

Cyber Risk & Supply Chains: The question is “Not if, but when?”

Cyber technology now connects almost every aspect of our lifestyle and business. Cyber-World continues to grow beyond our Real-World: there are now 16.8 billion mobile connections globally, more than double the world population of cir.8 billion, and email users now surpass 4.37 billion. Anything which has a chip is cyber-connected & thus exposed to the growing cyber-risk - from our hi-tech homes with Alexa/Siri, to CCTV, auto-home-locks, home appliances, online banking and even social media. The same applies to our business world which continues to be fully integrated with computers, cell phones, and chip-technology controlling or supporting functionality of all machines – manufacturing, processing, mobility, shipping and transportation, services, healthcare, banking, finance and almost anything you can imagine. Post Covid-19 pandemic, there is an increased drive by corporates and governments globally towards enabling remote work, increased digitization of operations and accelerated cloud adoption.



In the realm of advanced technology pioneers in the GCC, the Information & Communication Technology (ICT) industry takes the lead. By 2024, the UAE is projected to allocate an estimated US\$23 billion for ICT spending, with Qatar's spending expected to reach around US\$9 billion and Kuwait's spending predicted to hit US\$10 billion in that same year.



Supply-chains have become a necessity in our today's globally interconnected and interdependent world. No global supply chain is independent of maritime transport, and most, in fact, are existentially dependent on it. The sea and ports worldwide moved around 80% of global trade by volume and over 70% of global trade by value. The most common weak-link or vulnerable areas in the global supply-chains is now cyber-security which is growingly targeted by hackers causing severe disruptions. Mobile and Internet-of-Things (IoT) technologies along with the cloud are fast growing threat vectors

Recent cyber-attacks:

Cyber-attacks continue to impact almost every business and industry – from shipping & logistics, to manufacturing, banks and financial institutions, hotels, travel & tourism, aviation, consumer goods and social media industry. Cyber

risks have also compromised critical infrastructures such as hospitals, airports, ports, power & utilities, energy - oil & gas.

“Cyber-attacks are one of the top risks faced by Saudi Arabia's state oil giant Aramco, on a par with natural disasters and physical attacks”, the company's chief executive, Amin H. Nasser, said at an artificial intelligence summit in Riyadh in 2022. Recently, in November 2023, the world's largest oil company issued a warning that energy sector is vulnerable to cyber-attacks, particularly with the advent of new technologies, such as Generative Artificial Intelligence (AI). Amin H. Nasser, CEO of Saudi Aramco told the Global Cybersecurity Forum, that the energy sector is an attractive target and any large-scale disruption to the steady supply of energy would have an immediate and significant impact around the world. The warning resonates the 2012 monstrous malware cyberattack, Shamoon, on Saudi Aramco affecting 35,000 computers, followed in less than two weeks by the Qatari gas giant RasGas knocked offline by suspected state-sponsored cyber-attackers and Dec.2019 cyber-attack on BAPCO affecting 95% of computers (cir.2,000) and causing severe business disruptions for almost 2 weeks.

The onset of 2023 saw 16 car makers and their vehicles hacked via telematics, APIs and infrastructure. Impacted car models included Acura, BMW, Ferrari, Ford, Genesis, Honda, Hyundai, Infiniti, Jaguar, Kia, Land Rover, Mercedes-Benz, Nissan, Porsche, Rolls Royce, and Toyota.

The **Nagoya Port**, the largest in Japan in terms of cargo, is responsible for almost 10% of Japan's total trade volume and handles car exports for major automaker like Toyota. On early morning of 4 July 2023, Nagoya Port Authority confirmed that a glitch occurred in the computer system that manages container loading, unloading, and transport. By noon, operations were disrupted with the port being unable to load and unload containers from trailers. The shutdown at Nagoya port caused widespread delays in the supply of parts to Toyota plants across Japan. Domestic cars production was forced to halt for one day resulting in an estimated loss of 13,000 cars, translating to . The cyber-incident demonstrated the crippling effects on interconnected global supply chains.

On 10 November 2023 on the world's largest bank, **Industrial and Commercial Bank of China (ICBC)**, the U.S. broker-dealer, experienced a cyber-attack by LockBit that disrupted trading in the US\$ 25 trillion market for US Treasuries. The attack was so extensive that even the corporate email stopped working and forced employees to switch to Google mail. The blackout left the brokerage temporarily owing BNY Mellon, US\$ 9 billion, an amount many times larger than its net capital.

In another 2 days, on 12 November 2023, **DP World Australia**, part of DP World, the world's top port operator responsible for managing approximately 10% of global container traffic and 40% of Australian shipping, experienced a cyber-attack. The Australia cyber-attack affected 30,000 containers stuck at ports in Melbourne, Sydney, Brisbane & Fremantle, affecting services for a week or more.

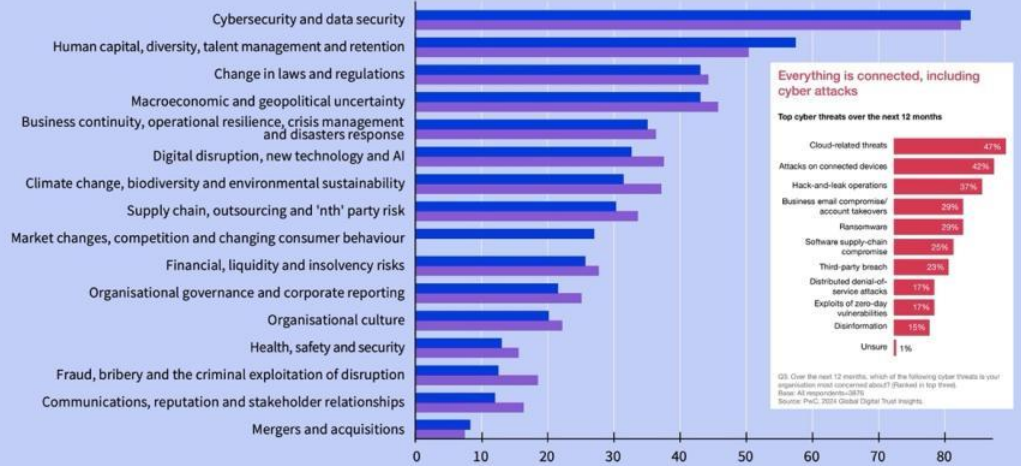
Since 2017, all 4 of the world's largest maritime shipping companies, viz. Maersk, COSCO, MSC, CMA-CGM, have been hit by cyber-attacks. Since 2020, there has been a 400% increase in maritime cyber-attacks and 900% increase in attacks targeting ships and port systems.

A recent business survey result of 700 Chief Internal Auditors across Europe reveal CYBER (cybersecurity and data security) as a TOP RISK faced by corporates worldwide. PwC's 2024 Global Trust Insights survey results also highlighted mitigating cyber risk as a top priority for 2024.

Businesses survey result of 700 Chief Internal Auditors across Europe reveal **CYBER as a TOP RISK** faced by Corporates worldwide & as per recent PwC Survey, mitigating Cyber Risk is ranked as top priority

What are the top five risks your organisation currently faces?

Business continuity and operational resilience moved up two places this year in response to continuing global turmoil with market changes coming in as a new category.



PwC's 2024 Global Trust Insights survey results also highlighted mitigating cyber risk as a top priority for 2024.

Can you imagine the speed & magnitude of cyber-attack disruption:

To understand the speed & magnitude of a cyber-attack, let's look at the biggest supply chain cyber incident, the NotPetya ransomware attack on MAERSK, which shook the global shipping industry. A.P. Moller-Maersk, is the world's largest shipping companies, hauling 20% of world's shipping containers, managing 76 ports and 800 vessels globally. A ship with 20,000 containers enters a port every 15 minutes.



Maersk suffered NotPetya cyber attack on 27 June 2017. In just about 7 minutes, 45,000 PCs, 4,000 servers and 2,500 applications across 600 offices in 130 countries were affected for 10 days requiring reinstallation of entire infrastructure. Maersk remarkably covered 80% of all shipping volume without any IT for 10 days ! In all, it took 200 Maersk personnel and 400 of their Deloitte contractor counterparts 10 days, working 24/7, to rebuild the Maersk network. A staggering US\$ 300,000,000 was the Business Interruption Loss estimate by Maersk for this cyber-incident.



MAERSK

Suffered NotPetya cyber attack on 27/6/2017

A.P. Møller-Maersk, the world's largest shipping companies

Hauls 20% of world's shipping container

Manages 76 Ports & 800 Vessels

A ship with 20,000 containers enters a port every 15 minutes

With 76 ports and 800 vessels the multinational's helplessness in the face of a total shutdown is a perfect example of the real-world disruption that NotPetya caused



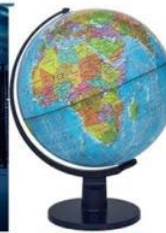
In just about 7 minutes



45,000 PCs Workstations,



4,000 servers & 2,500 applications (including routers, VoIP phones, physical access settings, and other infrastructure)



across 600 offices in 130 countries



were affected for 10 days requiring reinstallation of entire infrastructure

Maersk remarkably covered 80% of all shipping volume without any IT for 10 days. In all, it took 200 Maersk personnel and 400 of their Deloitte contractor counterparts 10 days, working 24/7, to rebuild the Maersk network. Months more were needed to bring about normal software functionality.

US\$ 300,000,000 was the **BUSINESS INTERRUPTION LOSS** estimate by MAERSK.

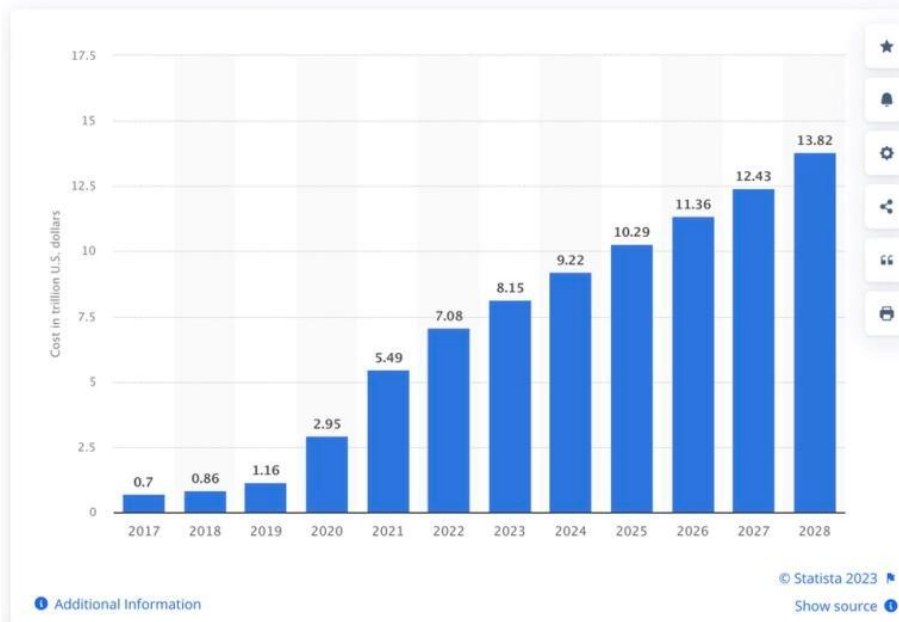
On average, a cyber-attack or data breach occurs every 39 seconds according to a study by Clark School at the University of Maryland. On average, companies take about 197 days to identify and 69 days to contain a breach according to IBM. This lengthy amount of time costs businesses millions of dollars. Companies that contain a breach in less than 30 days save more than \$1 million in comparison to those who take longer.

Cost of cyber-crime and data-breach

Estimated cost of cyber-crime world-wide is US\$ 8 trillion in 2023 and is poised to touch +US\$ 10 trillion by 2025 accordingly to Statista 2023 report. The costs of cybercrime not only include damage, destruction and theft of data and intellectual property, but also lost productivity, disruption and reputational damage, plus costs for forensic investigation and restoration of hacked assets.

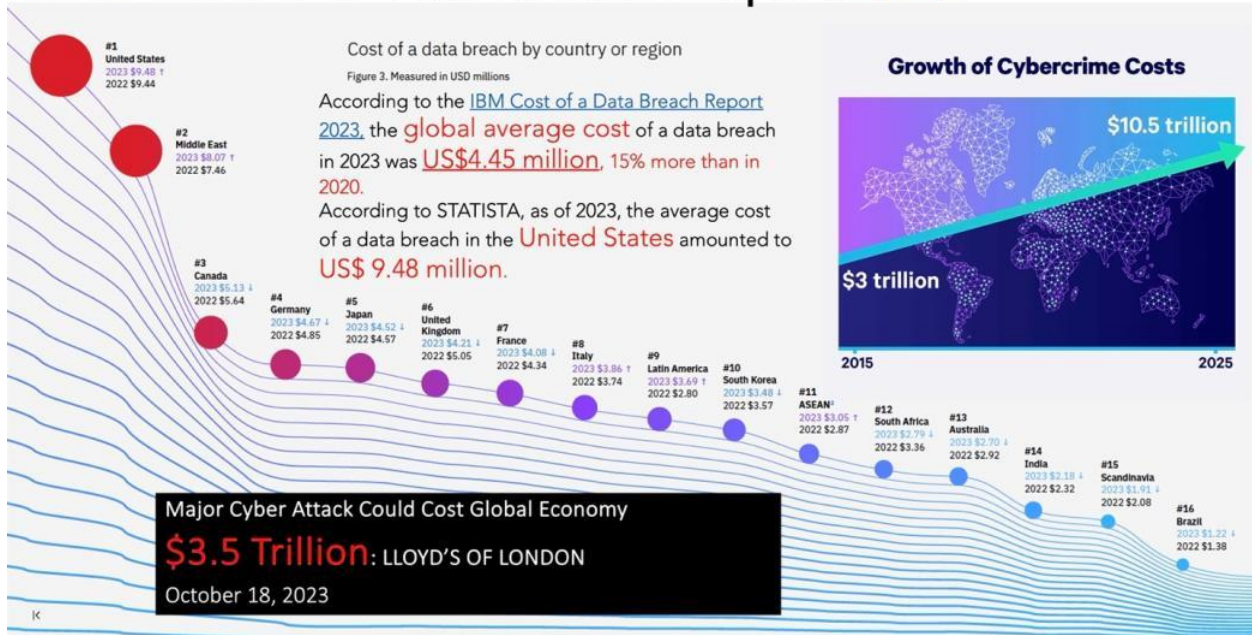
Estimated cost of cybercrime worldwide 2017-2028

(in trillion U.S. dollars)



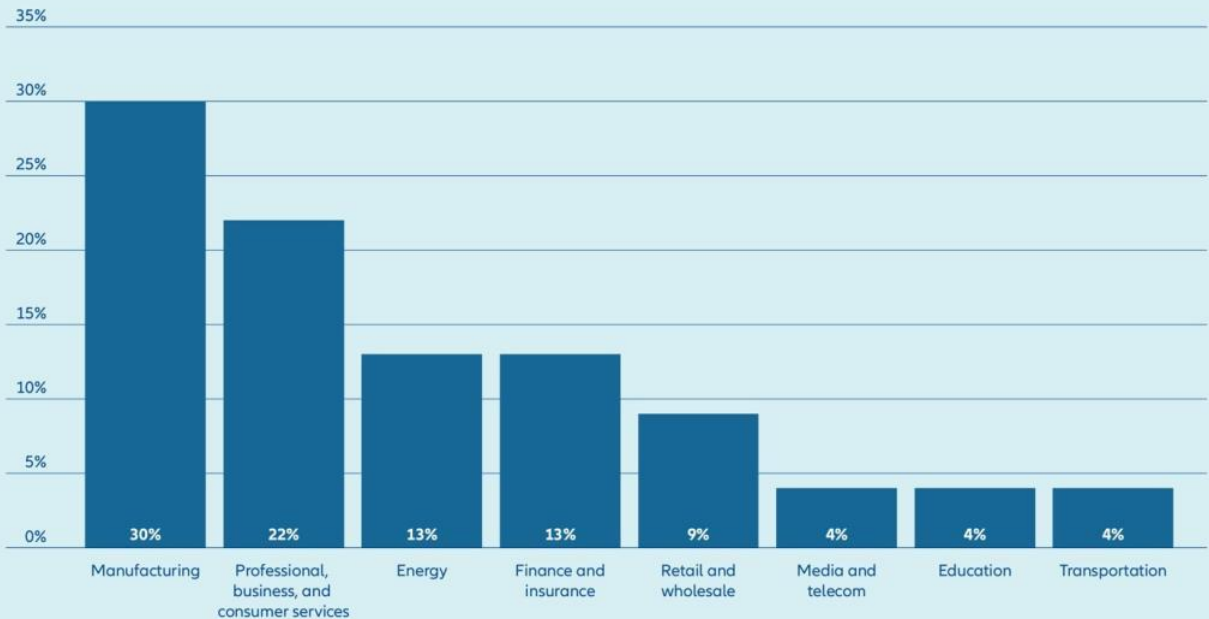
According to the IBM Cost of a Data Breach Report 2023, the global average cost of a data breach in 2023 was US\$ 4.45 Million, 15% more than in 2020. The United States topped with average data breach cost of US\$ 9.48 million in 2023, surprisingly trailed in the second place by the Middle East (specifically, GCC countries) with average cost of US\$ 8.07 million.

IBM Cost of a Data Breach Report 2023



Top industries targeted

The percentage of extortion cases by industry observed in incident response engagements in 2022.

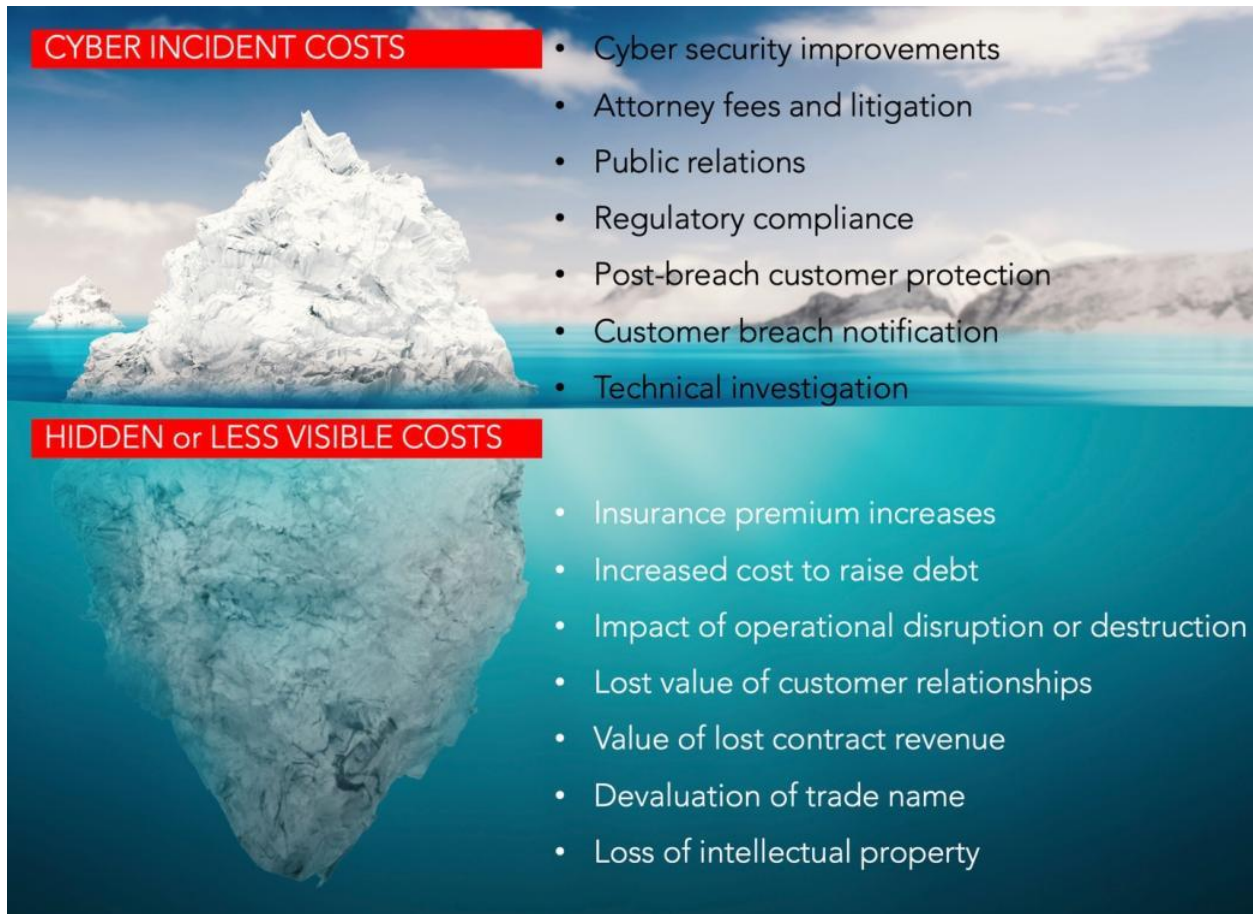


Numbers do not add up to 100% due to rounding.

Source: IBM Security's 2023 X-Force Threat Intelligence Index

Lloyd's of London, the world's oldest and largest reinsurance market has reported recently on October 2023 that a major cyber-attack could cost the global economy US\$ 3.5 trillion. According to ALLIANZ – Cyber security trends 2023 report, there is a 143% increase in the number of ransomware victims globally during the first quarter of 2023 and the approximate projected annual cost of ransomware by 2031 is US\$ 265 billion. Business interruption accounts for 50% of all cyber-related losses by value.

The impact of a cyber-attack is widespread across the organization resulting in a wide range of direct & intangible costs.



The image shows an iceberg floating in the ocean. The tip of the iceberg is above the water line, representing visible costs. The much larger part of the iceberg is submerged below the water line, representing hidden or less visible costs.

CYBER INCIDENT COSTS

- Cyber security improvements
- Attorney fees and litigation
- Public relations
- Regulatory compliance
- Post-breach customer protection
- Customer breach notification
- Technical investigation

HIDDEN or LESS VISIBLE COSTS

- Insurance premium increases
- Increased cost to raise debt
- Impact of operational disruption or destruction
- Lost value of customer relationships
- Value of lost contract revenue
- Devaluation of trade name
- Loss of intellectual property

Cyber Risk Management:

Cyber Risk Management



Cyber Risk is increasingly considered as ‘Critical’ or ‘Disruptive’ and Cyber Risk Management is a Board-Level responsibility, accountability and liability. The Securities and Exchange Commission’s (SEC) recently proposed rules in January 2023 cover most public companies, while the New York Department of Financial Services (NYDFS) proposed amendments target financial services firms registered in the New York state. Both, SEC & NYDFS, significantly expand compliance obligations and may create legal risks for corporate boards of directors. Regulatory framework continues to be updated and enhanced in UAE and GCC countries in line with progressive developments in global leading markets of US, UK & EU imposing greater responsibility for data security and holding the management board accountable for any lapses, including imposition of fines and penalties.

Cyber Risk Management involves prudential risk appreciation, identification, assessment, prevention and control, detection and mitigation, and financial loss and legal management including a robust Cyber Insurance protection.

Cyber Risk Insurance:

The cyber-threat environment continues to evolve, and as cyber risk management increasingly continues to become a top priority for corporates, the demand for Cyber Insurance has spurred phenomenally since the last few years. The global cyber insurance market tripled in volume in the last five years, expanding to gross direct premiums of around USD 13 billion in 2022, according to the Swiss Re Institute (SRI).

Cyber Risk Insurance provides a comprehensive financial protection for physical loss of or damage to Business Assets, any resultant Business Interruption Loss, and Business Liabilities claims as a result of any data-breach or any other cyber incident.

Cyber Risk Insurance Cover

<p>THIRD PARTY CLAIMS</p> <p>arising out of, or alleging financial loss as a result of,</p> <ul style="list-style-type: none"> a failure of the insured's network security or a failure to protect confidential information 	<p>INVESTIGATION & DEFENCE</p> <p>of regulatory actions arising out of</p> <ul style="list-style-type: none"> a failure of the insured's network security (or) a failure to protect confidential information. 	<p>FINES & PENALTIES</p> <p>of regulatory actions if allowable by law.</p>	<p>PCI-DSS Assessments</p> <p>(Payment Card Industry Data Security Standard) assessments for the failure to protect payment card data.</p>
<p>NOTIFICATION COSTS</p> <p>Costs of notifications, public relations & other services to manage & mitigate cyber incident</p>	<p>Legal Consulting & Monitoring Costs for victims of breach</p>	<p>FORENSIC INVESTIGATION COSTS</p> <p>due to a covered cyber event</p>	<p>Electronic Data Restoration Costs</p> <p>from duplicates or, if not possible, costs to research, gather and assemble electronic data due to a covered cyber event.</p>
<p>RANSOM PAYMENTS</p> <p>Reimbursement of ransom payments incurred in terminating a covered cyber event.</p>	<p>BUSINESS INCOME LOSS</p> <p>resulting from physical damage to property due to a covered cyber event</p>	<p>FIRST PARTY PROPERTY DAMAGE</p> <p>Loss associated with first party property damage due to a covered cyber event.</p>	<p>THIRD PARTY BODILY INJURY or PROPERTY DAMAGE</p> <p>Caused by a Security Failure or Privacy Event or breach of a computer system that is part of Insured's product</p>
<p>BREACH RESPONSE COSTS</p>	<p>FIRST PARTY</p>	<p>THIRD PARTY</p>	<p>eCRIME</p>

- Legal services
- Computer forensic services
- Notification services
- Call center services
- Credit monitoring, identity monitoring or other personal fraud or loss prevention solutions
- Public relations and crises management expenses

- Business interruption loss from security breach or system failure
- Dependent B.I. loss from security breach or system failure
- Cyber extortion loss
- Data recovery loss
- Data and network liability

- Third party information security & privacy coverage
- Full media liability
- Regulatory defense & penalties
- Payment card liability & costs

- Fraudulent instruction
- Funds transfer
- Telephone fraud
- Criminal reward coverage

Additionally, Cyber Insurers also provide value-added Risk Management Services which are immensely beneficial for corporates.

Cyber Insurance: Risk Management Services

Risk Management Portal	Employee Training	Vendor Discounts	Risk Management Webinars	Onboarding Video
Secure, out-of-band incident response preparation room	Onboarding call with Cyber Services	Incident Response Plan (IRP) review	M365 Cybersecurity Assessment	Ransomware & BEC best practices workshop
IT rationalization assessment	Crises Communication workshop	Crafting an IRP workshop	Phishing-resistant MFA keys	Simulated phishing campaigns
Board of Directors / C-Suite presentation on data security & training on cyber resiliency	Incident Response (IR) workshop with tabletop	Information Security Best Practices session	Business Continuity Planning (BCP) workshop	Ransomware Readiness Assessment

Cyber Risk Insurance, in current times is a very important financial and risk management protection tool which all Corporates (large & SMEs), including government and infrastructure entities, must consider to have to safeguard the business, operations, profitability and sustainability in the event of any disruptive cyber-attack.

Key consideration for Cyber Risk Insurance:

Cyber Insurance is evolving as the cyber-risk landscape keeps on shifting. While Cyber Risk ranks No.1 for corporates to manage, Cyber Insurance take-up is fractional. Global Cyber Insurance premium in 2022 is US\$ 9.2 billion, which is barely 0.14% of global insurance premium volumes of US\$ 6.78 trillion - a clear reflection of the gap between cyber risk-appreciation and insurance-protection. Since Cyber Insurance is still evolving, it is very important to negotiate with your Insurer a bespoke risk and financial protection which reflect your business exposures. Following are some of the key consideration while managing cyber risk and structuring a prudent cyber risk insurance program:

1. Cyber Risks are evolving and dynamic – thus risk appreciation & assessment has to be equally dynamic.
2. Cyber risk assessment must be holistic and involve all stakeholders – CIO, CRO, CFO, Risk & Insurance Head, Legal Counsel, External Panel Lawyer, CEO and the Board.
3. Review and update your Contract for 'Force Majeure' triggers to include Cyber Risks.
4. Choose your Cyber Insurance Partner with solid standing and Risk + Claims Management Services capabilities and ability to comprehensively service your local and global exposures.
5. Ensure to have an adequate insurance coverage limit based on external benchmarks and risk-specifics of your business operations to provide adequate financial protection in the event of any major cyber-attack.
6. Provide earmarked annual budget for Cyber Risk Insurance.
7. Annually review and update your cyber insurance protection to commensurate with evolving cyber risk landscape.



H.C. Barke

*CPCU(USA), AMIM(USA), AIC(USA), ARe(USA),
ACII(London), Chartered Insurer(London), AIRM(London),
FIII, AIII(General), AIII(Marine), B.Com (Finance), LLB
PGDM(Marketing), MIWWHS(USA), MCPCUS(USA),
Dipl. Da Vinci's Vitruvian Man (IBC – Cambridge)
Dipl. King's College (IBC – Cambridge), Dipl. Pi (IBC – Cambridge)
Certificate of Distinction (Insurance & Risk Management), IBC – Cambridge
'2000 Outstanding Intellectuals of 21st Century' – IBC, Cambridge
HARVARD Business School - Disruptive Strategy
WHARTON Entrepreneurship Acceleration Program –Scaling Your Business*

***President & Roundtable Lead - Supply Chain Finance,
Supply Chain Logistics Group (SCLG)***

***President & Chief Executive Officer
Prudence Insurance Brokers LLC – US . UK . UAE
(Broker at LLOYD's)***

Barke Capital LLC, U.S.

IRM Academy, U.S.

13 December 2023