Hanwha Vision

Beyond the lens:

Ensuring video surveillance networks are cyber-resilient.

Introduction

By John Lutz Boorman, Head of Product and Marketing, Hanwha Vision Europe.

The impact of a cyber–attack can be substantial. In addition to the immediate and often enduring impact on business operations and reputation, there is the significant cost of handling an incident – whether repairing and replacing systems, meeting legal costs, paying fines or obtaining regulatory approvals.

Indeed, according to IBM, the average cost of a data breach is now US$4.9 million, up 10% on the previous year. This is largely attributable to a rise in the cost of lost business and the cost of post–breach responses such as staffing customer help desks and paying higher fines.[1]

Then there is the reputational cost, which can be more challenging to quantify: customers may simply abandon a supplier as they no longer have trust in their technology and cybersecurity in the wake of an attack.

Cyber–attacks are on the rise

The number and complexity of cyber–attacks are on the rise. The European Union Agency for Cybersecurity (ENISA) observed a threefold increase in cyber–attacks in 2024 when compared with 2023, logging 11,079 incidents and including 322 incidents specifically targeting two or more EU Member States.[2]

In its "Threat Landscape" report of September 2024, ENISA noted a 78% increase in the number of reported data compromises compared with 2022, citing a context where "Today… we live in an interconnected society where cloud, edge and IoT technologies and applications produce huge amounts of data every second." Indeed, according to ENISA, "Edge devices, used for networking and security, remain a lucrative entry point" into systems for cyber criminals.[3]

Many motivators can drive an individual or group to carry out a cyber–attack, from insider threats to state–sponsored attacks, or organised crime circles stealing the data from compromised devices for blackmail or to sell on the dark web.

78

The percentage increase in the number of cyber–attacks compared with 2022

[1] *Cost of a Data Breach Report 2024*, IBM, July 2024. Last accessed at: https://www.ibm.com/reports/data–breach
[2] *ENISA Threat Landscape 2024*, European Agency for Cybersecurity (ENISA), September 2024, p.10.
[3] *ENISA Threat Landscape 2024*, p.24.

Video: a back door for hackers?

Against such a backdrop, no aspect of an organisation's technology infrastructure is immune from risk, and that includes video surveillance. The networked video camera is fast becoming ubiquitous in many systems' infrastructures, providing AI–based analytics at the edge of users' networks. As it evolves into a vital business tool, capturing and analysing vast amounts of data across the organisation, cameras, video management systems (VMS) and connected devices are becoming a more attractive entry point to malicious actors.

Governments around the world are moving to limit the risks of cyber–attacks on networked systems. In Europe, regulations such as the Network and Information Security Directive (NIS2) and the Cyber Resilience Act (CRA) aim to improve the cyber–resilience of critical networks and, therefore, video technology. Meanwhile, the National Defense Authorization Act (NDAA) in the United States of America prevents manufacturers from using silicon chips and other components sourced from blacklisted countries as they might present cybersecurity risks.

Mind the gap!

New Hanwha Vision Europe research finds that many IT and security managers across Europe are largely unprepared for NIS2 and CRA, and overestimate their cyber–resilience. Many lack basic protocols to ensure they are protected from cyber–attacks.

In fact, despite the growing regulatory demands and rising threat landscape, many users remain dangerously unaware of the cybersecurity practices they should be following, resulting in a false sense of security.

This report aims to uncover the gaps between perception and reality in video surveillance security and offer actionable insights on how businesses can better protect themselves from these evolving and increasing cyber threats.

The Network and Information Security Directive (NIS2) came into effect in October 2024

Users are highly confident that their systems are protected

There is strong optimism among leaders about the cyber–resilience of their security systems, with over 90% of respondents believing their systems are either “protected” or “highly protected”. Confidence levels vary slightly across countries, ranging from 83% in Spain to a high of 97% in Italy.

Respondents from larger companies tend to consider their firms as more secure, with a confidence level of 96%, compared to smaller companies, where only 70% believe they are protected. Across sectors, confidence spans from 80% in data centres and telecoms to 99% in the financial sector. Second was the transport and government sector at 96%. Similarly, confidence among different roles shows that 89% of IT leaders feel confident in their current cybersecurity and 95% of security leaders feel the same.

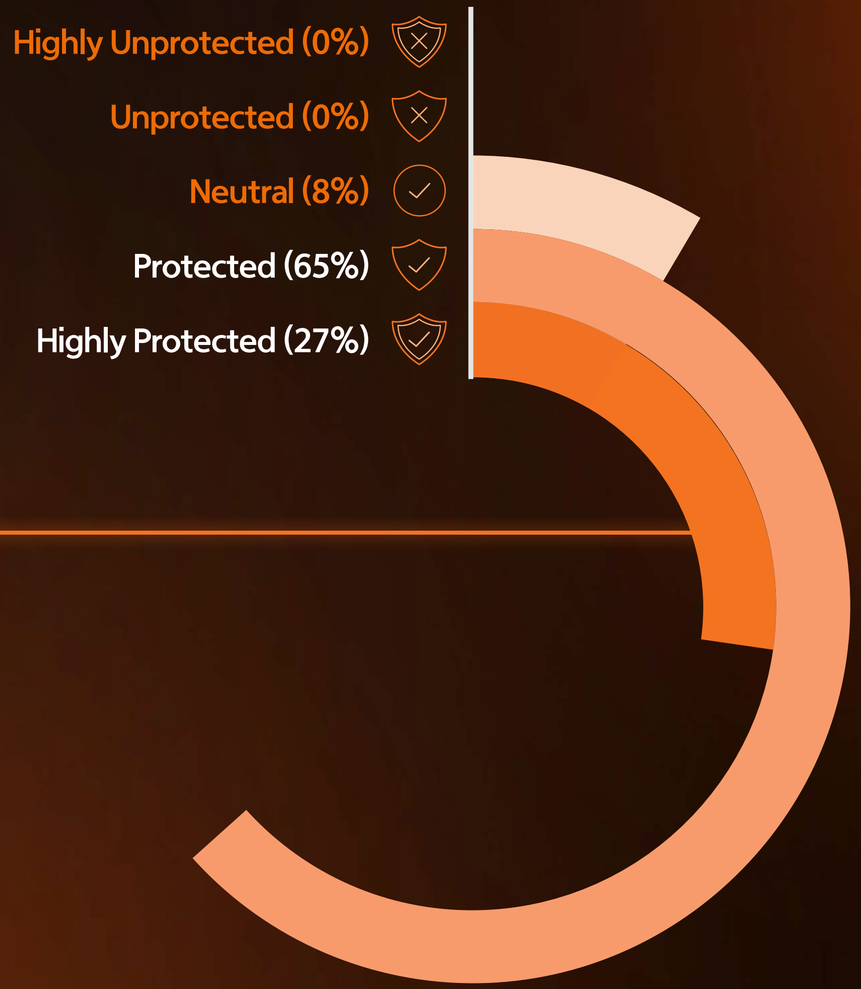
High confidence in the cybersecurity measures being taken to secure a video system jars with the reality of the cybersecurity protocols being taken. This is a cause for concern, as it can lead to complacency and a lack of proactive measures.

Users believe their systems are well–protected, though the research reveals that many fail to implement even basic cybersecurity practices, such as regularly updating firmware or changing default passwords.

Evidently, more robust cybersecurity measures are needed across many companies and organisations, but leaders remain unaware of the need.

Nine in 10 respondents believe their security systems are either “protected” or “highly protected”

Reason for optimism? Leaders are highly confident that their security systems are protected or highly protected:



There is a worrying lack of awareness of cybersecurity regulations and compliance mechanisms among users

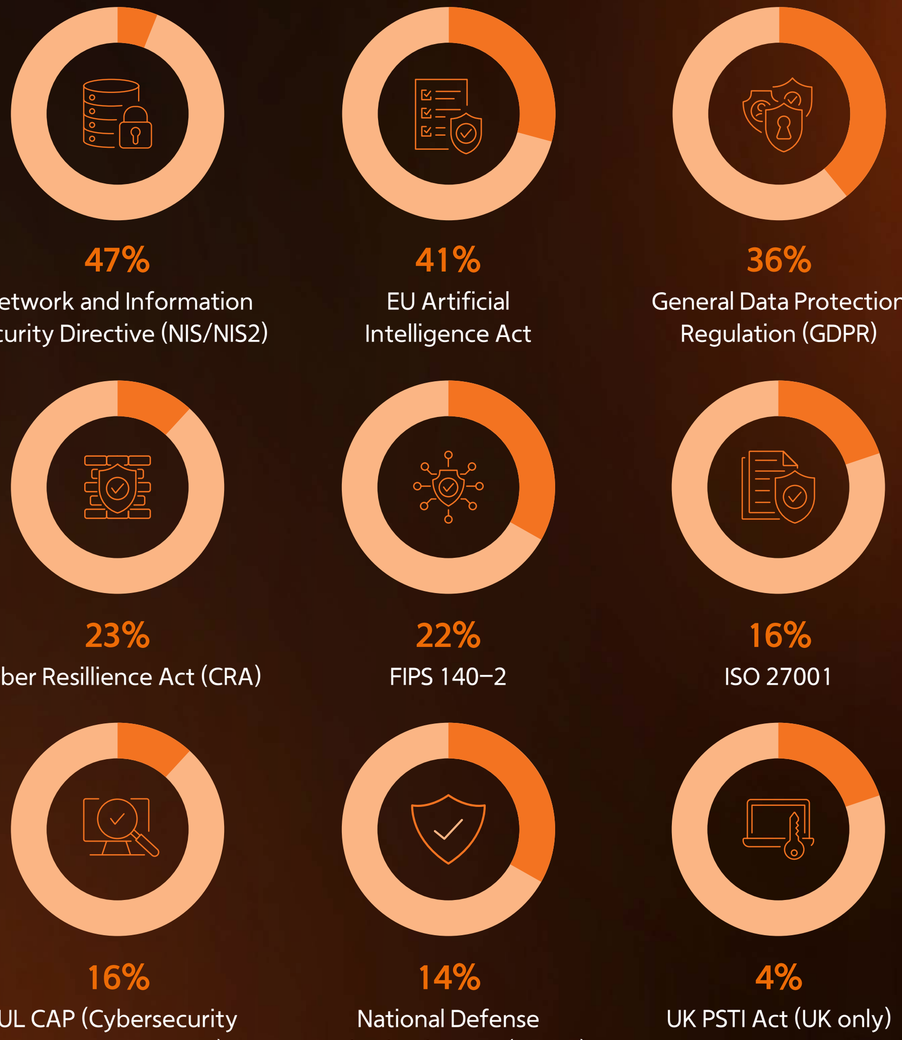
The research shows that many users are unfamiliar with forms of cyber compliance, regulation, or measures of trust. Knowledge of important regulatory frameworks, such as NIS2, GDPR, and the CRA, remains surprisingly low. Less than half (47%) of respondents are aware of NIS2, which came into effect in late 2024, and across the countries surveyed less than one in four (23%) is familiar with the CRA.

Even in larger organisations, where overall awareness of regulations and good cyber practices are somewhat higher (45%), the majority still remain unaware of crucial cybersecurity guidelines. Smaller firms, worryingly, show awareness levels as low as 18%. Given that 60% of small companies go out of business within six months of a cyber–attack[4], this is a knowledge gap that needs to be bridged rapidly.

Sector–specific data reveals that even in data–centric fields like IT and telecommunications, less than one–third (32%) of respondents are informed about critical compliance measures. This gap raises concerns about whether or not cybersecurity is being 'outsourced' within organisations, with security managers and users perhaps assuming that third parties, such as facilities managers or installers, handle compliance. The ambiguity over ownership of cybersecurity responsibilities, particularly in larger companies, may be leaving systems vulnerable to regulatory and security risks.

Only 36% are aware of the General Data Protection Regulation (GDPR)

A clear knowledge gap in cybersecurity best practices – organisations' awareness of key standards and regulation:



[4]"60 Percent of Small Companies Close Within 6 Months of Being Hacked", Cybercrime Magazine, January 2019, last accessed at: https://cybersecurityventures.com/60–percent–of–small–companies–close–within–6–months–of–being–hacked/

NIS2 Directive

The European Union's NIS2 Directive aims to strengthen cybersecurity in a number of sectors across Europe, especially for connected devices such as cameras and sensors. It features stricter requirements for risk management and incident reporting compared to its predecessor, the Network and Information Systems (NIS) Directive of 2016, with more hard-hitting penalties for non-compliance. Over 160,000 companies are predicted to be affected by NIS2, with 15 sectors covered – including video and connected devices.

As it is no longer a member of the EU, the UK falls outside of this legislation, but the UK Government has stated that it is planning its own NIS-equivalent changes in the upcoming Cyber Security and Resilience Bill. Even then, if a UK business wishes to work with European customers, it will need to comply with NIS2, regardless.

> The number, complexity and scale of cybersecurity incidents are growing, as is their economic and social impact
>
> – European Parliament

The Cyber Resilience Act (CRA)

With more smart devices in businesses and homes, the European Commission is looking to ensure an adequate level of cybersecurity in every product used within member states, with regular security updates throughout the product life cycle.
The Cyber Resilience Act, therefore, addresses the cybersecurity requirements for hardware and software products with digital elements available across the EU market. It applies to products that connect to the internet, such as smart TVs, WiFi routers, smart fridges, and video cameras.

Best practice in cybersecurity is not sufficiently promoted

Hanwha Vision's research found that many organisations aren't doing enough to promote best practices for cybersecurity across the company. This is essential in ensuring no weak links (or human error) will create a vulnerability that malicious actors can then exploit.

The research finds that less than four in 10 respondents support teams to better recognise phishing attempts, while less than one quarter (23%) stage mock cyber–attacks to assess and improve system resilience. Additionally, only one in four organisations promote multifactor authentication.

Best practice is in the minority – proportion of organisations that promote key cybersecurity measures:

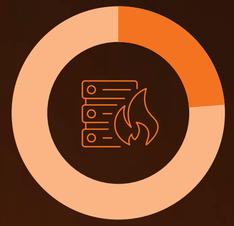
41%
Remaining up–to–date with updates and device firmware

39%
Recognition of phishing and how to report it

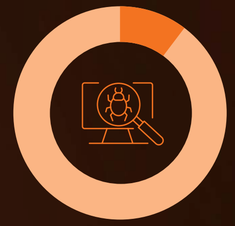
39%
Reminding staff of the risks associated with adding hardware onto a network

39%
Performing regular risk assessments of your buildings, networks and devices

26%
Multifactor authentication



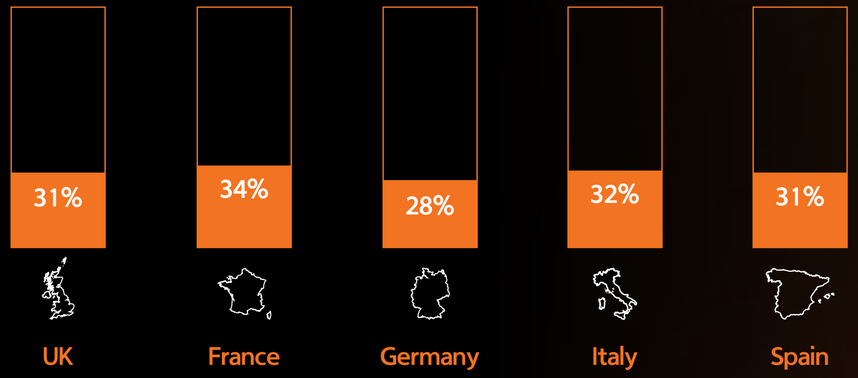
23%
Staging mocked cyber–attacks to assess system resilience



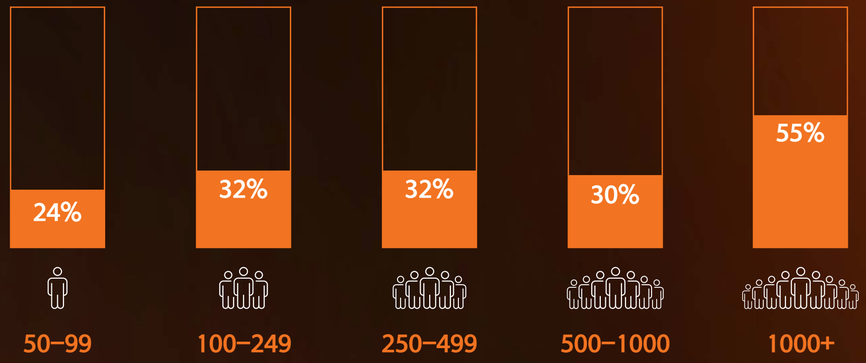
10%
Enabled tampering and defocus detection analytics

Best practice is in the minority – proportion of organisations that promote key cybersecurity measures (by country, organisation size, sector and role):

Country



Organisation size



Sector

Role

The results reveal only marginal differences between countries (28% to 34%) and sectors (27% to 38%) in their promotion of best practices, though larger organisations are more proactive, with 55% promoting sound measures to enforce cybersecurity compared to just 24% in smaller firms. Sector–specific data shows that while industries such as data and telecoms are slightly more engaged, even they fall short of adequate promotion, leaving significant room for improvement.

Again, this lack of promotion could stem from a mistaken belief that security is being handled by other parties, either internally or through outsourcing to facility managers or installers. Or it could be the result of complacency and the (misguided) belief that 'it couldn't happen here'. It might even result from inertia or a preference to maintain the status quo in the belief that it has worked to date.

Organisations therefore need a programme of regular cybersecurity training that reminds employees of best practices, such as firmware updates and using multi–factor authentication. Once the basic processes are in place and followed regularly, more advanced practices such as ongoing risk assessments, penetration testing, and not adding unauthorised hardware to networks can then be promoted.

7 cybersecurity best practices:

- Remaining up–to–date with updates and device firmware.
- Recognition of phishing and how to report it.
- Reminding staff of the risks associated with adding hardware onto a network.
- Performing regular risk assessments of your buildings, networks and devices.
- Multifactor authentication.
- Staging mocked cyber–attacks to assess system resilience.
- The use of strong passwords.

Security systems are not being adequately secured

As seen elsewhere in the research findings, a gap between confidence and action is apparent. The most basic, fundamental steps, such as securing physical access to network devices, enabling 802.1x certificate–based access control, and creating user–level accounts with the least privileges required, are not universally implemented. Then there are more advanced measures, such as using secure cloud for remote access, which are significantly under–utilised.

Even more technical steps—such as disabling guest access, enabling tampering detection analytics, and regularly checking device logs—are adopted by only a minority of organisations.

Specific cybersecurity measures being implemented by firms for video surveillance systems:

6%

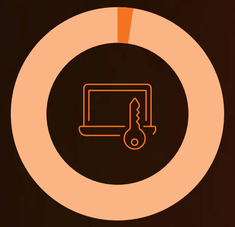
Secured physical access to Network Detection and Response (NDR) and other devices to permitted users only

29%

Enabled 802.lx certificate–based access control

39%

Enabled multifactor authentication



2%

Utilised a VPN or secure cloud for remote access

26%

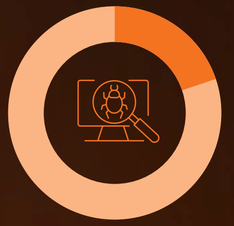
Changed camera /device usernames and passwords

12%

Ensured cameras /devices are running the latest firmware

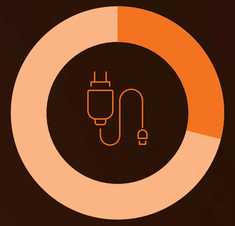
33%

Disabled guest /non–authenticated RTSP access



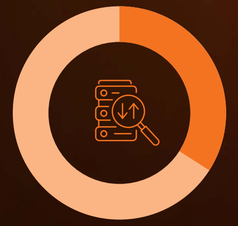
20%

Enabled tampering and defocus detection analytics



29%

Enabled network disconnect detection if using low voltage power

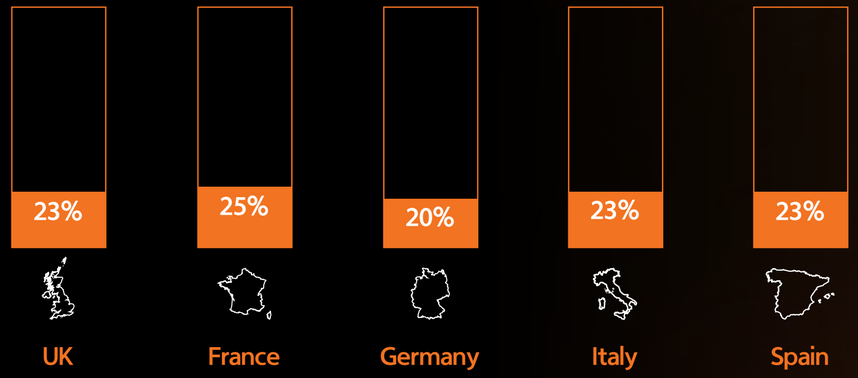


34%

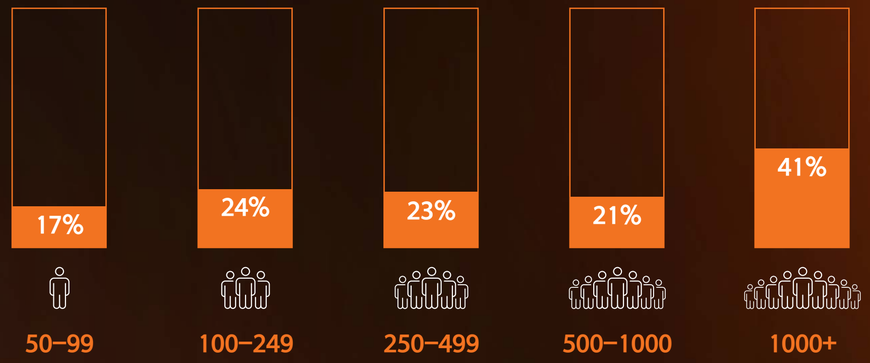
Checked device logs regularly

Proportion of firms implementing key cybersecurity measures for video surveillance systems (by country, organisation size, sector and role):

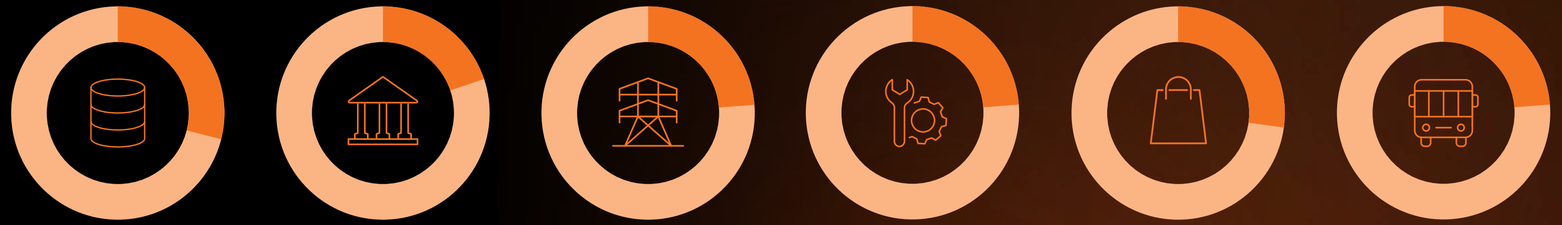
Country



Organisation size



Sector



29% Data Centres & Telecomms

20% Financial Services

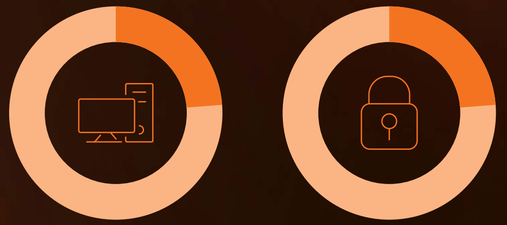
23% Industry (Energy, Mining, Utilities)

22% Manufacturing

26% Retail

22% Transport & Government

Role



24% IT Manager

22% Security Manager

10 video surveillance cybersecurity measures to adopt today:

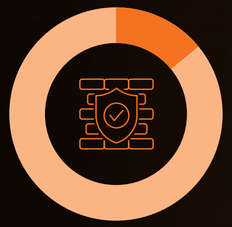
- Secured physical access to NDRs and other devices to permitted users only.
- Enabled 802.1x certificate–based access control.
- Created user–level accounts with least privileges required.
- Utilised VPN for remote access.
- Changed camera / device usernames and passwords.
- Ensured cameras / devices are running the latest firmware.
- Disabled guest / non–authenticated RTSP access.
- Enabled tampering and defocus detection analytics.
- Enabled network disconnect detection if using low voltage power.
- Checked device logs regularly.

The networks on which security systems sit are not adequately protected from cyber–attacks

Responsibility for securing video networks appears to be falling between the cracks of IT and security teams.

The research finds that an IT leader more often than their security counterpart carries out some tasks such as penetration testing and user account blocking. However, security managers more commonly place cameras on a separate network and deploy a VPN on a network. Moreover, an assumption that an installer or other third party has the task of securing network systems can lead to confusion and complacency.

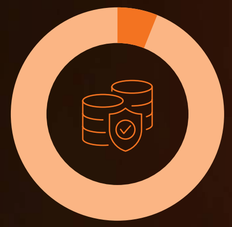
The weak link? The specific security measures implemented by organisations for the network their video system sits on:



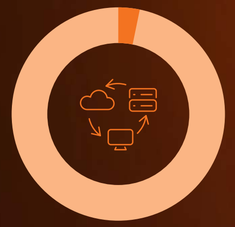
14%
Penetration tested your network for vulnerabilities

31%
Changed default ports and disabled unused ports, services and protocols

31%
Enabled multifactor authentication



6%
Placed cameras on a separate physical network to the corporate /other network(s)

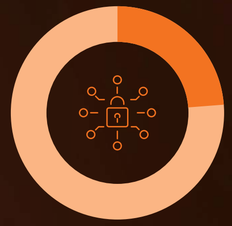


3%
Used a VLAN to keep the security network separate from a corporate /other network(s)

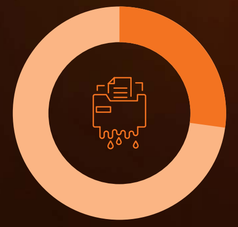
37%
Ensured all devices on the network are running the latest firmware

37%
Enabled IP filtering to restrict access to devices

20%
Enabled user account blocking



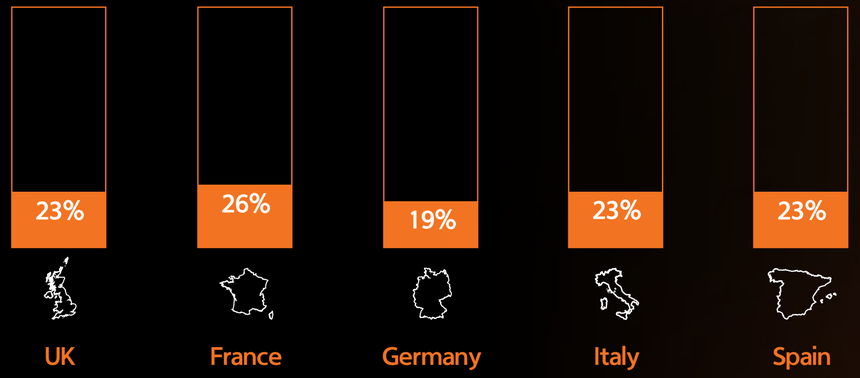
22%
Deployed a VPN on the network



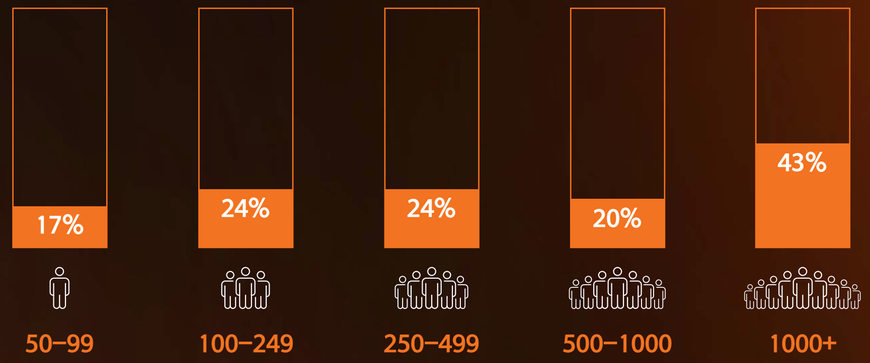
27%
Ensured buffer overflow protection

The weak link? Proportion of firms implementing key security measures for the network their video system sits on (by country, organisation size, sector and role):

Country

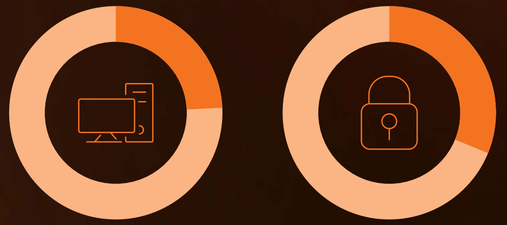


Organisation size



Sector

Role



When two different parties are accountable for cybersecurity, it is essential that communication and collaboration between the two occur regularly and with transparency. All stakeholders share a common objective of safeguarding the organisation against cyber–threats. Regardless of their specific role, all stakeholders share a common objective of safeguarding the organisation against cyber–threats, and have the same goal of protecting the organisation from a cyber–attack. Setting up regular cross–functional meetings, having easily accessible dashboards on video data, and providing ongoing training can help to better connect different departments.

Call for action: one sector that can do more.

The research reveals that financial services is a sector requiring improvement in cybersecurity practices – with only one in five (21%) leaders aware of key cybersecurity regulations such as NIS2, CRA, and ISO 27001. Additionally, just 41% of financial services organisations regularly remind staff of the risks associated with adding hardware to their networks. ENISA estimates that cyber–attacks on banking and financial services in the year July 2023 to June 2024 represent 9% of all incidents, placing the sector in third place behind public administration and transport as key targets of attacks.[5]

In contrast, the top–performing sector in the research is data centres, which more consistently implement a broad range of cybersecurity measures, from installing the latest firmware on hardware to changing default ports and disabling unused ports, services, and protocols.

10 measures to secure your network:

- Penetration tested your network for vulnerabilities.
- Changed default ports and disabled unused ports, services and protocols.
- Enabled multi–factor authentication.
- Placed cameras on a separate physical network to the corporate / other network(s).
- Used a VLAN to keep the security network separate from a corporate / other network(s).
- Ensured all devices on the network are running the latest firmware
- Enabled IP filtering to restrict access to devices.
- Enabled user account blocking.
- Deployed a VPN on the network.
- Ensured buffer overflow protection.

[5] *ENISA Threat Landscape 2024*, p.14.

Avoiding a false sense of security

While more than nine out of 10 (92%) respondents believe their security systems are well–protected, many are failing to implement even basic security practices, such as changing default passwords or updating firmware.

This gap leaves organisations vulnerable to cyber–attacks that could compromise not only video footage and personal data but also broader IT systems, posing serious operational, financial, and reputational risks. A lack of clarity of roles between security and IT worsens this situation.

Key vulnerabilities include a widespread lack of awareness around critical cybersecurity regulations, such as NIS2 and the Cyber Resilience Act, and the inadequate promotion of best practices such as multi–factor authentication and regular risk assessments.

However, these weaknesses offer a valuable framework for all stakeholders in video surveillance, providing them with important lessons.

Operators/users: Must know about and follow best practices that relate to their roles, regularly refreshing their cybersecurity knowledge to keep ahead of new threats.

Security managers: Need to understand their role and responsibilities as it relates to cybersecurity, working closely with IT counterparts to ensure no vulnerability remains.

IT managers: Working alongside security, they must educate other stakeholders (including security) on cyber threats, technologies to mitigate risk, best practices and more.

Installers: Should promote cybersecurity best practices and keep customers updated with new threats or video system features that will increase cybersecurity. They can also assist with their customer's cyber–resilience by only specifying products with security and privacy at the core of product development.

As regulations tighten and cyber–attacks become more frequent, users, manufacturers, and installers must prioritise cybersecurity. The current reality demands action – as every organisation and device is a potential target. The regulatory landscape is growing only stricter, and customers are increasingly expecting rigorously tested and secure products. Ongoing, robust cybersecurity for video surveillance is paramount for every firm, regardless of size or sector. It's simply too important to neglect.

References

1. *Cost of a Data Breach Report 2024*, IBM, July 2024. Last accessed at: https://www.ibm.com/reports/data-breach
2. *ENISA Threat Landscape 2024*, European Agency for Cybersecurity (ENISA), September 2024, p.10.
3. *ENISA Threat Landscape 2024*, p.24.
4. "60 Percent of Small Companies Close Within 6 Months of Being Hacked", Cybercrime Magazine, January 2019, last accessed at: https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/
5. *ENISA Threat Landscape 2024*, p.14.

Hanwha Vision Europe

Heriot House, Heriot Road, Chertsey, Surrey, KT16 9DT, United Kingdom

Tel : +44 1932 57 8100
Fax : +44 1932 57 8101

www.hanwhavision.eu

Updated November 2024

About the Research

The research was conducted online by Research Without Barriers (RWB) between 21st June 2024 and 3rd July 2024. It surveyed 1,154 IT and Security Managers/Directors from organisations with 50+ employees across the UK, France, Germany, Italy, and Spain. Participants represented key sectors, including Data Centres and Telecoms, Financial Services, Industry (Energy, Mining, Utilities), Manufacturing, Retail, Transport, and Government.

Hanwha Vision