Digitization has brought many great benefits, but it has also enabled a new form of crime: cybercrime. It’s in the news, seemingly daily. Equifax, one of the three largest credit-reporting agencies, suffered a breach that may impact more than 143 million consumers. The US Securities and Exchange Commission experienced a software vulnerability that, according to reports, provided a potential basis for illicit stock gains through its EDGAR system. In another high-profile incident, hackers injected a multi-stage malware program into Avast’s CCleaner, a software security program, in what appears to be a targeted attack on some of the world’s largest technology companies in an effort to steal intellectual property. These are organizations that many would expect to have among the highest levels of security because of the types of information they handle and the products they provide. They almost assuredly do, but an age-old adage has great relevancy in the digital world: a chain is only as strong as its weakest link. These breaches highlight the rapidly changing nature of cybercrime. From the late 1980s into the 2000s, cybersecurity was focused on preventing simple worms and viruses. The attacks were often perpetrated by hackers who did it to simply show that they could, and in other cases to highlight where vulnerabilities existed in an effort to fix them. Yet, interestingly, there was an element of good intentions among at least some cyberattacks. Simpler times. Much has changed. Fast forward to the present day. Cybersecurity incidents have become increasingly sophisticated. Massive distributed denial of service attacks, social engineering, data exfiltration, advanced malware and targeted attacks are prevalent. The threat landscape is constantly changing, as are the perpetrators’ motives and methods. Cyber criminals are increasingly financially driven, and organizations are being infiltrated as a part of nation state and targeted supply chain attacks. Their motives can be to disrupt competition, steal intellectual property and state secrets, or hold companies’ systems and data hostage through ransomware. The associated costs with these incidents are escalating as rapidly as the attacks. A report by Juniper Research indicates cybercrime will become a $2.1 trillion issue by 2019. All industries and all types of organizations will be impacted, including ocean container shipping, logistics, ports, and related businesses. There is often a lack of understanding regarding cyberattacks and what organizations can do to improve detection and lower risks, or even prevent attacks. This is true in the ocean container shipping industry, where digitization is being increasingly embraced, but not necessarily cybersecurity. The following methodologies are what companies should be looking at:

**PREPARE FOR WHEN, NOT IF**

Cybercrime can’t be eliminated, so every organization needs to prepare for an inevitable breach. A holistic cybersecurity program that addresses key threats to an organization’s assets is important, as is developing a culture of security within them by promoting awareness and ingraining strong security practices into the fabric of the organization. A firm and well-defined cybersecurity program should include risk-management practices that are focused on...
lowering an organization’s risk level in a cost-effective manner. This normally involves the implementation of a layered defense strategy that consists of a combination of different security controls. According to a report by IBM, 60% of attacks are carried out by insiders, either ones with malicious intent or those who carried them out inadvertently. Every organization needs to define a strategy in order to identify, categorize, investigate and remediate security incidents. This normally involves the development of detailed security incident reporting and handling procedures, as well as a refined and tested security incident response plan. Both are essential in dealing with security breaches, including those perpetrated by insiders. Awareness training, combined with specialized security technologies and detailed logging, are key components of a comprehensive strategy to detect breaches. Be prepared for when the next outbreak occurs. Not if, but when. To properly defend, an organization should assume the next cybersecurity incident is going to occur momentarily.

It won’t necessarily be a large, targeted attack that will make the news. Most incidents are small, but quite disruptive to the organization. In fact, it could be a single piece of malware from an employee browsing a website. That’s an important consideration. While most attacks may initiate internally, they can be accidental in nature. If an organization’s IT department is unprepared and its staff unable to identify or contain it, a larger and more damaging incident could result. Considering all possibilities is critical to determining a company’s adequate preparedness.

BRING YOUR OWN MALWARE

For cost and convenience reasons, a Bring Your Own Devices (BYOD) policy that permits the use of personal laptops, tablets, and smart phones, is now practiced and even encouraged by many organizations. This presents a new security issue. Most often, the threat of BYOD relates to business data being lost or stolen, including sensitive emails and files. Mobile phones, particularly Android devices, as well as personal computers, are frequently infected with malware, and those devices connect and interact with an organization’s network. Since these devices inevitably wind up processing or storing business data, it’s necessary to protect them in the same way a company would its corporate assets. This means at a minimum, the assurance of strong password usage; encrypting the devices’ storage, anti-malware protection, and in the case of mobile devices, ensuring they can be deleted remotely if they are lost or stolen. This last point is essential as there are clear legal considerations that businesses need to address where corporate and personal devices converge.

WE ARE ALL INTERCONNECTED

Managing security should not be viewed as simply an internal concern. We are all connected—employees with their companies, companies with their partners, partners with their customers. That needs to be considered with any effective and comprehensive cybersecurity program. Cybersecurity requirements with external partners can certainly be challenging at times. This often requires partners who demonstrate a strong commitment to cybersecurity. In INTTRA’s case, we work hard to select the right partners by using a risk-based assessment approach in order to identify if the partners or vendors meet our standards and requirements.

INTTRA takes cybersecurity very seriously. We work with our customers and partners to reduce potential dangers through joint efforts in order to provide safe container movements.

One of the lessons learned from recent cyberattacks is that leveraging reliable partners to assist in times of crisis is a valuable asset to business continuity when there is primary system failure. For example, INTTRA offers Business Continuity Services with the capability to submit booking requests, shipping instructions and VGMs through an alternative booking system that can be activated by INTTRA on behalf of partners in the event of temporary system interruptions. Some organizations in shipping may not have the IT resources to easily address many aspects of cybersecurity. A neutral network, such as INTTRA’s, helps lessen this problem by delivering core services across the network that enable all types of organizations to interact, regardless of their technical capabilities.

PREPARE NOW

As technology increases, and companies all agree to embrace these new technologies, we see three key actions that organizations in ocean container shipping and related industries need to take:

Prepare to defend now – Develop a cybersecurity program that addresses threats to an organization’s assets. To start, organizations of all sizes can benefit from using a free security framework, such as the CIS Critical Security Controls, to help prioritize actions that can be taken to protect against cyber threats. It’s a common framework that virtually any company can use as a start.

Develop a culture of security – Work from within the organization in promoting awareness by offering security training to employees. Remember that humans, not technology, are responsible for the majority of security breaches, so educating employees about cybersecurity is essential. Every employee needs to understand that they are part of the defense.

Work with your external partners – Select the right partners by carefully evaluating the threats and risks to using their services, but also communicate any concerns in order to foster relations and to establish mutual trust.

ABOUT THE AUTHORS

Inna Kuznetsova is the President and COO at INTTRA; the world’s ocean shipping SaaS B2B e-commerce portal, information and service provider. Inna provides strategic direction and holds full P&L responsibility for business growth, managing sales, marketing, service delivery, alliance, product and technology. Before joining INTTRA in early 2015, Inna was the Chief Commercial Officer at CEVA Logistics, and prior to that spent 19 years at IBM.

Gary Huber is the Director of Information Security at INTTRA, responsible for the company’s cybersecurity and risk management program. Gary joined INTTRA in mid-2017, bringing more than 20 years of diverse experience in information technology and information security. He most recently served as Director of Technology Services for Everest Re Group where he focused on securing the organization’s systems. Prior to that, he held cybersecurity roles for companies in the real estate and pharmaceutical industries.

Peter Spellman is Chief Technology Officer at INTTRA, responsible for leading global architecture, engineering and technical operations. Peter has over 25 years of innovative experience in devising, defining, delivering and managing complex software solutions with the last eight years focusing on cloud-based systems. Prior to INTTRA, Peter was founder and CTO of TraceLink, a pharmaceutical supply chain network platform. He has also held technology, engineering and product leadership roles at SaaS startups SupplyScape, Performaworks, and iWant, as well as the MITRE Corporation and Microsoft.

INTTRA is the largest neutral electronic transaction platform, software and information provider at the center of the ocean shipping industry. INTTRA’s innovative products, combined with the scale of our network, empower our customers to trade with multiple parties and leverage ocean industry information to improve their business.

ENQUIRIES

Website: www.inttra.com

ABOUT THE ORGANIZATION

INTTRA is the largest neutral electronic transaction platform, software and information provider at the center of the ocean shipping industry. INTTRA’s innovative products, combined with the scale of our network, empower our customers to trade with multiple parties and leverage ocean industry information to improve their business.