Deloitte.

GiDMC
GLOBAL INCLUSIVE DISASTER MANAGEMENT CONFERENCE

Cyber resilience

Building future-ready organisations

For private circulation only

Contents

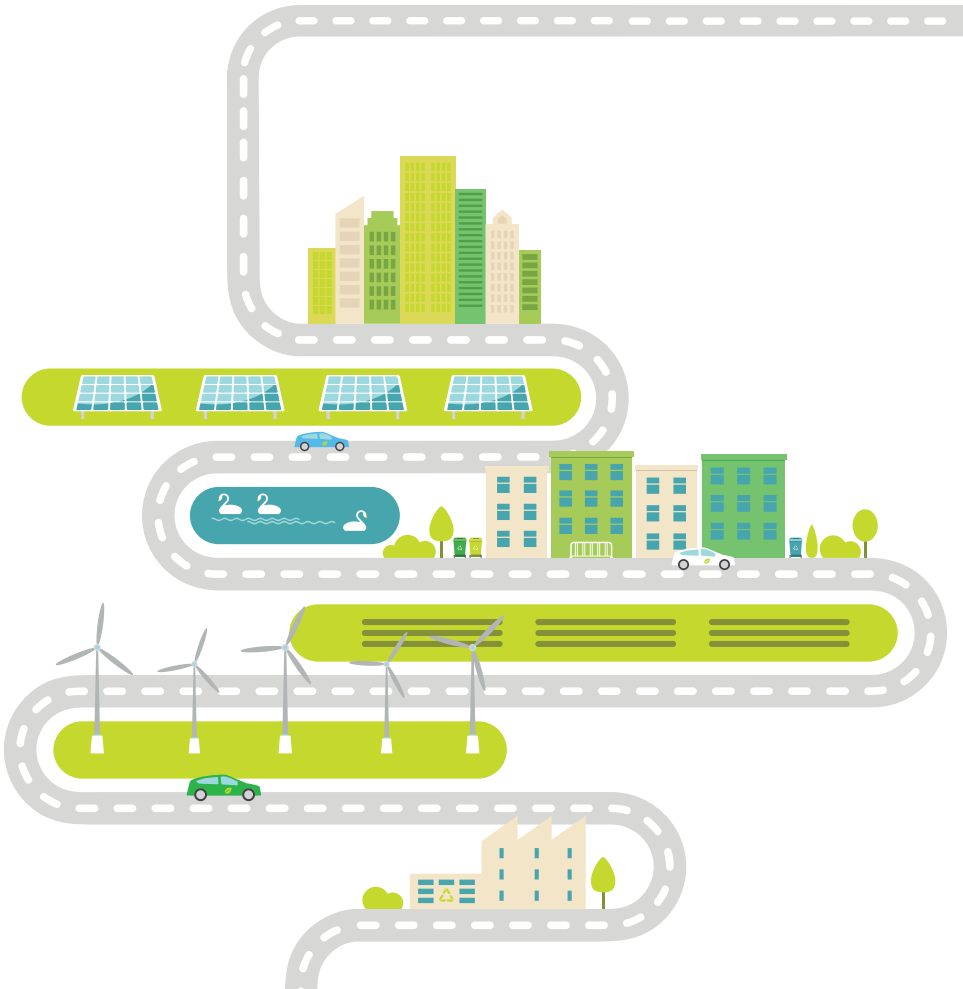
Abstract

In the recent past, the cyber landscape witnessed a shift from petty online crimes to election meddling carried out by state-sponsored actors, large-scale ransomware attacks (that have brought many organisations on the brink of collapse), and cyber espionage campaigns (targeted to extract information about competitive advantage that many large multinationals have).

Although data protection has always been the primary focus of cyber defenders, current cyberattacks have the ability to immobilise business operations. Cyber criminals have been increasingly targeting national critical infrastructure, including power grids and hospitals that often put people's lives on the line. They have also demonstrated their capabilities by ambushing highly secure and resilient infrastructure, and causing brief disruptions to time-sensitive services, including telecom and stock exchange.

For businesses modeled around providing uninterrupted services to customers, such interruptions drain their revenue with every passing minute of the outage and put their long-term viability in jeopardy. Even smaller disruptions, which are carried out with high persistency, can result in organisations spending significant efforts towards incident response and diverting their focus from their core business objectives. Hence, the underlining infrastructure, at the physical and logical levels, must be functionally present to ensure that businesses can continue to run at an optimum level. This is referred to as the principle of availability.

The paper explores why this principle is increasingly gaining prominence over the traditional cyber security approach (focusing solely on data protection). It also examines the threat landscape and the impact that the disruptions will cause. The paper talks about how businesses and governments should treat cyber resilience as a matter of priority concern. To conclude, the paper lays emphasis on the response and recovery strategies, including a focus on human dependency, which cyber defenders should consider in their playbooks.



The relevance of resilience in the current cyber landscape

The commercial adoption of technologies such as artificial intelligence (AI), machine learning (ML), big data, and cloud computing, along with the proliferation of affordable broadband and smartphones, has spawned several data-driven start-ups and unicorns. With such a change in the market scenario and businesses ushering in the era of a data-driven economy, the future will see abundant opportunities of growth.

Consumers willingly share their personal data with digital start-ups in exchange for innovative services that provide convenience at highly discounted rates or, often, at no cost. The digital revolution has also made services interdependent. For example, to book a cab, one might have to depend on the availability of a digital wallet. This interdependence has the potential to cause a cascading disruption. It can disrupt the entire supply chain if one or more services in the chain are disrupted. In this light, services such as digital payments, ride-hailing, and same-day delivery have become an intrinsic part of everyday life. These have also replaced or significantly reduced traditional operational models, increasing the likelihood of disruptions due to the unavailability of services.

Although consumers pay little attention to data privacy or security policies, they expect high availability from service providers. Frequent service outages or prolonged downtime can make a consumer shift to a competing service provider. Monopolistic industries, where the digital players have significantly disrupted the industry dynamics, have the potential to affect a large population.

Amazon Web Services (AWS) has a share of near 50% in the cloud services market; prominent businesses, such as Netflix and WeWork, depend on AWS's cloud infrastructure to conduct their operations. AWS was affected by a manual error that brought down services for some of its key customers.[1]

Google Cloud, a prominent competitor to AWS, also experienced the impact of high levels of network congestion, affecting its popular services, such as Gmail and YouTube.[2]

In the current fiercely competitive digital economy, ensuring continued consumer loyalty highly depends on the service provider's ability to attend to each and every service request, every single time. With competitors waiting to capture the market leader's customer share, businesses should think of resilience as a built-in design principle, opposed to a bolt-on design principle.

Government and civic authorities are also on the path of digital transformation, investing significantly in smart city projects and e-governance initiatives. Key public-private partnerships have enabled the deployment of AI and ML based analytical models and big data to enhance services, including traffic management, law-enforcement, and waste management. Smart city projects have led to the rapid research in the technology space, and the development of IoT devices and management platforms.

[1] https://www.geekwire.com/2018/state-cloud-amazon-web-services-bigger-four-major-competitors-combined/
[2] https://status.cloud.google.com/incident/compute/19003

Investments in 99 cities by sector

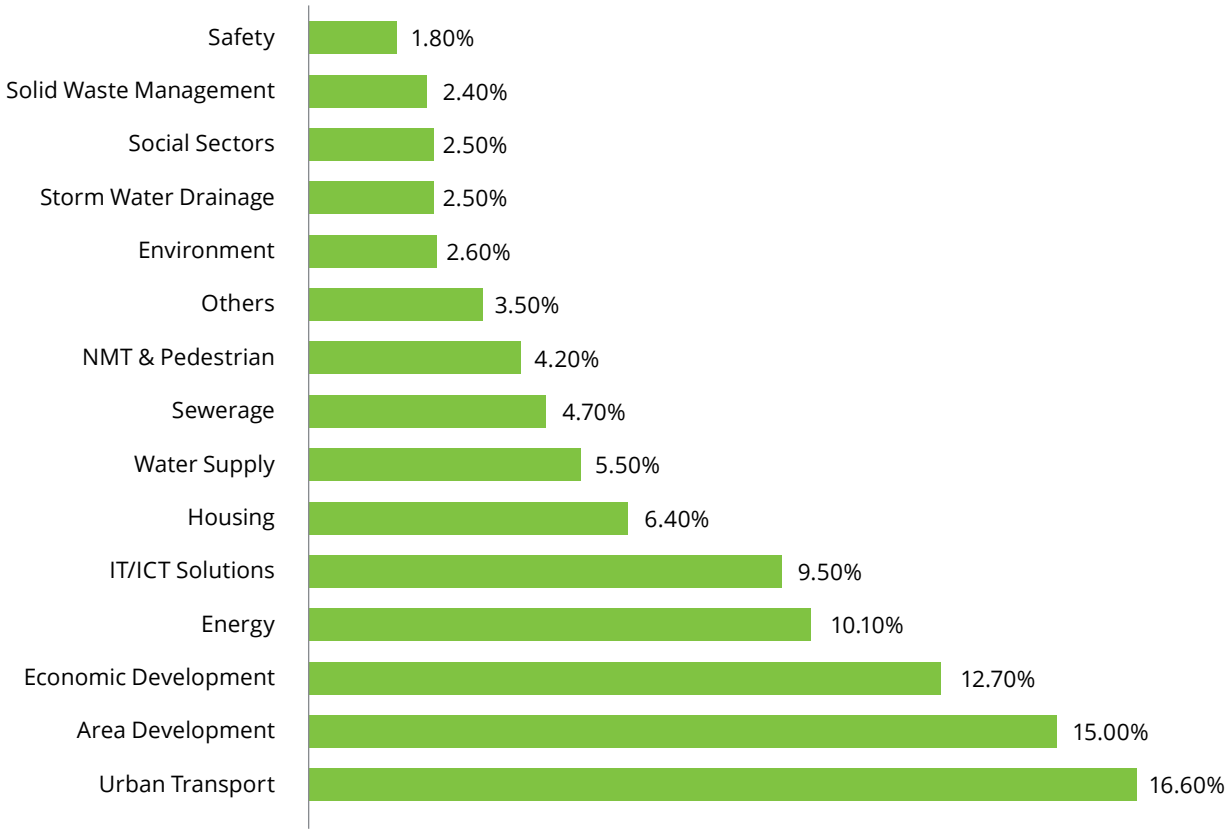


Figure 1. In the data, collated by the Ministry of Housing and Urban Affairs in 2018, we can see that IT/ICT solutions are one of the top five focal points in terms of investments made by the government[3]

Though smart cities and smart critical infrastructure promise a better future for citizens, cyber criminals and state-sponsored actors view this as an opportunity to cause wide-scale disruptions and, possibly, weaponise it against its adversaries.

In October 2016, the Mirai botnet, comprising about 100,000 IoT devices, took down numerous popular websites (Twitter, GitHub, Amazon, etc.) in a massive DDoS attack (1.2 TBPS) against the DNS provider Dyn.[4]

Digital organisations, when juxtaposed against traditional organisations, have to guard their physical space and protect their cyber footprint. Threat vectors, such as Distributed Denial of Service (DDoS) and ransomware, pose a serious risk to the mission of "keeping the lights on". The mission's objective is to keep the operations running with smooth and uninterrupted functionality.

[3] https://www2.deloitte.com/content/dam/Deloitte/in/Documents/public-sector/in-gps-CII-SmartCity_SustainableSmartCities.pdf
[4] https://www2.deloitte.com/content/dam/Deloitte/de/Documents/technology-media-telecommunications/TMT-Cyber-Security-Blockchain-March-2017-en-final.pdf

Attack vectors changing the cyber space

DDoS

What is it?
DDoS is a cyberattack aimed at making a computer or a network resource unavailable to its users

How does it work?
The attacker gains control of a large number of infected machines (bot). The BOT network is used to overwhelm the target resource by sending a lot of requests and ultimately bringing it down.

Ransomware

What is it?
Ransomware attack affects the target computer with a malicious programme encrypting files and restricting access.

How does it work?
The malware is delivered to the target computer by exploiting known system and human vulnerabilities. Once infected, the system's access is denied and can be returned only by paying the ransom using bitcoins. Attackers exploit enterprise vulnerabilities to ensure propagation without detection.

To understand the resilience risk landscape, one must understand the intentions of adversaries. Motives behind a cyberattack are no longer limited to financial gains. They have evolved to cause serious strategic disadvantages to businesses and governments. As availability increasingly becomes a key differentiator to a business' success, attackers often try to hamper operations using sophisticated DDoS and ransomware attacks.

Ransomware and DDoS attacks are at the forefront of the resilience risk landscape. These attacks are made possible due to a lack of security hygiene concerning the known vulnerabilities. Ineffective patch management practices, poorly implemented access management solutions, and inadequate data back-up and restoration schedules are some of the vulnerabilities often exploited by adversaries to cause large-scale disruptions.

Moreover, people often prove to be one of the weakest links in the chain. They are exploited using targeted social engineering attacks and spear-phishing campaigns. Some adversaries go to the extent of blackmailing employees based on the personal information gathered. At times, they resort to corporate espionage by implanting a rogue employee in the targeted organisation.

Cyber disruptions cause varied effects, ranging from short-term operational downtimes to long-term brand and reputational damage. Ill-prepared organisations suffer significant financial losses, resulting from loss of revenues, recovery and restoration expenses, and erosion of market value. Even after a complete recovery and resumption to the business as usual status, the affected entity would incur expenses resulting from regulatory fines, forensics investigations, legal fees towards customer lawsuits, and rebranding campaigns.

Regulators are also increasingly becoming stringent to maintain cyber security and resilience, and enforcing regulations on critical industries. They conduct periodic audits to assess the entity's preparedness and, in extreme cases, impose fines for non-compliance. Regulators set forth strict incident reporting requirements that mandate an entity to report a breach within a stipulated time. If the entity fails to do so, regulators may impose fines.

Under GDPR, serious non-compliance could result in fines of up to 4% of annual global turnover, or €20 million – whichever is higher.[5]

[5] https://www2.deloitte.com/nl/nl/pages/risk/solutions/general-data-protection-regulation-gdpr-vision-approach.html

Further, news of disruption proliferates quickly on social media, causing anxiety, knee-jerk reactions, and damage to organisations' reputation. The affected organisations often get a limited time to salvage the situation. Negative publicity in the social media, coupled with fake news, has often deteriorated customers' and shareholders' confidence, leading to the significant erosion of the affected organistions' market share.

Thus, cyber resilience risks have to be understood to build robust and future-proof defence mechanisms. Crisis manifests by exposing multiple risks at the same time and hence, a holistic approach is important to effectively prepare, respond, and recover from cyber disruptions.

Preparing for the turbulent future of cyber resilience risks

While the traditional cyber defence mechanisms help in thwarting conventional attacks, attacks of the future will need an all-encompassing strategy. The following design principles aim to provide organisations with a view on possible amalgamations of traditional and futuristic resilience risk mitigation strategies.

Data back-up and restoration set resilience hygiene

Back-up has been an age-old proven method to ensure recovery in case the primary copy of the data is corrupted or wiped out as a result of a cyberattack. A pre-defined back-up schedule and a strategy indicating what to back-up, when to back-up, and on which medium to back-up, prove to be a highly effective recovery strategy. The data back-up strategy should mandate periodic restoration checks to ascertain data quality, integrity, and usability.

Complementing IT-DR with "Golden Data Copy"

Recent ransomware attacks have exposed an intrinsic vulnerability in IT-DR whereby the ransomware infection has inadvertently infected the data and application instances replicated in the DR, thereby rendering it useless. Golden Data Copy is a clean back-up copy created, in addition to the data replicated at the DR, and is maintained in an air-gapped environment. Although Golden Data Copy does not have the same Recovery Point Objective (RPO) as the copy at the IT-DR, it ensures clean recovery after a ransomware attack with minimum data loss.

Integrating chaos engineering into the vulnerability testing programme

Traditional vulnerability programmes are limited to the defined periodicity, scope, and application boundaries. Chaos engineering performs ongoing resilience testing by orchestrating unexpected failures and assessing the system's ability to recover from the outage using designed controls. The chaos engineering principle enforces the need to consider resilience as a key principle in the design process and provides assurance about the system's capability to withstand faults.

Senior management crisis simulation workshops

The success of crisis management highly depends on the senior management's ability and preparedness to respond to a crisis. While the security function is recovering from the cyber outage, communicating effectively with customers, regulators, and key stakeholders is important. A well-documented and rehearsed crisis management plan guides the leadership on retaining customer confidence and providing assurances to regulators and shareholders. Through regular simulation exercises, the senior management is put through various potential threat scenarios, to help them understan real-life scenarios. The exercise also helps in defining the threat landscape.

Skilled responders and cyber-aware organisation

Trained, skilled, and experienced responders determine an organisation's capability to thwart sophisticated cyberattacks, originating from highly motivated and well-funded cyber criminals. Through investments towards skill enhancement and threat research programmes, a capable defence can be built to support the response and recovery effort. Moreover, cyber security awareness programmes, guided by visual e-iteration tools (such as emails, posters, and screen savers), could be used to make employees aware about cyber resilience risks and their potential repercussions.

Covering your cyber risks through insurance

Cyber insurance has gained popularity as a cyber-risk mitigation measure. The insurance covers the losses an organisation incurs as a result of a cyberattack. Although insurance is a lucrative option to cover cyber risks, businesses need to consider the fact that the insurance premium is directly proportional to their cyber security preparedness. Hence, it should not be treated as a risk transfer mechanism. Organisations considering cyber insurance needs to practise due care and due diligence, regardless of the insurance coverage. They should be aware about protocols pertaining to forensics and evidence management after a cyberattack for the claim to be honoured.

Netflix uses chaos engineering to randomly choose a server and disable it during its usual hours of activity. It has built redundancy and process automation to survive such incidents, without affecting the millions of Netflix users.[6]

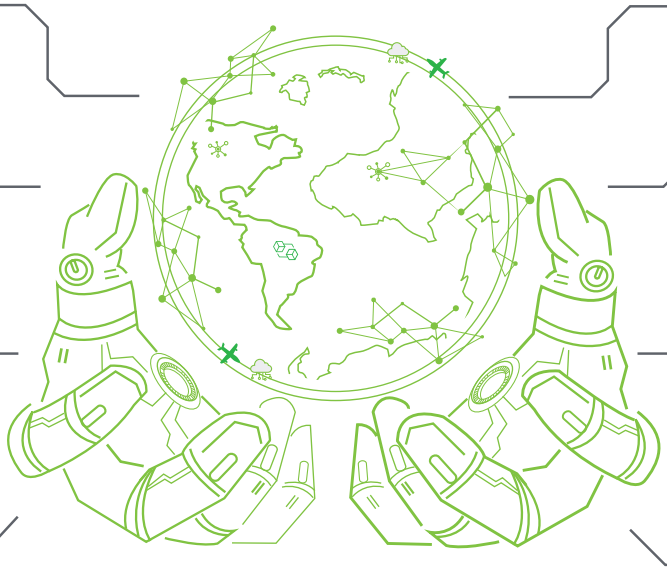
Other risk mitigation strategies also include:

Developing a threat hunting programme supported by a reliable threat intelligence provider

Getting DDoS protection from internet service providers

Creating a capable security operations centre (SOC)

Establishing a dedicated cyber security and resilience team



Choosing a reliable and reputed cloud service provider

Seeking security audit reports and demarcating security responsibilities

Assessing periodically resilience and security capabilities of critical third parties and vendors

Identifying and complying with legal, regulatory, and contractual obligations concerning cyber security and resilience

[6] https://publications.computer.org/computer-magazine/2018/11/15/netlfix-chaos-engineering/

Conclusive remarks

Cyber will continue to further blur the geographical boundaries and transform organisations and governments so that they make efforts to remain relevant in the digital world. A risk-aware culture is highly essential in building strong defences. Resilience will further get entrenched and become a non-negotiable integer for the continued success of enterprises. As cyber professionals, the need of the hour is to innovate, improve, and transform the existing defence strategies to protect organisations and critical infrastructure from attacks aimed at preventing organisations' from achieving their business objectives.

Finally, organisations must look at the future with a lens of proactive cyber risk response management, instead of a reactive response strategy.

Contacts

Rohit Mahajan
President–Risk Advisory
rmahajan@deloitte.com

Gaurav Shukla
Partner
shuklagaurav@deloitte.com

Vishal Jain
Partner
jainvishal@deloitte.com

Acknowledgements

George Ittyerah

Manoj Ajgaonkar

Rati Acharya

Salvi Sonal Sahay

Kalyani Deore

Shalaka Kaprekar

Deloitte.