Robert Bell makes a humorous point about a serious situation.

The Ticking Data Bomb

By Richard Cadena

How easily can your lighting system be hacked?

One minute, your lighting system is working fine, and you're happily triggering one cue after another. The next minute, you lose control of the entire system. The lights start flashing randomly, and there's nothing you can do to regain control. Your worst nightmare has been realized; your lighting system has been hacked.

That's what happened at LDI, except it wasn't really a hacker; it was a demonstration that Robert Bell, director of product innovation at Pathway Connectivity, put together.

Hacking into the lighting network was easier than you might expect. He simply programmed a small, standalone computer to output sACN with the highest priority (200) so it will override every other control signal with a lower priority, including those with the default priority of 100. Then he connected this "data bomb" to the network and watched it do its thing.

The demonstration was Pathway's clever, eye-opening way of demonstrating how easy it is to take over a lighting network with no security and to show how the company has locked down its network-connected products. First, it uses digitally signed software for updates to minimize the possibility that a hacker can intervene during the process. Second, it uses good authentication to access and configure a net-

work or device, meaning it has password protection. This is in response to the growing threat of network vulnerabilities and the California Civil Code Title 1.81.26, Security of Connected Devices.

Title 1.81.26 is a new law that went into effect on January 1, 2020, requiring all devices that can connect to a network to have "reasonable security features." It is designed to help close the gaping hole in the security of an alarming number of Internet of Things devices. Many IoT devices have little or no security at all, and the number of incidents is growing in which hackers gain access to private networks because of flaws in security. Oftentimes, it is due to very simple oversight or outright neglect by the manufacturer. There are, for example, lots of home security cameras being sold with no means of changing the default password, which is easily obtained by anyone with access to the Internet. Other devices have no password protection at all.

This can leave networks vulnerable to attack. It happened to a casino in Las Vegas in 2018 when someone gained access to the entire network by hacking into the digital thermometer in a fish tank. Then there was the time in 2019 when a security flaw in Chromecast allowed hackers to take over the video being cast to a television set. Imagine watching Netflix, and up pops a video promoting the YouTuber PewDiePie, asking you to subscribe to his channel, which is what happened to thousands of people. The hackers also hijacked printers and had them spit out the same message, all because Chromecast defaults to using universal plug and play (UPnP). UPnP leaves ports open to anyone, which makes it easy for hackers to gain access to the entire network without authentication. It's a feature in some other devices like Xbox and network switches that should be disabled.

It was just a matter of time before legislators got in the act. Not only has California passed a law, but there is a voluntary Code of Practice in the UK that is very similar. Basically, the law makes it mandatory for manufacturers to use unique passwords instead of a default like "password," and it requires other basic protections against hackers. And since a lot of computer and networking products are designed in California's Silicon Valley, it is likely to have far-reaching effects the world over. Also, since non-compliant products will not be allowed to be sold in California, it's also likely that it will impact our industry as well. The only question is how much of an impact is likely, since the wording is vague.

I've been wondering when this ticking time bomb would go off ever since I noticed that I could see the grandMA network, the production office network, and the audio network on my mobile phone right before the start of a show I attended. Had I been a mischievous hacker, I might have attempted to take them over during the show just for LOLs. And, on a university campus, like the one where this show took place, there are lots of young college students studying cybersecurity, who have the skills to exploit vulnerabilities.

To be clear, in order for a network to be hacked, it has to be accessible, and there are a couple of ways that this can be done. One is to access it locally, meaning the hacker must be able to physically connect to the network through a switch or wirelessly, and the other is to access it remotely, which means your network has to be connected to the outside world, typically via the Internet. You can quickly check to see which ports are open by using the command prompt and the command "netstat -ab" or "netstat -aon." Either one will provide a list of ports and the processes associated with them.

If all this talk of network security sounds like gibberish to you, then it's time you buckled down and did some research. It won't take you too long to learn the basics of Ethernet and network security. There are lots of great resources like YouTube and podcasts. One of my favorites is called "Security Now," hosted by Steve Gibson. It's a bit geeky, and if you're not used to the terminology it can be a lot like eavesdropping on a conversation in a foreign language. But once you listen for a few episodes, you'll start to get the gist. You might even backtrack and listen to some of the early episodes where he explains the basics of network security. They're really good.

It's time for the live event production industry to lock down our networks. This time, it was only Robert Bell and his data bomb that took over the network, and he's a nice guy. But the next time it could be Robert's evil twin.