RBCS
Ray Bernard
Consulting Services

Advancing the Mission of Security:

Reduce security risks to acceptable levels,
at an acceptable cost.

Sustainable Cybersecurity for Industrial IoT

By Ray Bernard

Version 1.1 – 25 January 2019

Sustainable Cybersecurity for Industrial IoT

The nature of Internet of Things (IoT) devices and the scale of their use is what makes securing them so hard. IoT devices emerged for industrial controls two decades ago and then expanded rapidly into business and consumer technologies.

The first IoT devices had important but limited capabilities. As embedded computing and networking technologies advanced, many tech trends – such as low power, miniaturization, massive increases in computer and memory chip density, digitalization, virtualization, and network capacity growth – turned small simple devices into intelligent high-powered networked computers. A perfect example is the rotary-dial analog telephone vs. the smartphone you carry with you.

Thus, today's intelligent industrial IoT devices are high-value hacker targets. Cybersecurity was not built into most of these devices, and many that did have security controls were still found to be vulnerable to certain kinds of cyberattacks. Many IoT devices were originally analog devices that were converted for Ethernet network use before the Internet or in its early days. There were no cybersecurity concerns at that time about industrial devices. Over time, IoT devices were enhanced as computing technology and networking advanced, before today's cybersecurity threat evolved to their current levels.

In recent years both industry and customer thinking about these devices has not kept pace with their technology advances and increasing vulnerabilities. That thinking must change significantly for these devices to be used safely without a high potential for catastrophic consequences to owners of the IoT devices.

Internet of Things Technology

The "Internet of Things" is a term coined about 20 years ago by Kevin Ashton, author and co-founder of Auto ID Center at the Massachusetts Institute of Technology (MIT). IoT refers to "networked physical devices that contain embedded computer technology to communicate and sense or interact with their internal states or the external environment." According to Ashton, radio frequency technology (RFID) was the foundation of the Internet of Things because – via RFID tags – it allowed computers to identify the things around them in the world.

The use of IoT technologies have undergone explosive growth in recent years. Estimates now place the number of connected IoT devices at more than 23 billion, three times the number of people on Earth.[1] Thus, it should be no surprise that the past two years have seen an unprecedented increase in the number, scale and type of cyberattacks against these devices. Not only is there a rise in the number of cyberattacks – the sophistication of the attacks is also increasing.

Many intelligent industrial IoT devices can be weaponized by malware and used to attack other targets. Because IoT devices operate on their own without continual user interface, they can be hijacked without their owners knowing about it. Any network-connected device is a potential target for outsider or insider threats and must have appropriate cybersecurity measures put into place.

[1] Sam Lucero, "IoT Platforms: enabling the Internet of Things." *IHS Technology Whitepaper.* IHS Markit, March 2016, https://cdn.ihs.com/www/pdf/enabling-IOT.pdf.

Sustainable Cybersecurity for IoT

Although industrial IoT devices are hard to secure for many reasons, their cyber risks can be significantly reduced through proper tools, attention and action. This should be a very high priority for owners of industrial IoT devices and systems, not just something that's given lip service. The way that industrial IoT devices are deployed and managed must change to follow the practices that have proven successful for the cybersecurity protection of IT infrastructure.

Successful practices in IT infrastructure protection can and must be applied to industrial IoT devices.

Cybersecurity for Non-IT Devices

Owners of intelligent IoT devices typically don't think of them as computers because they are not general-purpose computing devices. They are purpose-built for specific functionality. Device owners don't realize the computing and communications capabilities industrial IoT devices contain. Until recently, they also haven't recognized the need for their cyber security, although that is changing due to recent highly publicized cybersecurity events and device vulnerabilities.

Traditional computers, such as servers, workstations, desktop computers and laptops can be managed and protected using existing IT security practices and tools. This is also true for the standard networks that IP-addressable IoT devices communicate on.

However, intelligent industrial IoT devices are among the most challenging to secure, because standard IT tools don't work for managing device security. Thus, the devices have not had standard IT managed-infrastructure security practices applied to them, even though they are critical and costly technology assets. Instead, they have been subject to some manual ad hoc protective actions or none at all.

Standard IT tools for networks and computers don't work for securing industrial IoT devices.

Most companies who own and use industrial IoT devices aren't aware that they must be managed much differently than other industrial devices in order to achieve effective cybersecurity. Securing device networks alone is insufficient.

Case in Point: Intelligent Network Security Cameras

Today's network security video cameras, sometimes called "IP cameras", contain server software, which is typically an embedded Linux operating system with web-server software and video analytics applications. Using standard TCP/IP protocols, the cameras transmit one or more video streams to video recording appliances or servers, and optionally provide additional video streams for live viewing.

No one in IT or corporate management would think it okay to put hundreds or even just dozens of server computers around a building campus and network them together, placing some in lobbies, meeting rooms, and even outside the buildings, and not keep their firmware updated or closely manage their passwords. Yet this is common practice with network security cameras. In 2016, camera and recorder cybersecurity vulnerabilities allowed 1.5 million connected cameras and recorders (DVRs, NVRs and recording servers) to be hijacked to create the world's largest Mirai botnet.[2] The malware took full control of IoT devices' underlying Linux operating systems.

[2] Lorenzo Fenceschi-Biccheria, "How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet." Motherboard.com, 29 September 2016, https://motherboard.vice.com/en_us/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs

Network security alone doesn't provide enough protection for industrial IoT devices.

Connecting the cameras via a protected network is insufficient because it establishes only a single layer of defense with many attack points. If just one attack point is compromised, vulnerable cameras can be exposed to a myriad of automated and manual attacks. A single compromised camera can then spread the malware infection to other devices on the network, not just to other cameras. For example, malware on cameras could spread to servers and workstations. It could lock out all users from business applications by attacking the business's Active Directory system. The business disruption would last from a few hours to a few days, depending upon the recovery measures in place for business IT systems. But there would likely be a significant negative impact to the business.

Government Action Against Insecure IoT Devices

Governments are now starting to publish guidance and regulations regarding IoT device security. Password and firmware vulnerabilities are at the top of the United Kingdom's *Code of Practice for Consumer IoT Security*, published in 2018, which contains the government's Code of Practice for consumer IoT security for manufacturers, with guidance for consumers on smart devices at home.[3]

The State of California has banned IoT device default passwords.

The poor password practice situation has been so serious for both consumer and industrial IoT devices, that California has passed a law that bans default passwords for all IoT devices. Beginning Jan. 1, 2020, Senate Bill No. 327 requires manufacturers of a connected device to equip it with a "reasonable security feature or features." The bill mandates that manufacturers must provide default passwords that are unique to each device or prompt the user to generate a new password before using the product. Katie Malafronte, writing recently about hospital, school and university safety for *Campus Safety* magazine, said, "Most physical security and life safety systems are now connected to the Internet, making them vulnerable to cybersecurity attacks. Video surveillance, security cameras, and fire systems all fall into these categories."[4]

From a legal perspective, these types of government actions, combined with media coverage of major cybersecurity incidents, are establishing a de facto standard of care regarding security for the deployment of both consumer and industrial IoT devices. More is said regarding the impacts of cyber risks on insurance in the section titled, *Compliance-Based Device Management*, which starts page 11.

There are also privacy considerations that relate to information collected by IoT devices, and to any such information disclosure breaches that result from unauthorized access to devices. The first GDPR fine issued by Austria was to an entrepreneur who installed a security video camera whose field of view included a substantial section of a sidewalk. The fine was 4,800 Euros (about $5,500).[5]

[3] Department for Digital, Culture, Media & Sport, "Code of Practice for Consumer IoT Security." GOV.UK, 14 October 2018, https://www.gov.uk/government/publications/secure-by-design

[4] Katie Malfronte, "California Bans Default Passwords for All IoT Devices." CampusSafetyMagazine.com, 11 October 2018, https://www.campussafetymagazine.com/technology/california-bans-default-passwords-iot-devices/

[5] Baker McKenzie, "Takeaways from the First GDPR Fines." Globe Business Media Group, 18 December 2018, https://www.lexology.com/library/detail.aspx?g=a91ba97a-eae9-408c-a53f-c47d1c6d62ea

Even though privacy regulations are mostly outside this paper's scope, this incident highlights a relevant point. A data breach of an IoT device (such as a security camera), which has captured the image of a visiting European's person or vehicle, about could result in a significant fine under GDPR regulations.[6]

> Understanding how to balance the promise of IoT connected devices with potential security challenges will continue to be a mega-trend in the years to come.[7]

From several perspectives within the past few years, sustainable cybersecurity protection of IoT devices has become critically important for industrial IoT device owners and service providers.

Protecting Industrial IoT Devices

The remainder of this paper uses intelligent network video cameras to provide examples of how intelligent IoT devices can be protected from the most common cyberattacks. There are many other types of security system IoT devices including intercoms, loudspeakers, access card readers, and so on – and this paper is applicable to them as well as to non-security industrial IoT devices. Network video cameras were selected as the example IoT device category due to the widespread deployment of cameras and the high level of challenge involved in establishing and maintaining their cybersecurity, and the very high level of cyber risk for the very large-scale deployments that are attractive cyber targets. Additionally, this paper's author has deep expertise in the design and secure deployment of networked security video systems.

The Key Vulnerabilities

Industrial IoT device vulnerabilities are significantly amplified by the fact that the devices are not like end user devices that have individual owners who interact with them daily. Intelligent Industrial IoT devices can be infected with malware without the operators of the systems they connect with knowing about it. Cameras can become part of a botnet without their normal functions being compromised, until such point as the hacker or botnet controlling the cameras takes them over fully or permanently disables them (called "bricking", as the device becomes as useless for its intended purpose as a brick).

The key vulnerabilities of video cameras and other intelligent IoT devices fall primarily into two categories:

- Password vulnerabilities
- Firmware vulnerabilities

Addressing these two categories of vulnerabilities will stop most attacks from being successful, especially automated malware attacks. It is not just networked security camera surveillance systems that are impacted. Major cities are now using intelligent video cameras in automated traffic management systems. These deployments are examples of non-security video applications whose cybersecurity is even more critical than for video surveillance systems.

Addressing Password Vulnerabilities

Most cyber-attacks work by gaining access via user login credentials, and then exploiting device and system vulnerabilities to obtain a high level of access that gives attackers full control. Most automated

[6] Ray Bernard, "Big Data and Privacy for Physical Security." Security Industry Association, 14 November 2017, https://www.securityindustry.org/2017/11/14/big-data-and-privacy-for-physical-security/

[7] Christy Pettey, "The IoT Effect: Opportunities and Challenges." Gartner, 28 March 2017, https://www.gartner.com/smarterwithgartner/the-iot-effect-opportunities-and-challenges-2/

and manual cyber-attacks succeed through the existence of factory-default passwords, easily-guessed passwords, passwords discovered because they were transmitted in plain text, and weaknesses that allow device and system access privileges to be escalated.

Intelligent IoT device password management can be complicated. Unlike PCs, smartphones and tablets, a one-person to one-device owner relationship does not exist for industrial IoT devices. Industrial IoT devices are typically part of a system with hundreds or thousands of connected devices. IoT devices are typically in constant use by other devices, systems and software. Humans rarely access IoT devices directly, such as for installation or service tasks.

Poor Password Practices

For the sake of simplicity and convenience, many organizations provide a system's intelligent IoT devices all with the set of passwords, such as a master password, a system or device password, and a service technician password. This practice creates a significant vulnerability, as a person or a piece of malware learning the passwords of a single device then has the passwords to all devices.

The password situation is further complicated when personnel from the owning organization don't manage the IoT passwords themselves but delegate the management to service contractors. Since most industrial systems have a lifecycle measured in years, such password knowledge becomes a risk when service personnel change, some of whom may be disgruntled.

The password risk picture becomes even more complicated when contractor service personnel use their own "favorite" device passwords on the devices of more than one customer. This means that the personnel of a second customer of that same service provider – using the same type of IoT devices, may then obtain knowledge of the first customer's passwords. A competitor's personnel can have the passwords to an organization's IoT devices.

Furthermore, a successful hack or malware infection of any of that service technician's customers would then give the attacker the device passwords of the technician's other customers. It a worse scenario if a technician habitually leaves default device passwords in place, as the devices of all customers will be vulnerable to just about any malware or hacker that gains access to those customers' networks.

Password Management at Scale Has Been Impossible

Managing passwords is easy when the size of the intelligent IoT device network is small and has only a few devices. Automated password management tools are required for managing deployments with hundreds or thousands of intelligent IoT devices. Not only must the tools change the passwords in the devices themselves, they must change the stored passwords in the devices and software that connect to and use the IoT devices.

Such tools don't exist for most IoT devices. They are only now emerging for security video cameras, even though for over a decade, large enterprises have had security camera deployments with camera counts in the thousands. It is an industry shortcoming that is just now being remedied.

Tools are starting to emerge for managing IoT device passwords at scale.

Automated tools can be used to ensure that default passwords and easily-guessed passwords are not used. Secure (i.e. HTTPS) network connections can be used to ensure that passwords are not transmitted in plain text. Automated tools can change passwords as often as needed to accommodate service technician and other personnel changes. Such tools also allow IoT device owners to maintain control over password management and provide auditable records of conformance to password management policies.

Addressing Firmware Vulnerabilities

Cybersecurity is not the only reason to update IoT device firmware. Maintaining devices at their most recently-released versions of firmware is typically required by manufacturers for their provision of factory technical support. Additionally, modern technologies are continually updated for bug fixes as well as feature and performance improvements. Intelligent IoT devices can be expected to receive several feature and performance updates per year, and likely at least one or two security updates. Many current-technology cable TV set-top boxes are updated nightly by their service providers. However, this is driven by consumer market feature competition as well as bug fixes and security updates. Industrial IoT devices should not require daily updates.

Firmware Update Realities

There is only one way to deal with discovered firmware vulnerabilities: install new firmware that has its known vulnerabilities fixed. This is often not be a simple picture for intelligent IoT devices, and network video cameras are a good example of how complex it can get.

Managing firmware can be complicated due to version-dependencies of other device or system firmware or software. This is very true for networked video cameras. Version compatibility must be maintained with video management software's server applications, video analytics applications running on the camera, and video analytics software running on an analytics appliance or server. There are typically two or three such dependencies involved per make and model of camera. Because cameras, as well as the applications and systems that use them, are all evolving technologies these dependencies will remain for the foreseeable future.

Often the Video Management System (VMS) software version must be upgraded first, as well as server-based or camera-based analytics software, prior to the camera firmware upgrade. Thus, industrial IoT device uptime should be defined as the time that the device is available for full use by the system, not just the time that the device is powered up and network-connected. This is especially applicable to security video cameras and is why firmware/software version dependencies are important.

> Industrial IoT device uptime should be defined as the time that the device is available for full use by the system, not just the time that the device is powered up and network-connected.

Testing Firmware Compatibility

It is not enough that the various vendors of video software and camera analytics have lab-tested camera firmware for compatibility with their own products. These are bench-tests performed with test configurations that don't match the configurations used by end-user customers. The firmware of third-party products must be tested with the exact same product configurations that the camera owners are using to ensure full compatibility. Product vendor limited resources don't permit testing that is that extensive.

This means that camera owners, or their service providers, must establish and maintain a capability to test device firmware before deploying it. Organizations with high-camera-count deployments typically maintain a lab environment with systems and devices whose configurations match their deployed counterparts. Smaller organizations typically test selected deployed devices one at a time, which can usually be done with security video systems. For cameras deployed in 24-hour production environments where cameras are required for business reasons – such as a high-speed food or drug production line where video records of each item and its label are critical for quality assurance and compliance reasons – production-area cameras cannot be used for firmware compatibility testing.

Due to the large number of camera industry makes and models, video software manufacturers may not be able to test the firmware for all customer cameras in a time frame that is acceptable to customers. This is sometimes the case with infrared cameras or with cameras where the firmware update only relates to a feature that doesn't directly involve the software functionality, such as the camera's low-light capability. Sometimes the configuration of new firmware features requires a special video software development cycle for that feature. Testing of the camera firmware compatibility may be scheduled for after the software update is completed. Yet customers may want to perform an update sooner per their cybersecurity policy. This is another reason to be prepared for in-house camera firmware testing.

Device Firmware Profiles

Due to the complexities of firmware updates for high device-count IoT device deployments, an evolving best practice among organizations with significant IoT device deployments is the use of product lifecycle management, which includes inventory and control of hardware and software assets. Such asset management has long been an IT best practice and is also a practice mandated by cybersecurity frameworks like the CIS Controls by the Center for Internet Security and the NIST Cybersecurity Framework.

As part of overall device lifecycle management, for each make and model of IoT device, firmware profiles must be defined for each proven-successful combination of camera firmware and related product firmware/software version dependencies. These form the basis of the overall update plan to be followed. Example data to be collected include:

- Camera ID (unique identifier assigned to facilitate camera management)
- Camera Make
- Camera Model
- Original Firmware Version
- Current Firmware Version
- Compatibility Version Dependencies
    - Video Management System (VMS)
        - VMS Name
        - Current VMS Software Version
        - Required VMS Software Version
    - On-Board Video Analytics
        - Analytic Name(s)
        - Current Software version(s)
        - Required Software version(s)
    - Server-Based Analytics
        - Analytic Name(s)
        - Current Software version(s)
        - Required Software version(s)
    - Other system
        - System Name(s)

- Current Software version(s)
- Required Software version(s)

How to best organize the data depends upon the type and amount of data to be collected. The update plan – which can be as simple as a one-page outline – should specify which products, if any, must be updated to which versions before the camera firmware updates can be performed.

Device Firmware Update Procedure

Performing manual camera firmware updates for deployments with more than a few hundred cameras is usually not feasible. Typically, only three to six cameras can be safely updated per hour, *keeping auditable records of task performance*, if a sound manual firmware update procedure is followed. Such a procedure would include:

1. Log the start of the camera's update procedure.
2. From a web browser, connect directly with camera at the specified IP address.
3. Verify the camera make, model and current firmware version (in case the update fails, and the camera must be returned to its previous firmware version).
4. Check the camera error logs to make sure that the camera is not experiencing problems. If it is, note the error log details and put the camera on the service list.
5. Log into the video management system software (VMS) and stop the video recording and viewing streams.
6. Upload the firmware to the camera, then restart it.
7. From the web browser, log into the camera and verify that it is running the correct firmware version. Check the error log for the absence of errors logged during or after the update process.
8. If the update is successful, restart the video recording and viewing streams in the VMS software, and verify them.
9. If not successful, revert the camera back to its previous firmware version, verify the reversion was successful, and restart the video recording and viewing streams in the VMS software, and verify them.
10. Log the completion of the camera's update procedure.

According to service providers for large camera-count deployments, when such a procedure is followed, 1% to 2% of the cameras cannot be updated due to camera error conditions or firmware update failures. However, if steps 4 and 5 are not followed, between 10% and 20% of camera firmware updates could fail, depending upon the makes and models of cameras.

This procedure takes 10 to 15 minutes per camera by a skilled technician familiar with the devices and applications involved, when performed nonstop as a single-focus day-long task, providing that the camera inventory is complete and accurate, and that camera firmware profiles have been fully established in advance. It starts out taking twice as long for sysadmin staff unfamiliar with the devices and applications, but eventually the non-professional staff can sustainably perform the task in 15 to 20 minutes per camera non-stop if closely supervised.

Cybersecurity at Scale Requires Automation

Using network video cameras as an example, it is easy to see that managing cybersecurity for hundreds or thousands of intelligent IoT devices requires automation in order to:

- Eliminate human errors common with complicated repetitive tasks
- Provide detailed auditable records of cybersecurity compliance actions

- Give IoT device owners full control over device passwords, with auditable delegation of limited password responsibility to service providers
- Safely and automatically check for factory default and commonly-used passwords that can be found exist on newly deployed and some updated cameras.
- Reduce the costs for cybersecurity implementation.
- Reduce the staff time involved in password and management by 95%, from many months to just days.
- To make currently infeasible IoT device cybersecurity highly effective and easily sustainable.

For some insight into this picture, let's examine the costs and staff time aspects of updating firmware for 2,000 cameras – well over a $1 million technology infrastructure investment. We'll use the best-case cost and performance figures in Figure 1 below.

Figure 1. Cost and Staff Time to Manually Update Firmware for 2,000 Cameras

Cost Factor	**Value**
Number of Cameras	2,000
Task Hours Per Workday	6.5
Hourly Contractor Technician or Fully Burdened Employee Daily Labor Cost	$75
Daily Contractor or Fully Burdened Employee Daily Labor Cost	$600
Per-Camera Update Time	10 minutes
Cameras Updated per Hour	6
Cameras Updated per Workday	39
Labor Cost to Update Cameras Once	**$30,780**
Per-Camera Labor Cost	$15.38
Staff-Days to Update Cameras Once	51.3 Workdays in 2-1/2 Calendar Months

Add to the above labor cost the cost of supervision, and the cost to manually generate audit reports from the camera update work record logs and inventory. The manual approach of course results in an unverified audit, as there is no record of firmware update mistakes and no validation of the device inventory used. Furthermore, the total cost to perform three update cycles and generate at least one audit report would exceed $90,000 and take eight calendar months.

In reality the costs would be higher than in the above chart, as the chart represents an ideal non-stop high work performance scenario doesn't typically occur for boring human repetitive tasks, even when closely supervised. Jobs of that type typically also have a high turnover rate, involving personnel onboarding and training, further adding to the costs and calendar time for the work.

In contrast, using an automated tool would cost less and would provide 100% accurate audit reports based on electronically verified device states. Most importantly, the staff time required would be five workdays or less per update, not fifty days or more.

Automated and electronically verified processes and procedures are performed exactly as defined per proscribed practices in full compliance with all requirements.

Automated Password Management

Automated password management is an absolute requirement for high device-count intelligent IoT device systems. Once events occur by which passwords may have been compromised, the passwords must be changed immediately. It's not possible to manually change hundreds or thousands of device passwords instantly. That can only be done using automation. Managing unique passwords for each device is not a feasible manual task – but it can easily be done using automation. There is no question that automated password management is fully effective even at very high scale, and less costly. It's the only way to assure full compliance with password management policies for large scale device deployments.

Compliance-Based Device Management

Large organizations adopt a cybersecurity strategy that includes the adoption of a cybersecurity framework consisting of policies and practices which, when followed, establish the level of cybersecurity protection they want to achieve for their technology infrastructure. They monitor and manage compliance to those policies and practices to assure that they achieve their cybersecurity objectives. The U.S. Federal Cybersecurity and Infrastructure Security Agency (CISA) recommends that cybersecurity insurance firms encourage the implementation of best practices by basing premiums on an insured's level of self-protection.[8]

The NIST Cybersecurity Framework and the CIS Controls are two popular and highly-effective self-protection frameworks. Infrastructure asset management, strong password management, and using automation to assure compliance to the selected cybersecurity policies and practices are elements of both frameworks. Having these elements in place can be expected to help reduce the cost of cybersecurity insurance premiums, which some companies negotiate annually.

IoT device infrastructure has been excluded from the scope of IT cybersecurity in the past because the devices and systems were separate from corporate business networks considered to be unlikely targets for attacks. Today, however, camera video systems are now connected to business networks because the provide value to business and facility operations, with the most publicized business applications being retail video analytics and point-of-sale security applications. Unprotected IoT devices and networks are a high cybersecurity risk, and recent high-profile business cyber losses via IoT devices[9] means they need to be managed in accordance with standard corporate IT infrastructure management and security compliance programs.

Comprehensive IoT device firmware profiles as described on page 8 establish an auditable security baseline that enables IT to include IoT systems and devices in its cybersecurity management and reporting activities.

For details of how IT cybersecurity practices and frameworks such as the CIS Controls apply to intelligent IoT device deployment, as well as how purpose-built monitoring and service assurance tools for IoT devices and systems differ from standard IT tools, see the Viakoo online white paper titled, "Video System Cyber and Performance Assurance".

[8] Cybersecurity and Infrastructure Security Agency (CISA), "Cybersecurity Insurance." CISA, 26 November 2018, https://www.dhs.gov/cisa/cybersecurity-insurance

[9] Brian Krebs, "Target Hackers Boke in Via HVAC Company." KrebsOnSecurity.com, 5 February 2014, https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Sustainable Cybersecurity for Intelligent Industrial IoT Devices

Now and going forward, product evaluations, proof-of-concept tests and acceptance tests for intelligent IoT devices must verify that firmware and password management can be performed using automated tools. Secure device configurations should be the default and manufacturers should provide device and system hardening guidance where security configuration options exist.

Now that automated tools are emerging for intelligent IoT device management, organizations can finally secure their industrial IoT infrastructure to the standards they have set for the rest of the organization's critical technology.

About Ray Bernard

Ray Bernard is a security consultant and author who has provided pivotal direction and advice in the security industry and the security profession for over 30 years. Ray is President and Principal Consultant of Ray Bernard Consulting Services (www.go-rbcs.com), a group of highly expert corporate, physical and IT security consultants with outstanding track records in their fields of expertise. Ray has led many noteworthy security projects for international airports, nuclear disarmament facilities, sports stadiums, water districts, electric utilities, manufacturing plants and multiple-tower high-rise facilities.

He is also the Convergence Editor for *Security Technology Executive* magazine, for which he writes the monthly "Convergence Q&A" column as well as a highly-regarded articles about the Convergence of Physical Security and IT. He is a regular contributor to *Security Business* magazine (formerly *Security Dealer & Integrator*). He also writes the *Real Words or Buzzwords?* bi-weekly article series for SecurityInfoWatch.com.

Ray was recently named as one of the IFSEC Top 50 Fire and Security Global Influencers for 2018, #12 in the Security Thought Leadership category. Ray was named one of security's Top 10 Movers and Shakers of 2006 by *Security Technology & Design* magazine.

Ray has recently authored the book, *Security Technology Convergence Insights*, published by Elsevier and available on Amazon and elsewhere. He is a contributing author to the *Encyclopedia of Security Management, Second Edition*, covering the topics "The Convergence of Physical Security and IT", "Access Control Levels", and "Authentication, Authorization and Cryptography."

Ray is a Physical Security Professional (PSP) , a designation awarded by ASIS International, of which Ray is an active member. Ray is a member of and participates in the educational committees of the Physical Security Council, the IT Security Council, and the Security Applied Sciences Council.