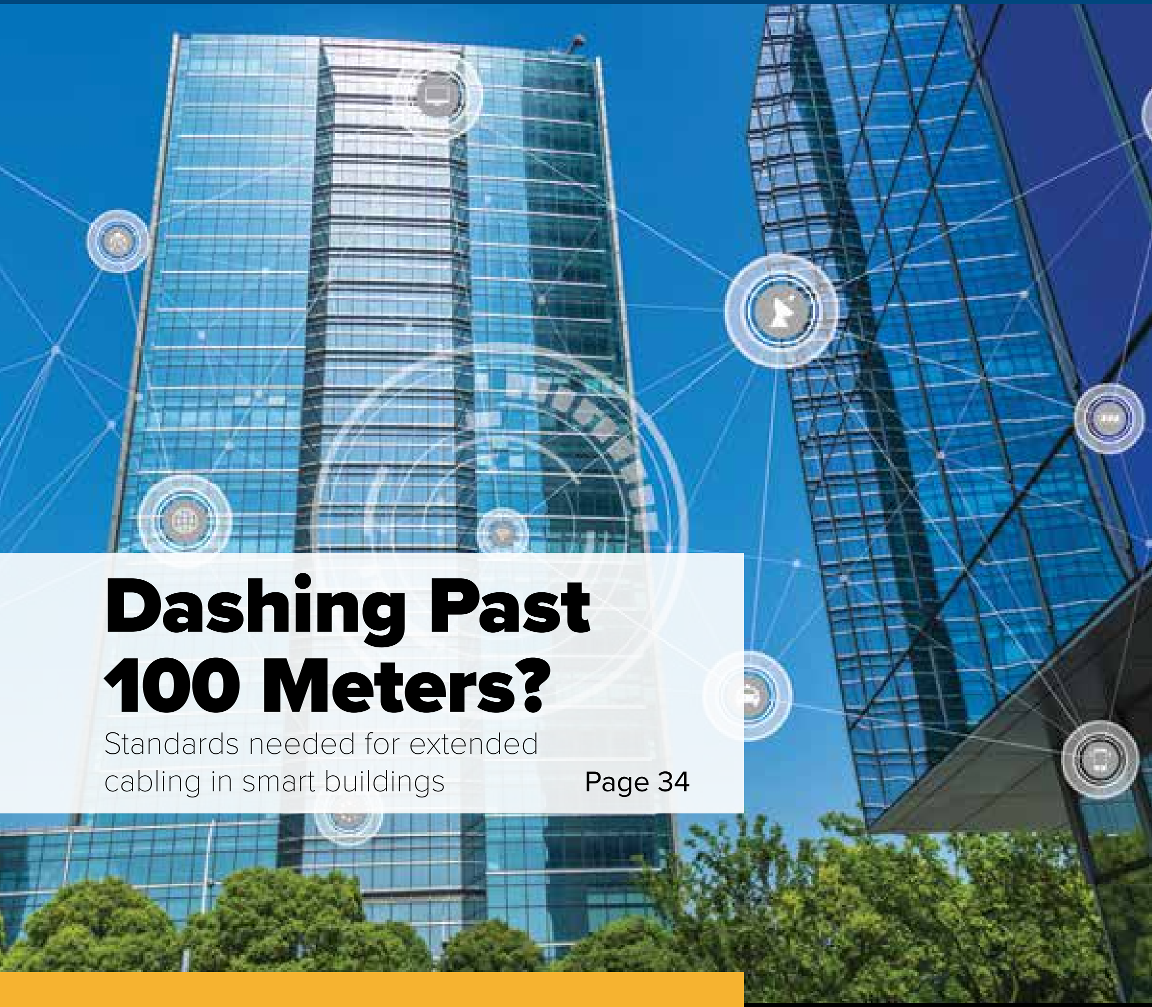
TECHNOLOGY Insights

Fall 2023

Volume 11, Number 2



Dashing Past 100 Meters?

Standards needed for extended cabling in smart buildings

Page 34

Hacking Away

Major incidents lead to more cybersecurity rules

Page 22

Can You Hear Me Now?

A security solution can improve medical outcomes

Page 44

Going Mobile

Credentials on smart devices gaining acceptance

Page 50

SNG™

SECURINGNEWGROUND

Oct. 17 – 18, 2023 | NYC

The Security Industry's Executive Conference

Once a year, the security industry's brightest minds, biggest players and most driven entrepreneurs come together in New York City for two days of information sharing, top-level networking and security industry business analysis. At Securing New Ground trends are spotted, connections are formed, and minds are opened. Join us at SNG!

About Securing New Ground

- Founded in 1996
- The executive conference of the Security Industry Association (SIA)
- 2 days of intelligence sharing, education, analysis and networking
- Attended by 250+ senior-level industry leaders

Attended by Leaders

Luminaries. Entrepreneurs. CEOs of the Leading Companies. Global CSOs. Investors. They're all at SNG.

Securing New Ground has a reputation for attracting the people who drive growth and change – those who will reshape the future of the industry.

> **THE GLOBAL SECURITY MARKET IS EVER EVOLVING** and to stay ahead, you have to understand the market trends and network with the people influencing those trends. That is why **I ALWAYS GO TO SECURING NEW GROUND.**
>
> *Fredrik Nilsson, VP Americas*
> *Axis Communications*

SECURINGNEWGROUND.COM

TECHNOLOGY Insights

Fall 2023 Volume 11, Number 2

SIA Technology Insights is published twice a year, in the spring and fall, by the Security Industry Association in Silver Spring, Md.

All editions are available at no charge at www.securityindustry.org/techinsights.

Questions, comments and article proposals may be submitted to the editor, Ron Hawkins, at rhawkins@securityindustry.org.

Analyzing Data to Protect People and Assets

Intelligent security operations can support comprehensive risk management

Alan Stoddard (alan.stoddard@intellicene.com) is the President of Intellicene (www.intellicene.com).

ORGANIZATIONS ACROSS ALL SECTORS FACE AN ARRAY OF SECURITY AND SAFETY CHALLENGES. From workplace violence and terrorism to theft and natural disasters, the stakes are higher than ever before. It is clear that traditional approaches to protecting infrastructure, people and data are no longer sufficient. As risks continue to evolve, there is a growing need for real-time, predictive responses to ensure the utmost protection.

Security professionals recognize the importance of adopting a fresh perspective. They understand that comprehensive risk management entails modernizing security and safety efforts. At the same time, there has been an exponential increase in the demand for digital transformation.

Because of this, there has also been an unprecedented surge in Internet of Things (IoT) applications. The driving force behind this growth is straightforward: Stakeholders yearn for

greater access to data. The transformation of raw data into valuable information holds the key to making informed decisions and fortifying security measures.

This push for digital transformation has flooded organizations with vast amounts of data from IoT and IP-powered devices. At any given time, a business or facility may be supporting hundreds, if not thousands, of systems and solutions. While some of these technologies are intertwined with other functions, many are powering the security infrastructure. Organizations need modern ways to capture, correlate and analyze data from these investments to make informed decisions.

In mission-critical environments, an integrated response enables comprehensive threat management.

> “AS RISKS CONTINUE TO EVOLVE, THERE IS A GROWING NEED FOR REAL-TIME, PREDICTIVE RESPONSES TO ENSURE THE UTMOST PROTECTION.

Unfortunately, traditional security systems operate in silos, making it nearly impossible to gain meaningful insights. In these disconnected environments, stakeholders must manually coordinate data from multiple systems, which is time-consuming, complex and costly.

The concept of intelligent security operations seeks to address this challenge. It brings together multiple systems and devices into a unified interface, exposing them to an analytic layer. Leveraging artificial intelligence and deep learning tools, critical data is automatically identified, providing a comprehensive view of enterprise-wide activities and their impact on operations. By automating the aggregation of information to detect and protect against risks, organizations have a greater opportunity to establish a predictive threat model.

Collecting intelligence from IoT systems, such as video surveillance cameras, building management systems and

> “ THE TRANSFORMATION OF RAW DATA INTO VALUABLE INFORMATION HOLDS THE KEY TO MAKING INFORMED DECISIONS AND FORTIFYING SECURITY MEASURES.

mobile devices, empowers organizations to identify potential anomalies more efficiently. This approach allows businesses to manage and respond to situations such as theft or product tampering attempts more efficiently.

Organizations that have a single, enterprise-wide view across diverse systems and technologies experience heightened situational awareness, reduced operational costs, and increased employee safety. Furthermore, this centralized approach enables seamless information sharing with external agencies, employees, citizens and first responders, which is particularly valuable when swift action is crucial.

Intelligent, informed operations have become a top priority for security leaders as they strive for increased visibility, control, cost reduction and regulatory compliance. The focus on security combined with the promise of the connected world fosters collaboration among various stakeholders and departments. It empowers employees in facilities and

corporate offices, providing them with continuous visibility, detection, response and incident management capabilities. In any industry, adaptability is key, and the ability to embrace change quickly and effectively leads to improved efficiency and operations. By merging technologies, best practices, and services, leaders can take their operations to the next level.

In this era of heightened security concerns, leveraging the power of data becomes crucial. The industry can take advantage of innovative technologies and a holistic approach to stay one step ahead of evolving threats. With intelligent security operations and a center of intelligence, organizations can achieve comprehensive risk management, make informed decisions, and protect their assets, employees and data. ◀

> "
> LEVERAGING ARTIFICIAL INTELLIGENCE AND DEEP LEARNING TOOLS, CRITICAL DATA IS AUTOMATICALLY IDENTIFIED, PROVIDING A COMPREHENSIVE VIEW OF ENTERPRISE-WIDE ACTIVITIES AND THEIR IMPACT ON OPERATIONS.

Leveraging the Advantages of Access Control and Intercom Integration

When combined, the two systems can enhance security and operations

Brad Kamcheff (brad.kamcheff@aiphone.com) is the Marketing Manager for Aiphone (www.aiphone.com).

TRUSTED AND COST EFFECTIVE, INTERCOMS HAVE LONG BEEN A MAINSTAY in the entry control space. They are recognized as one of the first tried and true technologies to manage access into controlled areas. Today, they continue to be successfully deployed in environments such as multi-tenant facilities, educational institutions, healthcare campuses and corporate offices, to name a few.

On their own, intercoms are a powerful security tool. The technologies within intercoms enable facilities to screen people before permitting entry to a secure area. Two-way audio allows security staff or front desk personnel to communicate with a visitor, while an intercom equipped with an IP camera enables visual verification.

When an intercom is integrated with an access control system, the capabilities of both technologies are enhanced and the solutions work in tandem to improve security. Together, they enable facility directors to screen visitors, track their whereabouts, and document and record access control activities.

For facility executives, having these capabilities is critical to managing access, reducing risk, and ensuring the safety of employees and visitors alike.

> TOGETHER, THEY ENABLE FACILITY DIRECTORS TO SCREEN VISITORS, TRACK THEIR WHEREABOUTS, AND DOCUMENT AND RECORD ACCESS CONTROL ACTIVITIES.

INCREASE SECURITY

The adage “two is better than one” accurately describes the benefits of combining access control and intercoms to significantly enhance building security. Access control systems autonomously prevent unauthorized entrance by requiring a person requesting access to either present a credential

"FACILITY EXECUTIVES CAN LEVERAGE THE NATURAL TWO-FACTOR AUTHENTICATION CAPABILITIES OF A COMBINED ACCESS CONTROL AND INTERCOM SYSTEM.

– such as a badge – enter a passcode on a keypad, or use an enrolled biometric identifier. Intercoms, meanwhile, provide a communication tool and enable front desk staff or security personnel to verify identity and to speak with visitors before they are permitted to enter.

When used together, intercoms and access control systems provide a multi-layered approach to security. This is especially important for sensitive areas like IT server rooms, cash rooms and pharmacies. These spaces typically require both a badge in and badge out action and the ability to identify who was in a space at a particular time through event logging.

Facility executives can leverage the natural two-factor authentication capabilities of a combined access control and intercom system. A secure area such as a cash room may require that an individual announce their presence using the intercom before badging in

through the access control system and entering the space.

IMPROVED MONITORING

It can be challenging for facility managers to monitor building access. Intercom systems combined with an access control platform can alleviate this problem by providing real-time monitoring of both successful and failed access attempts.

If, for example, a person makes several incorrect entries on an access control keypad, security personnel can use the intercom's two-way audio to communicate with the individual. They can ask the person if they need assistance, as in the case of an authorized employee who forgot their entrance code, or, if someone who is not permitted to enter the premises is trying to gain access, security personnel can tell them that they are not authorized and to leave the property.

ENHANCED VISITOR MANAGEMENT

Some spaces, such as schools and certain areas in a hospital, need to always remain secured. A video intercom system allows administrators or security personnel to visually confirm an individual's identity and talk to the person about the nature of their business before permitting them to enter.

When paired with an access control system, personnel can maintain secure areas throughout a facility. A visitor can be given a badge that allows them to only access certain floors in a hospital, or specific wings or areas in a school.

BETTER RECORD KEEPING

Knowing who has entered and exited a building is important, especially in the event of an emergency, such as a fire or an active shooter incident.

Intercoms and access control systems can provide valuable data on all individuals, whether they are employees, delivery people or visitors. An integrated video intercom system can automatically record interactions with visitors at the front door, while the access control component can record access point data, showing exactly where a person entered the building.

By requiring a person to swipe out, not just swipe in, data can be collected to confirm that an individual left an area at a specific

time, or that a person no longer remains in a section of a building that is unsafe.

Swipe-in and swipe-out information can also prove immensely valuable for investigative purposes, as when assets are missing from a secure area or a security breach occurs.

SCALABILITY AND FLEXIBILITY

As a business grows, its security needs to evolve. This is why it is important to install an access control system that is flexible, can scale up to meet the demand for additional door entry controls, and can integrate with other solutions.

A growing medical practice may find that it needs to incorporate several additional intercom systems throughout its facility to provide communication between patients and medical staff. An X-ray technician, for instance, can use the intercom to safely communicate with a patient while standing in another room.

By combining intercoms and access control systems, facility executives can improve security and operational efficiencies in a variety of ways. Security staff can monitor and restrict access into buildings and areas, while taking advantage of the direct line of communication to the person at the door to quickly diagnose and resolve any access control issues. ◀

> “
>
> BY REQUIRING A PERSON TO SWIPE OUT, NOT JUST SWIPE IN, DATA CAN BE COLLECTED TO CONFIRM THAT AN INDIVIDUAL LEFT AN AREA AT A SPECIFIC TIME, OR THAT A PERSON NO LONGER REMAINS IN A SECTION OF A BUILDING THAT IS UNSAFE.

Mapping Security Back to the Business

Data is critical to showing value

Ryan Schonfeld (info@hivewatch.com) is the Founder & CEO of HiveWatch (www.hivewatch.com).

MORE THAN EVER, PHYSICAL SECURITY LEADERS ARE BEING ASKED TO DO MORE WITH LESS (or more with the same) to optimize their security programs and deliver results. This involves a thorough understanding not only of risk, but also of how the business handles that risk – and its potential impact on the bottom line.

It is no secret that, traditionally, security leaders have struggled to tie the value of robust security programs to the overall goals of the business, but one of the key assets that security can now bring to the table is data. For example, using data from a platform that provides a better understanding of a company's third-party guard resources spend, operator efficiencies, device health, and hours spent on false alarms can point to savings in time and resources. Providing this level of insight can enable security leaders to make meaningful operational decisions that save money for the business and, thus, shift security from more of a cost center to more of a business enabler.

The hours that security operators spend just triaging false alarms, for example, can be considerable. If a security leader can calculate this time expenditure, they can use the data to persuade upper management to invest in a tool that will remediate the issue.

How can this be achieved? There are three things that need to be addressed when planning a conversation with company leadership.

> “PROVIDING THIS LEVEL OF INSIGHT CAN ENABLE SECURITY LEADERS TO MAKE MEANINGFUL OPERATIONAL DECISIONS THAT SAVE MONEY FOR THE BUSINESS AND, THUS, SHIFT SECURITY FROM MORE OF A COST CENTER TO MORE OF A BUSINESS ENABLER.

WHERE TO START

The place to begin is with an assessment. A security program cannot be optimized without first knowing what is currently in place – the data coming in, the risks being addressed, and the segments of the budget that require analysis.

PLANNING A CONVERSATION WITH COMPANY LEADERSHIP

- ▶ Begin with an assessment that identifies the unique needs of each site.
- ▶ Engage stakeholders and encourage communication within – and between – all levels.
- ▶ Deploy data-driven solutions that maximize technology investments.

The initial assessment, then, is critical to every other decision that will be made and mapped back to the original objective of meeting business goals.

This can also mean that not every site within a security program is going to fit into a cookie cutter outcome. The needs of the program will vary based on the business needs of the site, along with the ultimate goal of the site. For example, in a high-crime area, more guards, cameras and other technologies may be necessary.

There are ways for security leaders to look at the overall design of each site and determine not only where the spend occurs, but also where savings can be found. In addition, it is important to examine how spending and needs have changed with the increase in hybrid and remote work. This might free up additional budget that can be used for technology improvements.

WHO IS INVOLVED

Engaging stakeholders at all levels provides security teams with the ability to identify potential roadblocks to success as they relate to physical security program implementation. Building community within the security team by encouraging leaders to listen to the concerns of operators and sharing them with executive leadership can help build morale. It can also reduce turnover, which can be a drain on resources and budgets at a time when security staffing is scarce.

Establishing a baseline with their teams will set leaders up for success because the group will be able to identify what the security strategy will be. Without this key piece of the puzzle, teams will not be empowered to make cost-cutting decisions that align with business goals. Rather than top-down, it becomes a shared community initiative.

Discussions should include teams on the ground, not just those in the C-suite. At sites in high-risk areas, it is important to listen to employees and understand what will make them feel safe going to and from work. The balance becomes listening and learning with actionable processes and policies.

Another avenue to pursue is a risk-based approach. Many successful security leaders partner with business continuity teams and crisis management teams to understand the various exposures of their assets to risk and tie this risk back to business interests.

> A SECURITY PROGRAM CANNOT BE OPTIMIZED WITHOUT FIRST KNOWING WHAT IS CURRENTLY IN PLACE – THE DATA COMING IN, THE RISKS BEING ADDRESSED, AND THE SEGMENTS OF THE BUDGET THAT REQUIRE ANALYSIS.

CONSIDER TECHNOLOGY ENHANCEMENTS

Once a security program gathers risk assessments and input from stakeholders, then decisions can be made about how to provide more comprehensive, data-driven approaches.

Focusing on deployments that help to avoid the “rip-and-replace” cycle that

> FOCUSING ON DEPLOYMENTS THAT HELP TO AVOID THE "RIP-AND-REPLACE" CYCLE THAT MANY SECURITY LEADERS FIND THEMSELVES IN CAN HELP MAKE IT EASIER TO NAVIGATE FINANCIAL DISCUSSIONS.

many security leaders find themselves in can help make it easier to navigate financial discussions.

In order to leverage the technology that is already in place, investments should be made in platforms and systems that are vendor-agnostic. In addition, organizations can begin layering artificial intelligence (AI) technology that allows operators to identify false alarms, find the root cause of alarms, and respond quickly and efficiently to real threats.

Security technology enhancements can improve business operations in multiple ways.

- **Reduce administrative burdens:** Mobile-first management, such as mobile credentials,

and remote access technology advancements can significantly decrease the demand on time and resources.

- **Enhance how data is collected:** This encompasses the use of low-cost movable sensors that are emerging in the market; things like proximity sensors, lower-cost technologies to collect data that can be an alternative to rip-and-replace. These investments may not be long term, but they can provide significant value and help gather more data for security teams.
- **Optimize the data:** System centralization and the integration of disparate security devices and data from cameras, access control, environmental sensors, and more allows leaders to visualize incoming data in a meaningful way. This takes some of the highly manual, time-intensive tasks – like clearing large numbers of false alarms – from operators, giving them time to perform more meaningful work and provide more value to the business.

Security leaders have the monumental responsibility of not only keeping people, assets and the brand safe, but also ensuring that the work they do is aligned with business goals. This is the only way for physical security to show value, put a spotlight on risk, and move the needle for the company they serve. ◀

Cybersecurity Incidents Lead to New Standards, Requirements

Mirai, SolarWinds push U.S., E.U. to act

Wayne Dorris (wayne.dorris@axis.com) is Business Development Manager - Cybersecurity for Axis Communications (www.axis.com).

MAJOR CYBERSECURITY BREACHES HAVE HISTORICALLY LED TO STANDARDS AND LEGISLATION ACROSS THE GLOBE aimed at preventing similar incidents, up to and including the recent announcement from the White House about a new cybersecurity labeling program for Internet of Things (IoT) devices. Similarities in standards from different countries are helping global manufacturers comply.

Virtually no security manufacturers are exempt from the perils of cybercrime. If an event were to occur, the results could be ruinous on many levels, particularly financial. Cybercrime is the greatest threat to every company in the world, according to a Cybersecurity Ventures report that expects global cybercrime costs to grow by 15 percent per year over the next three years, reaching a level of $10.5 trillion by 2025. The vast costs of cybercrime include damage and destruction of data, financial loss, theft of intellectual property, theft of personal and financial data, loss of productivity, disruption to business, and reputational harm.

Because the traditional security industry relies on a multi-tiered model where many products go from manufacturer to distributor to security integrator to end user, manufacturers often are unaware of the final destinations of – and applications for – their products. Therefore, they should understand the provisions of relevant cybersecurity standards – not just those in the United States but around the world.

Many cybersecurity standards in the U.S. are directed at the 16 critical infrastructure

> “THE VAST COSTS OF CYBERCRIME INCLUDE DAMAGE AND DESTRUCTION OF DATA, FINANCIAL LOSS, THEFT OF INTELLECTUAL PROPERTY, THEFT OF PERSONAL AND FINANCIAL DATA, LOSS OF PRODUCTIVITY, DISRUPTION TO BUSINESS, AND REPUTATIONAL HARM.

16 CRITICAL INFRASTRUCTURE SECTORS IDENTIFIED BY DHS:

1. Chemical
2. Commercial Facilities
3. Communications
4. Critical Manufacturing
5. Dams
6. Defense Industrial Base
7. Emergency Services
8. Energy
9. Financial Services
10. Food and Agriculture
11. Government Facilities
12. Healthcare and Public Health
13. Information Technology
14. Nuclear Reactors, Materials, and Waste
15. Transportation Systems
16. Water and Wastewater

sectors identified by the Department of Homeland Security (DHS). Video surveillance, access control, intrusion detection, and intercom systems are commonly deployed in all 16 DHS-defined sectors. Physical security device manufacturers must ensure that their products have a secure default baseline with additional hardening measures able to be configured. Complying with cybersecurity standards is good business, regardless of whether or not such compliance is mandated and enforced.

While some cyber professionals may want to know what to expect in the future, it is difficult to anticipate coming requirements. At their foundation, cybersecurity standards – and subsequent legislation that puts teeth into many standards – almost always are based on the fallout from cybersecurity incidents. The two most significant recent incidents in the cybersecurity timeline were the Mirai botnet of 2016 and the SolarWinds breach of 2020.

THE MIRAI BOTNET

The Mirai botnet was responsible for some of the biggest and most disruptive distributed denial-of-service (DDoS) attacks in the eastern U.S. and parts of Europe. The malware attacked and infected IoT devices, such as smart home security cameras and routers, by using default username and password combinations, turning the devices into malicious bots that attacked larger networks. This led, over several days, to massive website outages that affected some of the Internet's most prominent sites, including Amazon, Twitter, Netflix, PayPal, Reddit and others.

The response to Mirai from both the U.S. and Europe was a call for a basic level of security in all IoT devices. Many security industry products, like network surveillance cameras, are considered to be at the high end of the IoT scale. However, there are many low-end, consumer IoT products that have limited security features because they are created quickly, are low cost, or are too small to contain extensive compute power.

Four years after Mirai, the IoT Cybersecurity Improvement Act of 2020 required the National Institute of Standards and Technology (NIST) to develop standards and guidelines for federal agencies on how to secure IoT devices. Following up on the consumer IoT baseline that NIST had developed in 2017, more measures were added to raise the security requirements for devices going onto a federal network.

An additional response to the Mirai cyberattack, as well as ongoing attacks on critical infrastructure, was the establishment by the U.S. Department of Homeland Security (DHS) of the Cybersecurity & Infrastructure Security Agency (CISA) in 2018. CISA

> “WITH EO 14028, THE FEDERAL GOVERNMENT ALSO TURNED TO “ZERO TRUST” ARCHITECTURE – A SECURITY MODEL, A SET OF SYSTEM DESIGN PRINCIPLES, AND A STRATEGY BASED ON AN ACKNOWLEDGEMENT THAT THREATS EXIST BOTH INSIDE AND OUTSIDE TRADITIONAL NETWORK BOUNDARIES.

“

EO 14028 AND NIS2 SHOW HOW TWO MAJOR GLOBAL ENTITIES HAVE WORKED TO ALIGN CYBERSECURITY REQUIREMENTS.

is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience.

THE SOLARWINDS BREACH

In 2020, SolarWinds Corporation was at the center of what Microsoft President Brad Smith described as “the largest and most sophisticated attack the world has ever seen.” The hack targeted the network management company’s Orion software, injecting it with malware that was then sent to approximately 18,000 public and private organizations through a customer software update. This “supply-chain cyberattack” gave hackers wide access to both government and corporate information systems.

The response in the U.S. to the SolarWinds breach was a May 2021 executive order by the Biden administration (EO 14028) that charged multiple agencies – including NIST – with enhancing cybersecurity through a variety of initiatives

related to the security and integrity of the software supply chain. One of the key components of the order is that it provides clarity on how the government and private sector should collaborate to improve cybersecurity.

Some of the provisions of EO 14028, which directs that “all federal information systems should meet or exceed the standards and requirements for cybersecurity,” came from existing NIST guidelines, such as the Secure Software Development Framework (SSDF). This is an important tool as most IoT devices were focused on coding only what was needed for the device to function. SSDF ensures that password complexity, authentication, encryption, software updates, and vulnerability management occur throughout a product’s lifecycle. Putting security into software in the design phase is more efficient than trying to change or adapt code after it has been released. EO 14028 requires that companies that license or sell software to federal agencies attest that they follow SSDF guidelines.

SSDF provides software developers with a set of practices that, when implemented, help reduce vulnerabilities. Some manufacturers, especially global ones, may already have been in compliance with SSDF, because the principles are also a part of the European Union's Secure by Design framework.

Another key component of EO 14028 is the directive to issue guidance identifying practices that enhance the security of the software supply chain. Companies that the federal government procures products from must provide a software bill of materials (SBOM) for each product, either directly or by publishing it on a public website. Consider the operating system of a camera or audio device, for example. In addition to the manufacturer's own code, that operating system also may contain open-source software and be built up from thousands of other components.

During product procurement, an SBOM provides the government with a formal record of the details and supply chain relationships of various parts used in developing software. This requirement is a response to not knowing, with SolarWinds, exactly what components were part of the Orion software. It can help

agencies stay informed about which pieces are secure and which may have vulnerabilities.

With EO 14028, the federal government also turned to “zero trust” architecture – a security model, a set of system design principles, and a strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. It eliminates implicit trust in any one element, node, or service and replaces it with continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses. If a device is compromised, zero trust can help contain the damage.

The European Union, in response to the SolarWinds breach, issued the NIS2 Directive in November 2022. NIS2 prescribes minimum security requirements and mandates the reporting of serious incidents to national authorities or the European Computer Security Incident Response Team. While its earlier iteration, NIS1, already applied to essential businesses, the new directive also covers “important” medium and large companies, such as those in manufacturing and the food industry, digital providers, postal and courier services, and several others.

“UNDER NIS2, COMPANIES THAT FAIL TO COMPLY AFTER A WARNING RISK BEING FINED UP TO 10 MILLION EUROS OR 2 PERCENT OF THE ORGANIZATION’S GLOBAL ANNUAL REVENUES.

NIS2’s cybersecurity requirements, in essence, mimic those found in EO 14028. In addition to four overarching directives that focus on risk management, corporate accountability, reporting obligations, and

EO 14028 PROVISIONS INCLUDE:

- ▶ Removing barriers to sharing threat information
- ▶ Modernizing federal government cybersecurity
- ▶ Enhancing software supply chain security
- ▶ Establishing a cyber safety review board
- ▶ Standardizing the federal government's playbook for responding to cybersecurity vulnerabilities and incidents
- ▶ Improving detection of cybersecurity vulnerabilities and incidents on federal government networks
- ▶ Improving the federal government's investigative and remediation capabilities

business continuity, there are 10 baseline security measures that essential and important businesses must implement:

- ■ Risk assessments and security policies for information systems
- ■ Policies and procedures for evaluating the effectiveness of security measures
- ■ Policies and procedures for the use of cryptography and, when relevant, encryption
- ■ A plan for handling security incidents
- ■ Security around the procurement of systems and the development and operation of systems; this means having policies for handling and reporting vulnerabilities
- ■ Cybersecurity training on basic computer hygiene
- ■ Security procedures for employees with access to sensitive or important data, including policies for data access; affected organizations must also have an overview of all relevant assets and ensure that they are properly handled
- ■ A plan for managing business operations during and after a security incident; this means that backups must be up to date, and there must also be a plan for ensuring access to IT systems and their operating functions during and after a security incident
- ■ The use of multifactor authentication, continuous authentication solutions, voice, video, and text encryption, and encrypted internal emergency communication, when appropriate
- ■ Security around supply chains and the relationship between the company and direct supplier; companies must choose security measures that fit the vulnerabilities of each direct supplier and must assess the overall security level for all suppliers

SOME ALIGNMENT AMONG STANDARDS

EO 14028 and NIS2 show how two major global entities have worked to align cybersecurity requirements. This is particularly seen in such requirements as multifactor authentication and zero trust, the unification of incident response, and reporting obligations.

However, one stark difference between EO 14028 and NIS2 concerns penalties. While EO 14028 is intended to help private companies become more cybersecure, there are no penalties – financial or otherwise – that can be imposed. Under NIS2, though, companies that fail to comply after a warning risk being fined up to 10 million euros or 2 percent of the organization’s global annual revenues. As the NIS2 Directive is set to be transposed into law by Oct. 17, 2024, affected organizations should take steps to improve their cybersecurity posture in order to prepare for compliance. This includes global manufacturers who already sell products in E.U. countries.

CYBERSECURITY LABELING PROGRAM

One section of EO 14028 directs the secretary of commerce to initiate pilot programs to educate the

> UNDER THE PROPOSED FEDERAL PROGRAM, CONSUMERS WOULD SEE A NEW SHIELD LOGO ON PRODUCTS THAT MEET CYBERSECURITY CRITERIA PUBLISHED BY NIST.

public on the security capabilities of IoT devices and software development practices, and to consider ways to incentivize manufacturers and developers to participate in these programs.

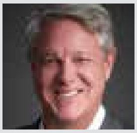
On July 18, 2023, the Biden administration announced a cybersecurity certification and labeling program to help American consumers more easily choose smart devices that are safer and less vulnerable to cyberattacks. The new "U.S. Cyber Trust Mark" program proposed by the Federal Communications Commission (FCC) would raise the bar for cybersecurity across common devices, including smart appliances, smart home control systems, smart personal

devices, and more. In addition, several major electronics, appliance and consumer product manufacturers, retailers and trade associations have made voluntary commitments to increase cybersecurity for the products they sell. Under the proposed federal program, consumers would see a new shield logo on products that meet cybersecurity criteria published by NIST. The FCC is seeking public comments on the program, which is expected to be up and running by late 2024.

As cyber criminals get more sophisticated, cybersecurity protections must become more advanced. Cybersecurity standards can help address threats and provide guidance on secure methods of product development, security controls, vulnerability, and lifecycle management. As NIST explains, “Well-developed cybersecurity standards enable consistency among product developers and serve as a reliable metric for purchasing security products.” ◀

Security Installations in a Wireless World

Smart buildings demand a future-ready infrastructure



Bill Geary (https://www.linkedin.com/in/bill-geary-9550a312b/) is Executive Vice President & General Manager – Communications & Security Solutions for Wesco (www.wesco.com).

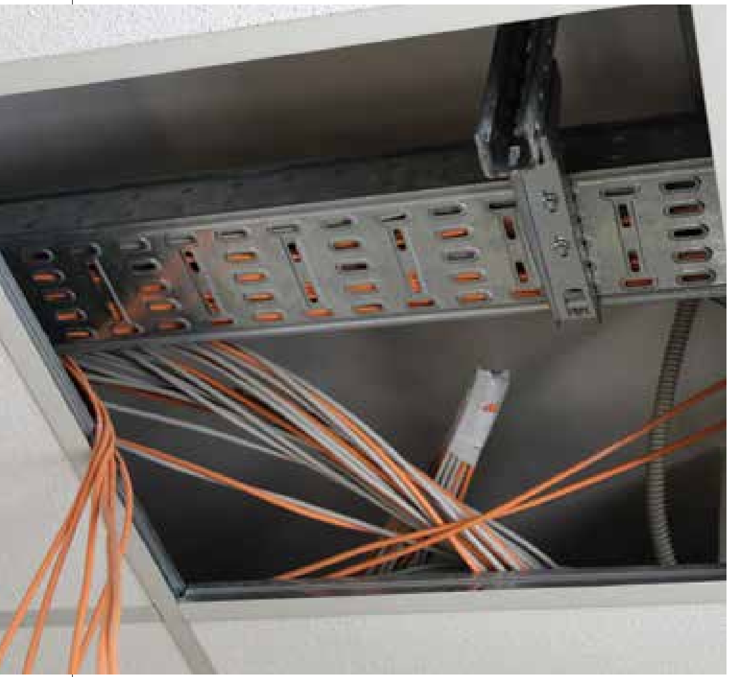
IN RECENT YEARS, BUILDING INFRASTRUCTURE HAS BEEN REDEFINED to include communication systems and broadband networks, with cabling playing as important a role in the foundation of a building as concrete and plumbing. Smart buildings and the Internet of Things (IoT), along with connected devices that deliver improvements and advances in the workplace, have accelerated this redefinition of what infrastructure entails.

Always-on connectivity is required to provide the benefits of smart buildings and IoT enablement, and without a future-ready infrastructure, a building simply cannot operate at maximum efficiency. Further, the pace of technological advancements is increasing the number of devices and the amount of data and power needed to make it all work. With technology outpacing every other lifecycle in the built environment, the cost of technology refreshes far outstrips

the initial investment in high-performance infrastructure.

Smart buildings are no longer a trend, they are an expectation. In commercial buildings, IoT improves the operation of environmental controls, lighting, safety and security – all of which have an impact on sustainability initiatives. And the development of the connected ceiling has led to an entire ecosystem directly above that enables not just lighting, but also access points and a multitude of devices.

Another element to consider is that standards development is not keeping pace with smart building technology. There is a direct correlation between the increase in connectivity demands and the need for beyond-standards verification. The Communications Cable and Connectivity Association (CCCA) recently published a whitepaper on the need to measure beyond-standards performance. It calls out the trends requiring a verifiable testing capability that will eventually create new standards for cabling installations.



Considering technology refreshes on networking gear, the emergence of IoT in the workplace, and the continued explosion of demand for technology at the edge, there is a clear need for a robust foundational layer that can support the growth and operation of these building subsystems. The inevitable conclusion is that, for a relatively small increase in upfront investment, clients will have an infrastructure capable of supporting escalating bandwidth needs through multiple generations of technology, without

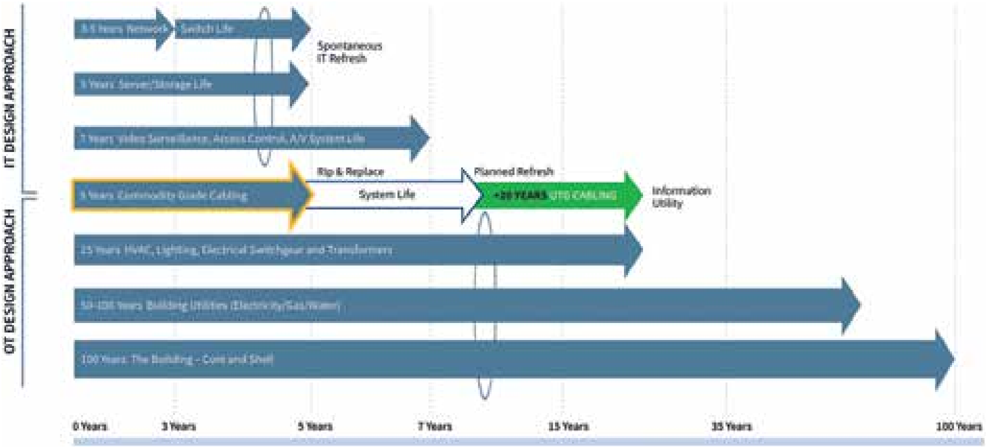


Figure 1. Lifecycles across the built environment

having to replace their cabling infrastructure in the middle of its lifecycle. This, ultimately, saves money on the cost of future upgrades.

Technological advances in the development of the mobile phone illustrate this. Just 20 years ago, the capabilities of a phone were limited to calls and rudimentary texting. But, on June 29, 2007, all that changed. The iPhone made a cellphone smart, with photos, video, and an entire cottage industry of applications. Something similar can be said of buildings where applications in both IT and OT are joined together on a common network.

With this convergence of trends, there are new capabilities and expectations that require a new way of looking at infrastructure and its importance to every element of operations, including security, within the commercial building. Technologies that are not even being considered today will be deemed essential tomorrow.

> STANDARDS DEVELOPMENT IS NOT KEEPING PACE WITH SMART BUILDING TECHNOLOGY.

EVOLUTION OF SECURITY IN COMMERCIAL BUILDINGS

Security solutions for commercial buildings have evolved from locks with keys and guards patrolling with dogs to access-controlled doors and camera surveillance. The 1990s brought two pivotal developments to the security industry: the creation of the first IP surveillance camera and the use of radio frequency identification (RFID) for access control. With these innovations, building security could be managed from a central location, occupancy data could be collected and analyzed, and better processes for emergencies within the facility could be developed. Additionally, these inventions became catalysts for other advances in physical security, such as server-based networking and data management, as well as video management systems shifting to video analytics.

Since 2000 – and mostly in the past 15 years – there has been an increase in new technologies and systems to support the many needs of commercial buildings, and, with it, a more urgent requirement for fail-proof infrastructure. For

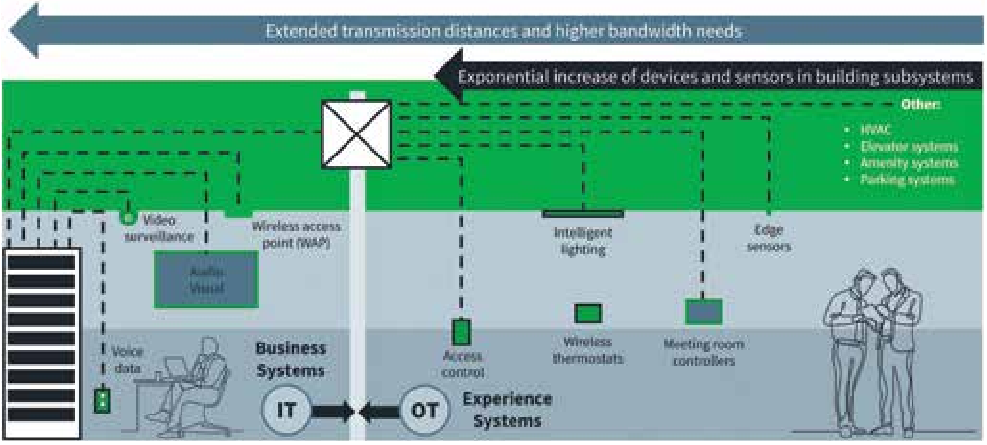


Figure 2. The convergence of IT and OT building subsystems

example, the traditional surveillance camera started as CCTV, evolved to recordings and better optics, and ultimately become a sensor platform offering numerous applications, including condition monitoring, productivity data, safety, and even facial recognition.

The most recent development in the evolution of commercial building security comes from the connected ceiling – or digital ceiling – that utilizes the lighting network. Adding sensors to HVAC and other systems makes the workplace more comfortable for employees and guests, while delivering energy efficiency. The open access and flexibility of a ceiling's design also makes it effective as a digital space. The addition of new or upgraded devices like wireless access points and ceiling cameras is relatively easy compared to the difficulties of installing behind walls.

> “
>
> TECHNOLOGIES THAT ARE NOT EVEN BEING CONSIDERED TODAY WILL BE DEEMED ESSENTIAL TOMORROW.

With the rising number of connected systems on a network and their increasing importance in building security, it is essential for the cabling that keeps them all running to provide reliable performance and scalability.

POWER REQUIREMENTS FOR COMMERCIAL BUILDINGS

Security installations are among many technology evolutions underway. But there is one common element to all of these technologies: they need electrical power. A building and its subsystems and applications can be powered in a number of ways, and the alphabet soup of choices is growing. DC, AC, PoE, FMP, SPE, plus the associated cabling selections for fiber, copper and hybrid, are among the options, with the central considerations for installers being integration simplification and craft friendliness.

The current recommendation for a smart building that checks the boxes for installation simplification and ease of use and maintenance for end users is Power over Ethernet (PoE). With a structure that can deliver both power and data over a single cable, PoE is increasingly the power system of choice for state-of-the-art commercial buildings. However, designers and decision makers may not be fully aware of PoE capabilities.

PoE is increasingly helpful for security installers who want to

expand their capabilities, as well as scale operations to include installation of various endpoint devices in order to increase overall market share. The convergence of IT/OT applications and additional low-voltage installations provide security installers with the ability to grow their businesses with increased capabilities in low-voltage products and solutions.

GOING PAST 100 METERS

Not long ago, the commercial building industry was excited about the possibilities presented by smart buildings, but it was not prepared to take advantage of the benefits. Digital transformation, IoT and IT/OT convergence were all buzzwords and good ideas, but they were something for the future. Now, digital transformation and IoT are top of mind for nearly every organization, regardless of industry or market. And as IoT enablement and digitalization takes hold, IT/OT convergence will continue to be a top priority.

> WITH THE RISING NUMBER OF CONNECTED SYSTEMS ON A NETWORK AND THEIR INCREASING IMPORTANCE IN BUILDING SECURITY, IT IS ESSENTIAL FOR THE CABLING THAT KEEPS THEM ALL RUNNING TO PROVIDE RELIABLE PERFORMANCE AND SCALABILITY.

The CCCA pointed out the need for extended cabling distance measurements and standards: “We are seeing movement in creating extended distance standards, which will help eliminate confusion in the marketplace and prevent manufacturers from making marketing claims without the testing to back them up.”

Though there are some striking claims around extended distance and performance, they are not rigorously tested by unbiased third parties, and they are not the same as achieving validation, verification or testing and measurement that can equate to a standard. The CCCA whitepaper goes on to say, “Anyone looking to extend the distance of twisted-pair copper cabling beyond 100 meters should talk to their cabling manufacturer and ask the right questions to verify performance before investing. If marketing claims appear farfetched, look to reputable cable manufacturers that stand by empirical evidence and warranty their cables for applications and power levels to realistic distances."

OPTIONS FOR EXTENDED REACH

With extended reach solutions in demand and standards bodies showing interest in developing new requirements, how can installers drive future-readiness now and ensure a quality installation? There are a handful of measures that can be implemented to run a network beyond 100 meters and increase the number of endpoint devices served by the infrastructure.

Adding a TR (telecommunications room) closet is one way to ensure that devices have the power and bandwidth needed to operate while staying at or below the 100-meter distance limitation. These are relatively small, localized network closets or rooms with switches and network gear that extend connectivity to the areas of a building beyond the

100-meter mark. It is the most expensive option for extending reach in a commercial building.

Using an extender is another way to move network distances beyond 100 meters. They are more cost effective than TRs, but they require a power supply on both ends. When connecting to multiple devices, a switch is also needed at the device end.

All of the factors mentioned above – infrastructure, power, standards and extended distance – are underpinned by one thing: performance. Infrastructure needs to perform at a certain level, which is why standards were created. Every power source is measured by performance factors and is subject to standards. Now, standards performance testing is needed to validate solutions that extend networks beyond 100 meters.

As CCCA noted, "It wasn't long ago that we saw cabling standards established, and now the industry simply wouldn't operate without them. While industry standards do not currently address extended-distance deployments due to all the variables, there is light at the end of the tunnel. Collaborative efforts between several cable manufacturers, standards bodies, and distributors are already helping to establish verified methods of measurement that guarantee results and protect design intent for extended reach, standards-based installations."

All of this highlights the importance of security integrators staying up to date on current and upcoming trends. The demands on infrastructure related to distance, bandwidth and number of endpoint devices, combined with developments in power and technology, are enabling more and more low-voltage installations that once required a specialist but can now be included with other endpoint device and sensor installations. For the well-informed security installer, this can offer the opportunity to grow a business with not only more cameras, but also increased capabilities across the technology stack supported by a future-ready infrastructure. ◀

Enhancing Communication to Improve Medical Outcomes

Real-time audio solutions provide multiple benefits to clinicians and patients

IN THE FAST-PACED AND HIGH-STAKES ENVIRONMENT OF THE HEALTHCARE INDUSTRY, effective communication can make the difference between successful outcomes and disasters. Real-time audio solutions have revolutionized healthcare communication, providing healthcare professionals with swift and accurate information exchange capabilities that enhance collaboration and decision-making and lead to better patient outcomes.

The solutions facilitate immediate access to vital information, allowing healthcare professionals to share updates, medical data, and test results seamlessly. They can significantly reduce diagnosis and treatment times, improving efficiency and, ultimately, saving lives. Additionally, they ease coordination during complex medical procedures that require multiple clinicians.

Tom Reilly (t.reilly@commendusa.com) is the President of Commend Americas (www.commendusa.com).

OPTIMIZING WORKFLOWS AND ENHANCING SAFETY

By integrating real-time audio solutions into healthcare facilities, communication barriers are broken down and workflows are optimized. This leads to more efficient patient care, reduced medical errors, and improved patient safety. Healthcare professionals can quickly consult with experts, call for assistance, or escalate emergencies, creating a safer environment for patients and staff.

The solutions also contribute to heightened situational awareness within medical settings. By providing instantaneous updates on patient conditions, vital signs, and medical equipment status, they enable healthcare professionals to respond swiftly to changes and take proactive measures to prevent adverse events. This increased awareness leads to better decision-making, reducing the risk of medical complications.

> HEALTHCARE PROFESSIONALS CAN QUICKLY CONSULT WITH EXPERTS, CALL FOR ASSISTANCE, OR ESCALATE EMERGENCIES, CREATING A SAFER ENVIRONMENT FOR PATIENTS AND STAFF.

THE INTEGRATION OF REAL-TIME AUDIO SOLUTIONS WITH ELECTRONIC HEALTH RECORDS HAS PROVEN TO BE A TRANSFORMATIVE COMBINATION.

With advancements in real-time audio technology, healthcare professionals can remotely monitor patients through two-way audio and video. This capability is especially beneficial for telemedicine and virtual consultations, allowing healthcare providers to assess patients’ conditions, provide guidance, and make informed decisions, regardless of location.

SEAMLESS INTEGRATION AND EFFICIENCY ENHANCEMENTS

The integration of real-time audio solutions with electronic health records (EHRs) has proven to be a transformative combination, streamlining healthcare communication and patient care. This innovative approach allows healthcare professionals

to gain immediate access to critical patient data during conversations and consultations. By eliminating the need for manual information retrieval, the integration provides caregivers with up-to-date information, facilitating quicker decision-making and better patient outcomes.

One solution that exemplifies the power of seamless integration is a comprehensive virtual care system that seamlessly integrates with an industry-leading EHR platform. By embedding directly into the EHR system, this solution eliminates the need for siloed third-party platforms and additional licenses, ensuring that healthcare professionals can access all essential patient information from a single interface.

The benefits of this integration are far-reaching. Not only does it enhance efficiency by reducing documentation and workflow efforts, it also allows healthcare teams to collaborate more effectively, breaking down communication barriers between departments and fostering a sense of shared responsibility for patient outcomes.

FUTURE OF HEALTHCARE COMMUNICATION

Real-time audio solutions are expected to become even more sophisticated, incorporating artificial intelligence (AI) and machine learning algorithms to analyze data, detect anomalies, and provide actionable insights. These advances will further enhance medical decision-making and contribute to more personalized patient care.

The technology has emerged as a transformative force in the healthcare industry, revolutionizing communication and patient care. With the ability to facilitate swift and accurate information exchange, optimize workflows, enhance situational awareness, and support remote patient monitoring, real-time audio solutions are driving improvements in healthcare outcomes and patient safety. As the technology advances, the potential for additional innovation and integration can support a more

efficient, collaborative, and patient-centric healthcare landscape.

In the not-so-distant future, the continued evolution of the technology will empower healthcare professionals with AI-driven support, immersive training experiences, and seamless integration with other cutting-edge technologies. This ongoing revolution in healthcare communication is leading to a future in which timely and informed decisions are the norm, and patients receive the best possible care regardless of their location or medical condition. The potential positive impact on healthcare outcomes is immense. ◀

> “THE CONTINUED EVOLUTION OF THE TECHNOLOGY WILL EMPOWER HEALTHCARE PROFESSIONALS WITH AI-DRIVEN SUPPORT, IMMERSIVE TRAINING EXPERIENCES, AND SEAMLESS INTEGRATION WITH OTHER CUTTING-EDGE TECHNOLOGIES.

Mobile Access Gains Ground in the Security Industry

BLE, NFC, UWB power flexible solutions

Ivan Kravchenko (ivan.kravchenko@corewillsoft.com) is the Founder and CEO of CoreWillSoft (www.corewillsoft.com).

IN AN INCREASINGLY CONNECTED WORLD, SMARTPHONES ARE NO LONGER MERE COMMUNICATION DEVICES. They have evolved into multi-functional gadgets that are deeply interwoven into our daily lives, serving both personal and professional needs.

From ordering a meal to managing complex business processes, smartphones' expansive applications have revolutionized many sectors, including the security industry. One trend that has emerged prominently in the security landscape is mobile access, spurred by the multiplicity of business use cases that smartphones cater to.

The need for mobility and real-time access is more pronounced than ever. Consequently, mobile access is becoming increasingly adopted within the security industry, driven primarily by technologies such as NFC (near-field communication), BLE (Bluetooth low-energy), and UWB (ultra-wideband).

The early wave saw BLE technology gain substantial momentum, but the tide is gradually shifting toward NFC and mobile wallets. UWB, with its ability to measure precise distances (in conjunction with BLE), has significant potential, especially in use cases like car unlocking. However, the transition to mobile access also brings its share of challenges, such as data security and privacy, debates over personal or corporate device ownership, and acceptance

> THE EARLY WAVE SAW BLE TECHNOLOGY GAIN SUBSTANTIAL MOMENTUM, BUT THE TIDE IS GRADUALLY SHIFTING TOWARD NFC AND MOBILE WALLETS.

> BIOMETRICS AND OTHER MULTIFACTOR AUTHENTICATION MECHANISMS TO ENSURE CREDENTIAL-TO-DEVICE BINDING OFTEN COMPLEMENT MOBILE ACCESS FOR ENHANCED SECURITY.

levels among employees.

Mobile access has several advantages, including flexibility that allows for remote and spontaneous granting and withdrawal of access permissions. It enhances security through multifactor authentication and introduces a host of usability concepts. For instance, mobile devices and smartwatches can facilitate hands-free opening, location-based verifications, and more. But there are disadvantages too, including technical hurdles to integrating smartphones into existing infrastructures. Also, mobile access lacks the visible identity confirmation that physical badges provide.

Mobile access rides on the back of several technological innovations. NFC, BLE and UWB facilitate communication between devices over short distances. Remote access via IP comes into play when the access control system is accessible from outside the company intranet. Biometrics and other

multifactor authentication mechanisms to ensure credential-to-device binding often complement mobile access for enhanced security. Mobile wallets like Apple Wallet and Google Wallet seamlessly integrate mobile devices into existing access control systems, promoting wider adoption of mobile access.

Companies operating in the security industry have devised various business models to monetize mobile access. Some leverage the software-as-a-service (SaaS) model, where costs are based on usage, while others adopt a simple approach of charging a one-time cost per credential.

> “
>
> WALLETS USING VARIOUS TECHNOLOGIES ARE SEEING WIDESPREAD POPULARITY, ALTHOUGH BUSINESS MODELS CAN DIFFER ACROSS COUNTRIES AND REGIONS, LEADING TO SOME SLOWDOWN IN ADOPTION.

Standardization of mobile credentials is a critical aspect of mobile access, and there have been notable developments in this regard. In Europe, the Open Security Standards (OSS) Association has introduced the OSS Mobile Access Standard, while the United States has the Public Key Open Credential (PKOC) initiative from the Physical Security Interoperability Alliance (PSIA). Wallets using various technologies are seeing widespread popularity, although business models can differ across countries and regions, leading to some slowdown in adoption.

The future of mobile access seems promising as the adoption of mobile technology continues to rise, paving the way for increased application in access control systems. However, certain challenges persist. Data privacy remains a significant concern, as does the task of standardizing mobile access technology across devices and platforms. While mobile access will likely gain a larger market share, physical credentials will still find relevance in certain sectors.

A trend that is starting to emerge is the rise of cloud mobile access platforms. These platforms aggregate communication with access control and identity management systems and electronic components, while managing the credential lifecycle. They offer added integration value to businesses through various use cases, such as booking office space or hotel rooms, granting access for a certain period of time, reserving a parking spot, or enabling visitor access.

Moving forward, the technology will evolve, bringing both new benefits and innovative solutions to mitigate challenges. With this evolution, mobile access will likely become an integral part of the future of the security industry. ◀

> A TREND THAT IS STARTING TO EMERGE IS THE RISE OF CLOUD MOBILE ACCESS PLATFORMS.

Digital Technology Is Transforming Banks

Customer demands are driving the need for enhanced services and options

IN RECENT YEARS, THE TERM "DIGITAL TRANSFORMATION" HAS GAINED PROMINENCE across various industries, signifying a fundamental reimagining of how organizations leverage technology to improve business processes.

Within the financial and banking sectors, digital transformation has become synonymous with the increasing shift toward mobile and online banking, as well as the widespread adoption of cloud-based services to enhance customer engagement and streamline internal operations. The retail banking industry today is experiencing a profound shift, driven by new technology, increasing competition, regulatory complexity, consolidation, and evolving customer expectations. To remain relevant and competitive, banks must embrace digital transformation as a critical pathway to modernization.

CHANGING CONSUMER TRENDS

Technology has played a pivotal role in the growth of the banking market in recent years.

Matt Tengwall (matthew.tengwall@verint.com) is General Manager, Fraud and Security Solutions, at Verint Systems (www.verint.com)

Major institutions report a significant increase in the amount of financial activity conducted on mobile devices and in the number of digitally active customers. Instant access to a wide array of banking services is now expected, and customers prefer digital self-service through mobile apps and online platforms over traditional in-person or phone banking. The Covid-19 pandemic accelerated this trend, as customers increasingly turned to digital channels for convenience and safety.

To respond to these demands, banks must prioritize seamless digital experiences across all channels. This not only fosters better customer engagement, it also leads to richer lines of communication, strengthening the bank-customer relationship.

> THE ADOPTION OF CLOUD TECHNOLOGY IN THE FINANCIAL SECTOR IS GAINING MOMENTUM AS BANKS RECOGNIZE THE ADVANTAGES IT OFFERS.

ELEVATED CUSTOMER EXPERIENCE

Competition in the financial services industry is intensifying, prompting banks and credit unions

AUTOMATION WILL PLAY A CRUCIAL ROLE IN IMPROVING OPERATIONAL EFFICIENCY, REDUCING COSTS, AND ENABLING BANKS TO FOCUS ON PROVIDING PERSONALIZED, VALUE-ADDED SERVICES TO CUSTOMERS.

to prioritize the customer experience in order to stay ahead. To do this, financial institutions must invest in the right talent, foster diversity within their teams, and leverage technological capabilities to analyze customer data and improve products and services.

A customer-centric approach is vital in today's market, where consumer loyalty can make or break a bank. By collaborating across business units, including on product development and design, banks can better understand customer needs and preferences, leading to tailored solutions that enhance the overall experience.

THE CLOUD IN BANKING

The adoption of cloud technology in the financial sector is gaining momentum

as banks recognize the advantages it offers. Cloud migration, while complex for financial institutions because of their diverse IT and hardware landscape, presents significant benefits.

Lower maintenance and operational costs are among the primary advantages of cloud adoption. In addition, cloud infrastructure is scalable, allowing banks to adjust resources based on demand, reducing the need for expensive physical hardware. This flexibility enables faster innovation, accelerated product development, and improved time-to-market for new services.

Security concerns have discouraged some banks from fully embracing the cloud. To overcome this obstacle, banks must approach cloud migration with a well-defined strategy, ensuring a smooth transition while maintaining stringent security measures to protect sensitive customer data.

NEW AND EVOLVING RISKS

As digital banking expands, new risks and challenges are emerging, requiring banks to implement robust security measures. The shift to digital channels has provided criminals with new opportunities to exploit vulnerabilities in bank infrastructure, leading to incidents like ATM "hook and chain" attacks.

To combat these security challenges, banks must adopt a layered approach to security. Relying solely on traditional security approaches is no longer sufficient as criminals become more sophisticated in their tactics. Implementing advanced technologies, such as multifactor authentication and AI-driven analytics, can significantly enhance a bank's security posture and protect against emerging threats.

THE PROMISE OF FUTURE INNOVATIONS

As banks embrace the digital transformation, the potential for future innovations is vast. Mobile banking and artificial intelligence (AI)-based solutions are expected to continue evolving, revolutionizing the way banks interact with their customers and adjust their internal processes. Automation will play a crucial role in improving

operational efficiency, reducing costs, and enabling banks to focus on providing personalized, value-added services to customers.

Data analytics will help banks better understand customer behavior, allowing them to tailor products and services to individual preferences. By leveraging data insights, banks can make informed decisions and offer targeted financial solutions, further enhancing the customer experience.

Digital transformation is no longer a choice for banks; it is an essential pathway to staying relevant and competitive in the rapidly evolving financial services landscape. By prioritizing customer experience, adopting cloud technology, mitigating emerging security risks, and exploring future innovations, banks can accelerate their modernization and create a more efficient, customer-centric, and resilient financial ecosystem. ◀

> DIGITAL TRANSFORMATION IS NO LONGER A CHOICE FOR BANKS; IT IS AN ESSENTIAL PATHWAY TO STAYING RELEVANT AND COMPETITIVE.

Physical Access Control Joins the IoT Ecosystem

A security solution leads the way to digital transformation

BUSINESSES WORLDWIDE ARE UNDERGOING A PROFOUND CHANGE. Embracing process automation and artificial intelligence (AI)-driven data capture, they are embarking on the journey of digital transformation.

Amidst this technological revolution, the Internet of Things (IoT) has emerged as a critical enabler, linking devices and creating a connected world. However, one aspect often overlooked as a driver of this transformation is physical access control – a fundamental element of an organization's security infrastructure that not only ensures safety but also plays a pivotal role in shaping and enhancing IoT strategies and overall digital transformation.

Jeff Ross (jeffross@acre-co.com) is the Director of Marketing for Acre Security (www.acresecurity.com).

In the past, physical access control systems were perceived as antiquated compared to their network access counterparts because of a reliance on simple methods like mechanical locks, keys or basic badge systems. These traditional methods lacked sophistication and presented challenges when updating the system, making them vulnerable to security breaches. Lost, duplicated or stolen keys posed serious security risks, and the lack of data insight limited their effectiveness.

> MODERN ACCESS CONTROL SYSTEMS HAVE EMBRACED CUTTING-EDGE TECHNOLOGIES LIKE BIOMETRICS, FACIAL RECOGNITION, MOBILE CREDENTIALS AND IOT INTEGRATION.

The landscape of physical access control has undergone significant advances in recent years, however. Modern access control systems have embraced cutting-edge technologies like biometrics, facial recognition, mobile credentials and IoT

integration. This has elevated physical access control from a mere security-focused function to a powerful tool for data-driven decision-making, streamlined operations, and overall business intelligence. Today, it is recognized as an essential component of modern, digitally transformed, and highly secure businesses.

But how does physical access control contribute to driving IoT strategies and digital transformation?

These systems are inherently IoT devices themselves, consisting of interconnected solutions that collect and exchange data over networks. As a result, they contribute to the establishment of a broader IoT network within organizations, becoming a cornerstone of digital transformation efforts.

The integration of physical access control with other IoT devices enables seamless interoperability across multiple platforms, facilitating real-time data exchange. This data-driven approach empowers businesses to identify operational inefficiencies, make informed decisions, and formulate effective strategies. Consequently,

companies can streamline operations, optimize resource allocation, and enhance overall productivity, accelerating their digital transformation journey.

The convergence of physical access control with IoT devices opens new horizons for innovation. By combining access control systems with sensors or automation systems, businesses can create intelligent operations in which tasks like lighting, heating and air conditioning are automated based on occupancy. This not only improves user experience but also promotes sustainability by reducing energy consumption.

The data generated by these converged systems also aids in understanding space utilization, leading to more efficient workplace design and can be crucial for contact tracing during health emergencies.

> THE INTEGRATION OF PHYSICAL ACCESS CONTROL WITH OTHER IOT DEVICES ENABLES SEAMLESS INTEROPERABILITY ACROSS MULTIPLE PLATFORMS, FACILITATING REAL-TIME DATA EXCHANGE.

Cloud-based systems

“

BY COMBINING ACCESS CONTROL SYSTEMS WITH SENSORS OR AUTOMATION SYSTEMS, BUSINESSES CAN CREATE INTELLIGENT OPERATIONS IN WHICH TASKS LIKE LIGHTING, HEATING AND AIR CONDITIONING ARE AUTOMATED BASED ON OCCUPANCY.

offer scalability, allowing businesses to add or remove access points and requiring no significant hardware modifications or software installations for users – a vital feature for organizations anticipating growth or operational changes.

Undoubtedly, physical access control remains a linchpin in maintaining the security of businesses, protecting tangible assets, confidential data and, most importantly, personnel. Beyond establishing secure perimeters, access control systems mitigate security risks associated with the expansive IoT ecosystem. As the number of connected devices increases, the risk of data breaches and cyberattacks grows. Access control devices ensure that only authorized individuals have physical and digital access to the system, its data, and its network path.

Looking ahead, the future of physical access control will probably be driven by innovations like

AI, which will enhance security measures by identifying abnormal behavior, such as tailgating, leading to proactive threat detection and more robust security protocols.

The fusion of physical access control with IoT strategies can be a vital contributor to the digital evolutions experienced by organizations, including those in the healthcare, pharmaceutical and critical infrastructure sectors. These strategies extend beyond enhancing security; they boost operational efficiency, drive innovation and support sustainability.

As businesses continue their journey through the technology landscape, physical access control systems will remain pivotal tools that steer the future trajectory of IoT and digital transformation. With their ability to seamlessly integrate with IoT devices, collect valuable data, and enhance overall security, they become indispensable assets for modern businesses aiming to thrive in the digital age. By embracing these transformative technologies, companies can pave the way to a more connected, secure, data-driven future. ◀

Containerized Video Management Systems in Education

An innovative approach presents more options to forward-looking institutions

FROM ELEMENTARY SCHOOLS TO UNIVERSITIES, VIDEO MANAGEMENT SYSTEMS (VMS) SERVE as the bedrock of security. However, challenges in scalability, adaptability and cost efficiency are proving traditional VMS solutions to be increasingly inadequate. The advent of containerization is ushering in a new era of robust, flexible and future-ready video management that is aligned with the dynamic nature of the modern educational environment.

John Rezzonico (jrezzonico@edge360.com) is the CEO of Edge360 (www.edge360.com).

CHALLENGES WITH TRADITIONAL VMS

Traditional VMS solutions in the education sector often fall short when it comes to scalability. This is especially problematic for large and expanding institutions, where adding systems for new buildings or campuses can be a tedious and expensive task. Integration with other security measures, such as access control and intrusion detection, raises compatibility issues, exacerbating the problem.

At the same time, many educational institutions find themselves in a position where they must purchase everything from one manufacturer. This one-size-fits-all approach creates a lack of flexibility that can hinder long-term growth, slow adaptation to new technologies, and even become a financial burden. Furthermore, the constantly evolving security needs of schools and universities make traditional systems look static. Demands on VMS are continually diversifying and expanding, and antiquated video systems may not be agile enough to adapt.

> “THE REMOTE MANAGEMENT CAPABILITIES AND THE REDUCED NEED FOR HARDWARE RESOURCES MINIMIZE ON-SITE ENGINEERING AND OPERATIONAL COSTS.

WHAT CONTAINERIZATION MEANS FOR VMS

Containerization, within the context of VMS, involves encapsulating an application or system within a “container.” Imagine receiving a fully assembled, ready-to-use product in a compact package; that is what containerization means here.

This new approach offers portability and flexibility, as containerized applications can run anywhere without significant configuration changes. The pre-configured nature of all dependencies makes the deployment process simple and efficient. Moreover, applications are packaged with everything they need, allowing seamless integration with other technologies and systems.

FUTURE-PROOFING VIDEO ENVIRONMENTS

Containerization allows institutions to adopt new security technologies without limitations. This adaptability ensures that they remain on the cutting edge of safety and security. It also enables centralized management and control for institutions with

multiple locations. This supports a smooth scaling process across different sites, ensuring uniformity and efficiency.

Furthermore, containerization brings significant savings to educational institutions. The remote management capabilities and the reduced need for hardware resources minimize on-site engineering and operational costs, freeing up funds for other essential educational initiatives.

A STRATEGIC SHIFT

The transition to containerized VMS is more than a technological upgrade; it symbolizes a paradigm shift in how educational institutions envision and build security.

> TRADITIONAL VMS SOLUTIONS IN THE EDUCATION SECTOR OFTEN FALL SHORT WHEN IT COMES TO SCALABILITY.

By embracing containerization, schools and universities synchronize their security infrastructure with broader educational goals and philosophies.

This alignment fosters a more dynamic, responsive and innovative security environment, reflecting the open environment that educational institutions strive to provide.

> THIS SHIFT TRANSCENDS MERE TECHNOLOGY, RESONATING WITH A BROADER VISION FOR WHAT SECURITY IN EDUCATION CAN AND SHOULD BE.

Containerization also leads the way to a secure future, preparing institutions for unforeseen challenges and uncertainties. The flexibility and resilience embedded in this approach ensure that educational establishments are equipped to change and progress along with the security landscape.

Containerization within VMS represents a profound evolution in the approach to educational security. By directly addressing the unique challenges faced by these facilities, it opens up a pathway to a more flexible, efficient and progressive security environment.

This shift transcends mere technology, resonating with a broader vision for what security in education can and should be. Containerized VMS mirrors the innovative and adaptable nature of contemporary education, offering a solution that safeguards the present and builds a resilient foundation for the future.

In an age where education is in constant flux, security must keep pace. Containerization provides a solution that is as vibrant, innovative and forward-focused as the educational institution it safeguards. Now is the time for campus administrators and security personnel to embrace this new paradigm. The next generation of learners deserves nothing less. ◀

Verified. Bench Tested.
Proven. Compliant. Trusted.