SourceSecurity.com®

Technology Report

Meeting the Cybersecurity Challenge of IP Video Systems

About the author

An experienced journalist and long-time presence in the U.S. technology marketplace, Larry Anderson is the Editor of leading digital publication SourceSecurity.com. Mr. Anderson is the website's eyes and ears in the fast-changing security sector, attending industry and corporate events, interviewing leaders and contributing original editorial content to SourceSecurity.com. He leads a team of dedicated editorial and content professionals, guiding the editorial roadmap to ensure that SourceSecurity.com and SourceSecurity.com US Edition provide the most relevant content for industry professionals. From 1996 to 2008, Mr. Anderson was editor of *Access Control & Security Systems* magazine and its affiliated websites. He has written many articles for and about some of the largest companies in the security industry and has received numerous awards for editorial excellence. He earned a Bachelor of Arts in Journalism from Georgia State University with a minor in Marketing.

Cybersecurity at a Glance

Meeting the Cybersecurity Challenge of IP Video Systems

Today we call it the video surveillance market, but for many years (and still in some places) it has been known as CCTV – closed circuit television. The keyword is "closed," as in separate and distinct from other systems and from the rest of the world. Closed implies protected, safe and out of reach.

However, in today's networked world, systems are far from closed. Video is data and, as such, is essential to a business. Beyond security uses, video data today also contributes to other aspects of an organization, from providing business intelligence to making operations more efficient. End users want to be able to access video from anywhere – from their computers, laptops, tablet devices, and even their smart phones. A cost of video becoming more useful and more available is that video surveillance systems are no longer closed – and, unfortunately as a result, no longer as safe.

To make video available when and where it is needed, Internet protocol (IP) cameras and other system components connect to a network and often to the Internet. The components of IP systems – cameras, network video recorders (NVRs), digital video recorders (DVRs) and other equipment – are appliances on that network. Any connection to the Internet comes with risks, specifically cybersecurity risks that cannot be fully eliminated. The challenge of cybersecurity cannot be "solved." Rather, the risks can only be managed.

This **SourceSecurity.com Technology Report** will look at how cybersecurity risks of video surveillance systems can be minimized, and highlight the role manufacturers, installers/integrators and end users should play to make IP video systems as safe from cyber-attack as humanly possible. Manufacturers, in particular, are stepping up to drive the industry's efforts, and Hikvision USA is a leader in educating the market to address cybersecurity threats.

> *Manufacturers, in particular, are stepping up to drive the industry's efforts, and Hikvision USA is a leader in educating the market to address cybersecurity threats.*

A cost of video becoming more useful and more available is that video surveillance systems are no longer closed – and, unfortunately as a result, no longer as safe.

Waking Up to Cybersecurity Risks

In addition to its high profile in news reports every day, cybersecurity has garnered attention from top U.S. government officials, including the President.

"*Cybersecurity is a top priority for me, for the President, and for this Administration*," says Jeh Charles Johnson, U.S. Secretary of Homeland Security.

Cybersecurity threats are costly, too. Worldwide, it has been estimated that cybercrime costs businesses $365 to $575 billion each year. For example, the Carbanak cybersecurity attack on financial institutions in 2015 enabled a hacker group to steal more than $500 million by using phishing emails to introduce malware that provided illegal access to money in various ways.

Potentially anyone who has access to the Internet can commit a cybercrime, which might take a variety of forms including viruses, malware, bots, or exploitation of software vulnerabilities. If someone wants to spend enough time and effort, they can find a way to get onto any device attached to the Internet.

Hackers can access computers (including embedded systems like those used in IP video surveillance systems) remotely and leverage their computing power for nefarious goals. For instance, hackers have been known to install "bitcoin miner" malware that searches the Internet to "mine" and steal the virtual currency to send it to someone else. Even embedded systems must close gaps to prevent such invasions.

And it's a global problem, too. Not only do threats come from all over the world, but so do the solutions. In fact, many top virus protection firms are located across the globe. Like IP video cameras, cybersecurity protection is clearly a global business.

"*The reality is we live in an interconnected, networked world,*" Johnson says. "*Cybersecurity must be a balance between the basic security of online information and the ability to communicate with and benefit from the networked world.*"

It's impossible to predict when a cyber-attack might occur. Cybersecurity professionals know that the second you think you're not vulnerable, you are. It's a never-ending game of chess, or cat and mouse, between the designers of malware, viruses and other cybersecurity threats and those tasked with protecting against them. Companies who train their employees to handle cyber-attacks appropriately spend 76 percent less on security events when attacks occur, according to the 2014 U.S. State of Cybercrime Survey.

As IP video systems increasingly leverage the power of the Internet, the video surveillance market must address the delicate balance required to make video data both easily accessible and safe.

Demonstrating Leadership on Cybersecurity

The time is now to address the impact of cybersecurity threats on the IP video market. In the case of video surveillance systems, the main motives of cyber-attackers are usually to either cover up video evidence of crimes or to gain access to video that should be private.

"The use of video surveillance is growing across North America, not just for safety and security but for operational purposes as well. As it becomes more widespread, it's important for users to understand the risks as well as the benefits," explains Bob Germain, Director of Product Management for Hikvision USA. "*Hikvision has a strong commitment to educate our dealers and end users about best practices for cybersecurity as it pertains to video surveillance.*"

"*We have established a special task force at our headquarters, the Network and Information Security Lab,*" Germain adds. "*They are responsible for setting the company's security standards, performing security evaluations and testing, and responding to security issues if they arise. We also have partnerships with third-party security data and analytics companies, which perform ongoing penetration tests and vulnerability assessments of our products.*"

"*We firmly believe that manufacturers, security installers, and end users must work together to ensure the greatest level of cybersecurity possible,*" Germain says.

Hikvision has worked to increase cybersecurity by eliminating the use of default passwords, and by providing flexibility to change default ports to make IP appliances less "visible" on the network and, therefore, less prone to attack. By embracing third-party testing, the company seeks to find any cybersecurity vulnerabilities before they can be exploited. Hikvision's software limits where network traffic can originate. A variety of software tools make firmware and software updates easier, and the Hikvision website's "Security Center" provides cybersecurity information and tools for integrators and end users.

"*Once an item or video appliance is on the Internet, it is vulnerable*," says Joe Coe, Sales Engineer for Hikvision USA's Northern California region. "*However, there are simple best practices that can help*." Coe is an expert with 20-plus years of experience providing network security support for the telecommunications industry and the Federal government. He was the network security manager for three Olympics Games, in Atlanta, Salt Lake City and Sydney. He shares his extensive knowledge of cybersecurity with Hikvision's customers.

Hikvision has a strong commitment to educate dealers and end-users about best practices for cybersecurity as it pertains to video surveillance.

How Vulnerability Testing Ensures Cybersecurity of Products

Vulnerability testing is part of any holistic IT security program. Often, manufacturer companies like Hikvision will test products prior to releasing them or as part of an annual security review. Additionally, compliance regulations such as the Payment Card Industry Data Security Standard (PCI DSS) require regular penetration testing.

As with all embedded devices that could pose a risk if compromised, it is imperative to conduct a vulnerability test on IP video systems to ensure that the implemented security controls are effective at mitigating risk, says Andrew Whitaker, Senior Manager, Global Services, of Rapid7, a provider of security data and analytics solutions.

Once testing is completed, Rapid7 encourages its clients to conduct remediation tasks and retest. The retest will confirm that vulnerabilities are adequately remediated and that any new security controls do not introduce additional risk.

Whitaker notes that some of the most common vulnerabilities facing IP video systems include:

- Shell (remote command line) access that could allow sensitive information disclosure (e.g., accounts, encryption keys), the ability to spy on camera feeds, and/or leveraging the shell access to launch further attacks on a network.
- A malicious actor that attacks the hardware with a UART (universal asynchronous receiver/transmitter) connection to gain command line (CLI) access; this may reveal hard-coded encryption strings or memory vulnerabilities that could allow for remote code execution.
- User interface vulnerabilities that allow for unauthenticated access to view live video feeds.

These vulnerabilities can be addressed in a number of ways that vary significantly from manufacturer to manufacturer. Common mitigation techniques, however, include adding tamper-proof hardware controls, input validation, output encoding, memory protections, and strengthening cryptographic implementations.

Rapid7's testing methodology for IoT embedded devices, such as Hikvision's cameras, revolves around demonstrating the real world risk facing those devices. This includes testing the user interface, the underlying software/firmware, and the hardware itself. By using the same tactics and tools that a malicious attacker might use, Rapid7 provides insight into the risk facing companies like Hikvision, says Whitaker.

Rapid7's testing methodology includes the following:

- **Reconnaissance and Enumeration, which includes a blackbox assessment of the device and network transmissions.** Rapid7 maps device interfaces to determine possible attack vectors and will enumerate listening services. Then Rapid7 leverages open source intelligence (OSINT) to search for any public information that may lead to previously disclosed vulnerabilities related to the device or services running on the device.
- **Hardware Testing, which looks at the physical security and internal architecture of the device.** Rapid7 examines internal components to determine the breadth and depth of an attack surface. This may include component indication, firmware extraction, indication of test points, reconfiguring the device's hardware to bypass authentication, intercept traffic, and/or inject commands that may pose a significant risk to an organization and its clients.
- **Protocol Testing, which focuses on testing the communications to and from the device.** This includes testing the cryptographic security of encrypted transmissions, the ability to capture and modify transmissions of data, fuzzing of the communication protocols. Rapid7 then assesses the security of communication protocols in order to determine the risk to an organization and its clients.
- **Firmware Analysis, which focuses on extracting and examining the content of the firmware.** Rapid7 reviews firmware content in an attempt to discover backdoor accounts, Injection Flaws, Buffer Overflows, Format String and numerous other vulnerabilities. This process generally includes upgrading various device firmware to protect against vulnerabilities.
- **Device Endpoint Testing, which looks at how the device configuration can affect the security of the application and how the application stores data on the device.** Rapid7 uses a variety of tools to perform testing of device endpoints. Rapid7 will intercept traffic and manually review the requests and responses to identify vulnerabilities with endpoints the device communicates with. The endpoints will be reviewed for common vulnerabilities such as: Command Injection, SQL Injection, Buffer Overflows, Information Leakage, Access Escalation, Insecure Communications, and others.
- **Root Cause Analysis and DREAD Reporting, which is Rapid7's method for compiling the results of the penetration testing and building comprehensive findings for all issues found.** Rapid7 will provide analysis and reporting of each identified risk with documented attack chains and proof-of-concepts (PoC.) [DREAD is a risk-assessment model that encompasses five categories: Damage, Reproducibility, Exploitability, Affected Users and Discoverability.]

Best Practices for Cybersecurity

Making smart choices about the cybersecurity of video surveillance systems will help integrators and end users more effectively protect the valuable assets they are already guarding with physical security. Coe lists several best practices for video surveillance system cameras, NVRs and other components, which are similar to best practices for any appliance connected to the Internet.

Keep firmware and software on video appliances up-to-date: As manufacturers find cybersecurity issues, they create fixes and patches to address those issues and prevent cyber-attacks. However, a patch to fix a cybersecurity vulnerability of an installed IP surveillance component is ineffective unless it is downloaded to the device. Therefore, end users and their designated integrators/installers must be vigilant to update firmware and software. Updating doesn't have to be a complicated process, and the alternative is a much greater risk. Due diligence is required, both to report any issues and to implement updates to solve them.

Assign user names and passwords: Not changing user names and passwords from the default settings is one of the major vulnerabilities of video cameras. The issue recently came to light with "nannycams" – some websites even created links to cameras in private homes to demonstrate how easy it was to access private video. The increased attention led more manufacturers to address the problem of default passwords. (Hikvision and some other manufacturers have eliminated the use of default passwords to ensure a basic level of security.) In some cases, end users don't know about the option to change a default password; in other cases, the problem is complacency.

Choose passwords that are difficult to guess: Hacker applications can guess many simple passwords easily. It's better to choose a password that is difficult to guess. Passwords should be at least eight characters long, and combine upper/lower case alpha characters with numbers and symbols. Everyone should be assigned their own username and password, and passwords for mission-critical operations should be changed at least every 90 days.

Use password lock-out systems: If there are several unsuccessful log-in attempts, a system component should lock out the user and provide a notification to the system administrator or someone else in the organization who can act quickly to address the situation. Forgotten passwords can be a hassle, but having to reset a password is a small price to pay for additional cybersecurity. Putting processes in place to address such situations is a basic requirement of an effective cybersecurity system.

Limit access only to necessary users: Each user account should only be given the authority to access the resources required to fulfill his or her specific responsibilities. Every transaction that occurs on an appliance should be logged so that there is a record for forensics later. Keeping IP video surveillance systems safe involves authentication, authorization and accounting. All appliances should implement these functions.

A patch to fix a cybersecurity vulnerability of an installed IP surveillance component is ineffective unless it is downloaded to the device.

Track who accesses appliances: Anytime anyone interfaces with an appliance, their log-in information should be captured along with the MAC address they are using. Use of a user name and password not only restricts access to a device, but also ensures accountability for operators, whose involvement with the system is clearly documented. (Hikvision has the ability to create up to 50 user accounts on its appliances.) Authorization ensures only operators who have the required credentials can perform specific tasks. For example, a security officer whose job is to watch video screens should not be authorized to delete or copy video. Accountability stems from the capture of "events" related to the video system – including the operator's user name and password. Information is captured to provide forensics to validate later what took place.

Install a firewall appliance between IT assets and the Internet: The basic need for a firewall applies just as much to IP video as to any other IT system. At the very least, a system should use NAT at the Internet gateway. NAT (network address translator) involves virtualization of IP addresses, which helps to improve security and decrease the number of IP addresses an organization needs. The more mission-critical the data, including video surveillance data, the better the firewall should be. Firewall appliances, located between any IT assets and the Internet, are a barrier to keep destructive elements out of a network or specific device. IP video surveillance manufacturers provide instructions to walk integrators/installers and end users through how to set up firewalls. Hikvision IP systems include software that can limit where traffic can originate, right down to the MAC address.

Resources to Help with Cybersecurity

There are resources to help guide an organization's management of cybersecurity risks, most prominently from the National Institute of Standards and Technology (NIST) and the U.S. Department of Homeland Security.

NIST defines cybersecurity as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."

NIST has developed a framework to provide voluntary guidance, based on existing standards, guidelines, and practices, for critical infrastructure organizations to better manage and reduce cybersecurity risk. The NIST Framework Core (**http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf**) consists of five concurrent and continuous functions:

- **Identify.** Understand how to manage cybersecurity risks.
- **Protect.** Put safeguards in place to protect assets and deter threats.
- **Detect.** Monitor continuously.
- **Respond.** Devise an action plan to react promptly in case of a cyber-attack.
- **Recover.** Maintain resilience and recover capabilities after a cyber-breach.

In addition to helping organizations manage and reduce risks, the framework was designed to foster communications about risk and cybersecurity management among both internal and external organizational stakeholders.

The Department of Homeland Security (**http://www.dhs.gov/topic/cybersecurity**) offers a wealth of resources to guide businesses to minimize cybersecurity risks, to promote information sharing, and to develop new and innovative solutions to cybersecurity problems.

Don’t use default ports (“security through obscurity”): In the Ethernet infrastructure used for IP video systems, information (including video) travels on specific ports, or logical pathways. There are thousands of available ports, including 1,024 that are defined, and also available ports between 1,024 and 65,099. Network traffic can travel on any port, but appliances such as network cameras arrive from the factory programmed for a default port. Information about the default ports of major video manufacturers is easily available and advertised on the Internet. A potential hacker could therefore identify from the port being used the brand of the camera or other component. They can also find cameras based on which ports they are using. The combination of ports being used provides clues to hackers, allows them to make generalizations, and gives them a starting point to enter a system. Therefore, integrators/installers should choose cameras and other equipment that allow them to change the port(s) being used. Many available cameras do not offer this option (although Hikvision cameras do). Choosing an uncommon port creates an extra step for hackers. It makes it more difficult for hackers to identify camera brands and to find cameras among the many available ports, thus providing an additional layer of cybersecurity. Another best practice is to “lock down” (not allow access to) all ports except those being used.

Put video surveillance system assets behind closed doors: Any hacker with physical access to a system component can almost certainly hack into it. Therefore, it is critical that integrators/installers and end users locate equipment behind locked doors. Schools should not have NVRs sitting on the principal’s desk. Doors should not be propped open. Cleaning crews should not be allowed access to equipment. Instead, all equipment should be in an equipment room, locked away separate from other equipment (not in a telecom closet, for example). Physical access also opens the possibility of someone unplugging a system component and walking away with it. Therefore, video should always be recorded on multiple devices simultaneously to ensure redundancy.

The combination of ports being used provides clues to hackers, allows them to make generalizations, and gives them a starting point to enter a system.

The question isn’t whether a manufacturer has cybersecurity vulnerabilities – any of them might – but rather how quickly and effectively they respond when a vulnerability is found

The Role of Manufacturers

Any installer/integrator or end user who identifies what they think is a cybersecurity flaw in a camera or other system component should notify the manufacturer immediately. Anyone who works with software knows that the possibility always exists of cybersecurity vulnerabilities and is aware of the need to work constantly and consistently to address any problems. Hikvision does not interpret the report of a cybersecurity problem as derogatory toward its products; rather, the company is eager to identify and address any problem to avoid a more widespread vulnerability. Hikvision appreciates input from integrators/installers and end users in the market to help them identify and deal with cybersecurity vulnerabilities.

The question isn’t whether a manufacturer has cybersecurity vulnerabilities – any of them might – but rather how quickly and effectively they respond when a vulnerability is found.

When Hikvision receives a report, the first thing they do is perform testing to confirm the problem and diagnose how it can be solved. Typically, any “fix” involves a revision in firmware or software. Firmware and software updates are posted on Hikvision’s website. Periodically checking manufacturers’ websites for updates is another (often overlooked) best practice.

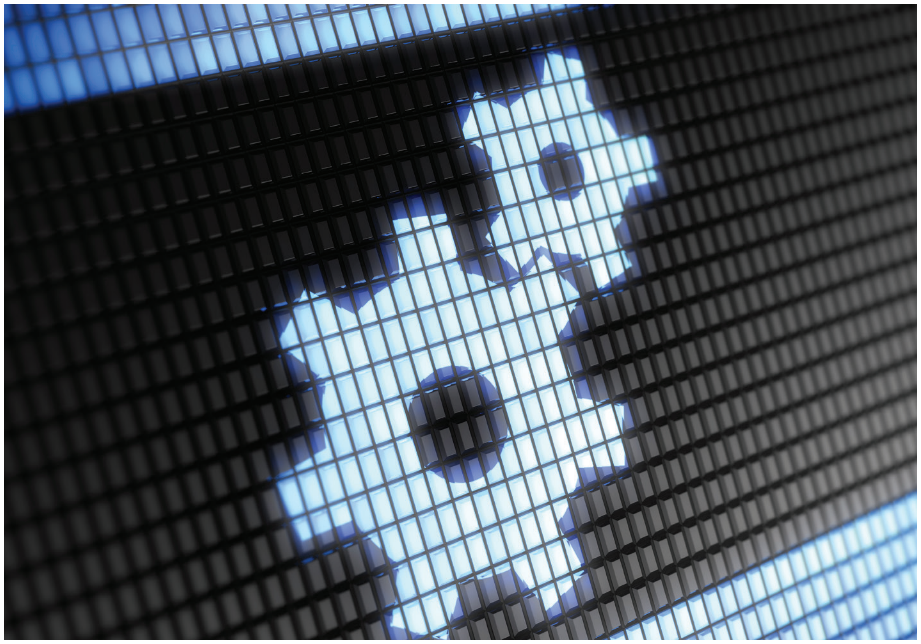
Other roles for manufacturers in cybersecurity include:

Providing the most secure equipment possible: Cybersecurity considerations should be applied to every element of a system. It’s always better, safer and more effective to design cybersecurity into a product than to add it later.

Periodic testing: Manufacturers employ third-party firms to test their products and to identify any vulnerabilities before cyber-criminals find them. (Hikvision’s cameras and other IP system components were tested by Rapid7, a provider of security data and analytics solutions, in December 2015.)

Communicating information clearly: Providing useful information on a manufacturer’s website and in corporate literature can go a long way towards addressing cybersecurity vulnerabilities. Clear information is essential, especially basics like how to change passwords and upgrade firmware. Hikvision offers information on these topics on its website’s “Security Center”. Videos can be a helpful tool to demonstrate processes. (Hikvision provides videos about changing passwords and upgrading firmware at **http://www.youtube.com/hikvisionusainc**.) A manufacturer’s customer-facing employees also work to communicate cybersecurity information.

Making cybersecurity upgrades as easy as possible: Software tools can help. Hikvision has a toolkit that includes a “batch upgrade” tool that can identify the appliances on a network and push a firmware update file to each appliance (assuming all are in the same series and all use the same firmware), then reboot and bring them back online.



Training their technical support staff to respond appropriately to a cyber-attack or vulnerability: Defined processes should be in place to escalate the responses to any problem to involve people who can solve it in a timely manner. If somebody contacts a technical support staff member about a problem, the manufacturer should test the vulnerability immediately and then begin writing code to correct the problem. Documentation and accountability should ensure processes are followed.

Providing appliances with embedded systems: The use of embedded software is inherently safer than software based on the Windows operating system (used in some video surveillance applications). In fact, the well-known vulnerability of Windows (which is logical given Microsoft's size and the product's ubiquity in the market) is often the route hackers take when they enter a target company's system through the video surveillance system. Even Linux systems are vulnerable if they are not hardened appropriately. Using an embedded system with proper precautions minimizes the likelihood of a successful attack; for instance, only software libraries that are needed to run a specific application should be installed and loaded on an appliance. Hikvision streamlines its embedded systems to remove all but the most essential software libraries, thus preventing extra potential entry points for hackers. Nothing can be installed on a Hikvision system component except by using the company's utilities, written specifically for the system (although no precaution is 100 percent preventative).

Turning off any Telnet command line: Telnet is a protocol for remotely accessing a computer (including an embedded IP system component). Using Telnet, an administrator or another user (including a hacker!) can access someone else's computer remotely. Manufacturers should turn Telnet access "off" as the default (as does Hikvision), and should also have any allowed Telnet access "time out" after a period of time, say five minutes. The average user does not need the function, and interfacing with a system should generally be limited to a graphical user interface (GUI). Telnet accessibility should be eliminated as an easy route for hackers.

Even Linux systems are vulnerable if they are not hardened appropriately. Using an embedded system with proper precautions minimizes the likelihood of a successful attack.

Role of Installers/integrators and End Users

In addition to manufacturers' responsibilities, integrators/installers and end users also have important roles to play in cybersecurity. Integrators and installers are just now beginning to contemplate issues of cybersecurity – and it's long overdue.

More awareness and training on cybersecurity: In general, the video surveillance market is playing catch-up on cybersecurity. For too long the market has downplayed or even ignored the possibility of a cyber-attack. Driven in part by increased public awareness (including publicity about hacked "nannycams"), the industry is finally embracing the need for more cybersecurity awareness and education. More industry and convention programming now centers on these topics, which provides an opportunity for installers/integrators to make up for lost time. Among other factors, the future success of their IP video surveillance business depends on how well they address cybersecurity issues.

Playing an active role in education about cybersecurity: Installers/integrators in particular should also play a role in educating their customers about cybersecurity. They have access to manufacturers' engineers and/or sales team who can train them about cybersecurity. Their role includes sharing the benefit of that training with their end user customers. Most importantly, integrators and installers should not misrepresent any IP equipment as "completely secure," which is naive at best and irresponsible at worst.

Creating processes to respond: In case a video appliance is being compromised, or even if you think it might be, there should be a plan (process) in place about who to notify and how to respond. If a vulnerability may be due to a flaw with the product, the manufacturer should be notified so that they can test the product. If an issue is found, they can work to fix it.

Leveraging expertise from inside the enterprise: An end user's information technology (IT) department is well aware of threats from cybersecurity and is well-positioned to help with applying cybersecurity best practices to an IP video surveillance system (in addition to the rest of the enterprise IT infrastructure). The IT department is increasingly involved in the buying decisions on IP video systems and should also be called on for help with cybersecurity issues.

Using available resources: Many end users are not aware of cybersecurity challenges, although the U.S. Department of Homeland Security is making great strides to provide useful information. The DHS Website (**http://www.dhs.gov/topic/cybersecurity**) is a great resource.

No one is immune to cybersecurity threats – just lucky. If you haven't been a target, the fact is that you just haven't been a target yet.

A Cyber-Attack Could Happen to You

No one is immune to cybersecurity threats – just lucky. If you haven't been a target, the fact is that you just haven't been a target yet.

Any device attached to the Internet is hackable, given enough time and effort. If a system makes hacking more difficult, it can often avoid trouble, especially given all the targets on the Internet that make hacking easy. But it takes effort.

Reckless finger-pointing is not the solution, and in fact does not contribute to the productive working relationship required among various stakeholders to address the problem intelligently and proactively. Cybersecurity is not anyone's "fault" (unless you want to blame the hackers), but rather an undeniable reality in the age of the Internet. We can't ignore it.

Ensuring the cybersecurity of IP video surveillance systems is an industrywide problem. In a sense, the need to deal with cybersecurity is a price we all pay to achieve the many other benefits of networked systems. Importantly, cybersecurity is not just a manufacturer's problem, or an integrator problem, or something for the IT department to worry about. It will take every facet of the industry working together, creating innovative systems to address cybersecurity threats and robust processes to respond when (not if) a cyber-attack occurs.

Our industry's future depends on it.

It will take every facet of the industry working together, creating innovative systems to address cybersecurity threats and robust processes to respond when (not if) a cyber-attack occurs.

SourceSecurity.com®