By Alexandra Walsh

ARE YOUR SYSTEMS CYBERSECURE?

An interview with expert Barbara Rasco on best practices for protecting against attacks.

No one would want to work in a building without a fire detection and evacuation procedure, few would be willing to leave their building without locks, surveillance and burglary alarms and yet still today, too many cold storage businesses are not investing enough focus and resources in defending their business against cyberattacks.

In a recent meeting with Dutch cold storage businesses, experts “Techniek Netherland” put the challenge in stark terms. The risk that a European cold storage business might face a fire incident is 1 in 8,000, the risk of being burgled is 1 in 250, but the chance of being subjected to a serious cyberattack is 1 in 5.

In today’s interconnected, increasingly automated world it is not a matter of IF your business will be victimized by a cyberattack, but when. So, businesses across the cold chain must act, and even if businesses remain reluctant or inert to doing so, regulators across the developed economies are putting in place regulations that will require them to do so.

One individual determined to help prevent GCCA member companies from being victimized by cyberattackers is Dr. Barbara Rasco, BSE, PhD, JD. She is a food safety and food safety regulations expert at the University of Wyoming and a member of the Global Cold Chain Foundation (GCCF) Council of Scientific Advisors. She is assisted by Susan Borhan, a cybersecurity faculty member at Colorado Technical University.

Cold Facts Editor in Chief Alexandra Walsh sat down virtually with Rasco, who shared her thoughts on the importance of cybersecurity awareness in the industry.

AW: Why is cyber security awareness so vital in the food industry?

BR: The food industry supply chain can be vulnerable to cyberattacks. Hackers may target critical components such as logistics software, IoT (internet of things) devices or communication systems to disrupt the flow of goods or gain unauthorized access to sensitive data.

User awareness training is an extremely cost-effective form of defense. An untrained user is often the entry point of a breach, which can be prevented with the proper training and system configurations.

Companies store a vast amount of data related to shipments, routes, inventory and customer information. Data breaches can lead to the exposure of sensitive information, including trade secrets and personal data, which can be exploited by cybercriminals. If the company’s records are hacked, the personal information of all the companies’ staff may be exposed. Think about how often social security numbers appear on documents.

In addition to potentially exposing the personal information of employees, vendors and customers, and disrupting the food supply chain, one of the most distressing problems these targeted companies face is downtime, the losses from which can cost billions of dollars. I know of a number of food companies that have been hit with ransomware attacks.

AW: Where are the greatest vulnerabilities?

BR: Looking at the problem realistically, human error is the greatest risk to a company’s cyber security. Insider attacks can also pose a threat but far more common are unintentional acts by employees that can lead to a data breach or compromised information.

Legacy systems (those that haven’t been updated) provide major vulnerabilities to cyberattack. If the company has an older IT infrastructure, it is harder for IT staff to keep up with needed upgrades and patches. The consequence of not remaining updated is you can’t protect your systems against attacks. Updating and applying patches to your devices and systems is crucial.

Anywhere there is an exchange of information between you and another person, there’s risk of a cyber breach. For this reason, end-to-end encryption plays an important role in the exchange of data as well as access control settings on accounts.

Personal phones are a huge vulnerability. How can we assure employees’ personal phones are secure? The company might make a decision to ban personal phones or limit apps on the worksite. Or it could come up

Dr. Barbara Rasco, BSE, PhD, JD, University of Wyoming, and member of the Council of Scientific Advisors.

For more advice on how to protect your business from cyber threats go to:

U.S. Federal Trade Commission
https://www.ftc.gov/business-guidance/small-businesses/cybersecurity

Canadian Center for Cyber Security
https://www.cyber.gc.ca/en

European Cybersecurity Competence Center and Network
https://cybersecurity-centre.europa.eu/nccs-0_en

U.K. National Cyber Security Center
https://www.ncsc.gov.uk/section/advice-guidance/all-topics

with another solution, such as geofencing that can disable personally enabled phones in the company vicinity.

The IoT devices or smart devices are increasingly used in operations, logistics and transportation from tracking shipments to monitoring temperature and humidity in refrigerated containers. IoT devices can be vulnerable to cyberattacks if not properly secured or their software/firmware updated. This could affect the integrity of food products during transit or lead to data breaches.

Not just internal systems can be vulnerable, so can any interface with vendor, state and municipal governments. Power grid and water systems across the United States have been targeted already and present another risk for those companies generating electricity to sell back to the grid.

It is crucial that security stays up to date and one step ahead of attackers as technologies become more sophisticated and networks more interconnected.

Hacked systems can also represent a facility safety issue and the lack of physical security that is integral in a company's security at large. This could ultimately impact any physical access method or infrastructure that is connected to entry systems, traffic lights, lifts and of course, food temperatures.

AW: What are the most common methods of attack?

BR: Attackers use vulnerabilities in devices, take advantage of legacy systems and exploit insecure networks and IoT devices.

Ransomware targeting networks is the most common attack within the industry. But also exploiting the IoT is a vulnerability that is becoming more common.

Most concerning is phishing and other social engineering scams that have become very sophisticated. Cell phones, laptops, workstations, RFID tags (and there are lots on food packaging), IoT software or firmware, entry systems operated by Bluetooth devices all now have some type of software that interfaces with a facility's network. A switch used to turn on a light. Now lights turn on through hardware built into the network. If a network is compromised, all of these devices can be subject to manipulation from a threat actor.

Employees in the food and transportation industry may be targeted through phishing emails or social engineering tactics. If successful, these attacks can compromise sensitive information or provide attackers with access to critical systems.

Adware can be hidden on website click ads, icons, graphics, and links associated with ads. Using the same password across multiple sites might save time, but it also poses a major vulnerability. Artificial intelligence (AI) makes it even easier to figure out passwords. Targeting c-suite emails for passwords isn't such a challenge when AI can find patterns for passwords.

Insiders with access to logistic systems and data can pose a significant cybersecurity risk. For the most part, it is unintentional acts by employees that can lead to data breaches or system compromises.

The same is true with vendors, customers and even IT experts. It can be hard to screen a software solutions vendor. Any third party could introduce an additional cyber risk to your system in a way that leaves it vulnerable if adequate security measures are not in place.

CF: What kind of cyberattacks are impacting the cold storage industry?

BR: A cold storage operation was victim of a ransomware attack in 2023. A food processor's facility shut down for days impacting just-in-time delivery and first in/first out operations with a significant impact on regional supply chains. Any day of lost productivity in a highly concentrated and vertically integrated sector can have a massive

Know Your Enemy

Here's your Cold Facts guide to the contents of the cyberhacker's toolbox.

Malware

Malware is harmful software that disrupts computer systems, steals private information, or gains unauthorized access to information or systems. It includes viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, wipers, and keyloggers.

Ransomware

Ransomware is a type of malware that blocks access to personal or business data unless a ransom is paid. It disguises itself as a legitimate file and encrypts the victim's files, making them inaccessible.

Adware

Adware is software that generates revenue for its developer through online advertisements. It can be either legitimate or malicious, with the latter designed to damage and disrupt a system.

Phishing

Phishing is a type of scam where attackers deceive people to get sensitive information or install malware. It's becoming more sophisticated, often mirroring the targeted site and bypassing security measures. As of 2020, it's the most common type of cybercrime.

Smishing

SMS phishing or smishing is a type of phishing attack that uses text messages to deliver a bait message. The victim is usually asked to click a link, call a phone number or contact an email address provided by the attacker. Smishing messages may also come from unusual phone numbers.

Vishing

Vishing is a type of phishing attack carried out using telephony, often employing Voice over IP (VoIP) features such as caller ID spoofing and automated systems to avoid detection. Attackers pose as legitimate entities, like banks or internet providers, and use live callers or automated text-to-speech systems to steal personal information such as credit card numbers for identity theft.

MAC◆RAK

RACK REPAIR RACK GUARDS

#1 IN USA ◆ LIFETIME WARRANTY ENGINEERED

Mac Rak is the number one manufacturer of pallet rack repair kits in the USA. All products are exclusively manufactured at our facility in Missouri. In addition, our extensive dealer network allows us to serve customers across the entire USA from coast to coast.

All products are manufactured to exceed the highest industry standards. Stamped engineering approval available. Mac Rak products are backed by the best impact warranty in the industry.

We provide a complete solution from inspecting your site to component design, manufacturing, and installation.

CONTACT US
MACRAK.COM
815-723-7400

impact on the income of the company, its suppliers and customers and cause significant interruption to the food supply.

A U.K. logistics company was forced into bankruptcy because of a data breach. The company was unable to secure urgent investment after the breach. It was considered a high risk and was unable to secure short-term bridge funding.

In Alaska where rail is vital to trade, a third party gained unauthorized access to the railway's systems. All kinds of sensitive and personal information were taken.

For the individuals victimized by these hacks, having their personal information hacked is more than just a huge hassle – it can ruin their life.

State-backed hackers conduct a massive quantity of espionage operations each year and capitalize on any flaw or mistake in critical services to wreak havoc. Utilities and key infrastructure is being targeted. Recently, Chinese hackers targeted Hawaii because of its isolated military installations and proximity to Taiwan. Also targeted are infrastructure at major ports and oil and gas pipelines in the U.S. Northwest.

AW: Can you offer a few best practices in preventing a cyberattack?

BR: Everybody shares the responsibility for maintaining security, and there are lots of preventive measures that can be taken.

Most important, be vigilant and operate on updated systems. Learn what you can about your networks and systems, so you are able to detect something. If IT tells you to update your password, make sure it's a legitimate request. Update passwords frequently, and ensure they meet a high level of complexity.

Ensure only certain people have access to systems and that accounts allow and limit access based on the relevance of the particular role. These can be implemented with role or attribute-based controls on particular accounts. For example, a staff member in the billing department doesn't need access to the same functions as someone in the HR department. If you can effectively segment the roles, you can strengthen company networks as a whole.

In a facility, you might need an outside expert to direct you to do that. Many companies don't have team members with the expertise to prevent hacking. Think about bringing on a specialist to monitor regularly your cybersecurity.

If you haven't already, consider implementing biometrics and multifactor identification. Face ID, fingerprints, iris scans and even images can all be used in combination with a memorized password.

AW: Individually, what can we do to take personal responsibility for cybersecurity?

BR: You are expected to take a security-sensible approach by asking yourself these things about any outside communication you are receiving:

- Does it lack context?
- Is it from someone you don't know?
- Were you expecting it?
- Does it pressure you with urgent or threatening language to click a link, or pass on sensitive information?

Also beware of fake invoices – stop and think whether you're the person who usually gets that invoice.

And remember, if it's too good to be true, it probably is.

Regulators Take Action Around the World

European Union

In January 2023 the European Union adopted an update to its NIS2 (cybersecurity) Directive. This set rules for what each EU Member State must implement in national law, this includes requirements on the government and on private companies. The new law expands the scope of affected companies, from only the largest companies, to medium size (more than 50 employees) in key sectors that include both transport and food processing/distribution. This means new requirements to have in pace policies, training and reporting obligations for many cold chain businesses across Europe coming in to force in 2024.

Brazil

In May 2023, the Lula administration proposed new legislation to create a new national cybersecurity policy (PNCiber), including the creation of three new institutions: a national cybersecurity agency, a national cybersecurity committee, and a national management office of cyber crises. The Carnegie Foundation called this "the administration's boldest, clearest, and most ambitious vision for reforming Brazil's approach to cybersecurity." But they also noted that there were big hurdles and uncertainties over the speed at which they would be implemented.

United States

In July 2023, the Securities and Exchange Commission (SEC) adopted rules requiring public companies to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance.

The new rules will require registrants to disclose any cybersecurity incident they determine to be material and to describe the material aspects of the incident's nature, scope, and timing, as well as its material impact or reasonably likely material impact on the registrant.

ALEXANDRA WALSH is a Senior Publishing Consultant with Association Vision and Editor-in-Chief of COLD FACTS.

EMAIL: awalsh@associationvision.com