Cyberstar

Cybersecurity Beyond Technology

Assess
Plan
Practice
Respond

OUR APPROACH

Assess

Before an effective plan can be formulated and materialized - there must be a current-situation assessment which will create a clear picture of existing and potential risks.

Knowing where cyber threats may be coming from, what vulnerabilities and gaps exist, what the current capabilities are and whether the company has compliance issues - is critical in order to optimize the plan going forward. Our experts will evaluate your company's status and provide management and operational levels, actionable deliverables which will enable you to fully understand your current landscape and cyber posture.

- Cyber Maturity and BCP Assessment
- Threat Profiling
- IR Assessment
- Penetration Testing and Vulnerabilities Assessment

Respond

A cyber crisis is much more than an IT crisis. It involves various stakeholders such as customers, vendors, partners, authorities, regulators, as well as multiple business functions, processes and systems – operational, commercial, HR and others.

Senior leadership will be required to make many difficult decisions in a highly chaotic and stressful situation. We offer to partner with you in managing such incidents, whether in "end to end" event management mode or in consulting to C levels, based on our extensive experience in managing cyber crises and our profound, native understanding of the specific concerns and pain points of the maritime and logistics industry under such a "black swan" event.

- IR management
- C-Level Management consulting and support

Plan

Cybersecurity threats are becoming increasingly severe, disruptive and unpredictable. The shipping and maritime sector is being targeted more than ever, and each company in the sector, whether large or SME, must have plans and controls in place to mitigate the threat and improve its chances for quick recovery. Cyberstar works with maritime and logistics companies to develop customized cyber strategies, policies and action plans that meet the customer's priorities, risks and budgets.

- Cybersecurity Strategy and Policies
- Cybersecurity roadmap planning
- Corporate Incident Response Plan
- Business Continuity Plan

Practice

"Train hard, Fight easy"- this famous and deeply insightful quote of Alexander Suvorov, the Russian military leader, is applicable to the cyberspace as well.

Having a solid strategy and plans is a great start, but only practice materially raises the chances of withstanding an actual attack unscathed, only practice subjects the plans to "pressure testing". Our comprehensive training program goes from staff awareness and readiness to Clevel workshops, through tabletop exercises, and up to highly complex and elaborated cybersecurity real-world scenarios, which enable the customer to experience what it's like to be under the "incoming fire" of a real cyber-attack.

- Awareness training
- Leadership workshops and exercises
- IR Training
- Cyber-attack table-top simulation - Crisis Management

ASSESS

Threat profiling

The Cyber Threat Profile is a strategic business document based on a combined thorough assessment that enumerates the cyber threats facing the corporation and outlines the resources necessary to mitigate the risk and recover from cyber events.

We will review the position of your company, considering the ever-changing cyber threat landscape and potential threat actors and their likely tools and techniques, and provide you with insights on how parties with malicious intent view your company and primary assets when they have you "in their sights", as well as the nature of their ultimate goals and how this is likely to affect the specific form of the attack.

Cyber Competencies Assessment

Cybersecurity competencies assessment provides an independent 3rd party review of your company's cybersecurity capabilities in terms of people, systems and processes.

Our highly experienced cybersecurity team will evaluate the cyber competencies based on various frameworks (such as NIST) and provide the key stakeholders with a scorecard across the various parameters, comparing the organization's current state to best practice, identifying key gaps and prioritizing the next steps to be taken to effectively address the points for improvement and upgrade to the required state based on each customer's risk agenda and budgets.

IR Assessment

Our team will perform an in-depth review of IR capabilities to provide an independent view on current IR processes and procedures. Our IR Maturity review will address questions such as:

- - Do you have the required IR skills to face a cyber incident?
- - Which skills should be provided by 3rd parties?
- - Do you have proper procedures that elaborate what should be done, how and when?
- - Is your team technologically equipped to identify various cyber compromises, assess and investigate them and address them appropriately (contain, eradicate, recover)?

Penetration Testing and Vulnerability Assessment

Penetration testing and Vulnerability assessment are a key component of any security assessment program, aimed to identify vulnerabilities and misconfigurations throughout the IT systems and architecture.

After determining the scope of the desired scans, we use best-of-breed technologies deployed by our senior security professionals to scan your key IT assets for known vulnerabilities.

You will receive detailed actionable reports for immediate remediation by your system administrators and cybersecurity practitioners.

PLAN

Cybersecurity Strategy and Policies

The Cybersecurity Strategy statement is a managerial-level document which defines the general principles underlying the protection and defense of organization assets and information as part of achieving the business goals (the "What" and "Why").

The Cyber Security Policy Principles document defines the intentions and direction of the organization as expressed by its top management regarding the methods used to implement the Cybersecurity Strategy and preserve confidentiality, integrity and availability of information (the "How").

Cybersecurity multiyear "roadmap"

Based on the various assessments performed, we will formulate a multi-year plan for the management of cyber protection. The work plan is the practical translation of the Cybersecurity Strategy, Cybersecurity Policies, and cyber risk analysis. It is based on your company's unique needs, priorities, and budget.

Corporate Incident Response Plan

The CIRP is a plan that defines the procedures and capabilities required to manage cybersecurity events. It defines the company-level procedures for managing and recovering from a cyber crisis, addressing all business aspects and including management and stakeholder responsibilities, workflow, and timetables. The plan improves company-wide readiness and creates capabilities for confronting a range of cyber events. Such an event may evolve rapidly and have strategic business-wide consequences.

Business continuity plan

A significant cyber incident will most likely disrupt critical business processes. In order to mitigate such disruptions, we will develop a Business Continuity. Plan (BCP) in the context of a cyber incident. Such a plan is based on mapping critical processes, creating contingency plans and "work arounds", documenting them in a BCP procedure and working with business and operational units, to develop tailor-made solutions.

PRACTICE

Awareness training

As statistics clearly suggest, many cybersecurity compromises are caused by users with suboptimal information security knowledge and understanding, and poor security "hygiene". This is becoming increasingly important in the new era of remote work.

We offer on-prem or off-prem awareness training to your staff, which can be tailored to your specific needs and budget. Through lectures, movies and/or web training applications - using simple terms and no "cyberspeak" geeky terminology - we will engage your staff and onboard them to improve their cybersecurity practices.

Leadership workshops and exercises

Our leadership workshops, tabletop drills and scenario-based discussions are aimed to train and improve the readiness and effectiveness of senior management's response to cyber-attacks, upgrade decision-making processes, discuss the potential impact of and level of readiness for extreme cyber scenarios, examine the adequacy of current risk controls, and coordinate actions against cyber threats.

IR Training

We conduct scenario-based exercises specifically for IT and the IT security team to test and improve their technical detection and response to cyber-attack. During such exercises, the teams practice event detection, communication, analysis and understanding of attack targets and methods.

The team will usually discuss several relevant preagreed scenarios from detection to response and recovery.

Cyber-attack table-top simulation

Having a corporate-level response plan is an excellent first step, but it can create a false sense of security unless accompanied by repeated exercise. Nothing better prepares you to face and manage a severe incident than a full-scale cyber crisis simulation. Such rehearsals enable you to test your plans and policies, identify and remedy gaps, and consistently improve the effectiveness of your plan. From our experience, these simulations also serve as a very strong engagement factor in onboarding the participants to the desired cybersecurity culture and mindset.

RESPOND

IR management

Cyber crisis management is a "black swan" event, and not something that organizations engage with every day. When a cyber incident occurs, it is critical that the organization engage in the right activities, at the right time, even while under intense pressure to resolve the crisis.

Our IR team is well equipped to support you with:

- Technical Containment and Hardening Actions - to prevent the crisis from deteriorating.
- Technical Forensics - to investigate the source of the attack and what led to the event.
- Security Tools Implementation - to perform hunting activities and prevent further expansion of the scope of the attack
- To perform managed recovery and back-to-normal procedures

C-Level Management consulting and support

A cyber crisis is so much more than a technological crisis, and it presents numerous decisions and dilemmas that are outside the scope of IT, including: how to handle customers, partners, vendors, authorities, employees and so on, and how to ensure that the response efforts are properly coordinated among all parties, tech and business. In all the chaos that is a cyber crisis - we can offer our wide ranging experience in the management of such incidents and save senior leadership a lot of pain and mistakes based on lessons learned.

Cyberstar

WHAT MAKES US DIFFERENT?

1. Cyberstar comes from maritime. For over 75 years, our parent company, Zim Shipping, has been a recognized industry leader in global maritime shipping and logistics.

2. Cyberstar comes from cyber. Our other parent company, Konfidas, is a leading cybersecurity and data protection firm. We know cybersecurity, and we excel at building the right solution to the right challenge.

3. Our experts engage the whole organization. No single group in any organization can effectively mitigate cyber threats; all stakeholders need to be actively involved. From business leaders to operational teams, from finance to logistics, from customer service to purchasing and everyone in-between – cybersecurity requires all hands on deck. Cyberstar consultants help you mobilize your entire team through awareness training, workshops and exercises, IR training, red team exercises and cyber crisis simulations.

4. We help you better prepare. Our consultants take a deep dive into your cybersecurity posture. We identify strengths that you can leverage – and gaps and vulnerabilities that need shoring up. Then we help you prioritize investments and choose the right tech for the right job.

5. ...and rebound faster. Business resilience is key. That's why, in addition to lowering the risk of cyberattack, Cyberstar consultants focus on ensuring that your organization rebounds faster after an attack occurs. We help you develop the procedures and contingencies that harden critical processes. And we work together with you to create structured methodology that helps you navigate cyber incidents.