Cybersecurity: Legal requirements push toward good practice

BY **ROBERT BELL**

IN NOVEMBER, we were in Las Vegas for LDI and as a colleague and I waited at a light outside the convention center we spotted a motorcyclist riding without a helmet. I said, as a Canadian, how very odd that looks and my colleague just responded, "Organ donor."

The iconic 1969 film *Easy Rider* chronicles the story of two convicts (Peter Fonda and Dennis Hopper) making their way from California to Mardi Gras in New Orleans, agreeing to take along their square ACLU lawyer that helped them get out of jail (Jack Nicholson). Their trip starts in California where wearing a helmet was the norm (but not actually law for another 20 years), Fonda asks Nicholson if he's got a helmet. He replies "Oh, I've got a helmet. I've got a beauty." It sure was; a too-small golden football helmet. Perhaps it was not the most appropriate brain-bucket for riding on a chopper, but probably better than nothing. And it sure provided a comical contrast to Fonda's Captain America helmet.

California is not shy about leading the way in progressive law-making. For decades, its emissions standards have exceeded the federal guidelines put forward by the Environmental Protection Agency, which has led to car manufactures working harder to build more fuel-efficient vehicles. On January 1, 2020, California will be the first state to enforce cybersecurity and IoT related legislation. Oregon, New York, and Massachusetts are following suit. California's law is *Title 1.81.26 "Security of Connected Devices"* which mandates manufacturers of Internet-connected devices to equip their products with **reasonable** security features

that are **appropriate** to the nature and function of the device. Among other things, if a device uses a gateway, the law requires the manufacturer to either supply unique passwords for the device or force users to change the password before being able to use it. This means that baby monitors and doorbell cameras may no longer be shipped with the Username: "username" and the Password: "password."

The law, is purposefully vague. In total, it's less than 1,000 words! For example, the law states that the manufacture must provide features that are "designed to protect the device and any information contained therein from unauthorized **access**, destruction, **use**, modification, or disclosure." The terms "access" and "use" is further defined as any access or use that is not authorized by the consumer. "Connected device" is defined as any device that is capable of connecting to the Internet, directly or **indirectly**, and that is assigned an Internet Protocol address or Bluetooth address. For conservative lawyers of large manufacturing firms with a lot to protect, the broad use of the terms in **bold** above are particularly troublesome. I predict that this law's practical implementation will not be sorted without the help of the courts in the years to come.

Background of Ethernet networking in entertainment

Ethernet has been used for lighting networks as early as 1990, before the popularity of the World Wide Web when security wasn't as much of a concern as it is today. These systems were not designed for environments that were exposed to the public Internet and were generally used to connect two consoles together, offering redundant backup. In fact, in the early days, Ethernet and DMX512 didn't cross paths. Even PC to PC networking was nothing like it is today. We had just moved away from connecting our PCs directly with 10Base2 coax to using hubs and 10BaseT RJ45s. The earliest version of WYSIWYG used very sophisticated PC hardware to receive DMX512 directly, and it wasn't until 1996 that CAST and Artistic License manufactured the first purpose-built box, the Vision 2000, to get DMX512 into a computer using TCP/IP. The ubiquitous Pathport was released in 2000 and not only was it one of the first generic Ethernet devices to get DMX from point A to B, but it also was the first device in our industry to use the new *IEEE 802.3af, Power Over Ethernet*.

Today every department in the theatre uses Ethernet. The sound department uses CobraNet and Dante, lighting uses Art-Net and sACN, stage management uses PoE coms and cue-lights, and rigging, like everyone else, connects their computers using Cat5 and switches. More and more devices are going wireless with either Bluetooth or Wi-Fi and connecting to the World Wide Web is as easy as tethering your phone or finding a hot-spot. New facilities are consolidating networks and IT is installing high-speed backbones, allocating VLANs for each department. Long gone are the days of three separate snakes (lighting, sound, and coms) snarling their way from front-of-house to backstage.

Networking today and the threat from bad actors

It's difficult to go a day without hearing a news story about some catastrophic data breach on one network or another. Banking institutions, government agencies, and building management systems are constantly under threat. As the Internet of Things connects us and our devices together, work must to be done to prevent bad actors from permeating to the heart of our networks.

While inside a building, VLANs prevent interdepartmental crosstalk, but, you're not to expect a malicious attack coming from a fellow crew member working on the same gig as you. As directors and producers worry about the actors on the stage, manufacturers must work to ensure to mitigate any threat of bad actors entering the theatre uninvited. Some productions deal with security by building a big wall around their insecure legacy systems, but in this day of IoT connectivity, it is becoming more and more difficult to remain an island. A single laptop at the production table connected to the entertainment network can join a Wi-Fi

If this is the extent of your network security today, you may want to revaluate your choices when building production infrastructure.

access point to access email. This could be the hole in the dike that brings down your entire production.

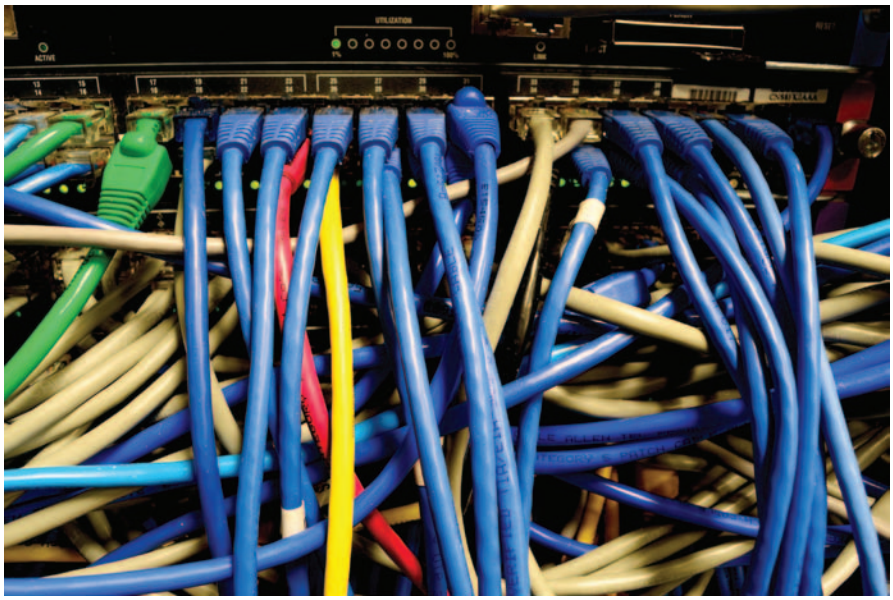
Proliferation of connected devices

Permanent installation, like an architectural lighting install, have very different needs from that of a rock tour or theatre production. There isn't trained staff on hand every time the show is viewed, but things can still go wrong even when it's all cued from a clock. In these situation, it's better to be informed directly from your system using clever monitoring software rather than getting a call from an unhappy client. You look much better when the first they hear of a problem is knowing that you're already on the case to fix it.

And, it's not just complex systems such as building management, banking, and show control. The world is getting used to everything being connected. You want to know if your furnace failed before you arrive home to frozen pipes. We have the technology; let's employ it.

All this connectivity comes at a price. There is an initial cost to install and configure these systems, but the real cost comes when we begin to rely on them and they ultimately fail, either by an act of God or by malicious intent. Ransomware is a real thing for governments and corporations, and perhaps we must count our lucky stars that it hasn't happened (to my knowledge) in major theme parks or sporting arenas insofar as the entertainment networks are concerned. Is it possible? Yes. Is it probable? Likely, especially if we don't do anything to protect ourselves. See the sidebar for three seemingly simple ways to bring a production to its knees.

High profile architectural installations are prime targets for network hackers.



The proliferation of connected devices on modern productions makes it very difficult to keep every department an island.

What can be done to protect us?

We have the know-how to protect ourselves. Cryptographic libraries and protocols are getting better and better, thanks to whistle blowers like Edward Snowden. It has been a very long time since people have been apprehensive about using online banking and debit cards. Chip-and-Pin and 2FA (two factor authentication) have alleviated much of the fear. Below are some of the tasks engineers should seriously consider implementing to not only comply with new laws, but to protect our productions and our industry.

Tamperproof the firmware upgrade processes

Software and firmware updates should

be digitally signed to ensure they only accept verified software from their known developer and cannot be turned into bots. Any attempt to upload modified firmware must be ignored.

Password protect the networks

Only allow authenticated access to your devices and their configuration. Passwords must be unique per network or device.

Plug the holes

Evaluate your operating systems, background processes, and open ports. Apply all security patches and close all vulnerabilities exploited by bad actors. Only allow access to protocols such as SSH and VNC after the user accepts the risks.

Device to device authentication

In the absence of central server access to the devices, each device on the network should be aware of who its friends are. This means they must all share a known secret key-phrase so new devices on the network are ignored.

Audinate had already done a good job with their Dante Domain Manager, a software package that manages user authentication, role-based security, and audit capabilities for their networks. The CPWG has a task group working on the Next-Gen protocols that will take a serious bent towards security.

Managing technical debt

Products produced ten years ago have ten-year-old security standards. Legacy applications, older consumer operating systems, and past-expiration-date technologies pose real risks to productions, and the risks grow larger with each passing year. If this stuff is technically possible to protect, often using open source libraries, why hasn't it been done yet? It's call technical debt.

Companies delay resolving their technical debt for various reasons. The most common excuses are that it's time consuming, expensive, and will take away from other, presumably higher-priority projects, such as releasing the newest flashy gadget before the next trade show or other work done in earnest to win the next bid.

TCP v. UDP – Tomato/Tomahto

It will help to have a little background on the "bits" of the network that can be secured and the other bits which just need to be there. Are you ready for some networking four-letter words? Sometimes all the acronyms can be a little off-putting, but you will likely recognize a lot of these as they roll off the tongue. Ethernet, IoT, the Internet, and cellular networks have similarities, but they are not the same thing. They all use parts of the seven-layers of the Open Systems Interconnection model or OSI.

The first two layers of the OSI model are the **data link** and **physical layers**. These define the *IEEE 802.x* family. We know these as Ethernet, Virtual Bridged LANs, and Wi-Fi, which people generally group into a category they'd identify as their local area network. The physical layer is the electronics in the Network Interface Controller (NIC) and are most commonly identified by the Recommended Jack 45 (RJ45) and Category cable (Cat5, Cat5E, Cat6, and Cat7). Fiber and its transceivers are also included in the physical layer. At the other end of the OSI model is Layer 7, the application layer, which is the bit that interfaces data and the user. These applications include DHCP, HTTP, RSTP, TLS, OSC, Dante, ACN, sACN, and many more. In the middle is the transport layer and includes TCP and UDP. I want to talk a bit more about TCP and UDP.

TCP is a connection-oriented protocol and UDP is a connection-less protocol. Think of TCP as the old RS232 DB-9 serial connections to plotters. There are two ends to the connection and pins used to establish the connection and control of the data flow such that the receiver can't be swamped by the sender. TCP also guarantees the delivery of its packets and the order in which they are sequenced before they even get to the application layer. You don't need to send checksums to verify the integrity of the data. Because it's point to point (generally, but not exclusively), it is rather difficult to get in the middle of. Even if a bad actor can use clever routing to spoof the system to intercept the communications, the sequencing and arbitrary port numbering makes it harder to go incognito. This is not designed as a security feature, but it does aid in making the communication more robust.

UDP, on the other hand is more akin to opening your front door and shouting at your neighbors. It's likely they'll hear you, but you really don't know if they got the message. If you want to be sure, you'll just repeat the message again. This is how many xDMX protocols work and in fact, how DMX512 works on RS485. Streaming ACN over UDP is efficient as there is no error detection or recovery service and works multicast, meaning one sender and many receivers, again, similar to DMX512. This means it might be easier to spoof as you can forge and insert a packet with an arbitrary IP address and it should get to the application layer. Open Sound Control (OSC) is also transported using UDP. *ANSI E1.17*, ACN, uses Session Data Transport (SDT), a reliable multicast transport protocol that lives in the application layer. This adds a lot of overhead in both processing power and code development, which is the reason pure ACN has not been widely adopted.

Does that mean TCP is more secure than UDP? Not necessarily. Neither were designed to be secure, and today we must rely on physical security, like locked doors and security lanyards, until the manufactures add the security to the applications we use. The market is currently enjoying all the benefits of protocols like OSC and sACN without the need for SDT and the overhead of added security protocols. So far, it works well, and to my knowledge bad actors have been confined to the stage, not backstage. It is comforting to know that ESTA's Control Protocols Working Group is contemplating the next generation of entertainment control protocols, and security is high on the list of features it must include.

Threat examples: Please don't try these at home.

Scenario 1: Disgruntled employee

Many of our industry's products have been designed specifically to be friendly to configure. Often knowing the IP address of the device is enough to surf to its interface or freely downloadable software that discovers and modifies properties. If these systems are not locked down, a bad actor can get on the network minutes before the curtain and default all configurations to factory defaults (or worse). Almost definitely stage management would have to hold the show, if not clear the theatre. Please don't do this!

Scenario 2: Accessible network jacks

The home town hockey team has invested in a moving light rig above the nets. When the home team scores, gobos, and color flash over the ice. A bad actor in a closet can open a laptop and wait for this cue to happen and record it. Then, during play, replay the ballyhoo at the highest sACN priority distracting both teams. Until they shut down the entire lighting system, nothing can be done on the network side to stop it. Please don't do this!

Scenario 3: Eavesdropping

There is a high level of ethical professionalism from sound technicians. Wireless microphones are often worn into dressing rooms and actors are not trained to mute their mics when rushing from A to B or using the facilities. But their voice only goes to the RF rack (tech #1) and the sound console (tech #2). It is their job to handle the mutes and be discrete with their use of solo. In the world of Audio over Ethernet, it's easy to leave a PoE mic in a green room and route it to any PC on the network. Please don't do this!

R&D engineering groups don't want to touch legacy products for fear of breaking them. The original tool-chains needed to modify the firmware, and moreover, the original developers, may no longer be with the company. Therefore, it takes a serious amount of foresight and support from the invested parties to tackle this technical debt. Some companies don't have the resources to manage these projects or cannot convince senior management to make it a top priority. Yet others may want to bury their heads in the sand or simply be unaware of the real security threat and the associated risks.

On my return home from Vegas, I checked the motor-vehicle law. Everyone of any age is required to wear a helmet while driving a motorcycle in Nevada. Only three states, Illinois, Iowa, and New Hampshire, have absolutely no helmet laws whatsoever. Clearly our biker friend was breaking the law and choosing not to be protected. The laws are there to protect us and although they may seem like a real burden, they often result in the desired consequences. Canada enforced automatic daytime running lights in 1989 and have statistics to show that it has reduced head-on accidents. Car makers have gone from no seatbelts, to lap belts, to three-point harnesses, driver-side airbags, passenger airbags, and now side impact airbags. These changes are a result of consumers wanting more protection and the manufacturers are only too happy to oblige.

Any helmet you buy today will meet Federal Motor Vehicle Safety Standards. Presently, there aren't standardized crash-tests for networks, and we rely upon the manufactures to demonstrate they have done their due diligence. So, you must decide, are you going to choose the Captain America helmet like Fonda, or Nicholson's ill-fitted football helmet, or go fancy free like Hopper, the easy rider organ donor? ■

Robert Bell is the author of *Let There Be Light, Entertainment Lighting Software Pioneers in Conversation*. He has been a contributing member of ESTA's Control Protocols Working Group for more than 16 years. Robert is currently the Director of Product Innovation at Pathway Connectivity. He can be reached at rbell@pathwayconnect.com.