CANADA'S OCCUPATIONAL HEALTH & SAFETY MAGAZINE

JULY/AUGUST 2019

OHS CANADA

BLACK HAT HACKER

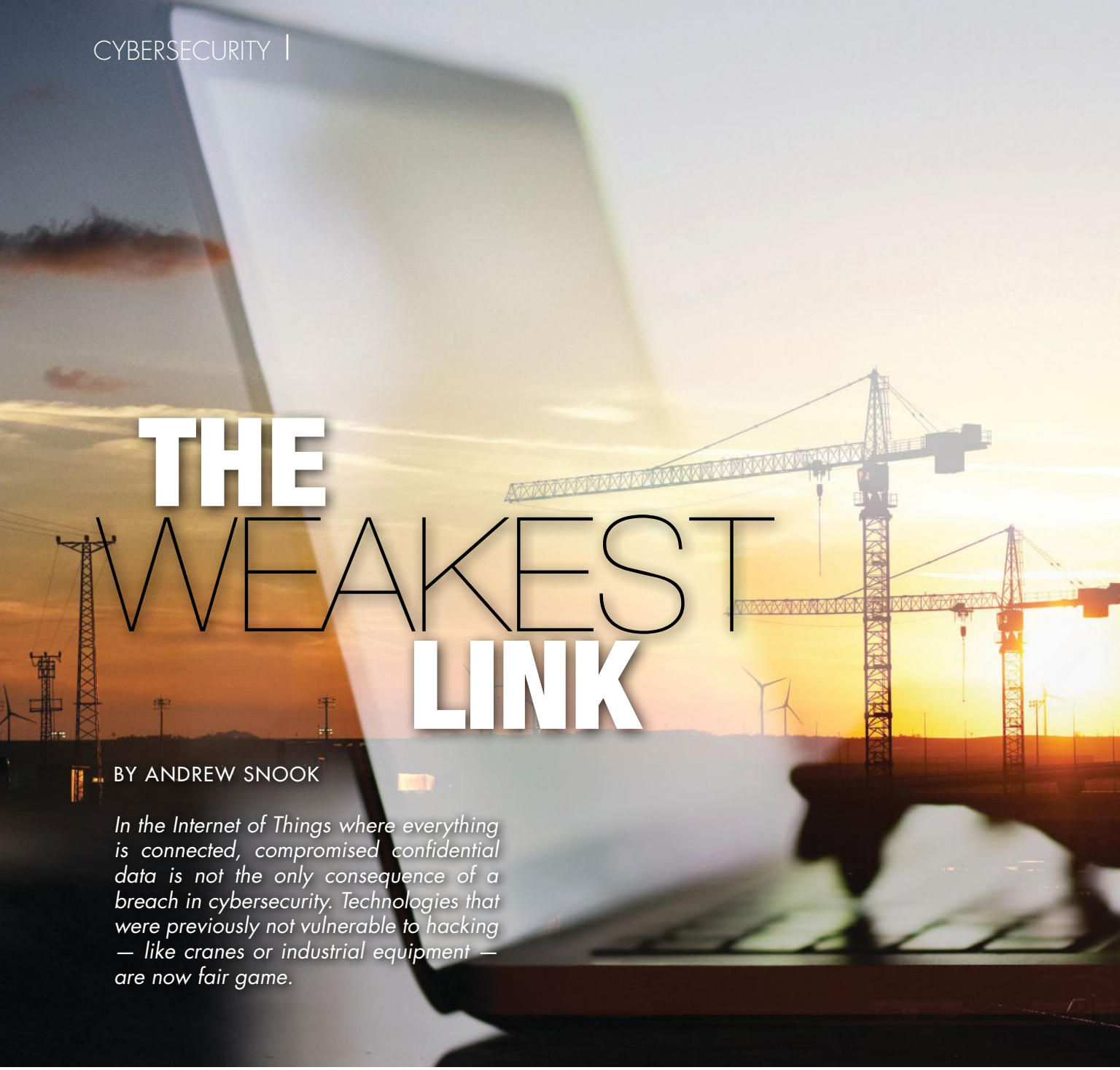
The dark side of connectivity

DUST EXPLOSIONS
Avoiding combustible dust mistakes

SAFETY IN NUMBERS
Cross-jurisdictional data highlights underreporting

OCCUPATIONAL EXPOSURE
Working safely with formaldehyde

IN THE EYE
Ready access to eye-rinsing facilities



THE WEAKEST LINK

BY ANDREW SNOOK

In the Internet of Things where everything is connected, compromised confidential data is not the only consequence of a breach in cybersecurity. Technologies that were previously not vulnerable to hacking — like cranes or industrial equipment — are now fair game.

Depending on who you ask, the hacking of technologies has taken place for more than a century. Some published articles date hacking all the way back to the days of manipulating switchboards for phone companies like Bell Telephone in the late 1800s, while others trace the origination of the term "hack" to the 1960s when members of the Massachusetts Institute of Technology's Tech Model Railroad Club used to "hack" their train sets in an effort to modify them. No matter when you date it, the hacking of technologies has come a long way.

A case in point is an online video, posted earlier this year, of a tower crane's radio frequency controller being hacked into and taken over in Italy by an ethical hacker to demonstrate cybersecurity weaknesses within the technology, with the permission of the company overseeing the jobsite.

As tower cranes typically work in high-density urban areas, hoisting tens of thousands of pounds of equipment up into the sky, the potential for physical and financial toll from hacking is high. But construction equipment is only one of many areas where cybersecurity breaches can create occupational health and safety risks.

"The minute you have networks, and the minute you are connected to the outside world through these networks, cybersecurity becomes an issue," says Harry Sharma, director of innovation and technology with The Conference Board of Canada in Ottawa.

Thanks to the interconnectivity and digitization of the manufacturing and construction industries, hackers with malicious intent today have a wider pool of targets than ever before. "It can lead to a lot of physical damage as well

as potential financial damage, so the challenges are in both realms," Sharma says.

For this reason, cybersecurity plays a more prominent role than before in workplace-safety planning. But what does cybersecurity mean in today's ever-changing world?

Chris Dodunski, chief executive officer of CyberHunter Solutions in Toronto, defines cybersecurity as a blend of people, process and technology. "What you are doing is you are instructing people, or defining process, or configuring technology to protect the confidentiality, data integrity and digital availability of whatever it is you are protecting," he explains. In short, cybersecurity is guarding confidentiality, integrity and availability, or what he calls the CIA Triangle.

Dodunski says every industry weighs its CIA Triangle differently, with varying focus on the each of the three aspects of this triangle. "If you are looking in the healthcare industry, obviously, confidentiality is very important. But so is the integrity of the information that you are looking at," he says. In the case of the banking or commerce sectors, data availability would be of greater importance.

And how does this apply to workplace safety? Technologies that typically exist in industrial and manufacturing spaces are no exceptions since most things have gone digital these days.

"We are constantly modernizing and networking these environments in order to improve efficiency or to operationalize things from an automated workflow perspective," Dodunski says. "We are connecting on these things that were previously never online and never part of the Internet, or never available to the Internet."

That means technologies that were previously not vulnerable to hacking are now fair game. "If someone can get into your industrial control systems, then they can start tampering with safety controls — things like your monitoring systems or shutdown mechanisms, or whatever is happening inside that environment."

It is the threat to workers' physical safety that makes breaches at industrial plants and construction sites that much more dangerous and vulnerable. There are a variety of ways through which cybersecurity breaches can create risks for employees at these facilities. An example is environmental systems.

"People don't realize a lot of what you see in terms of the thermostat, the lights, the communication system — it is all delivered through online technology. So while it creates incredible efficiency, it creates incredible risk," suggests Katherine Thompson, chair of the Canadian Advanced Technology Alliance's Cyber Council in Ottawa. The financial damage to a manufacturer and the risk to those who work in that environment is high if hackers manage to hack into the lighting system in a manufacturing plant that is very much climate controlled and take over that feature.

Or a hacker with a personal vendetta against mining companies who managed to shut off air-purification and ventilation systems in a mine, Dodunski illustrates.

WORLDS COLLIDING

The line between physical security and cybersecurity has been blurring as technologies continue to advance and break down barriers that once separated these two worlds.

"These have been independent silos," Dodunski explains, citing the physical security guys who deal with cameras and door access, and cyber people who work with computers, networks and wireless access. "But companies are beginning to recognize the importance of merging these two worlds to improve the security of their organizations."

These worlds are not the only ones that can no longer remain in silos. With so many systems now interconnected and digitized, the need for a company to merge workplace safety with cybersecurity planning is higher than ever before.

"Cybersecurity is the pivotal technology for both safety and security," says cybersecurity expert Claudiu Popa, chief

executive officer of Datarisk Canada in Toronto. "Without cybersecurity, humans are at risk of data and privacy breaches, personal attacks and physical violence. Mechanical systems are electronically controlled and remotely inspected. There is no longer a line between the physical and the electronic when it comes to occupational health and safety risk management."

Workplaces that have adopted remotely controllable technologies, video surveillance and the Internet of Things have effectively opened a 'backdoor' for malicious access and unauthorized activity, he adds.

"There is no longer a line between the physical and the electronic when it comes to oh&s risk management."

THE HUMAN FACTOR

There are several theories out there in regards to best practices for cybersecurity hygiene, how often systems should be tested and the best answer to the risks presented by bring-your-own-device (BYOD) practices in workplaces.

But one thing most experts agree on is that employees are still the most vulnerable point in most companies' cybersecurity strategies. "The weakest link is people," Thompson says. "Year after year after year, study after study shows us the biggest source of data breaches in an online incident is human error."

Dodunski agrees, adding that his own company uses social engineering as one of the ways to test the level of cybersecurity in companies. The method involves leaving USB sticks with enticing tags like "Salary Increases" or "Honeymoon pics XXX' around public areas on a campus like lobbies and bathrooms.

"Most people are curious enough to put a USB stick into their computer, their laptop, or whatever it is to see what's on it. And in fact, the statistics are pretty high," he reveals. And weaponized media is a big deal. "You plug in the wrong thing, and all of a sudden, you have got a compromise."

In addition to weaponized media, email, weak passwords, improper configuration of your security stack and the web are still common ways for hackers to infiltrate companies' networks. "The web is still a huge vector of attacks. So if you don't have proper controls on how people use the web, just going to the wrong website can invite attackers into your organization," Dodunski explains.

Although employees are often the targets of hackers looking for an easy way to access companies' networks, corporate culture need to take on some of the blame when breaches occur. "Much has been said about cybersecurity hygiene, but without a corporate culture that enforces discipline and supports operational security, the best cybersecurity framework will have an effective lifespan numbered in weeks instead of years," Popa says.

The challenge is often a lack understanding by employees of the roles they play in the cybersecurity of their company. "The problem is one of communication," Popa says. "People have different expectations, and if you don't communicate to them the degree to which they are accountable for what they do with their privileged access, they assume that it is somebody else's job."

Seemingly small actions can have a big impact on a company's cybersecurity, says Brennen Schmidt, principal of ALEUS Technology Group in Regina, Saskatchewan. A Facebook quiz could mean an empty bank account. An employee who plugs into a router to work from home could be the very thing that a hacker uses to bring down the power grid of the company the employee works for.

"Putting up a fence at a job site won't do much good if the threat is coming through online and out-of-sight channels. It is time to start putting the same level of effort on cybersecurity as companies do on their job sites," Schmidt says.

Many companies invest in hardware like firewalls to protect a company's computer network and security cards for staff to get in and out of a building, but overlook the importance of arming those people that use technologies with the understanding and knowledge of the role they play in terms of security and securing their environment.

"Cybersecurity is not just an IT issue," Thompson says. "It involves the responsibility of operations or infrastructure; it is a full engagement."

Computer practices that offer the most convenience also present the biggest risk. "Convenience, as I always say, is the opposite of security," Popa says.

It is vital for companies to impress upon all their staff that security is everybody's business. "If you are touching anything that is sensitive, that means you have privileged access to technology and resources," Popa says. "You are a valued member of the company or the organization. As such, you are responsible for everything that you touch."

MANAGING BYOD

The bring-your-own-device (BYOD) practice has always been a hot topic for debate. For Thompson, BYOD practices also create exponential risk to an organization.

"A lot of these devices coming in have downloaded various amounts of apps that are very easy for a hacker to exploit," she explains. "If you look at the most secure environments in terms of national intelligence, national security, they do not allow any kind of BYOD device be within the walls of their organization."

Just the camera feature on a phone can create incredible risk for an organization — taking pictures of surrounding infrastructure, the technology and confidential files. "There is a lot of power for good, and a lot of power for not so good, in a handheld device," Thompson notes.

Dodunski says managing cyber risks is all about visibility. "You need to be watching how people interact with your data, how people interact with your digital resources, and you need to understand what's normal and what's abnormal. If you cannot see that a new device has been brought into the network and is starting to download every file off of your file share, then you are going to be in trouble," he says. "But BYOD certainly makes it that much more difficult, because everything you are bringing in is potentially another threat actor."

According to Popa, BYOD is typically an indicator of risk maturity in an organization. "An organization that has the right cybersecurity framework in place will be just as secure with or without BYOD," he says. "An organization that does not have a proper framework in place will be very vulnerable by the adoption of bring-your-own-device practices, because if they don't have controls to enforce proper practices, then every single device will be different, and every single device will be at a different threat factor."

Popa stresses that the main safety check to address the risk of BYOD is to have a standardized framework of controls in place. Cyber-risk assessments need to be conducted as part of an effective cybersecurity program, but they should be broken up into phases to maximize their effectiveness.

"An organization-wide assessment is a lot to do at one time, and the value of a point-in-time assessment is limited, leaving large gaps for exposures to creep in during the year," Popa explains. "Risk assessments should be performed monthly or quarterly and add up to a complete cycle of security, and privacy assessments completed every year."

> "Employees are still the weakest link in most companies' cybersecurity strategies."

Spreading cyber-risk assessments over the year also enables the respective processes of auditing policy enforcement and reviewing device configuration, security posture from an external perspective and detective controls to be rolled out month by month. "These are all distinct efforts that should not be carried out simultaneously, because it just ends up being a sweep of noise. And then suddenly, you are looking for the signal in that noise," he says.

Popa advises companies to inform employees that cyber-risk assessments are being performed. "Don't do it in a vacuum, and don't do it independent of your workforce, because they are part of the organization."

WHEN BREACHES OCCUR

In the event that a cybersecurity breach has occurred, Popa says all suspected incidents should be brought to the attention of an appointed risk manager within an organization.

"If it is identified as a data breach, the company's cyber-insurance company will appoint a breach coach who will facilitate the process and take things from there," he says. "It is no longer a confusing process, but a straightforward activity that should be adopted by all organizations."

Schmidt stresses that communicating cybersecurity risks with the necessary team members is vital before a breach takes place. "It is best to get a crisis-response team in place ahead of a breach so everyone has an idea how they are to respond," he suggests. "A failure to notify customers, regulators and other third parties could prove costly, especially if a breach involves information or activities which span multiple borders."

Dodunski concurs that an incident response plan is necessary for every organization. "If you are taken down by ransomware, are you still going to be in business 30 days later? Are you prepared for that? Business-continuity planning, disaster response and incident-response planning is an essential piece to the overall cybersecurity program you have."

Since November 1, 2018, most organizations are subject to *The Personal Information Protection and Electronic Documents Act* (PIPEDA), which requires organizations to report to the Privacy Commissioner of Canada any breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals. They must also notify the affected individuals about those breaches and keep records of all breaches.

"It was a law that should have come 20 years before and, unfortunately, it came 10 years after it was enforced in the United States," Popa says. "It is going to be very difficult to catch up."

Canada has been seen as an oasis for hackers because of the ignorance and apathy, and the lack of capability around detecting breaches," adds Popa, who attributes this primarily to a lack of incentives in detective controls. He cautions that Canadian companies that are not investing in security today will no longer be competitive tomorrow.

Educating employees on cyber risks and how their actions and online practices can make their company vulnerable to cyber attacks is an important element of a cybersecurity-awareness program. For such a program to be effective, "it needs to be applicable, interactive, accessible, enforced and maintained," Popa says. "Its monitoring and enforcement must be distributed in nature so that everyone can participate in its health and effectiveness."

He expects cybersecurity in Canada will eventually improve, but not without heading down the curve first, particularly over the next 18 months.

"I imagine some companies are just going to go out of business because they literally have not been planning for the kind of investment they need to make in cybersecurity," Popa speculates. "But certainly, the next 18 months will present the inflection point in the risk maturity of Canadian businesses." •HS

Andrew Snook is a writer in Toronto.