Honeywell
THE POWER OF CONNECTED

Cyber Security

Cyber Security and IP Video Surveillance 2017

Table of Contents

1. Introduction

Analog video solutions rely on outdated technology. These systems have made way for more secure, IP-based video surveillance systems to provide reliable and cost-efficient solutions in today's information-rich, digital world.

Modern IP technology can enable effective and manageable video surveillance to protect people, their information, their properties, and help ensure continuous operation. It can also create the potential for enhanced safety and security benefits for our society to prevent costly security incidents. However, the cyber security of IP technology has been challenged by the pace of technology transition and development, creating potential safety and economic risks.

Cyber-attacks at the local and global scale are on the rise, and according to a 2016 report published by Grant Thornton, the total estimated global financial loss associated with cyber security attacks is estimated to be U.S. $315 billion each year. One example of a major cyber-attack occurred in the U.S. in October of 2016. Internet access was denied to many major websites, including Twitter, The Guardian, and CNN. This attack, which was the largest of its kind at that time, was conducted by a botnet virus called "Mirai" from infected Internet Protocol (IP) video devices on the internet.

Honeywell takes cyber security seriously. This paper is intended to provide an overview of Honeywell's approach to cyber security, including its latest IP video surveillance products and systems designed to intelligently prevent dangerous attacks.

2. Threat and Vulnerability

The importance of cyber security in the IP environment is widely recognized. It requires protecting devices, networks, programs, and data from being copied, changed, or destroyed by unintended or unauthorized access. Since video surveillance products such as IP Cameras, Network Video Recorders (NVRs), and Video Management Software (VMS) are IP-enabled, they can be accessed from a remote location using internet connectivity, which means they have the same vulnerabilities as other devices and systems in the open IP world.

The *U.S. National Strategy to Secure Cyberspace* is a report that outlines a five-level threat and vulnerability model, including home/small business, large enterprise, sector/infrastructure, national, and global categories.

In the report, the U.S. government expresses concerns about:

- the network devices used to attack critical infrastructures;
- large-scale enterprises being increasingly targeted by malicious cyber actors, both for the data and the power they possess; and
- the fact that cyber vulnerabilities could directly affect the operations of a whole sector or infrastructure.

Not only has cybercrime caused significant interruptions for businesses and negatively impacted infrastructure in recent years, but it has also led to large-scale data breaches. According to PwC's survey, *Global Economic Crime Survey 2016*, the risk of cybercrime was the second most reported type of economic crime affecting 32% of organizations in 2016. Furthermore, the average cost of a data breach to organizations is $4 million, up from $3.8 million in 2015.

Many countries and international organizations have been working on data-protection legislation, national standards, and regulations in most sectors. These regulatory initiatives will help reduce vulnerabilities and clarify questions of liability.

Business Interruption

Business interruption is a type of cybercrime that is usually launched by inserting malicious code on a company or infrastructure network, which limits the network's ability to provide service and inhibits a company's ability to conduct business.

Malicious code, or "malware," comprised of viruses, worms, botnets, etc. can be injected into IP devices with weak points, propagate itself to seek more victims on the network, and steal sensitive information for the purpose of economic benefit.

A botnet, short for "robot network," is an aggregation of computers compromised by bots (automated machines or robots). These bots are controlled by malicious cyber actors by launching Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks to targeted critical infrastructures or enterprises.

DoS and DDoS pose a serious threat to business service. In June 2015, hackers grounded ten planes belonging to a Polish airline and blocked flight plans sent to planes by launching a DoS attack. The Mirai attack mentioned earlier is also an example of a DDoS attack.

Data Breach

The video system is the core of a security system and contains critical information, including system data, deployment, event, and alarm information. When this data is compromised it's called a data breach and this crime can cause significant security and safety risks

Video surveillance in private and public applications may capture and record video images of people not relevant to security and safety incidents. Many countries are working toward privacy-protection legislation to prevent privacy breaches by intruders and inside employees. For example, in the U.S., 47

states have breach-notification laws in effect and in Ireland, it is illegal to post video surveillance footage on the internet.

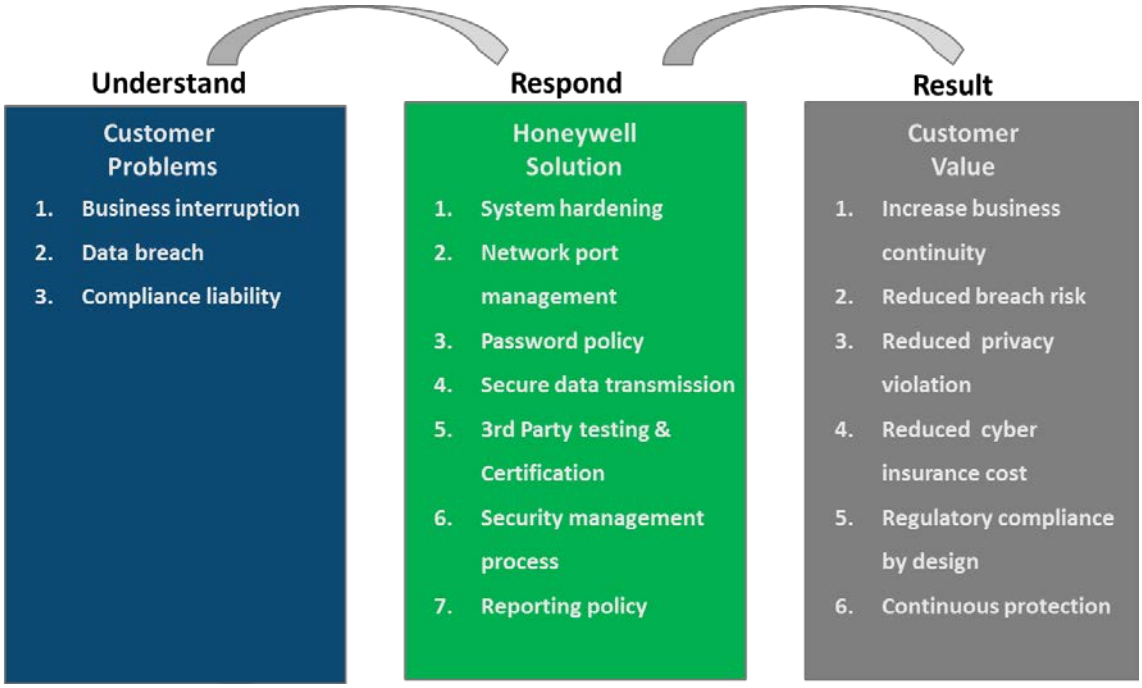
Compliance and Liability

With cyber legislation, national standards, and sector regulations in place, regulatory compliance will become a rigid entrance requirement for IP systems, including video surveillance. It will impact the framework for product design, sales, industry entrance, system integration, and user operation.

Meanwhile, there is also a market trend of increased cyber insurance sales spurred by the awareness of broader cyber risks. A vulnerable system will be forced to upgrade or be replaced for regulatory compliance or the customer will have to pay a much higher premium to cover the liability every year. This is why Honeywell is committed to providing a forward-looking, cyber-secure video solution for its partners and customers.

3. Honeywell Cyber Security Solution

Many businesses haven't conducted a cyber-threat analysis and don't know how vulnerable they are to cyber threats. Honeywell can help by analyzing customers' problems, then implementing best practices to execute optimal product and system design. Honeywell has also developed cyber-security management processes and released vulnerability reporting policies to help its customers face a growing cyber-security challenge.



Rigorous System Hardening

At the product and system design and development phases, Honeywell uses in-house and third-party testing tools to evaluate product vulnerabilities and fix issues to harden the system. To mitigate the risks associated with malicious code, data privacy breaches, and system misconfiguration Honeywell employs the Information Communication Technology (ICT) industry's security guidelines, which addresses specific video surveillance requirements.

Since IP video surveillance can be installed in both private and public networks the exposed cyber threat can vary accordingly. It is necessary to target system hardening according to the specific application it is deployed for. System hardening needs to be aligned with the process of cyber security management,

system management, and business operation. Customers of Honeywell Video Systems can configure product and system settings to address threats specific to the planned implementation.

System hardening is usually the process of securing a system by reducing its vulnerability. Common system hardening practices include:

- Disabling unused ports and unnecessary services by default
- Enforcing password rules and changing default password at initial login
- Updating security patches to stay current
- Web communication with up-to-date encryption protocols, such as, TLS 1.2 encryption at the time of this writing
- Payment Card Industry Data Security Standard (PCI DSS) compliance and Underwriters Laboratories Cybersecurity Assurance (UL CAP) certification

Network Port Management

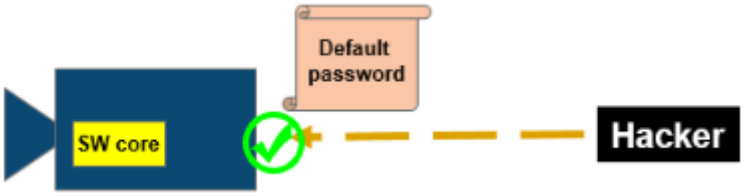
A network port is a logical end point for communication purposes. To connect to external services, IP devices use network ports identified by specific numbers from 0 to 65535; ports between 0 and 1023 are considered reserved and are officially assigned by the Internet Assigned Numbers Authority (IANA).

A network port is always associated with the IP address of the host and the protocol of the communication, and completes the destination or origination network address of a communication session. Well-known port numbers are allotted to the standard process applications of an IP device. For example, Port 21 is used for File Transfer Protocol (FTP), Port 23 is used for Telnet remote login service, and Port 80 is used for Hypertext Transfer Protocol. These well-known ports are highly vulnerable to cyber-attacks. Honeywell disables unused communication ports by default – such as FTP port 21, SSH port 22, and Telnet port 23 – to eliminate hijacking risk via vulnerable legacy protocols.

Password Management Policy

When users log in to Honeywell IP camera software for the first time they receive a prompt to change the product's default password. If the default password isn't changed, the notification will be shown at log in until the action is completed.

The default password should only be used for the first log in, for demos, and for technical support purposes. If the device's default password has not been changed hackers could log in to the device remotely.



With Honeywell IP cameras password rules are enforced to increase the strength of new passwords. A password must contain a minimum of 8 characters with uppercase, lowercase, and special characters. These rules result in more than 600 trillion combinations that hackers would need to attempt to access a

user's account. As Trustwave stated in its 2016 Global Security Report, 7% of cyber-attacks occur due to weak passwords.

To cope with automated attacks, Honeywell devices lock for 15 minutes after 5 failed login attempts; this means it would take approximately 3 billion years to try 600 trillion combinations.

Data breaches are another type of cyber threat that need to be prevented in system and process design. Data breaches may not occur inside the devices, but on the remote client. In Honeywell Video Systems all passwords stored on the device and system or transmitted between them are rendered unreadable. So even when cyber-attacks compromise a remote work station or transmission between them, the passwords are still protected.

Secure Data Transmission

On the web, Hypertext Transfer Protocol (HTTP) is the foundation of data communication protocols. When we type strings of a website address starting with "http://" we send access requests to the web page. Behind the scenes, the HTTP protocol enables a session with a sequence of network request-response transactions, which transmits the web page to the end-user.

HTTP sites are not encrypted, and are vulnerable to man-in-the-middle and eavesdropping attacks. A more secure protocol, "HTTPS," also called Hypertext Transfer Protocol Secure, takes the place of HTTP and builds a more secure communication by providing both encryption of the communication and authentication of the remote hosts.

In a video system data may transfer through an untrusted or unsafe network. Honeywell uses the HTTPS protocol to provide bidirectional, encrypted communication between devices and systems. Please check Honeywell web page https://mywebtech.honeywell.com/Account/Login for the latest list of products supporting HTTPS encryption. For products without HTTPS encryption capability, please avoid use them in untrusted networks, or install them behind firewall to migiate potential risk.)

When an HTTPS session request is sent to an IP camera, the camera and server will authenticate each other by exchanging certificates. Only after both identify and authenticate the other is a secure session established.

Throughout the entire encryption process, private keys are critically important and must be kept secure. If the private keys are compromised the encrypted data streams could be intercepted and decrypted.

In selected Honeywell IP cameras, private keys are securely stored inside a non-retrievable hardware chipset. If there is no secure, hardware-based key storage the private keys will have to be stored in the device file system, which is more vulnerable to cyber-attacks.

The Advanced Encryption Standards (AES) is a specification for data encryption. It was adopted by the U.S. government to protect classified information and has since been adopted worldwide. In the AES specification, 128-bit and 256-bit keys are used for encryption and decryption to protect critical data. 128-bit keys create $3.4x10^{38}$ possible combinations and 256-bit keys create $1.1x10^{77}$ possible combinations. Fifty supercomputers that could check a billion (10^{18}) AES keys per second would require about 3×10^{51} years to exhaust the 256-bit key space. Honeywell leverages the AES specification to protect IP communications.

Third Party Cooperation and Certification

Like Honeywell, companies across industries have become more sophisticated with regard to cyber security, and the set of resources and tools available to improve and assess security programs likewise has grown dramatically.

Honeywell uses the experience, tests, and certifications of third-parties to manage its supply chain from the cyber security perspective, specifically tracking vulnerabilities associated with the software and hardware components provided by outside vendors. Increased awareness can help Honeywell identify where and how to apply security measures.

In addition, Honeywell also partners with the industry during product design, testing, manufacturing, and system integration to identify vulnerabilities, detect irregularities, respond to potential incidents, and recover from damage to or disruption of IP Video systems.

Honeywell has formed a qualified network security team composed of experts certified by the International Information Systems Security Accreditation Alliance to enhance product safety by applying safety measures to the product development lifecycle.

Honeywell has actively participated in industry discussion relating to cybersecurity and has supported the development of industry standards and certification.

PCI DSS Compliance

Cyber compliance is not new to the banking and finance industry. PCI DSS released its first, optional version in 2004 and version 3.0 in 2015. PCI DSS compliance involves an ecosystem of payment devices, applications, infrastructure, and users. When deploying an IP video system for banking application PCI DSS compliance is mandatory. The video system needs to be compliant with PCI DSS requirements, including network and data protection, vulnerability management, access management, and security policies. Honeywell equIP series IP cameras and the development process adhere to the rules of the PCI DSS ecosystem, video surveillance, and common IP cyber security requirements at the same time.

Security Management Process

Honeywell has developed a robust system for considering security at the outset of product conception and during development, as well as responding to potential vulnerabilities in existing products. This system, Honeywell's Secure Software Development Lifecycle (SSDLC) initiative, has evolved and grown even more robust over the past few years.

Under Honeywell's current SSDLC program, cyber security is integrated into the development process through baseline security requirements, threat modeling, static analysis, security testing and audits.

Early on in the product development process, Honeywell requires its team to identify the security requirements that may be relevant to the product. Any New Product Introduction (NPI) project must apply ANSI/ISA62443-3-3 security requirements as the baseline requirements for the products, and the SSDLC program requires that a Security Architect signs off that this task is completed.

Honeywell also requires its NPI projects to undergo threat models. Threat Modeling following the Microsoft STRIDE process, using the Microsoft Threat Modeling Tool to evaluate illegally accessing tampering, repudiation, data breaching, risk of DoS, and elevation of privilege. Once the team completes threat modeling, it must export the results from the MS Threat Modeling Tool and evaluate each unmitigated threat using the Common Vulnerability Scoring System (CVSS). Honeywell has developed policy standards to govern the expected disposition of threats.

Honeywell product development teams also must utilize Klocwork static analysis tools. Klocwork is a well-established software solution for Statuc code analysis. It is used by thousands of customers, including many of the foremost brands in the automotive, mobile devices, consumer electronics, medical technologies, telecommunications, military, and aerospace sectors. The program analyzes syntax, semantics, variable estimation, and control and data flow to find issues that are difficult or impossible to find through manual testing.

Honeywell requires new products to undergo comprehensive security testing, and there is a centralized team within Honeywell to help the development team to meet this requirement. The security testing is tailored to product at issue, but the company uses a wide array of tools and techniques to check for vulnerbilities , including Nesus and HP WebInspect.

For some products, Honeywell Security and Fire's legal counsel may request and direct next level penetration testing that goes well beyond standard security testing. It is performed by an independent group within HBT, separate from engineering.

An audit team of Honeywell performs checks to ensure that security deliverables required under Honeywell's NPI process are completed.

Honeywell Security and Fire outline training programs for its employees on the company's security process and on specific cybersecurity concerns and solutions, All software engineers in Honeywell Security and Fire receive formal training on software development process and General Cyber/Product security.

Honeywell Cyber Security Reporting Policy

Cyber security is a moving target that requires continuous process. The changing environment and technology evolution will bring new cyber threats and vulnerabilities to video surveillance products and systems on the internet. Even when security is included at the design stage, vulnerabilities can be discovered in products or systems after they have been deployed.

Honeywell understood the importance of the soliciting and considering feedback from independent third parties about the security of its products. Accordingly, since August 2012, Honeywell HBT has utilized a process called the Product Security Incident Response Team (PSIRT) to consider and respond to third-party reports of vulnerabilities involving HBT.

Issues can be reported through various means. First, Honeywell maintains a public webpage (https://honeywell.com/Pages?vulnerabilityreporting.aspx) for anyone to report vulnerabilities. The email connected with this reporting (security@honeywell.com) is monitored 24/7 by the Honeywell Global Security Operation Center (SOC). Security researchers typically also use the security@honeywell.com address. Alternatively, Honeywell has received vulnerability reports from blogs, customer inquiries, etc.

When a security issue is reported, the SOC sends the issue to the PSIRT leader, and his or her manager. The PSIRT leader enters the issue into the PSIRT JIRA database and assigns it to the

product security leader for the strategic business unit (SBU). Each SBU has a product security leader who coordinates and drives PSIRT issues. This person is typically a security professional. The product security leader must send an acknowledgement of the receipt of the issue back to the submitter within 24hours and must outline the next steps the Company will take to validate or address the issue.

Next, the issue is assessed and assigned to a technology team in that SBU. The Company strives to validate the submitted issue within 24 hours, although highly technical issues can take up to five days to validate. PSIRT generally sends an acknowledgement of validation to the submitter, along with a planned timeline for mitigation. After validation, the echnology team diagnoses the issue, creates a plan to fix the issue, and implements the fix. Mitigation times vary depending on the issue.

Please refer to www.honeywell.com/contact-us/vulnerability-reporting for the detailed information.

4. Conclusion

Honeywell IP video solutions are not only deployed for large enterprises, critical sectors, and infrastructures in the global market, but are also appropriate for small and medium-sized businesses. To protect people, property, and service, Honeywell puts tremendous effort into product and system design, third-party testing and certification, security-management processes, and vulnerability-reporting policies. All of this work results in minimum system downtime, business continuity, lower risk of data and privacy breaches, and reduced cyber and compliance liability to enhance customer satisfaction.

References

1. *National Strategy to Secure Cyberspace*, White House of USA
2. *Global Economic Crime Survey 2016*, PwC
3. *2016 Cost of Data Breach Study*, IBM Global Report
4. *A guide to Cyber Risk*, Allianz
5. *Security Breach Notification Laws*, National Conference of State Legislatures
6. *Responding to a Data Breach*, PCI Security Standards Council
7. *2015 Cost of Data Breach Study*, IBM
8. *Best Practices for Maintaining PCI DSS Compliance*, PCI Security Standards Council
9. *Cyber security regulation and best practice in the US and UK*, LexisNexis
10. *Strategic Principles for Securing the Internet of Things*, U.S. Department of Homeland Security
11. *DDoS Quick Guide*, National Cyber security and Communications Integration Center
12. *Malware Threats and Mitigation Strategies*, US-CERT Informational Whitepaper
13. *2016 Global Security Report*, Trust wave
14. *Transport Layer Security*, Wikipedia
15. *Symmetric-key algorithm*, Wikipedia
16. *Advanced Encryption Standard*, Wikipedia
17. Best Practices in Cyber Supply Chain Risk Management,

Honeywell Security and Fire
Aston Fields Road
Whitehouse Industrial Estate
Runcorn, Cheshire, WA7 3DL
United Kingdom
Tel: +44 (0)8448 000 235
www.honeywell.com

Honeywell Security and Fire
Honeywell Security Office -
Emaar Business Park, Sheikh Zayed Road
Building No. 2, 2nd floor, 201
Post Office Box 232362
Dubai ,United Arab Emirates
Tel: +971 44541704
www.honeywell.com

Honeywell Security and Fire
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Tel: 1.800.323.4576
www.honeywell.com

Honeywell