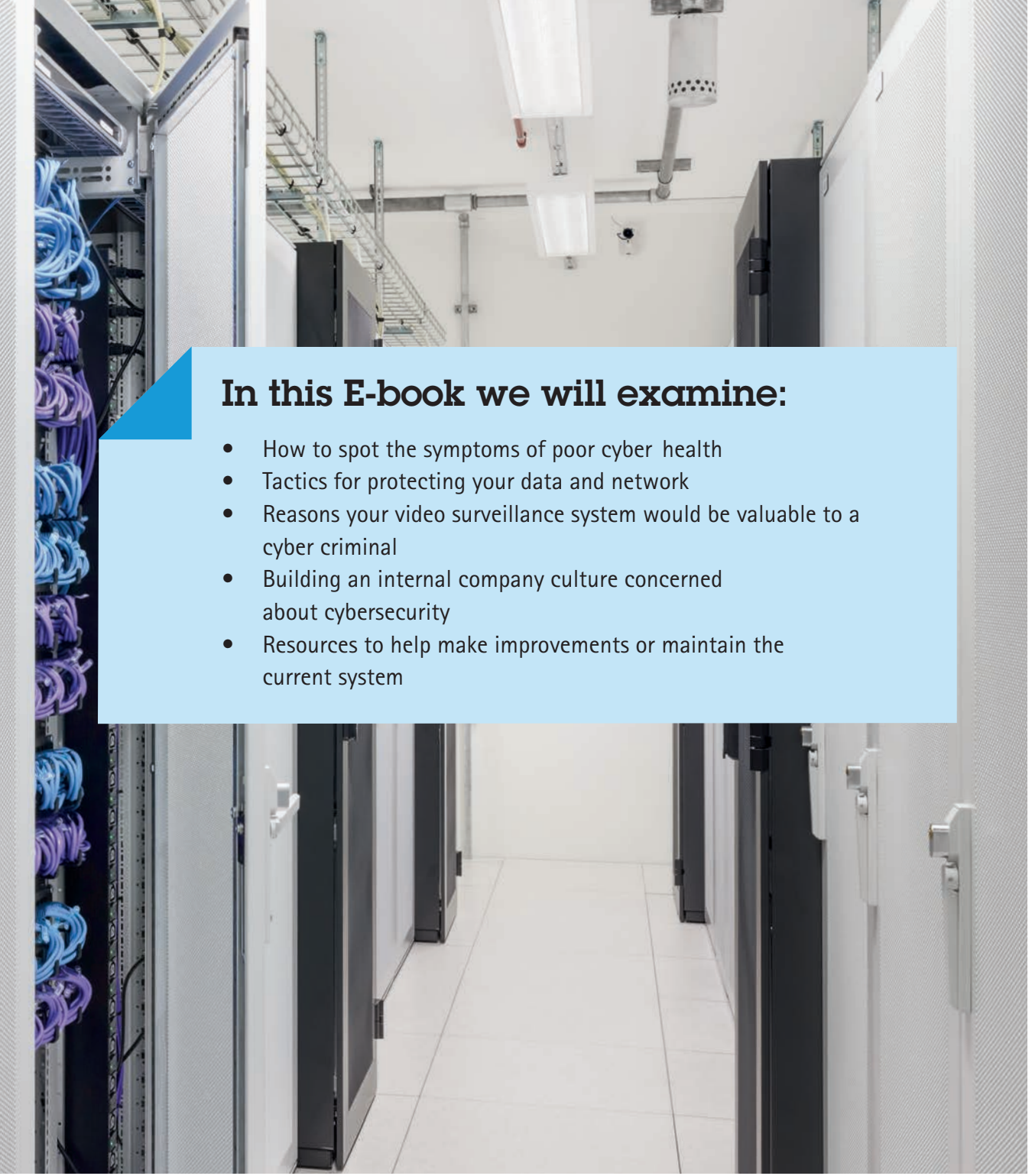
With the frequency of cyber attacks making headline news, no wonder cybersecurity is top of mind. Cybersecurity threats to businesses are at an all-time high, escalating in frequency and level of sophistication.

However, recent statistics show that many organizations may not be ready for existing threats or the new ones that are evolving, with 2 out of 3 CIOs and CISOs saying that their organizations don't see cybersecurity as a priority.* But the good news is, you can stop the majority of attacks by understanding your cyber weaknesses and creating and executing a plan for limiting your vulnerabilities.

Is your organization effectively planning for information security? If a breach were to happen, do you have a cybersecurity incident response strategy? Have you actively trained your staff in your cybersecurity policies?

Knowing how to spot vulnerabilities and ensure healthy network health are important aspects of cyber resilience. But truly securing your network from threats while still making it accessible to those who need it can be challenging. That's why it is so important to be able to identify the symptoms of poor network health and to become proactive in improving the security of your network.

* 2015 Global Megatrends in Cybersecurity" Ponemon Institute LLC – conducted for Raytheon



In this E-book we will examine:

- How to spot the symptoms of poor cyber health
- Tactics for protecting your data and network
- Reasons your video surveillance system would be valuable to a cyber criminal
- Building an internal company culture concerned about cybersecurity
- Resources to help make improvements or maintain the current system

Like physical security, effective cybersecurity is an ongoing cycle of identifying vulnerabilities, assessing threats, and implementing appropriate measures. The need to strongly secure your network becomes more evident every day. To ensure a strong defense, consider the hardening of not only the network, but all the devices attached to it. Is your network as secure as it can be?

Spotting the symptoms of poor network health

If you have a strong, hardened network paired with policies, processes, and people all proactively monitoring and responding to cyber threats – and aligned with your organization's stated cybersecurity goals – then you are in great shape! For the rest of us, with the focus on cybersecurity so high and the risks increasing, we need to consider taking proper measures to avoid the proverbial hot seat.

A network with poorly implemented security is very attractive to hackers and in many cases will lead to an accelerated spreading of viruses, malware and other cyber threats. But with so many users active on your network, it can become difficult to maintain a high level of security without it affecting productivity.

Are you and your network prepared for an attack? Let's take a look at some ways to spot if your cyber health needs improvement. Once spotted and assessed, you can start correcting policies and procedures in order to build a cohesive cybersecurity plan.

1

Your IT and security teams are not aligned

Your IT team has probably been thinking about cybersecurity since the internet was invented by Al Gore.* IT policies likely exist for your operation network when it comes to concerns like password management and standard network protocols. But perhaps your IT policies are not being applied to your IP surveillance network.

Oftentimes IT and loss prevention teams are not speaking the same language but it's important to get aligned, especially when it comes to cybersecurity. Some clear signs you may not be aligned include:

- Different or lack of policies and processes for disparate networks
- Poor or unclear password management
- A lack of ownership or responsibility to review security measures on all systems
- The latest advanced encryption methods are not being used for video streams sent over the network
- Hardware and software connected to your network are not aligned with your IT policies

* Yes, we know he didn't really invent the internet, but you get the point.

42% of individuals say end user failure to follow policies or carelessness were to blame* when asked for an example of human error during a security breach.

* CompTIA "2015 Trends in Information Security"

2

Your network users are not following (or are unaware of) policies and procedures

Do you have policies and procedures in place? Are they documented for all users to easily understand?

Hey IT! Quick tip:
Enforce your IT policy and make sure they are pushed out to company computers and servers.

If your answers are no, you may be the victim of this symptom of poor network health. Below are some additional questions that may also diagnose this symptom:

> Are your employees regularly trained on your IT policy?

> When a new employee comes on board, do they also receive proper training?

> Are there specific guidelines for employees when it comes to device passwords?

3

Your installation and maintenance plans are not clearly documented

Physical installation (of an IP surveillance camera or any other network device) and maintenance problems can also be cause for concern when it comes to cybersecurity. Installers sometimes do not understand the specific needs that you require at the time of installation. With so many vendors, it's possible that the installer missed any or all of their security best practices.

Even worse, too often we see that security, IT, facilities and maintenance departments are not aligned on the maintenance plan. Maybe they aren't even performing routine maintenance on the systems all together.

Do you have a documented plan for installing and maintaining all of your network-attached devices?

"The trouble with doing something right the first time is that nobody appreciates how difficult it was."

- Walter J. Wright

4

Your technology vendors aren't talking to you about cybersecurity

Questions to ask your vendors:

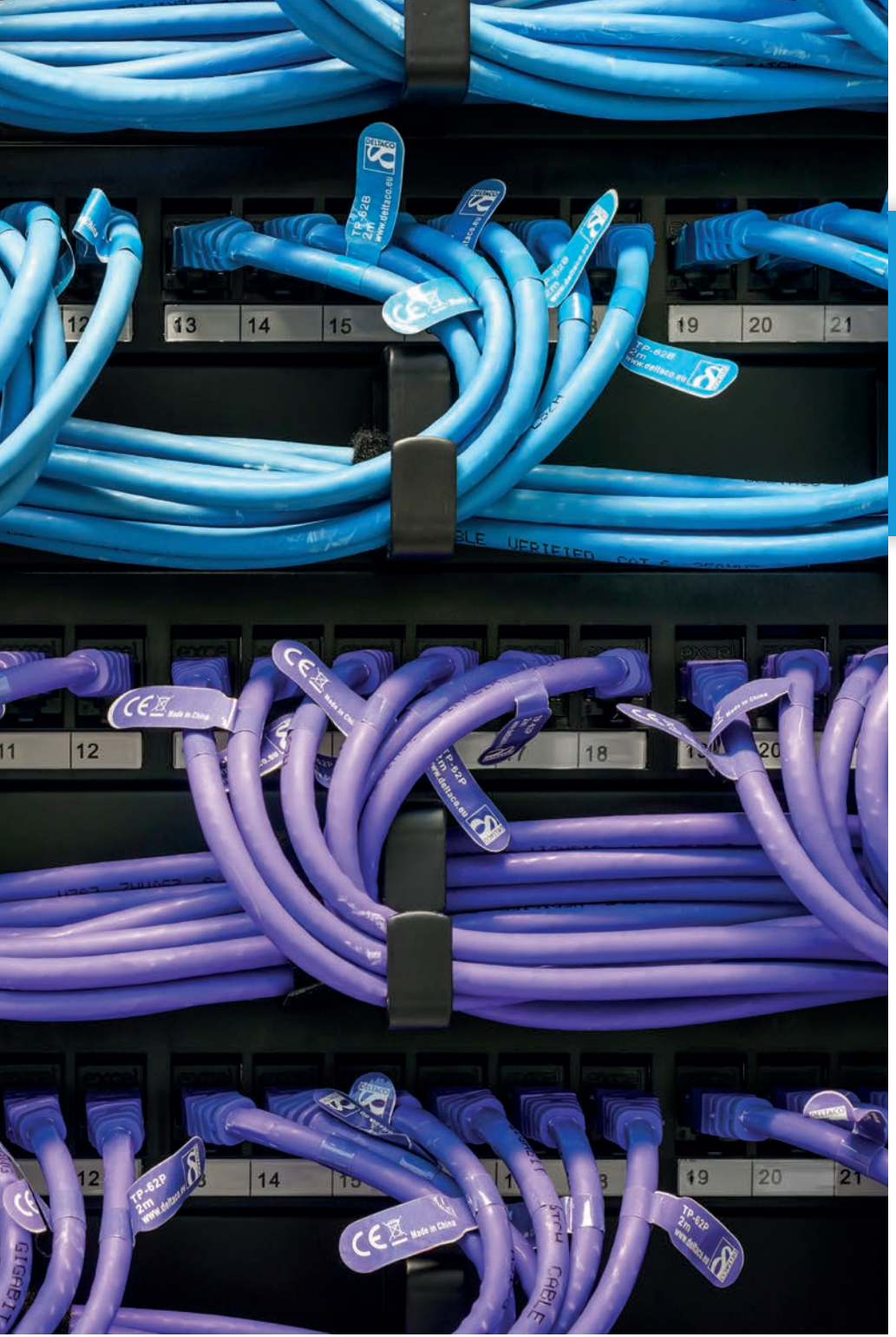
> Are there any backdoors with your products?
> Do you do any data collection?
> Where can I find your latest vulnerability reports?

Does the equipment you choose fit into your IT policy? Or are you trying to work your policy around your vendors? Choose wisely!

Warning signs from your technology vendors include:

> They aren't talking about cybersecurity.
> They don't have device hardening guides or best practices guides.
> They don't perform penetration tests on their products.
> They aren't working with a third party cybersecurity consultant to evaluate their product risks.

Each technology is part of a bigger system and oftentimes systems are not fully secured. It might be that only some pieces of the ecosystem are secured while others can't be. You are only as strong as your weakest link. Is each piece of the puzzle as secure as possible?



10 best practices for a healthy network

Now that we have identified how to spot poor cyber health, it is time to look at what you can do to improve your network's cybersecurity. Along with your IT, security and facilities management teams, you can work to mitigate many of the common risks.

1

Use strong, unique passwords

Most IP-based devices are shipped with default passwords and default settings. Sometimes, these passwords are easy to guess and even published online. This is the most common way that a cyber criminal can gain unauthorized access to your system.

The most effective ways to leverage passwords to stop attacks are to:

- Set strong, unique passwords
- Ensure good password management
- Use certificates in lieu of passwords
- Change your passwords on a regular basis

Did you know?

A password that is just a single common word or name is cracked within seconds regardless of length. A password-cracking calculator estimates how long it would take to crack an encrypted password based on the number of characters. How long would it take a seasoned hacker to crack your password?

By the way, we recommend using a hard-to-guess password with a minimum of 8 characters.

2

Deploy and install devices in the recommended way

Leaving unused services enabled when deploying a device may leave it vulnerable to an attack. For example, a cyber criminal could install malicious applications and scripts using file transfer protocol (FTP) or an application platform from an untrusted developer. Disabling unused services and only installing trusted applications reduces the chances that a would-be perpetrator could exploit a system vulnerability.

Installing devices properly will also help avoid security problems. For example, placing a camera within a person's reach puts that camera in danger of being tampered with or vandalized. Cameras should be installed not only where they provide the best angle of view to clearly observe your scene, but also where they're out of reach to a potential attacker.

3

Define clear roles and ownership

In many organizations, network security failures happen simply because there haven't been clear rules and procedures established for which employees have particular access rights.

For example, it may not be clear who is responsible for reviewing security measures for the surveillance system to ensure best practices are being followed. We recommend organizations use a principle of "least privileged accounts." This means users are limited to only the resources they need to perform their job.

To reduce exposure, any device that accesses video should not be allowed to access cameras directly, unless it is required by the solution. Clients should only access video through a Video Management System (VMS) or a media proxy.

4

Use the latest applicable firmware

Bugs or flaws in operating systems found on workstations, servers, cameras, printers, and other network devices can put your organization at risk.

The well-known Heartbleed bug from 2014 is a good example of this, a security vulnerability in OpenSSL that would allow hackers to steal server private keys and user passwords.

A patch was released almost immediately after the vulnerability was made public, but if users didn't install the patch they were still vulnerable. This is part of the reason why it is so important to have a well-documented maintenance plan, and to keep network devices current with firmware and any security updates.

Many vendors publically post common vulnerabilities and exposure reports that document solutions or workarounds to a specific vulnerability. Are your devices updated with the latest firmware available?

5

Perform a risk analysis

A cyber threat analysis will define how much you can lose and how much you should spend on protection. Make an analysis of potential threats as well as the possible damage and costs if the system is attacked or otherwise compromised. Identify your key assets and prioritize efforts to protect what you value most.

Ask yourself:

- What needs to be protected?
- Who/What are the threats and vulnerabilities?
- What are the implications if assets are damaged or lost?
- What is the value to the organization?

Remember to consider any asset vulnerabilities that may put you in danger. Think about both internal and external threats as you prepare your analysis and priorities.

60% of cyber attacks in 2015 were conducted by insiders and 44.5% of those were considered "malicious".*

* IBM "2016 Cyber Security Intelligence Index"

6

Gain knowledge on system protection and possible threats

Following the risk analysis, take a closer look at the exact systems that run on your network. Work closely with your entire supply chain of vendors to understand any possible threats to your network in using your selected devices.

Many IT vendors now offer documented best practices or guides for hardening their devices on your network. If your selected vendors are not providing you with this information, it's important to start that conversation or source other user-generated documentation.

Remember to understand the system as a whole, not just each individual device, since- in a truly integrated system-the devices will need to speak to each other. Ideally, all devices should fit into your IT policy on their own as well as when configured to work together.

7

Change your devices' factory default settings

Do not rely on any device's default settings, especially the password. This should be the first thing you change and is one of the most important steps you can take to protect your system.* After all, passwords are the gateway to the entire network.

Default administrative account IDs and passwords for most common devices are easily discoverable through a simple Google search. Keeping factory default settings makes it much easier for the hacker to get in. Be sure to enable and configure the device protection services and always disable any services you will not be using.

Only use default settings for demonstration purposes. Even the smallest system is vulnerable if it relies on default settings.

* Yes, we said this already in #1, but it's that important!

8

Use encrypted connections

Encrypted connections should be used on all networks, even local or 'internal' ones.

Make sure your systems are using at least of one the common authentication protocols: HTTP digest authentication and HTTPS. This ensures that all information is encrypted before being sent across the network. These protocols effectively reduce the chance of an eavesdropping type of attack, where malicious code listens for unencrypted transmissions. Even if you're not securing financial data, your data is still important enough to secure with encryption.

Learn this and impress your IT team!

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 currently the most common data encryption protocol. HTTPS is identical to HTTP, but with one key difference: the data transferred is further encrypted using Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

9

Secure the network

If network protection is breached, it increases the risk of snooping for sensitive information and attacks on individual servers and network devices.

Understand your firewalls and filters. Taking the time to secure your network from the backbone helps to support all your other efforts to implement cybersecurity best practices.

Work with your IT team through the whole process, from selecting a system through its implementation and maintenance.

10

Maintain your systems and processes

A well-maintained system is one of the more difficult practices to achieve but is critical for overall system health.

Monitor all devices on a regular basis and enable system notification when applicable and supported. You should also check access logs regularly to detect any attempts for unauthorized access.

Once the plan is executed, it will need to be reviewed and assessed regularly. When it comes to the fast-paced world of technology, new updates, features and best practices are created all the time. Be sure to document your maintenance procedures to ensure existing and future colleagues understand your processes.

The reality of video surveillance and cybersecurity

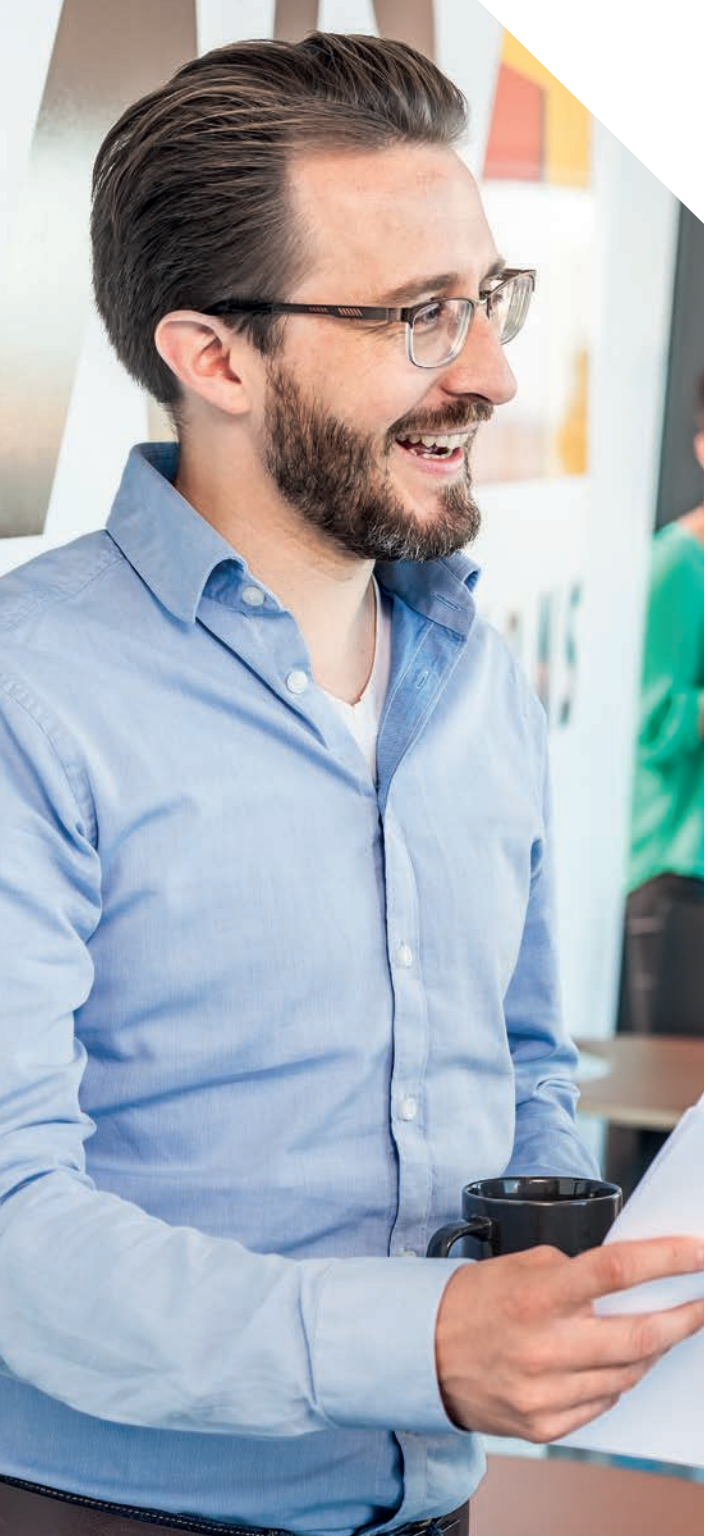
You may have already asked yourself, "why is Axis Communications interested in my cybersecurity?" The reality is that surveillance video is a valuable data asset, and like any other sensitive data, video can be used for many nefarious purposes. Criminals can observe stolen video to identify high-risk asset areas, follow VIP patterns or even use it to disrupt operations via camera sabotage. Tampering, vandalism and denial of video service are other potential threats.

IP surveillance systems reside on the local area network and have to be considered in any IT policy. And IP cameras need to be protected just like other network devices, clients and servers.

Threats must be managed on a system level. Your organizations' cybersecurity is not your concern alone; responsibility to secure the network, its devices and services falls across the entire vendor supply chain. Together, you should consider people, processes and technology.

The majority of network security breaches are due to human error, negligence, misconfiguration, and poor maintenance. IT network security policies are not always applied to surveillance networks, but it is imperative to factor in those policies.

You have the power to choose. Be sure to select video surveillance manufacturers who recommend how to install a protected video system that does not degrade the existing network protection. Work with your IT team and solution providers to handle risk analysis, system deployment and maintenance.



Building a company culture for cybersecurity

All too often poor cyber health plagues organizations. Don't let this happen to you! It's reported that increasing employee knowledge on cybersecurity practices can cause a 30% decrease to security risks.*

Form cybersecurity allies. The more people who are familiar with your IT policy in your organization, the better. Even individuals outside the cybersecurity team should not only agree and abide by the policy, but also fully understand it.

BONUS best practice!

Creating and maintaining a secure network is a team effort and requires support from many different departments. You can't do it alone. Once a plan is in place, communicate it through the organization and keep it top-of-mind when selecting and installing new devices on the network.

How can you build and maintain a culture for cybersecurity? As you develop your regimen consider:

> Investing in employee health training
> Educating new employees on the processes as they onboard
> Encouraging senior leaders to enforce the importance of cybersecurity
> Continuously learning about the evolving cyber threats as they emerge and communicating known threats to appropriate members of the organization
> Examining cybersecurity as a requirement when choosing new network equipment
> Implementing a BYOD (bring your own device) policy
> Creating and applying a cybersecurity incident response strategy for if and when a breach occurs

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.

* 2015 Global Megatrends in Cybersecurity (Rep.). (2015). Ponemon Institute LLC. Conducted by: Ponemon Institute©

Conclusion & additional resources

Cybersecurity threats are increasing and evolving, and as a result, being proactive about your network health is more important than ever before. Having a plan to mitigate risks and how to respond in case of a breach will prepare your organization to mitigate current vulnerabilities and avoid future potential hacks.

By following the tactics for protecting your data and network, you have made a breach difficult and expensive – in both time and resources.

Remember the key factors to success:

> Implement your IT policy on all networks, including your surveillance network
> Involve your entire supply chain
> Prioritize user education
> Embrace cybersecurity into your company's culture
> Define user-friendly processes
> Ensure proper system configuration, updates, and monitoring
> Leverage available resources and take action

Cybersecurity shouldn't be scary. Keep in mind that most attacks are not successful; we just don't hear about the unsuccessful ones. As long as you're putting measures in place to protect your data and network, you're working to improve your cyber health and mitigating the risks of a breach.

So, how healthy is your network and the devices that run on it?

Hardening guide

The Cybersecurity Storm: an infographic

Product Security webpage

SANS webpage

Cybersecurity webpage


AXIS®
COMMUNICATIONS