INTERNATIONAL INSURANCE SOCIETY

An affiliate of The Institutes | Risk and Insurance Knowledge Group

Critical Infrastructure and Cyberspace

Abstract

This year commenced with continuation of the COVID-19 pandemic, supply chain disruptions, war in Europe, a commercial passenger plane crash, and a volatile crypto market. Governments, risk managers, and security officers must be vigilant of cyber activity, especially for critical infrastructure and crown jewel assets in cyberspace, which could lead to physical damage and bodily harm. Critical systems such as ports and container terminals undoubtedly need attention. Necessity is the mother of invention—it leads to innovation as the digital assets in the intangible world outnumber the physical assets.

Cyber activity is proportional to digitization. For critical infrastructure and supply chains, this is digital twin technology, where a virtual copy of the critical infrastructure is created to simulate activity and improve decision making. It uses multicloud strategies, which are types of cloud computing, for each critical infrastructure, creating efficiency.

This architecture generates data and events that require monitoring for cyber integrity using a security operations center (SOC). The SOC, which is controlled by a chief information security officer (CISO), generates information known as threat intelligence.

Cybersecurity must be mitigated and apply data and cyber integrity, which tags assets in cyberspace so they can be tracked. Larger risks can be transferred to insurance vehicles or capital market solutions, such as insurance-linked securities (ILS), through a pre-agreement contract between the CISO of the critical infrastructure and the insurance underwriter.

The first asset in cyberspace was Sputnik I, which was launched into orbit on October 4, 1957, by the Soviet Union, marking the start of geopolitical developments encompassing science, technology, and defense.[1] After that, the cyberattacks in Estonia in April 2007 (the first state-sponsored cyberspace attack in history) and the NotPetya attack in June 2017 (which targeted Ukraine and affected Maersk/Merck) seriously affected data and cyber integrity.[2,3] Now, with the current war in Ukraine, the world must assume data compromise, as cyber war would likely target critical infrastructure.

Military technology is now high tech, making it vulnerable to cyberattacks. Tanks, drones, and guided missiles have digital twins that contain executable computer code and processes that can be compromised. However, the defense industry has mainly bootstrapped their cyber risks. Supply chains, on the other hand, were weakened by the COVID pandemic, so they remain vulnerable to cyber risks.

Industrial sectors exist in silos faced with systemic risk due to rapid digitization and inadequate risk transfer. C-suite management frequently view cybersecurity assessment and mitigation as an issue that should be handled by the cost center and IT rather than as a profitable business service and key boardroom function.

A pattern of cyberattacks has been developing over time, hence the reason the Baltic region houses the North Atlantic Treaty Organization's (NATO's) cybersecurity headquarters and data embassies were created.[4] Estonia became the world's first fully digital society and a model for others. However, the dark side of increased digitization now rears its head and brings the potential for cyber compromise to the doorstep of every responsible nation.

Has the lack of robust data and cyber integrity allowed viruses and trojan horses to be unleashed already?

Energy, telecommunications, water utilities, and nuclear power stations are stringently cyber protected, but there is no room for complacency due to constant changes. However, the transportation industry—especially the logistics, maritime, ports, and container terminals that connect the ships to supply chains—is more vulnerable because it took longer to set its standards and understand its cyber risk.

Increased digitization means that a container terminal, for example, is no longer a silo protecting its own risk profile idiosyncrasy. Instead, it is an interdependent entity posing systemic and accumulation risk. Current cyber insurance is also inadequate, and risk managers are demanding better coverage, higher limits, resilience, and remediation.

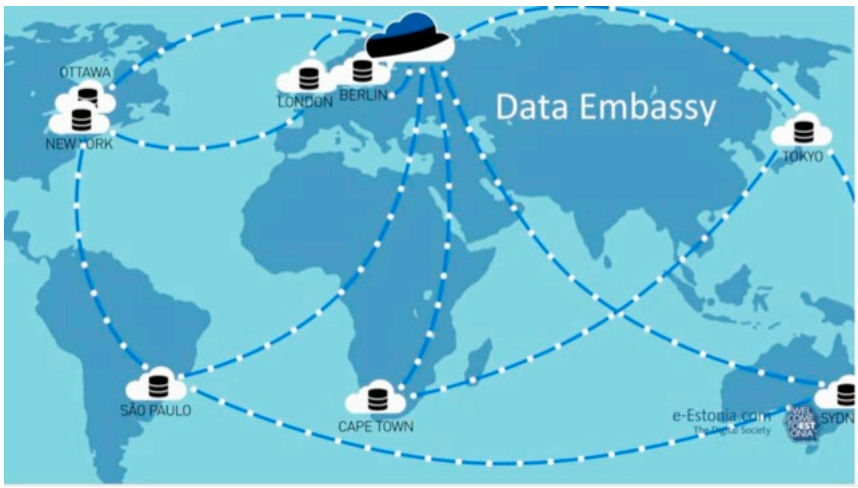
As world tensions escalate, critical infrastructure such as utilities, electricity, fuel pipelines, telecommunications, transportation, and factories will be prime cyber targets. This article addresses critical infrastructure in the cyber era in terms of protection and turning cybersecurity into a profitable advantage.

Data Embassies

Following the Estonian cyberattacks, the concept of data embassies was born. A data embassy is a tool used by nation states to ensure digital continuity with respect to critical assets. Data embassies consist of server clusters that store a country's jurisdictional data in another country to allow continuation of government when governing from within the home country becomes impossible. This situation could occur due to natural disasters, nationwide cyberattacks, or military invasion.

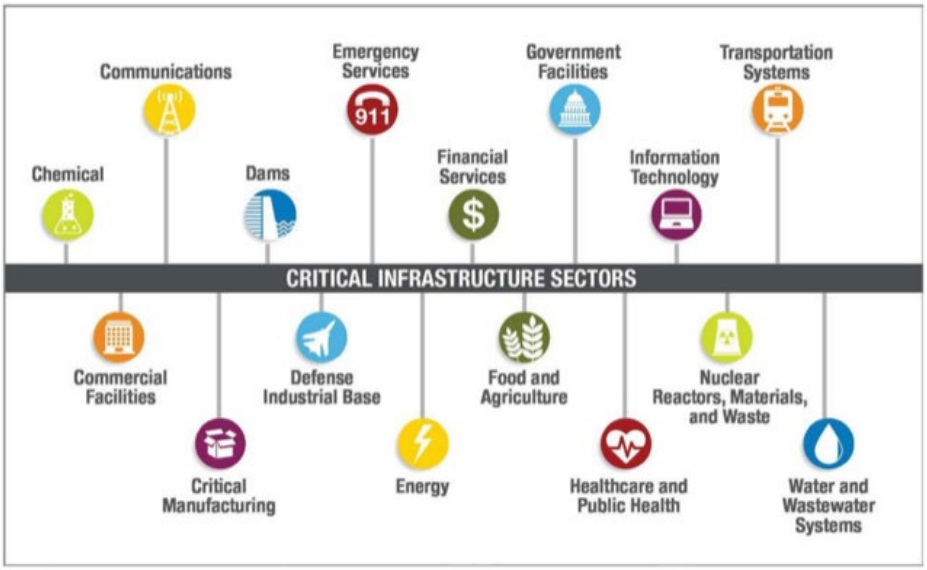
Data embassies may be attractive to countries that have already digitalized their crown jewel data and are located in the geographical vicinity of the aforementioned threat vectors. Currently, data embassy

innovation is based on the principles of the 1963 Vienna Convention and requires modernizing to be effective.[5,6]



Critical Infrastructure

The following diagram shows the critical infrastructure sector landscape.



Critical infrastructure sectors are interdependent and interconnected. Therefore, they are vulnerable to direct cyberthreats and collateral damage, which could cascade to an entire country's infrastructure network. Emerging remote sensing sectors such as small satellites and drone technology extend the risk.

Cyberattacks on critical infrastructure have increased recently. Inside knowledge of the configuration and administrative operations of control systems is necessary to cause physical damage and bodily injury. Cyber professionals use a cyber kill chain framework that models business targets to simulate that of military actions.[7] If power outages lasted for several weeks or ports could not operate for days, the affected country could experience serious economic effects on its gross domestic product and become a target in confrontations between nations.

Moving forward, critical infrastructure sectors can strengthen their cyber defenses by using cloud computing to improve efficiency and resilience with cyber hygiene. The Log4j remote code execution vulnerability of 2021 affected every sector of critical infrastructure. As a result, the Open Source

Security Foundation (OpenSSF) was created to close future gaps.[8,9] However, millions of devices were affected, so it will take years to patch and remediate every intrusion.

Cyberattacks vary in severity and frequency and can be caused by malicious outsiders or insiders. Malicious insider attacks may be more difficult to identify because the hacker has legitimate access to systems. When operating in the cloud-computing environment, everyone can be considered an insider. Data effectively becomes the perimeter of the organization, so a zero-trust strategy must be used.[10]

The table identifies some of the most important attacks on global critical infrastructure. It excludes the political attacks on the United States election system, which are blamed on Fancy Bear, but there are many political cyberattacks between governments that can spill over to critical infrastructure networks.[11]

Attacks on Critical Infrastructure

Date	Type of Attack	Geographical Location
2022	Wiper	Ukraine War—Caddy Wiper—critical assets[12]
2022	Ransomware	European oil ports in Belgium, Germany, and the Netherlands[13]
2021	Zero day	Log4j—all existing devices and operating systems
2021	Ransomware	Colonial Pipeline, U.S.[14]
2021	Malware	American Water Authority, U.S.—poisoning water[15]
2020	Ransomware	Oil refinery, Taiwan[16]
2020	Malware	SolarWinds technology company, U.S.[17]
2020	Malware	Water control systems, Israel[18]
2020	Data breach	Nippon Telegraph and Telephone, Japan[19]
2020	Data breach	Moderna, U.S. (COVID vaccines)[20]
2017	Triton malware	Petrochemical plant control system, Saudi Arabia[21]
2017	Ransomware/wiper	Country of Ukraine—Maersk/Merck, NotPetya
2016	Malware	National electricity company, Israel[22]
2016	Malware	Ukrainian power grid (Black Energy 3)[23]
2016	Ransomware	San Francisco municipal light rail, U.S.[24]
2015	Distributed denial of service	LOT, Polish national airline[25]
2014	Social engineering	Steel mill, Germany[26]
2013	Malware	New York dam, U.S.[27]
2010	Malware	Iranian nuclear program—Stuxnet[28]
2007	Data breach	Country of Estonia

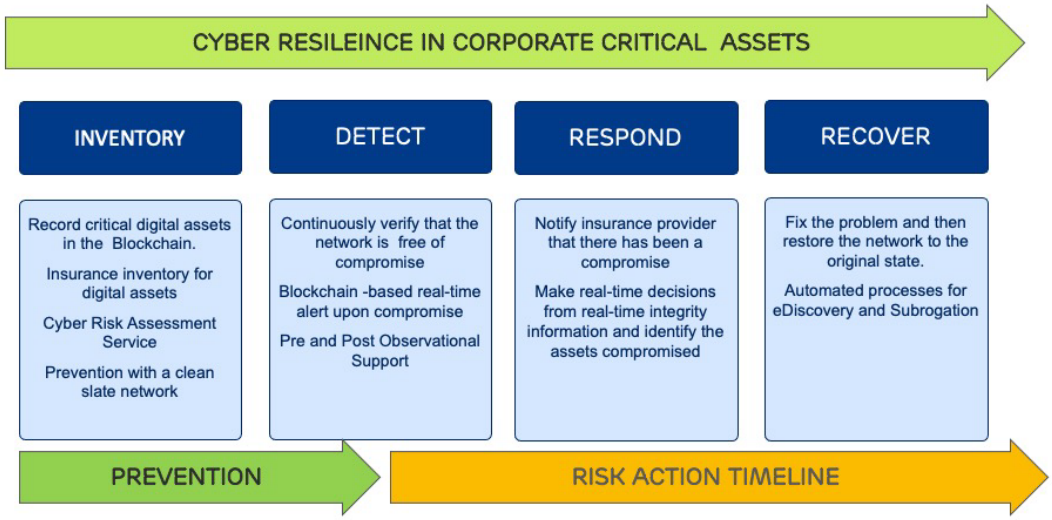
There is evidence of emerging cyber disruption in container ports. The COVID pandemic caused a significant increase in cybercrime, which created more demand for cybersecurity workers. Segmenting critical infrastructure networks and isolating industrial devices from bad actors can mitigate a black swan cyber event and limit lateral movement in the event of a breach, including where singular access via a virtual private network (VPN) can expose the entire network.

Operational technology (OT), unlike information technology (IT), has more legacy with systems, devices, and endpoints disconnected from the internet. Industrial control devices, which have existed for years as reliable workhorses, became a target and attack vector when they came online, as IT met OT in a sensor ecosystem.

IT professionals patch and upgrade security in modern hardware and software to protect their networks. OT staff manage proprietary network protocols, often without comprehensive security

controls like authentication, encryption, event logs, or audit trails, which can make incident detection and response challenging. OT systems are gradually being replaced with smart devices, so combining IT and OT will ease compliance and regulatory reporting and audits. Engineers from OT business units are well positioned to support incident response within the SOC.

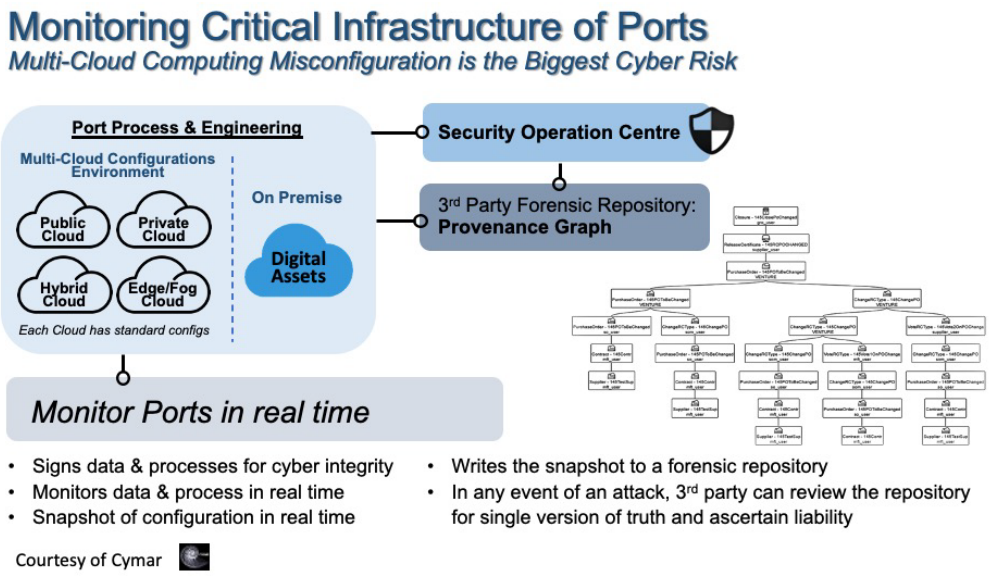
The complexity of cyberthreats and smart device digitization of critical infrastructure requires a stringent risk assessment process to reduce and mitigate cyber event probability and improve the network's ability to recover. Standards provided by the National Institute of Standards and Technology (NIST) can be used to develop a risk management framework.[29] The critical assets such as data, software, hardware, control systems, communications, and networks need to be identified and classified, and anomalies need to be detected, with standard response and remediation, as shown in the table. Critical assets are those with a high consequence and failure potential.



Multicloud Strategies

Increasing multicloud usage is considered the top risk of critical infrastructure with respect to cyber and data integrity, vulnerability, and opening new cyberattack surfaces. Tools must be introduced to monitor the increasing number of private, public, hybrid, and edge clouds that house sensitive data and critical business processes. Scalable technologies can be most effective at preventing misconfiguration and data tampering by taking forensic real-time snapshots across the clouds in a standardized interface.

Multiple clouds communicate with each other, which risks data being lost during transmission. Edge clouds shift data processing away from the SOC to devices at the edge of the network, such as ship technology or autonomous transport, which avoids risking a link to the internet when split decisions are required. The diagram shows an example of the multicloud protection strategies in a container port environment with an SOC central to the mitigation operation.



Security Operations Centers

Many smaller critical infrastructure sites, such as some container ports, do not have an SOC and outsource the operation, which requires third-party cyber compliance. Outsourcing to a managed service reduces the upfront costs of new hardware and software, as well as the cost of employing IT security specialists. It can take up to three years to set up a complete SOC because of cyber risk complexity, which is shown in the graph.

The SOC has a brain-like understanding of the business-threat landscape—the network components on premises; the endpoints, servers, software, and third-party services; and traffic flowing between

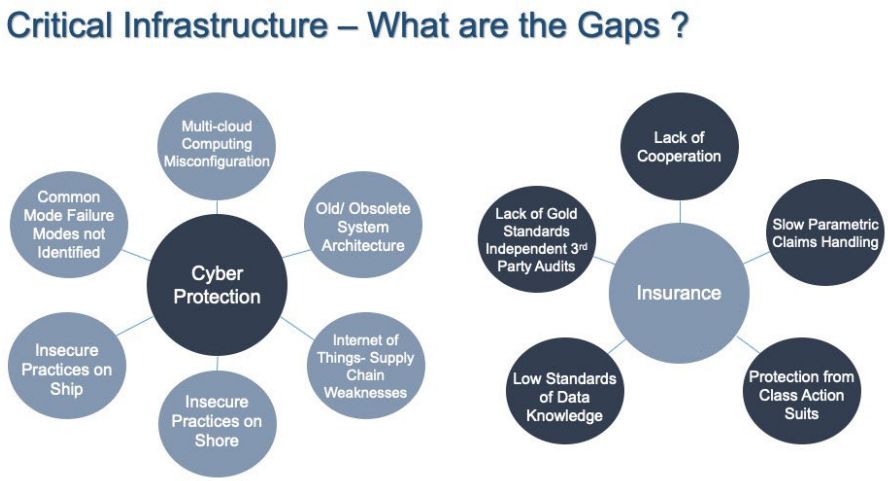
these assets. It continuously monitors cyberthreats and is notified immediately of emerging threats so it can prevent or mitigate damage.

The SOC acts as a first responder by shutting down or isolating endpoints, terminating or blocking harmful processes, stopping lateral movements, and deleting files and backups. When successful, these actions return the network to the state it was in prior to the incident.

Critical infrastructure SOCs can see up to one million security alerts daily. Key performance indicator (KPI) metrics, which show the SOC's effectiveness and improvement over time, include average incident detection time and average time from discovery to remediation. Critical infrastructure organizations differ in their SOC maturity, depending on the standards, framework, and technologies they use to protect critical business functions and processes, the digital supply chain, and the crown jewel data.

Underinsurance and Risk Transfer Issues

There are many gaps and emerging issues in the cyber insurance market, especially for critical infrastructure cyber incidents, which be seen in the diagram.



The internet is not attributable, so liability and indemnity can be difficult to determine. In order to deny or subrogate a cyber-related claim, reinsurance companies need to demonstrate that the claim is related to a state-sponsored attack or proxy group. Then they can enforce the war exclusion. Otherwise, the claim can lead to costly litigation and reserving. This is a good reason for policyholders to investigate parametric insurance and alternative reinsurance mechanisms. Political violence and cyber covers are best kept apart.

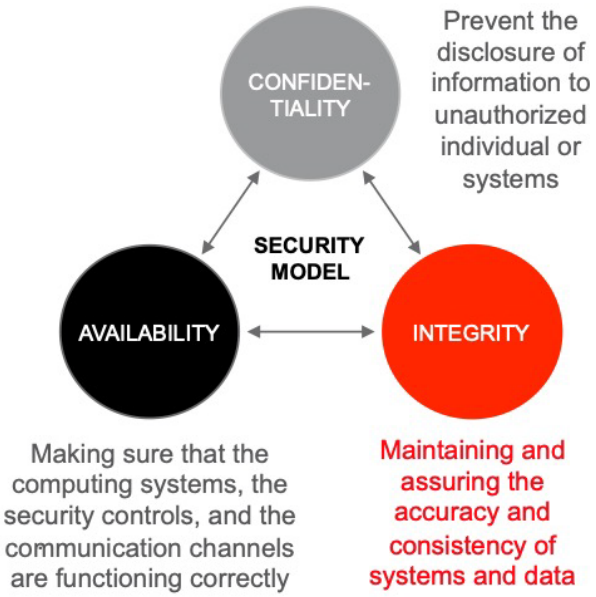
Any cyberattacks on critical infrastructure that result from the war in Ukraine may challenge the war exclusion clause in current insurance policies, as the war is hybrid, meaning that it combines military and cyberattacks. It’s possible that viruses planted will be triggered during or after military action. CISOs must assume compromise and be alert.

A court set a precedent when it found an insurer liable to pay a cyber claim related to the NotPetya attack because the policy exclusion wording was unclear.[30] Other insurance lines that may be affected include political violence, trade credit, property, marine, cargo, and aviation.

Cyber insurance prices rose 34 percent in 2021, and the hardening market is challenging insureds to find the right coverage at the right price.[31] This is driving risk associations to recommend a cyber captive approach and alternative risk transfer structures to their commercial members.

A cyber captive is an insurance company owned by a corporation tailored to handle cyber risk. As the market hardens, more companies will likely gravitate to them to build essential captive claim reserves, as the traditional market currently lacks access to retrocessional and reinsurance capital of any significance, and supply chain risk will likely follow suit. This requires accessing the capital markets to stimulate the primary cyber market by using ILS. Investors are now seriously considering cyber exposures and bespoke solutions relevant to the policyholders around ILS. Critical infrastructure risk is well-suited to this approach and will form part of a layered cyber catastrophe solution or reinsurance tower to spread the risk.

Modeling cyber risk both from the portfolio and scenario angles can help quantify and improve understanding of the cyber line, which can deploy threat intelligence into a model in which sponsor and investor interests align. Cyber risk is central to enterprise risk management and must be holistic. The overall risk for critical infrastructure organizations is failure to fulfil their CIA (confidentiality, integrity, and availability) triad goals due to the probability of a threat obstructing the goals.



Risk Management

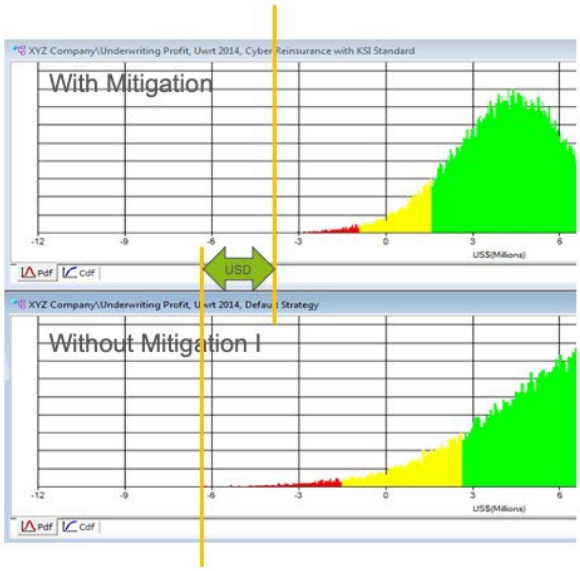
The reinsurance industry handles cyber risk that involves high-severity and low-frequency events; the primary market can handle small occurrences unless they aggregate into bigger events. Risk managers can now use captives for cyberspace, so they can tailor this risk for their organization rather than go to the open market for insurance. Data breaches are an expensive risk, and the captive can underwrite and pay claims from a cyber reserve, thus relieving the parent company of reputational issues.

Companies manage risk aligned to their risk profile and risk appetite. Although risk-based capital modeling had been the domain of reinsurers, risk awareness and risk assessment is currently on the radar of large corporations and family businesses that manage supply chains.

The modeling process uses mathematics to create future scenarios and simulations based on historical loss data. This correlates all of an enterprise’s risks into one holistic view, which needs to be applied in tandem using artificial intelligence (AI) techniques.

Cyber is operational risk and very hard to quantify. In the past, it was bundled and quoted as a percentage of gross written premium, which was an inadequate measure.

Insurance and reinsurance are not alternatives to a risk management program. Risk transfer programs should be used to address structural residual risk that remains after risk mitigation is considered. The diagram shows an example of a robust industrial risk modeling tool that looks at critical infrastructure cyber risk.



- Assuming each critical infrastucture had a limit of $5 million to a group limit of $30 m prior to data integrity cover and proof of provenance
  - No data centric model considered
  - Privacy and perimeter assessment only
  - Vulnerable to severe cyber
- With data mitigation possible to move to a group limit of say $500M USD
  - Need mitigation resilience caveats
  - Threat intelligence / hunting
  - In situ data integrity proving lower risk
- Mitigation costs can be covered by the costs of reducing risk

The green shading, which was determined based on historical data and the company's risk appetite, represents small claims that could result from a cyberattack. The yellow shading represents a move to riskier areas. The red shading represents the fat tail, or the black swan event, that could make the entity insolvent; it is the tail value at risk (TVaR) and the area that needs to be addressed by risk transfer mechanisms.

If data and cyber integrity mitigation is adopted, the residual risk represented in the top graph should be examined. The bottom graph shows the situation prior to mitigation, where a claims fat tail is affecting the company risk-based capital limits and solvency.

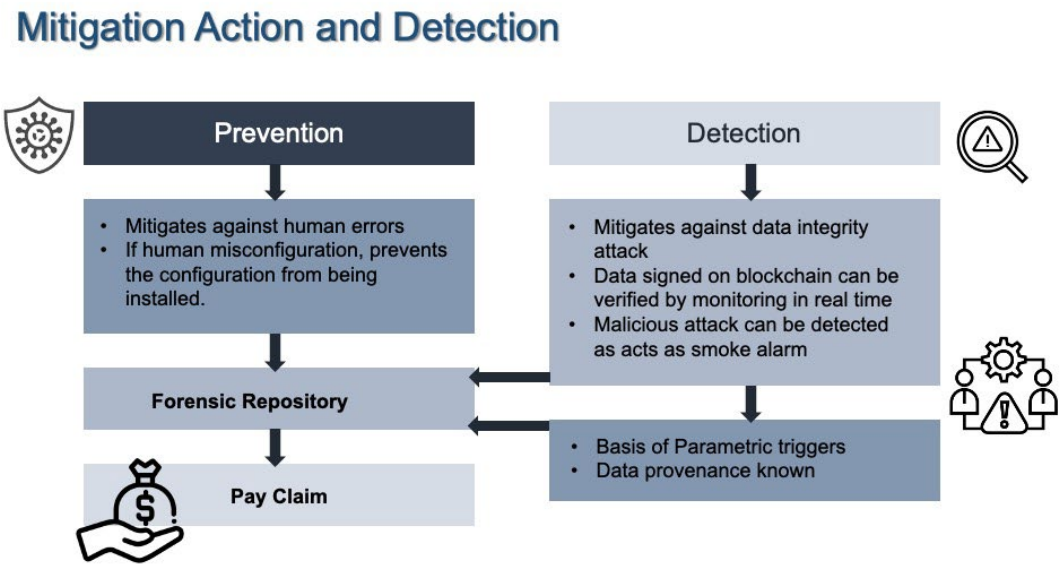
It is important for organizations to have access to a rating system of IT and outsourcing vendors regarding the quality of data and their mitigation of a data breach. CyberCube provides more information about cyber risk modeling.[32]

Parametric Insurance

Parametric insurance solutions, as an alternative to an indemnity approach, are suitable for critical infrastructure because they are bespoke, avoid exclusionary language, and pay claims immediately. Solutions are successfully deployed in the natural catastrophe sector. The container terminals example shows that most terminals are owned by the private industry, and port land is owned by the government, so this is remedial and prevents long claims and litigation processes, making a public–private partnership viable. This concept is gaining traction among corporations seeking solutions to expand capacity or protection not available in the conventional market.

When a predefined event occurs, a well-defined payment trigger can initiate payment for an insured's claim. Objective third-party data sources are used to define triggers, and these can be obtained from the threat intelligence and real-time data feeds applied to the asset in the monitoring process. There can be basis risk between the parametric loss payment and the actual loss suffered by the insured.[33]

For critical infrastructure multicloud risk, the data integrity, provenance, and single version of the truth provide an ideal component within a trigger when combined with other factors and compensate the insured for more of its true economic loss. The diagram shows how multicloud protection adds value to the process.



Cyberspace has many types of risk, including malware, ransomware, phishing, denial of service (DoS) attacks, Internet of things (IoT) attacks, advanced persistent threat (APT), and man in the middle, so there is an all-risks opportunity where the trigger definition can be intuitive. This is groundbreaking for business interruption to network security liability for monitoring and guaranteeing service on the upstream and downstream effect on supply chains and critical infrastructure process flows.

The underwriter and the CISO need to agree on the nature of the exposure and the data sources involved, and correlate that information to the liquidity following the event and strike a contract. A website outage, for example, involves a simple algorithm for downtime that addresses the number of people affected at a calculated loss figure. Other events may be more complex and require multiple triggers.

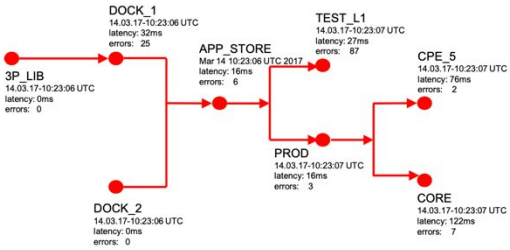
It should be noted that remedial services are still required to restore a network to a baseline after an event; this service is often supplied in an indemnity contract. However, for parametric, this service is provided by the SOC and risk mitigation services of the critical asset. Threat intelligence and hunting can provide good insight into trigger design.

Threat Intelligence

Threat management draws on many data sources, so it is essential to classifying and identifying crown jewel data and tag it in advance. This is composed of real-time event data generated from the SOC with compromise indicators acting as smoke detectors, providing provenance of data, proof of tampering arising from malware analysis, and external threat intelligence feeds. This includes data from IoT sensors communicating with each other.

The workflow integrates the whole process and connects the selected tools and people into an incident response when the SOC or equivalent identifies a critical event occurrence. Security analytics is then performed by applications using a combination of real-time and historical data to detect and diagnose threats. Sources of information include real-time alerts and feeds from the critical assets in the network. Particular attention is paid to network traffic volume, third-party threat intelligence feeds, and system logs. These logs can be a single point of failure if deleted or tampered with, so they are classified as essential crown jewel data. The diagram shows the tagging of a system log on

blockchain to obtain a provenance graph of actions and information regarding what actually happened from the log.



The security analytics process must comply with government and industry regulations. These can require monitoring and log data collection for auditing and forensics enforcing a single pane of glass for data events taking place providing proof of compliance and the ability to fix instances of noncompliance. The analytics make sense of the volumes of data flowing in and out of networks detecting potential threats. In combination with real-time intelligence and a historical record of past threats, this can protect critical infrastructure from or mitigate a data breach or cyberattack.

Cyberthreat Hunting

Cyberthreat hunting is a proactive security scan through networks and critical assets to hunt for malicious activities that have avoided detection by resident tools. Cyberthreat hunting adds an extra layer of protection over threat detection and should be used for critical infrastructure by default. Threat detection monitors critical assets for potential security issues and provides intelligence to the threat-hunting team, who then uses the data to identify and categorize potential threats. Once the risk plus frequency and severity have been determined, an investigation begins.

Baselining shows what an organization's clean slate network normally looks like, and threat hunters use that information for comparison purposes. Baselining for data integrity without using a blockchain hash is like looking for a needle in a haystack—how does one know what data is compromised in a big data lake? When crown jewel data is correctly tagged, the hunter has situational awareness of every piece of hay, which minimizes the time needed to combine baseline analysis with the benchmarking of bad actor behavioral techniques.

Technology: Blockchain, AI, and IoT

Every country should focus on strengthening its security and resilience of critical infrastructure and data against both physical threats and cyberthreats. Using a combination of blockchain, AI, and sensor technologies within a risk assessment framework is best practice. Critical infrastructure requires human intervention to detect and diagnose problems and then to make decisions and take action.

Systems are now increasingly digitized and connected through sensors, which require high reliability standards, hence the need for augmentation and technology co-workers created by AI. Cryptography-based blockchain systems remove single points of failure by distributing provenance of data over trusted, private networks or untrustworthy public networks. The integrity of the industrial control platform should be continuously monitored so that operators with access to management software can determine whether the system is true and correct against an approved configuration baseline. This can show absence of compromise, presence of malware in the software applications, and the configuration data responsible for operations.

Blockchain hash key technology built into an industrial blockchain signs all data across a system network, allowing independent verification of time, location, and authenticity for any moment in history. This evidence can be considered the single version of truth and stands up in a court of law.

There is no reliance on any single part, but confidentiality of the original data is retained, as the hash of data is stored on the blockchain instead of the data itself. This is highly scalable, as there is no blockchain mining or electricity abuse, and the amount of data signed can scale to billions of new data items each second, with the data item from the blockchain verified within the next second. The ability to transact data at subsecond speeds is essential to handling the increasing data requirements of a modern and smart-powered critical infrastructure.

One cybersecurity advantage is enabling a distributed escrow to maintain ordered, time-stamped data blocks that cannot be modified retroactively. This helps enhance trustworthiness and preserve data integrity where the data is transactional-related or system-to-system—challenges that currently threaten the security of critical infrastructure.

Because the hash does not store data, the data may be stored anywhere that enables cross-border integrity for supply chains. When it is attested by the system, the sender receives a signature from the data that shows its authenticity. Anyone with the original data and this signature can independently verify that the data was created authentically and claimed. The result is a system that establishes trust with only minimal infrastructure and no requirement for trust in any third-party entity.

By signing critical software functions, configuration files, and software, any counterfeit or malicious components may be quickly compared against known good states and validated in real-time without reliance on a trust anchor certificate, especially in automated and abstracted management environments such as IoT installations, smart ports, and factories. As a result, technology users strengthen their transaction system and detect vulnerabilities through rigorous test and evaluation capabilities, while observing the transactions and data, including all levels of testing, validating independently in real-time in coordination with governance policy rules providing log file integrity and change detection making the internet attributable.

AI-driven solutions use predictive analysis to detect and prevent many types of threats. By real-time monitoring of critical networks, AI can be used to detect vulnerable code in critical assets and block those containing malicious or exploitable code, while at the same time monitor devices for outdated software versions and misconfigurations. AI can quickly determine the safety of URLs, preventing users from unknowingly browsing unsafe locations, and can detect malicious apps before they are loaded or executed on a mobile device.

Because AI is an adaptive technology, it is well-suited to respond to both known threats and those that emerge during disruptions. Trust is essential to the use of AI, and a cybersecurity concern, which is why sensitive data needs to be grounded in cryptographic blockchains—to prevent AI algorithms

from falling into the wrong hands. When AI functions properly in critical infrastructure, it holds all the key data and could become the single point of failure and an attack surface, so data integrity is crucial.

Embedded blockchain, AI, and IoT have become seamless in everyday life. The AI in these embedded systems should provide a transparent, explainable outcome to the users as a result of machine learning and not hidden in a black box concept, and should be installed in devices at the original equipment manufacturer (OEM) stage.

Regulation

Twentieth century regulation still exists for 21st century technology, as regulations lag behind innovation. Until regulators become part of the ecosystem, key players must continue to innovate and protect in parallel while respecting existing regulations. A cyberattack will not wait for new regulations to be passed. Because critical infrastructure is public and privately owned, public-private partnerships are expected to mature.

Legislation regulating cyber-incident reporting requirements for critical operators—specifically regarding cloud-based services, telecommunications, and electronic communications; intelligent transport systems and autonomous vehicles; and space technology—is expected to escalate globally this year. The directives are expected to include more restrictive cybersecurity and risk management standards. Changes will affect encryption and supply chain security, and cyber incidents will be required to be reported within strict timelines.

New cybersecurity product certification measures for the private sector are also anticipated. Noncompliance could result in regulatory fines, which can lead to reputational risk. Security hardening of manufacturers is essential for small satellite development. Finally, more regulation is expected regarding tracking technologies for COVID immunization passports, which are necessary for critical infrastructure workers. Because of how quickly the tracking technologies were developed, they can be a target for threat actors.

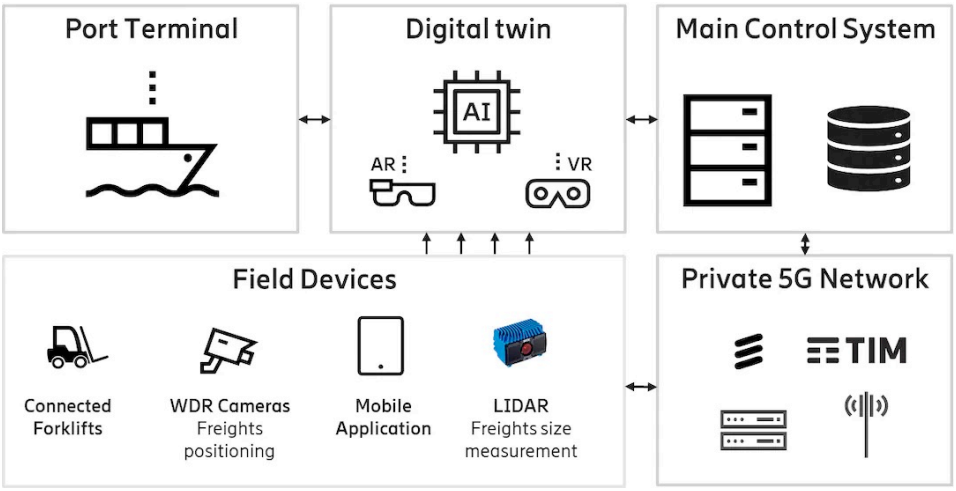
Many organizations around the world are expected to advance cyber regulation for critical infrastructure this year.[34,35]

Digital Twins

Digital twins are computer programs that use a digital copy of an organization to simulate potential behavior and scenarios, which can enable better management decisions. Digital twins require large amounts of data and information from the physical system to function. Providing them with real-world data ensures that, even in critical situations and with complex distribution systems, services will remain available. In the climate change space, energy consumption can also be reduced through more efficient asset operation and system planning. It is possible to unlock greater potential from critical infrastructure by sharing modeled data securely.

Digital twin models can help organizations gain greater insights into the effects of a cyberattack or an external disruption. In turn, organizations can better prepare for and make more informed decisions during such events. Digital twins can also help governments better understand the costs of maintaining and updating critical infrastructure by using sensors to collect data in real-time and then analyzing the datasets without human intervention.

The diagram shows a digital twin structure based on the Port of Livorno.[36]



First responders with access to digital twins can use augmented reality and virtual reality to provide immediate situation awareness for crises or incidents. By connecting digital twins, the attack surface is further expanded. This provides opportunities for cyberthreats and hackers, so it is important to ensure security and resilience to prevent a compromise deep within the supply chain, which could cascade through the chain and impact other purchasers.

Emerging Critical Assets: Small Satellites and Drones

Commercial drones can provide protection as part of the IoT software supply chain by performing inspections and accessing areas not suitable for humans. However, they come with new cyberattack risks.

One risk is the use of drones to fly over critical infrastructure, streaming AI data while looking for anomalies. Thousands of drones can fly at the same time, generating massive amount of data. For data integrity, data should be signed nearest the point of origin on the drone. The same applies to small satellites, which are the size of a bread basket and contain the latest smart technology in cameras, storage, and applications. The diagram shows how software code is verified on board the drone in real time to ensure that only valid code is executed.

Courtesy of Guardtime

Small satellites, which launch in increasing numbers every year, are experiencing commoditization and expansion, drawing parallels with the transition from mainframe computers to smaller cluster

computers. Small satellites fly in lower orbit in clusters at a fraction of the cost of older large satellites flying in deep space, which may be nearing the end of their life.

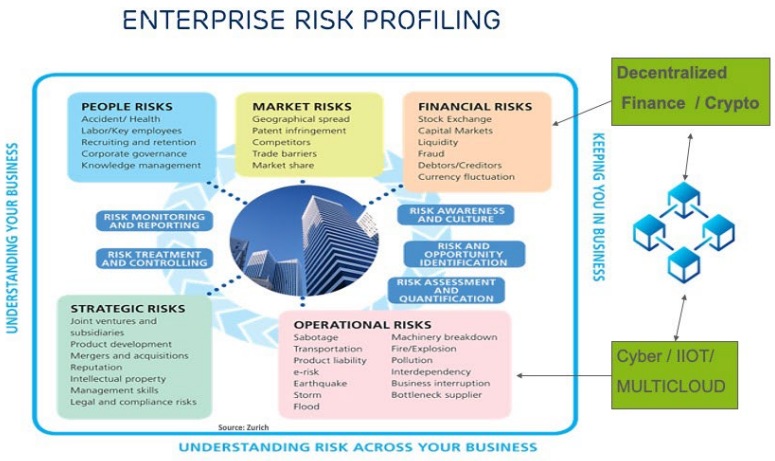
Small satellites are part of larger constellations. Any individual unit of a small satellite can fail without compromising the integrity of the whole constellation. The parallel between smaller satellites and smaller computers demonstrates the opportunity to bring them into the same integrated ecosystem.

The security industry already spends billions of dollars each year securing networks, computer clusters, and endpoints. If satellite constellations were normalized to behave more like traditional systems, then standard utilities become available not just for security, but also for basic operation.

Cyberthreats have kept pace with the growth in space technologies. Countries must protect current and future space assets, which are a source of data for weather and climate change.

Turning Cybersecurity Into a Strategic Advantage

C-suite leaders can turn investment in cybersecurity into profit center. The digital economy is highly competitive, and cybersecurity can be leveraged to enable new and measurable business value. Crown jewel data and digital assets must be protected, but cybersecurity should be embedded in the business strategy by design to avoid inhibiting innovation. Understanding the risk and enterprise profiling is critical to achieve risk estimation and modeling, especially as intangible assets dominate balance sheets.



Financial services professionals are seasoned in calculating risk, but not always in critical infrastructure industries. Some tend to see cybersecurity as a cost center and have stopped using part of the security budget to address data integrity. CISOs should be able to predict and track cyber risk in financial terms and work back from a worst-case scenario or black swan using a stochastic or mathematical model. This can demonstrate how cyber risk management contributes to the bottom line of the business.

Costs can be allocated to business units. Cyber then becomes a shared service provider with business integration dovetailing internal services with those delivered by external service providers, such as outsourcers and cloud service providers. These services then show up in each business unit's budget as a benefit or return on investment (ROI), recovering the cost of providing services through optimized pricing. This is important when addressing the issue of cost based on the level of risk and the financial (fines), reputational (stock market), customer retention, or service disruption effect of a breach on the business unit.

As the market develops a better sense of realistic cyber disaster scenarios, return periods, and the catastrophe layer structure and pricing the market needs to have in terms of frequency and severity,

then this will grow. Capacity providers need to understand those scenarios as well as the risk return profile of cyber risk and the loss scenarios.

The Future

Cybersecurity is addressing arguably the top global short- to medium-term risk, and where there is risk, there is opportunity. Innovation will rise from the ashes of conflict. After the Estonia cyberattacks, the country became a leading innovator. Technologies have evolved from a foundational cybersecurity base by design, into healthcare improvements, supply chain innovations, climate change initiatives, and new cryptocurrencies. When digital assets are secure by design, they concentrate on their purpose—giving financial returns to investors and functions to end users—without a retrofitting security concern.

Any attack on critical infrastructure is an attack on the sovereign state where it resides. The increase in digitization due to the COVID pandemic has multiplied vulnerability, especially in the transportation and logistics sector. As smart cities develop into smart nations, digital nations will emerge, bringing new continuity strategies, such as data embassies, to manage the ownership and protection of sovereign data. This is in the wake of increased cyber aggression and hybrid warfare, where advances in technology blur the lines of traditional military operations. Digital twins, which are used in the military and critical infrastructure, will become the foundation of the defense industry, and exponential technology to deliver productivity increases in all sectors by reuse.

Community-based technical developments are happening in parallel with the emergence of web 3.0 and the maturing of blockchain and AI technology, which will become embedded in the daily lives of corporations and people. Often called the metaverse, the virtual world has been developing for a generation, and cybersecurity needs to be embedded by design so that end users in the virtual world cannot trade security for new features around Global Positioning Systems (GPS), Quantum, and 5G. Critical infrastructure is no stranger to the metaverse, as digital twin technology has emerged as a vital component of hybrid activity between human and machine in the day-to-day operations using virtual reality and augmented reality.

Decentralized Finance (DeFi) is emerging as an alternate finance and money system based on leveraging cryptocurrencies and the blockchain infrastructure. This is a multitrillion-dollar industry in its infancy, and investors are looking at better returns.

Critical assets can use a stable coin as collateral in ILS, and collateralized reinsurance contracts as the issue of crypto volatility has been addressed.[37] The valuation associated with an ILS contract can be represented in a tradable digital asset with higher return without the physical ILS or reinsurance contract being digitalized, which would be a future development of trading in real time on the blockchain, producing more liquidity using parametric techniques.

Considering current geopolitical events, the blockchain highlights the DeFi theme of decoupling money and state so they are not correlated. The status quo is governments issue money, but now communities and some governments are going down the path where governments do not have to be the sole issuers of money. With an assumption that governments—not private citizens—cause wars, there is desire to noncorrelate and mitigate that effect by moving to a cryptocurrency decentralized approach in parallel with central bank digital currency.

As we discussed, there are vulnerabilities in the supply chain and transportation critical assets. If blockchain technology is used to tighten the processes in the chain, innovation will emerge in the way trade is done, there will be visibility upstream and downstream in the supply chain, and tokenization within the trades will incentivize better trades. For climate change, cybersecurity technology can be used to better balance the demand and supply of power based on predictive data, monitoring the detection and prevention of utility theft of water or power, plus the ability to predict power failures, predict water shortages, and to participate in the environmental, social, and governance (ESG) rating and scoring platforms emerging on climate change standards.

The integration of AI into critical systems is exponential, and the AI data needs to be made secure and transparent on the blockchain. AI-enabled critical systems are becoming feasible and accepted, as seen in semi-autonomous and autonomous transportation. Explainable AI will be key to understanding the data and how responsively critical systems behave. There have been several recent failures of autonomous vehicles and aviation that caused fatalities, which may indicate the consequences of not fielding a robust cyber-integrated hardware and software offering.

Digital twin technology can also be a major step forward for infrastructure protection. Public-private partnerships for cybersecurity will continue to be critical, as it is not possible to protect all critical assets without some kind of government backstop layer. Risk mitigation and response are stronger when collaborated across public-private ecosystems and converted into securitized assets.

It is misplaced to consider the data integrity of cybersecurity solely as a cost center, as once the data is valued and treated as an asset, a host of innovation opens up for better returns, new digital assets, and a more secure world.

The author would like to thank Ultimate Risk Solutions, Guardtime, and JLJ Martime for their contributions to this article. [38,39,40]

---

[1] https://en.wikipedia.org/wiki/Sputnik_1
[2] https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia
[3] https://en.wikipedia.org/wiki/Petya_and_NotPetya
[4] https://en.wikipedia.org/wiki/Cooperative_Cyber_Defence_Centre_of_Excellence
[5] https://en.wikipedia.org/wiki/Data_embassy
[6] https://en.wikipedia.org/wiki/Vienna_Convention_on_the_Law_of_Treaties
[7] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[8] https://www.wired.com/story/log4j-flaw-hacking-internet/
[9] https://openssf.org/
[10] https://www.lookout.com/glossary/what-is-zero-trust?utm_source=blog&utm_medium=web
[11] https://en.wikipedia.org/wiki/Fancy_Bear
[12] https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/
[13] https://www.bbc.com/news/technology-60250956
[14] https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack
[15] https://www.bbc.com/news/world-us-canada-55989843
[16] https://portswigger.net/daily-swig/taiwans-major-oil-refineries-struck-by-malware-causing-chaos-at-gas-stations
[17] https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R
[18] https://www.securityweek.com/israel-says-hackers-targeted-scada-systems-water-facilities
[19] https://www.bitdefender.com/blog/hotforsecurity/japanese-telecoms-giant-ntt-suffers-data-breach-takes-four-days-to-learn-of-intrusion
[20] https://www.reuters.com/article/us-health-coronavirus-moderna-cyber-excl-idUSKCN24V38M
[21] https://en.wikipedia.org/wiki/Triton_(malware)
[22] https://www.trendmicro.com/vinfo/de/security/news/cyber-attacks/israels-electric-authority-hack-caused-by-ransomware
[23] https://en.wikipedia.org/wiki/Ukraine_power_grid_hack
[24] https://www.usatoday.com/story/tech/news/2016/11/28/san-francisco-metro-hack-meant-free-rides-saturday/94545998/
[25] https://www.cnbc.com/2015/06/22/hack-attack-leaves-1400-passengers-of-polish-airline-lot-grounded.html
[26] https://www.industrialcybersecuritypulse.com/throwback-attack-a-cyberattack-causes-physical-damage-at-a-german-steel-mill/
[27] https://www.nbcnews.com/news/us-news/iranian-hackers-claim-cyber-attack-new-york-dam-n484611
[28] https://en.wikipedia.org/wiki/Stuxnet
[29] https://www.nist.gov/
[30] https://threatpost.com/merck-insurance-payout-notpetya-attack/177872/
[31] https://www.expert.ai/resource/how-cyber-insurance-has-evolved-in-2021/
[32] https://www.cybcube.com
[33] https://www.indexinsuranceforum.org/faq/what-basis-risk
[34] https://www.enisa.europa.eu/topics/nis-directive
[35] https://en.wikipedia.org/wiki/Cybersecurity_Law_of_the_People%27s_Republic_of_China
[36] https://www.ericsson.com/en/blog/2020/12/digital-twins-port-operations
[37] https://en.wikipedia.org/wiki/Stablecoin
[38] https://www.ultirisk.com/
[39] https://guardtime.com/

[40] https://www.jljmaritime.com/

5.2022

David Piesse
CEO, DP88

About the Author:
David Piesse is CEO of a family office, DP88, specialising in InsurTech initiatives in Asia - www,DP88.com.hk. David has held numerous positions in a 40-year career including Global Insurance Lead for SUN Microsystems, Asia Pacific Chairman for Unirisx, United Nations Risk Management Consultant, Canadian government roles and staring career in Lloyds of London and associated market. David is an Asia Pacific specialist having lived in Asia 30 years with educational background at the British Computer Society and the Chartered Insurance Institute.