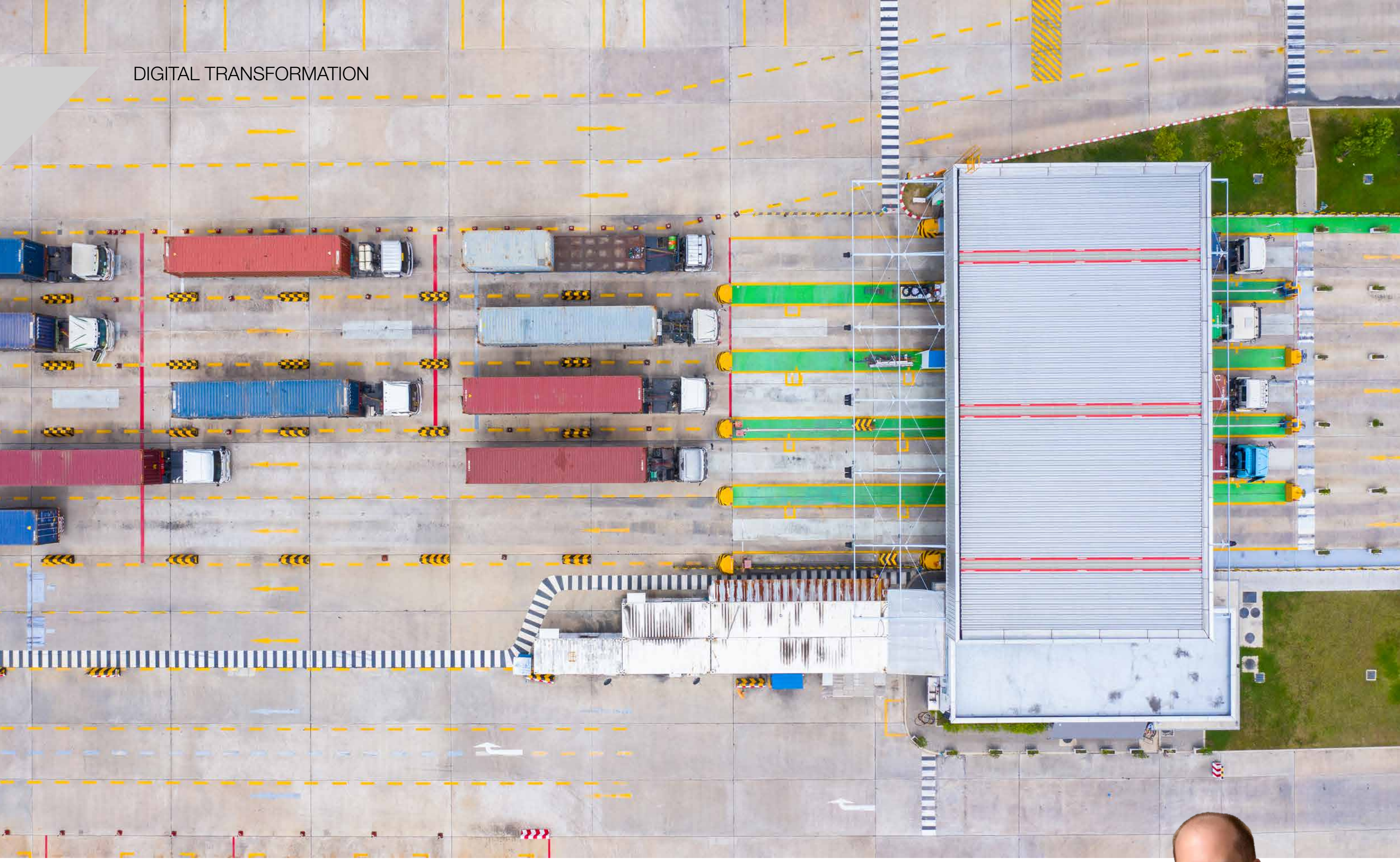


THE PREVENTION PARADOX - WHY PORTS CAN'T RELY ON CYBER DEFENSES AND WHAT TO DO ABOUT IT

Ronen Meroz, CEO, Cyberstar

Admiral Michael S. Rogers, a former director of the National Security Agency said: "The second component of cybersecurity is not just cyberdefense, but it's going to be resilience. It's about this idea about: 'Hey, so how am I going to continue to operate when an adversary penetrates my network?'"

That's a lesson that some terminals already learned the hard way on the cyber security front. In fact, only 19 per cent of cyber leaders feel confident that their organisations are cyber resilient, according to the World Economic Forum.

In the present era of never-ending cyber security attacks, many businesses fall into the trap of over-investing in cyber security defenses, but failing to prepare to react quickly to the breaches that will inevitably slip past those defenses.

Unfortunately, a day would come for many when the CIO phones urgently, alerting that a cyber-attack has occurred. Because the business placed too much faith in its security defenses and under-invested in response and resilience, it is now faced with a cascading crisis.

The terminal operations are suspended while engineers investigate the breach. Government entities demand answers while ocean carriers with inbound vessels can't enter terminals. Ships, trucks and trains sit idle, full of cargo that can't move. Billing shuts down. The business struggles to figure out who to notify and what to disclose about the attack. And even once the breach has been contained, it still takes weeks to fully restore affected data and IT systems.

"COMPANIES ARE NOT JUDGED BY WHETHER THEY WERE HIT BY A CYBERATTACK, BUT BY THE CHARACTER OF THEIR RESPONSE."

Unprepared management will spend considerably longer time for assessment of the situation, and likely have a variety of opinions about how to react to the attack. We know from experience that the first hours and days are critical, and the last thing the business and operations need is a leadership team struggling to form a consensus about how to move forward.

That's the risk terminals routinely face today. The good news is that the problem can be solved by investing in cyber resilience and exercises, which allows them to prepare to respond efficiently and effectively to attacks.

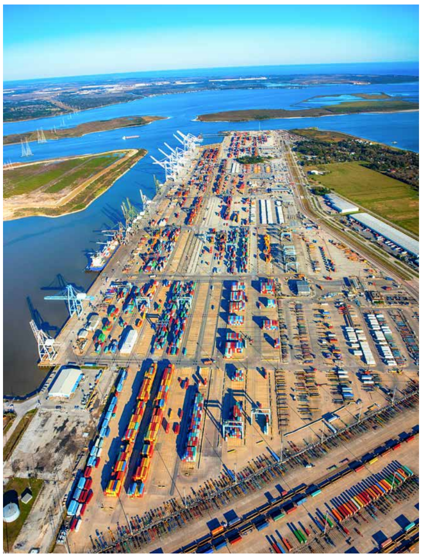
THE TERMINAL CYBER SECURITY CRISIS

"Companies are not judged by whether they were hit by a cyberattack, but by the character of their response" said Robert Silvers, US Department of Homeland Security (DHS) Undersecretary for Strategy Policy and Plans.

Despite the investments that businesses of all types have made in cyber security, each year continues to set new records for the frequency and financial impact of cyberattacks.

The maritime and logistics industry is no exception. Indeed, there's growing evidence that cybercriminals are increasingly keen to target logistics companies. In the past few years, Transnet and the Port of Houston, alongside each of the world's four largest shipping companies – including Maersk and COSCO (as well as their affiliated terminal companies) – have experienced significant cyberattacks.

In short, whatever maritime and logistics companies have been doing to try to prevent cyberattacks is clearly not working in all cases. They are being, and will continue to be, breached.



"MANY BUSINESSES FALL INTO THE TRAP OF OVER-INVESTING IN CYBER SECURITY DEFENSES, BUT FAILING TO PREPARE TO REACT QUICKLY TO THE BREACHES."

INVESTING IN CYBER RESILIENCE

Faced with a never-ending spate of attacks, what can terminals do?

Firstly, businesses must invest in cyber readiness, which we define as being composed of three central components:

- The readiness of the IT team to respond to the incident
- The readiness of the terminal management team to handle the crisis
- Establishment of an operational continuity infrastructure

Our experience working with terminals around the globe has shown us that many businesses fall short in all three elements of their cyber crisis readiness capabilities. While there are usually some plans in place for the IT and infosec team, there is simultaneously a distinct lack of procedure for the management. Where procedures and capabilities do exist, they usually pertain to short term crises, such as IT breakdown, rather than for severe cyberattack, which may last a week and possibly longer, as recent cases have proven.

CYBER RESILIENCE PILLARS

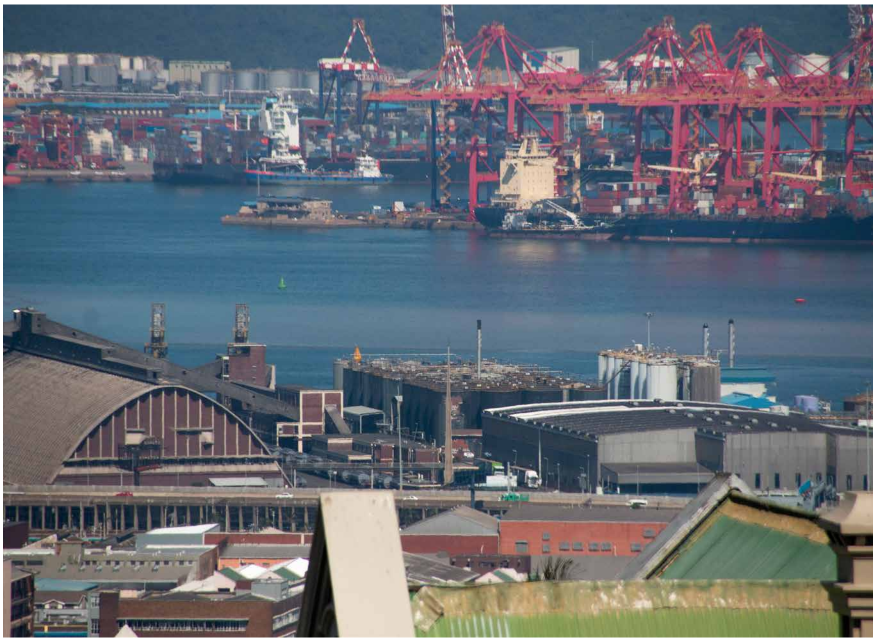
To avoid pitfalls like these, terminals must develop cyber security strategies to handle any crisis. The response strategies can range, pending the specific scenario, for example:

- Shutting down all terminal activity until systems are recovered
- Working at marginal capacity, based on few limited preplanned contingencies
- Working at maximum possible capacity (aiming for high double digit percentages) based on tangible contingencies and operational continuity solutions established and tested beforehand

Each strategy has pros and cons as well as commercial, operational, reputational, legal and financial implications.

When working with terminals on operational continuity we often face the conviction: "Without our IT systems, there is almost nothing we can do''.

Such an approach is hardly viable commercially, but even if the terminal's choice is to completely shut down



operations until full recovery, a cyberattack is likely to surprise the terminal in mid-operation. This means vessels undergoing cargo operations, dozens to hundreds of third-party truck drivers within the terminal area for delivery or pick-up, trucks queuing at the gate, trains under cargo operation, and inbound vessels and trains pending arrival.

Regardless of the operational strategy ultimately chosen by the management team, all terminals should develop a clear and detailed crisis management plan addressing several key aspects including:

- Shifting from business-as-usual to emergency mode
- Crisis management team nominations, roles, routines, and procedures
- Adversary engagement strategy
- Operational response plan
- Commercial and customer support response plan
- Legal response plan
- Communication and PR plan

The more the terminal management team discusses and prepares for such scenarios in advance and defines principles for action on each element, the easier it will be in real-time, with less damage to business and faster recovery.

ENTER CYBER EXERCISES

Developing a playbook is only one step toward cyber resilience. To leverage your playbook to maximum effect, you need to practice them using cyber exercises.

For example, a cyber event will lead to an overwhelming volume of enquiries at all levels in the terminal, looking to receive updated information. This requires having a solid and tested communication plan in place, one that provides structured and coordinated distribution of information to stakeholders during the event, considering that the website and email systems may be disabled.

Instances of cyber compromise may be limited to specific systems. But since all key systems are usually integrated, it can put the normal course of operations in jeopardy. For instance, while core operational systems such as Terminal Operating Systems (TOS) and Gate Operating Systems (GOS) may stay fully operational, the terminal's interface systems with external parties (emails and Electronic Data Interface) could be severely compromised. This would make it extremely challenging for the terminal to operate with stakeholders including shipping, rail and customs.

Terminals that exercise various crisis scenarios beforehand will be able to set up alternatives more quickly, maintaining their ability to continue working, even when most or all core operational systems are down. Our experience suggests that a key added value for the exercise is actually in the preparations. The mere fact that the terminal management team needs to prepare requires them to apply time and thought to the issue, review and refresh protocols, establish new ones, and discuss principles internally still before the simulation itself. If the preparation process is guided and facilitated properly, it will yield tangible outcomes even before the drill day.

INVESTING IN CYBER RESILIENCY WILL NEVER BE REGRETTED

A cyber incident is a complex managerial and operational challenge. Planning, building capabilities and readiness, practicing with the management team to build 'muscle memory' to deal with such an event will put your terminal in a completely different place on 'D-Day'.

As one of our customers, a manager of a large North American terminal said: "Cyber readiness is gradually becoming a key concern, on which our customers demand and expect highest standards from us. Terminals that can demonstrate such high capabilities, especially in terms of operational continuity, will gain competitive advantage over terminals who failed to do so."

At Cyberstar, we specialise in executing cyber exercises that help your entire team gain the skills and experience necessary to get back to work quickly when security incidents occur. Leveraging our unique experience in the maritime and logistics industry, we provide guidance and education that allows terminals to maximise their continuity and resilience in the face of never-ending cyber threats. We increase your resilience by planning a response tailored to your operations and partnering with you to help manage active incidents.

ABOUT THE AUTHOR

Ronen Meroz is a shipping and logistics industry veteran. For over 20 years, he has held leadership roles in maritime business development, corporate development and finance, and global operations.

At ZIM Shipping Lines (ZIM), Ronen was instrumental in the improvement of ZIM's vessel-terminal interface and performance globally, and was responsible for developing business continuity programs, enhancing digital capabilities, and optimising the key operational processes.

ABOUT THE ORGANISATION

Cyberstar is a boutique cybersecurity consultancy for maritime and logistics companies, created as a subsidiary of ZIM (NYSE:ZIM) and in partnership with Konfidas – a leading cybersecurity outfit.

Our mission is to empower organizations to rebound from major attacks with as little business disruption as possible.