Being Cybersecure

Guide to maximizing cybersecurity for surveillance

CONTENTS

INTRODUCTION

Cybercrime is having a greater business impact than ever before. Global spending on security-related hardware, software, and services is forecast to reach $133.7 billion in 2022, according to tech analyst IDC. Meanwhile, the average cost of cyber-crime for an organization has increased to $13 million.

With high-profile data breaches reported in the press almost daily, law enforcement agencies are witnessing new criminal tools and techniques that present new risks for organizations and individuals. These include everything from ransomware at-tacks, to mobile malware, ATM hacking, and digital identity theft on a massive scale.

Amid the boom in cyber-criminal activity, hackers are increasingly targeting organizations' security and surveillance systems alongside other mission-critical network elements.

They typically have one of three key aims.

The first is a basic attack, in which they infect the computer in the camera or NVR, and use those computing resources as part of an internet weapon called a botnet.

Alternatively, they may make a more targeted attack, gaining access to the camera or Network Video Recorder (NVR) in order to see if there is a more useful set of data; a financial database, HR records, and so forth.

Finally, in a very targeted attack, hackers want to get hold of security camera footage and other sensitive operational or end user data. This can then be used to compromise physical security at key locations, to disrupt critical processes, or to damage the organization's assets or reputation in other ways.

Is your surveillance equipment safe?

As the cybercriminals continue to target surveillance systems, the question for or-ganizations is how to protect themselves against malicious attacks, from outside and inside the organization. While many device manufacturers place the emphasis on correct installation, configuration and management, equipment must also be inherently secure to minimize the risk of a systems or data breach.

For this singularly important reason, **the security capabilities and credentials of surveillance manufacturers should always be a primary consideration** for organizations during the selection process for surveillance equipment. But what exactly should manufacturers be doing to protect their customers?

The role of manufacturers in cybersecurity

To ensure that systems, data and other company assets are protected from mali-cious attacks, surveillance equipment manufacturers need to embed secure design and development principles into every phase of the product lifecycle.

A true commitment to security on the part of the manufacturer is usually evidenced by secure design and development processes, as well as in-depth testing to ensure that product vulnerabilities are caught before they go into production. Additionally, the most security-conscious manufacturers provide clear guidelines on best practic-es for device installation, configuration and maintenance to ensure that customers' networks and businesses remain secure – as well as fixing vulnerabilities as soon as they are reported.

In this guide to maximizing surveillance security, we look at several key security issues that can potentially compromise the security of surveillance systems, and consider the role of manufacturers, installers and end customers in addressing them.

While many device manufacturers place the emphasis on correct installation, configuration and management, equipment must also be inherently secure to minimize the risk of a systems or data breach.

HIKVISION: CYBERSECURITY STATEMENT
CYBERSECURITY ASSURANCE FOR VIDEO SURVEILLANCE
By Hikvision CEO Hu Yangzhong

As a world leading video surveillance product supplier, Hangzhou Hikvision Digital Technology Co., Ltd. ("Hikvision") is continually investing in the development of innovative video technologies. In today's challenging environment, cybersecurity risks are ever-present with the potential for data and network breaches. At Hikvision, we believe it is our duty to be vigilant about cybersecurity. We also believe it is our responsibility to provide a cybersecurity assurance system, and to be a resource for our valued customers and the security industry as a whole.

Hikvision is a global, publicly traded corporation, dedicated to commercial success. The company adheres to the highest ethical standards in all of its business practices. Hikvision never, has, does or would intentionally contribute to the placement of "backdoors" in its products. The company will continue to cooperate with unbiased independent professional associations for product safety evaluations.

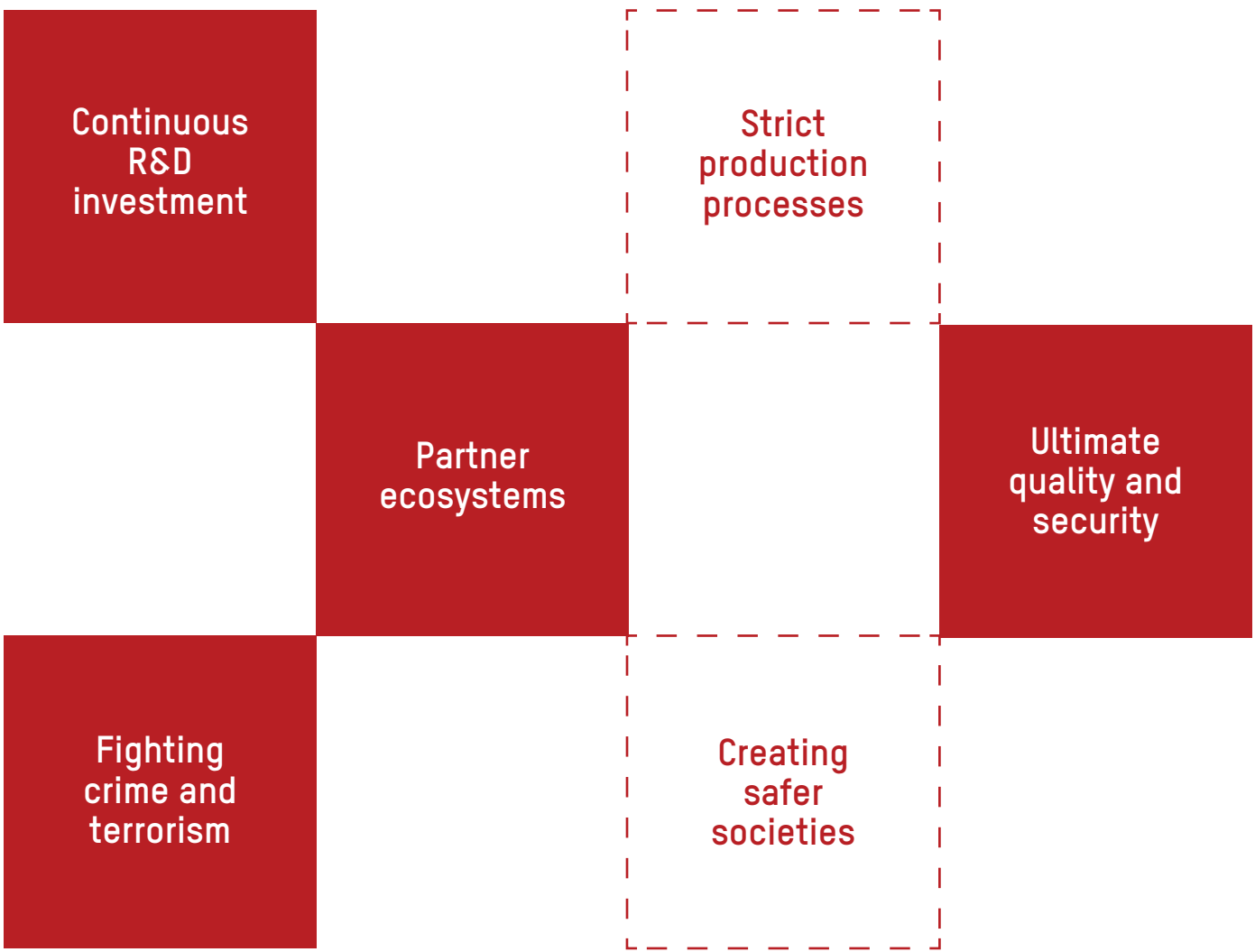
Hikvision complies with all applicable national and regional cybersecurity regulations and follows the best industry practices. We have also established a sustainable and reliable cybersecurity assurance system that encompasses the company's policies, organizational and operational procedures, technology and regulations.

Our Network and Information Security Lab uses the world's top known-vulnerability scanning tools and unknown-vulnerability discovery tools to verify and ensure that Hikvision products meet the industry cybersecurity standards and regulations. Our information security management system is also certified to ISO27001.

Hikvision cybersecurity assurance activities are built into all phases of the product lifecycle, from development and verification, to manufacturing, delivery and service. We are constantly evaluating and enhancing our cybersecurity efforts in order to provide our valued customers with the most reliable, highest quality products.

To further increase our cybersecurity capabilities, Hikvision actively works with customers, partners, competitors, and cybersecurity associations to ensure best practices and to mitigate threats. We will continue to contribute our own expertise and cybersecurity knowledge to industry, wide cybersecurity initiatives.

Hikvision security strategy



Vulnerabilities in product code

Issue 1

Any network-connected device is a potential entry point for hackers and other cybercriminals looking to access confidential information. With millions of lines of code needed for products to operate correctly, there is always a chance that securi-ty vulnerabilities will exist, particularly if manufacturers have no strong strategy in place for "security hardening" their products.

Look for a manufacturer with secure development processes

Another key way that manufacturers can help to reduce code vulnerabilities is by implementing a secure development process for all products. To ensure that products are "secure by design", best-in-class security toolsets should be used, and security planning and testing should be integrated into every aspect of the development workflow. These measures can help to ensure that all preventable code defects are identified at the earliest stage possible, and that they are addressed before they can be exploited by cybercriminals in live surveillance environments.

Assess manufacturer security using third-party sources

There are databases, reports and certifications that assess the performance of sur-veillance manufacturers based on known vulnerabilities and security breaches. By using these sources, organizations can choose a surveillance manufacturer that is able to identify and react to emerging security threats.

One such source is the Common Vulnerabilities and Exposures database, which lists security events for a range of devices and manufacturers. In addition, those ven-dors with UL source code certification can provide assurances to their customers that their network-connectable products and systems have been assessed for soft-ware vulnerabilities and weaknesses, malware, and security controls.

With millions of lines of code needed for products to operate correctly, there is always a chance that security vulnerabilities will exist, particularly if manufacturers have no strong strategy in place.

"Hikvision software incorporates a range of features that enhance cybersecurity. Code limits where network traffic can originate, reducing the risk of an attack, and it eliminates easy-to-hack default passwords. Users can also change default ports to make IP appliances less "visible" on the network and less prone to attack, and additional software tools make firmware and software updates easier, further enhancing device and network security."

Dr Wang Bring, Director of Network and Information Security Laboratory, Hikvision

Inadequate vulnerability testing

Issue 2

Hackers can gain unauthorized access to surveillance systems via a number of routes, from physical tampering, to remote access to, to malware infection. When it comes to ensuring that surveillance cameras or other network-connected devices are as secure as possible, vulnerability testing, and retesting, is of critical importance.

Cover all the vulnerability bases

Security testing for surveillance devices should reflect real security risks, from physical tampering to unauthorized remote access. To ensure that surveillance systems are as secure as possible, the best equipment manufacturers work with specialist testing partners who "think like hackers", probing and testing every aspect of the device's physical and logical security features.

Security testing carried out by, and on behalf of,manufacturers, should ideally include:

• **Hardware testing**
which looks at the physical security and internal architecture of the device, o determine the "attack surface". Testers will usually recommend products that include hardware anti-tampering features and the ability to re-configure hardware to bypass features that may pose a risk to the organization (such as authentication or traffic intercept features).

• **Software vulnerability testing**
which security-tests the user interface and firmware/OS. By mapping the software and looking at possible attack vectors, testers can uncover known vulnerabilities before devices are deployed in live environments. They can also assess the effectiveness of any in-build security features that protect against command line access or shell access, and much more.

• **Protocol testing**
which tests communications to and from the device, and assesses the effectiveness of encryption and other cryptographic security features over those protocols.

• **Device endpoint testing**
which looks at how the device configuration can affect the security of the device's applications and whether application data stored on the device is secure.

• **Penetration testing and reporting**
which includes in-depth analysis of all potential security threats and documented attack chains that show how they can be addressed and mitigated.

Ongoing testing to address emerging threats

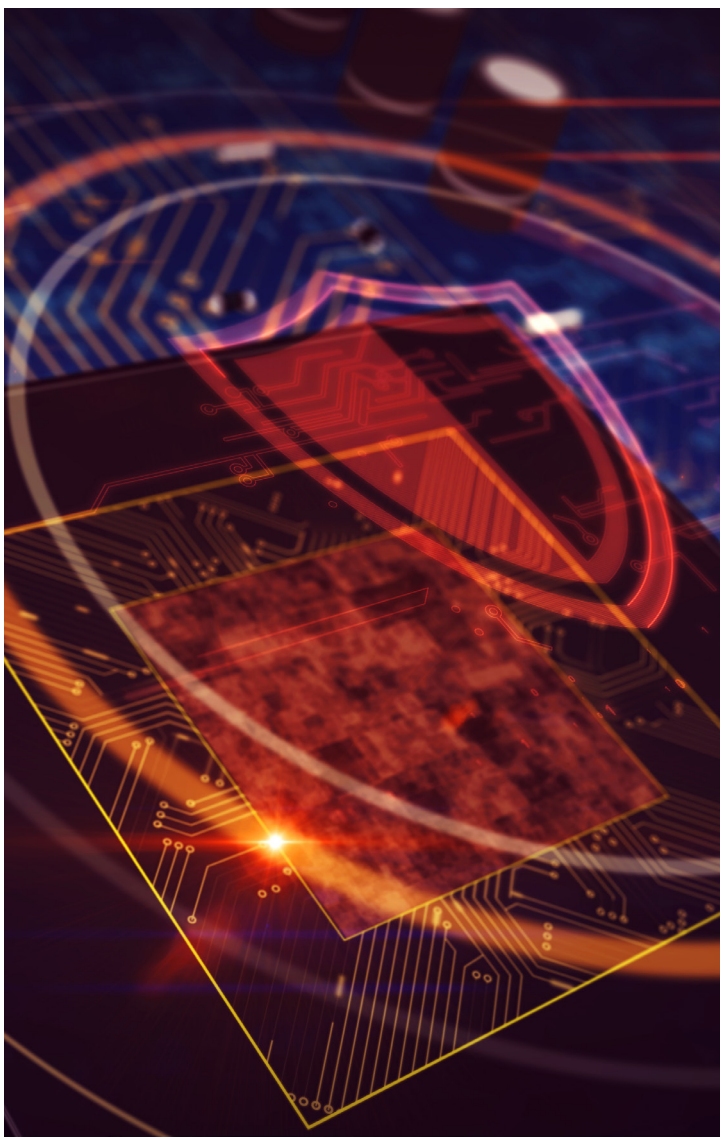
Cybercriminals and cybersecurity threats are constantly evolving. As a result, surveillance devices should be tested on an ongoing basis to ensure they can meet emerging security challenges.

For this reason, the best surveillance equipment manufacturers test products on an ongoing basis as part of an annual security review. This is not only a matter of best practice: it also enables manufacturers and their customers to comply with regulations.

Regular security testing also ensures that any new device features are secure, and that no new risks are introduced as a result of recent product development work. As such, ongoing testing ensures that new product developments actually increase device security – and never diminish it.

The best equipment manufacturers work with specialist testing partners who 'think like hackers' to probe and test every aspect of the device's physical and logical security features.

Hikvision works with specialist security testing partners who assess our products against more than 100 security requirements to minimize the risk of a security breach. Our testing partners review our hardware and software for any potential vulnerabilities, helping our customers to stay safer. Our products are also tested on an ongoing basis, ensuring that the latest enhancements meet the highest security standards.



Taking a collaborative approach to surveillance security

Issue 3

The security – or otherwise – of a network-connected device is never enough to protect against a network intrusion or data breach. Instead, organizations need to take an end-to-end view of network security, ensuring that all components are as secure as possible.

To achieve this high level of network security, organizations need surveillance systems that integrate seamlessly with other secure network infrastructure, including servers, routers, switches, and more. To deliver this, and to maximize end-to-end security, the top surveillance manufacturers are building industry partnerships with other security-conscious infrastructure and network providers, as well as business and cyber-security consultancies.

Why are security partnerships important?

By partnering with network security experts, surveillance manufacturers can ensure that their products are protected from all known vulnerabilities and attack methods. Additionally, it becomes possible to gain a deeper understanding of the potential cybersecurity risks impacting organizations, and to make changes to products to increase protection against unauthorized remote access and other threats.

Critically, partnerships with network security experts help surveillance manufacturers to counter emerging cybersecurity threats. In particular, the global expertise and resources of security partners can help surveillance manufacturers evolve their products and increase security as IoT and other new technologies that potentially pose new risks for enterprises.

Hikvision's partnerships with leading security experts

Hikvision partners with some of the world's leading network security experts and consultancies to evolve our products and protect our customers. By sharing their cybersecurity data and technologies with us, they help us to maximize device security, and to provide current, accurate cybersecurity advice for installers and end users of our products.

As well as focusing on device security, we partner with business process engineering and consultancy leaders to help us deploy cybersecurity industry best practices across all our teams and processes. This has helped us to boost our cybersecurity capabilities and to evolve our processes and products to respond rapidly to emerging cyber threats.

To combat cybersecurity risks and protect our clients, Hikvision is partnering with Brightsight, the largest security lab in the world.

"Hikvision takes cybersecurity concerns with the utmost seriousness and takes action every day to ensure that our products are not only innovative, but they meet the highest standards of cybersecurity best practices. Brightsight is a well-known cybersecurity lab globally, and our partnership will help us to strengthen the cybersecurity of all of our products."

Dr Wang Bring, Director of Network and Information Security Laboratory, Hikvision

Closing network and physical security loopholes

Issue 4

Installed and managed incorrectly, any network-connected device is a potential access point for hackers and security cameras are no exception. For this reason, surveillance manufacturers have a duty to work closely with installers and end-customers, ensuring that products are always deployed and used in the safest possible way.

Effectively communicating security best practices

The most effective way a surveillance manufacturer can help customers to close security loopholes is by outlining and effectively communicating cybersecurity best practices. Manufacturers, for example, should provide clear, concise information and guidance on a range of cybersecurity topics, including:

- **Correct device installation and configuration** to optimize network security

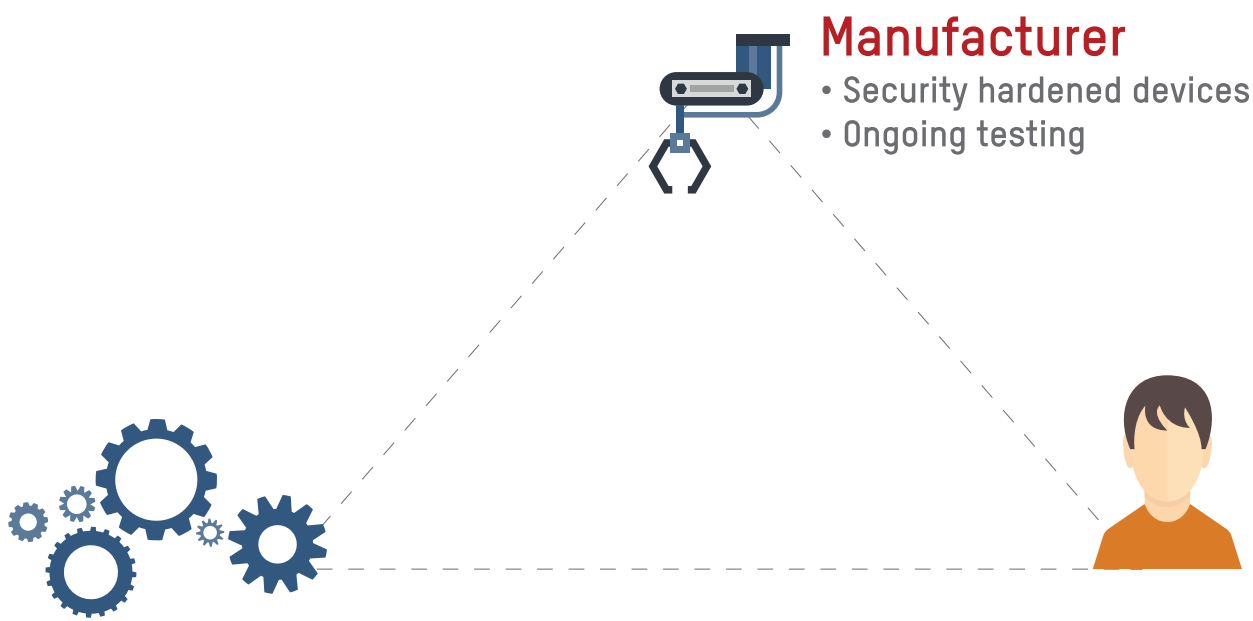
- **Maximizing device security** ensuring that any defaults are changed, setting user permissions and keeping firmware up to date

- **Building an effective DR plan** based on clear roles, responsibilities and actions in the event of a security breach.

This kind of information should be easily accessible on a manufacturer's website, with multi-media content such as videos making it as clear and easy-to-understand as possible. Additionally, a manufacturer's customer facing support team should be able to provide cybersecurity advice and guidance as required to ensure the safest possible installation and operation of devices in the network.

Surveillance manufacturers have a duty to work closely with installers and end customers, ensuring that products are always deployed and used in the safest possible way.

The Cybersecurity trumvirate



Keeping up with emerging threats
Issue 5

In terms of enterprise networks and surveillance systems, what's secure today may not be secure tomorrow. In the rapidly shifting cybersecurity landscape, only the most innovative, responsive manufacturers can protect their customers effectively against malicious attacks and systems breaches.

Responding quickly to reported vulnerabilities

In spite of secure development processes and multi-faceted testing programs, any device could have a security vulnerability. Once a vulnerability is discovered by a white hat hacker, an installer or a user, however, manufacturers must react extremely quickly to communicate to customers and the public, encouraging the prompt installation of fixes to greatly reduce the risk of attack against those devices.

Making firmware updates easy

Devices that are not updated can dramatically increase security risks. While the responsibility of updating cameras ultimately rests with customers, however, manufacturers need to make the process as fast, easy and painless as possible.

Getting serious about security R&D

Ultimately, a surveillance manufacturer's ability to respond to emerging cyber threats depends on the company's ability to innovate. By investing in security R&D in collaboration with security partners, innovative manufacturers can anticipate future risk trends and invest in development projects that keep their products one step ahead of the cyber criminals.

Hikvision's long-term cybersecurity commitment

Hikvision is constantly working to ensure that our products and processes meet the highest cybersecurity standards. Here are some milestones from our cybersecurity mission:

2014: Hikvision set up our Security Response Center to help clients reduce cybersecurity risks and react quickly and effectively in the event of attacks

2015: Hikvision established our Information Security Lab to enhance security in the IoT industry

2016: HikConnect platform launched, which to further bolsters cybersecurity, as well as delivering security enhancements such as email encryption and tools that prevent anonymous log-ins

Present: Hikvision offers mature tools for protocol security testing, vulnerability scanning, third party penetration testing and mainstream anti-virus integration. These capabilities are wrapped in a set of rules that deliver thorough security testing at every stage of deployment and operations.

In terms of enterprise networks and surveillance systems, what's secure today may not be secure tomorrow. In the rapidly shifting cybersecurity landscape, only the most innovative, responsive manufacturers can protect their customers effectively.

Tips

The Hikvision online Security Center

To help our customers maximize device and network security, Hikvision provides a wealth of information and cybersecurity best practices via our online Security Center. This also provides a single point of contact with Hikvision where our customers can report any issues or potential security vulnerabilities, and download the latest security patches.

Visit the Security Center **here.**

Top cybersecurity best practices

1) **Keep appliances current**
This requires organizations to update software and firmware regularly and to report any potential security vulnerabilities to the device manufacturer as soon as possible.

2) **Choose secure passwords**
If possible, all passwords should be at least 8 characters long, with a com-bination of letters, numbers, and special characters. Everyone should be assigned their own username and password to ensure auditability and ac-countability. In addition, passwords must not be re-used across multiple systems.

3) **Set access permissions**
Each user account should only be given the authority to access the re-sources required to fulfil their specific responsibilities

4) **Keep good records**
Every transaction that occurs on the appliance needs to be logged so that there is an auditable activity record for forensics in the event of a security breach. This record keeping can be critical to detecting and responding to security events.

5) **Use a firewall**
Stating the obvious, this should be deployed between your IT assets and the Internet. Additionally, you should place a firewall between your video surveillance network and other systems on your network to provide an additional layer of security.

6) **Increase physical security**
When possible, put network and IT assets behind locked doors to limit un-necessary access.

7) **Use password lock-out features**
This informs you about invalid login attempts, and prevents brute force password cracking. If you set up alerts on the password lock-outs, it will al-so give you visibility into any attacks on the network or devices.

8) **Build an action plan**
This ensures the right people are informed in the event of a security breach and swift action is taken to minimize the negative impact.

10. **Be aware**
Keep up to date with security trends and issues

For more in-depth information about security hardening your network and surveil-lance infrastructure, read the Hikvision Security Hardening Guide **here.**

LAST WORDS

Ensuring that surveillance systems are secure and protected against malicious attacks is a shared responsibility. Installers must follow strict guidelines while deploying and configuring systems, as well as consulting with end customers to ensure that their surveillance equipment is as physically secure as possible. End users also need to be extremely security conscious, ensuring that passwords are as strong as possible and that user permissions restrict unnecessary access to surveillance systems.

All of this good work can help to maximize network security, but surveillance devices must also be security hardened to minimize the risk of malicious attacks. This responsibility falls squarely at the door of manufacturers, who need strong strategies and processes for "security hardening" their products throughout every stage of their lifecycle, from design and development, to configuration, testing and ongoing maintenance.

For these important reasons, an organization's choice of surveillance manufacturer, and equipment, really does matter. Any selection process should be based on a thorough evaluation of the manufacturer's security hardening processes, including secure development and testing. Additionally, customers should look at how manufacturers support their customers to maximize security, both in terms of fixing reported vulnerabilities, and in terms of communicating security best practices for device installation, configuration and maintenance.
Any additional security capabilities offered by manufacturers -eliminating the use of factory-set passwords are an added bonus. After all, these kinds of technologies separate manufacturers who are serious about security, from those with less well-developed security capabilities.

Take the next steps to a more secure surveillance infrastructure

If you would like to discuss any of the topics covered in the ebook, or for more information about how Hikvision security hardens products and supports our customers with a wealth of security resources and expertise, please contact us at:

Hikvision Europe
Dirk Storklaan 3
2132 PX Hoofddorp
The Netherlands
T +31 23 5542770
info.eu@hikvision.com

An organization's choice of surveillance manufacturer, and equipment, really does matter. Any selection process should be based on a thorough evaluation of the manufacturer's security hardening processes, including secure development and testing.

Hikvision Europe
Dirk Storklaan 3
2132 PX Hoofddorp
The Netherlands
T +31 23 5542770
info.eu@hikvision.com

Hikvision France
6 rue Paul Cézanne,
93360 Neuilly-Plaisance
France
T +33 (0)1 85330450
info.fr@hikvision.com

Hikvision Poland
The Park, Office Building A
Krakowiaków 50
02-255 Warsaw, Poland
T +48 22 4600150
info.pl@hikvision.com

Hikvision Czech
BETA Building, Vyskocilova
1481/4, Prague 4
Czech Republic
T +42 29 6182640
info.cz@hikvision.com

Hikvision Germany
Flughafenstr. 21
63263 Neu-Isenburg
Zeppelinheim, Germany
T +49 69 401507290
sales.dach@hikvision.com

Hikvision Romania
Splaiul Independentei street
291-293, Riverside Tower, 12th
floor, 6th district,
Bucharest, Romania
T +31235542770/988
marketing.ro@hikvision.com

Hikvision Belgium
Neringenweg 44,
3001 Leuven, Belgium
T +31 23 5542770
info.bnl@hikvision.com

Hikvision Hungary
Budapest, Reichl Kálmán u. 8,
1031, Hungary
T +36 1 323 7650
info.hu@hikvision.com