

# Cyber Incident Response

Addressing Challenges and  
Strengthening Resilience

**A DSCI-CISCO POV Paper**

September 2023





# Contents

<b>Executive Summary</b>	<b>4</b>
<b>1 Background</b>	<b>6</b>
<b>2 The Impact of Geopolitics in Cyberspace</b>	<b>10</b>
<b>3 India Cyber Threat Landscape</b>	<b>12</b>
<b>4 Cybersecurity Regulations</b>	<b>16</b>
<b>5 Expectations and Obligations from Organizations in Digitalization Context</b>	<b>20</b>
<b>6 Towards Efficient Incident Response: Cyber Defense in Depth Strategy</b>	<b>24</b>
<b>7 Devising a Cyber Incident Response Strategy for your Organization</b>	<b>28</b>
<b>8 Supplementing Organizational Incident Response</b>	<b>36</b>
<b>9 Achieving Regulatory Compliance: Recommendations for Organizations</b>	<b>38</b>
<b>10 Solutions Enabling End-To-End Security to Enterprises</b>	<b>40</b>
<b>11 Conclusion</b>	<b>48</b>
<b>12 Encapsulate</b>	<b>50</b>
<b>13 Annexure</b>	<b>52</b>
<b>14 References</b>	<b>63</b>

# Executive Summary



The current cybersecurity landscape poses significant challenges that fetters the effectiveness of cyber incident reporting. There is underreporting of incidents, inconsistent reporting standards, limited information sharing, complex regulatory requirements, geopolitical volatility. Alongside, rapidly evolving threat landscape impede accurate threat assessment, information sharing, and collaborative response to cyber incidents.

In light of these challenges, the point of view paper addresses the intricacies of the evolving cyber landscape, explores the impact of geopolitics on cyberspace, and examines the vulnerabilities and challenges specific to the Indian cyberspace.

The paper outlines the phases of incident response and provides recommendations for organizations to devise a comprehensive cyber incident response strategy. It ingeminates the challenges faced by IT security teams in managing the multitude of cybersecurity technologies. The complexity of multiple security products from different vendors and the overwhelming number of alerts generated pose significant difficulties for organizations, it is further exacerbated by the scarcity of cybersecurity skills. This fragmented approach leads to silos in security data and gaps in threat detection and response.

## The paper highlights the expectations and obligations for organizations in the context of digitalization, with a focus on the responsibilities of Chief Information Security Officers (CISOs).

---

By acknowledging and addressing these complexities, organizations can better navigate the cybersecurity landscape, enhance incident reporting practices, and develop strategies to mitigate cyber threats more effectively.

Endpoint security is not the culmination; rather, it is a crucial element of a more comprehensive, unified security strategy. When endpoint security functions are in tandem with the other components of the security stack, it increases a security program's overall effectiveness and efficiency while giving modern, complex attack efforts greater visibility. Threat detection and remediation technologies such as Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), etc are the bedrock elements to strengthen and materialize end-point security objectives. The paper explores solutions that enable end-to-end security for enterprises, with a specific focus on XDR as one of the approach.

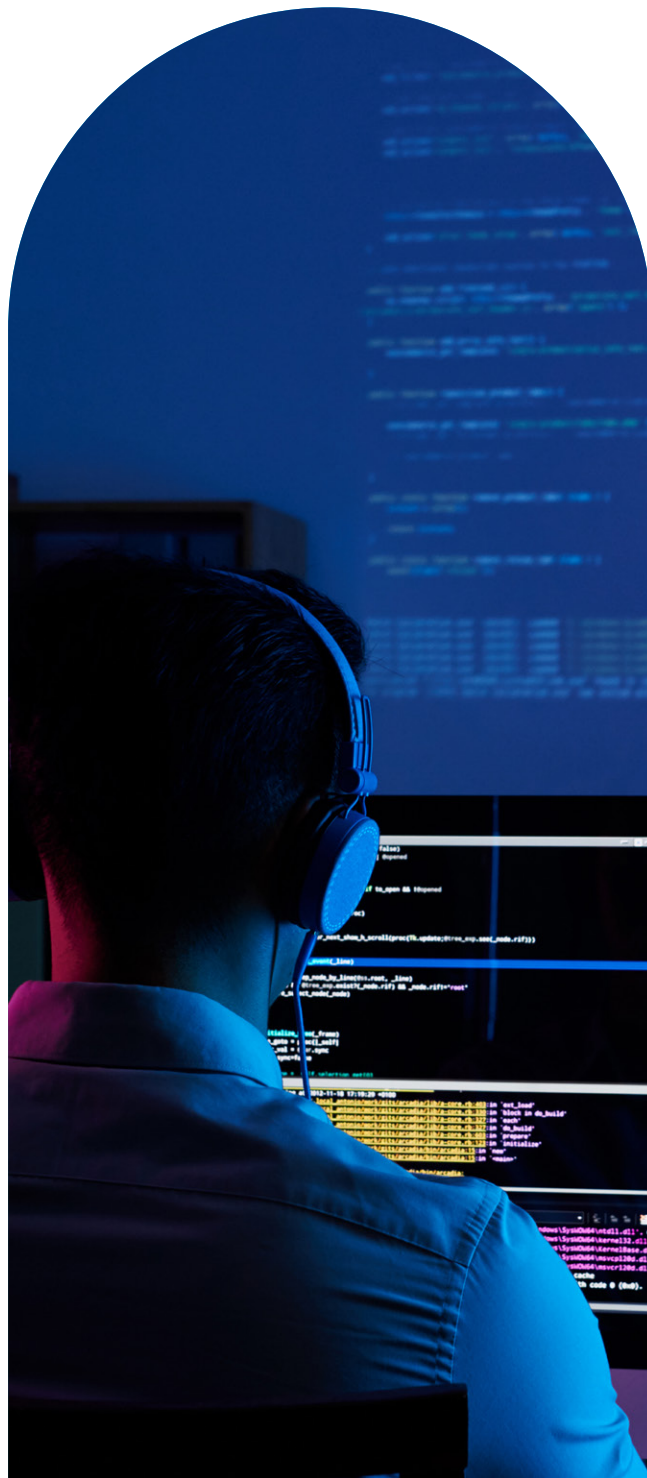
The paper concludes by emphasizing the need for organizations to prioritize cybersecurity, implement effective defense strategies, and comply with regulations to protect their data and infrastructure. By adopting proactive measures and

leveraging advanced security solutions like XDR, organizations can enhance their security posture, ensure adherence to the regulatory requirements and foster a culture of cyber resiliency.



1

# Background



**43%** cyber attacks are targeting MSME.<sup>1</sup>

**83%** MSME are not equipped to recover from a cyber attack.<sup>2</sup>

**35%** cost of a data breach can be saved with a robust incident response.<sup>3</sup>

**83%** of organizations have more than 1 breach in a year.<sup>4</sup>

**45%** of data breaches are cloud based.<sup>5</sup>

**31%** decline in the brand value due to a data breach.<sup>6</sup>

**\$1.75 million**

average business lost due to a cyber incident.<sup>7</sup>

**100-200 days**  
spent on detecting a breach.<sup>8</sup>

Figure 1: Global cyber threat landscape



A total of 11,58,208 cyber events were reported by Computer Emergency Response Team (CERT-In) 2020, more than three times as many as in 2019. In 2021, this uptick persisted with 14,02,809 incidences

Cybersecurity is becoming challenging in the ever-evolving modern Information and Communication Technologies (ICT) driven world. Migration to the cloud has given organizations new capabilities and opportunities for digitalization. However, the risks associated with these technologies have increased exponentially, jeopardizing the organization's safety in cyberspace.

Cyberattacks are expected to grow as technologies become increasingly ingrained in the world economy and infrastructure. Global cyberattacks grew by 38% in 2022 compared to 2021, with India experiencing 13.9 lakh cyber incidents in 2022<sup>9</sup>. The average cost of a data breach globally increased to \$4.35 million in 2022 from \$4.24 million the year before<sup>10</sup>. India has witnessed a 6.6% increase in the cost of a data breach in the year 2022 with a single incident costing organization 17.5 crore<sup>11</sup>.

Increasing data breaches can be attributed to the lack of 3.4 million competent cybersecurity professionals<sup>12</sup>. India needs 1 million Cybersecurity professionals to bridge the existing gap between the advancements in the hyper-digital society and the trembling cyberspace<sup>13</sup>.

The lack of skilled professionals, coupled with an exponential increase in data breaches, has left organizations vulnerable to attacks and breaches. A total of 11,58,208 cyber events were reported

by Computer Emergency Response Team (CERT-In) 2020, more than three times as many as in 2019. In 2021, this uptick persisted with 14,02,809 incidences<sup>14</sup>. Given the significant amount of friction between people, processes, and technology, the security efficacy is stagnating, and the average dwell time is still around 280 days<sup>15</sup>. Businesses are grappling with monetary losses, damaged intellectual property, compromised customer information, and decreasing valuations.

Investigation – Detection, Containment, Eradication, Recovery	Obvious Costs
Breach notification	
Geography specific compliance	
Ad-hoc litigation costs	
Cybersecurity process improvements	
Increase in cost of premium	Hidden Costs
Productivity loss	
Loss of customer relationships	
Loss of intellectual property	
Reputational damage	

Figure 2: Dissecting the \$4.35 million loss due to a cyber incident.

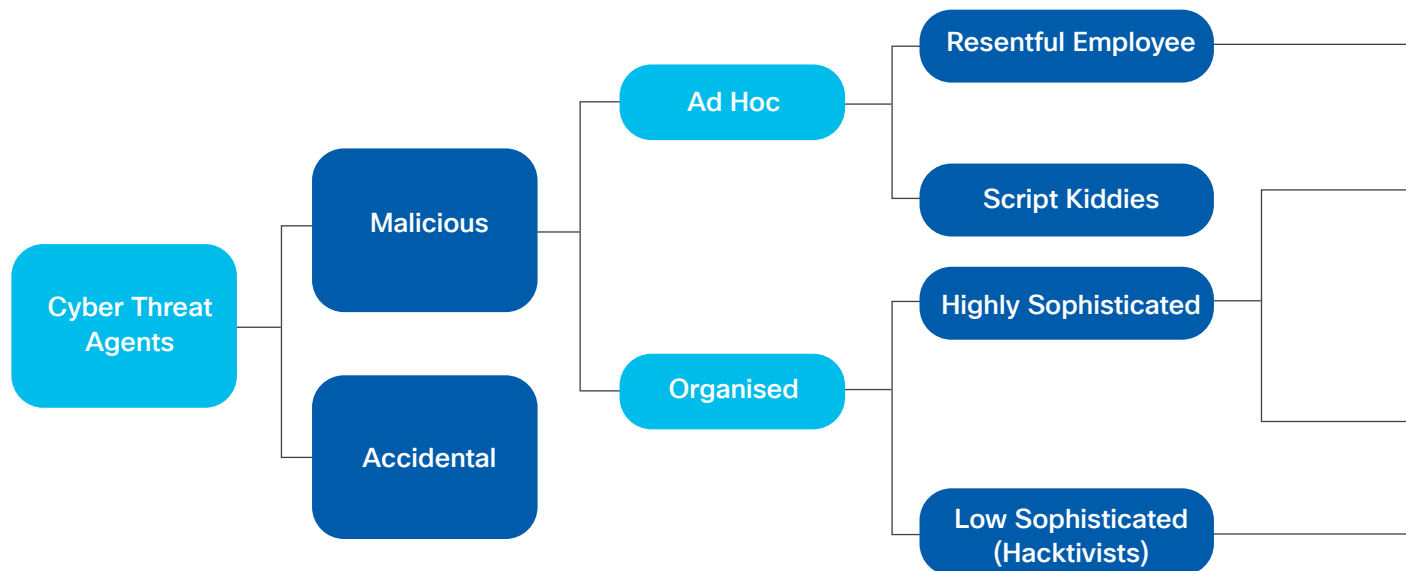
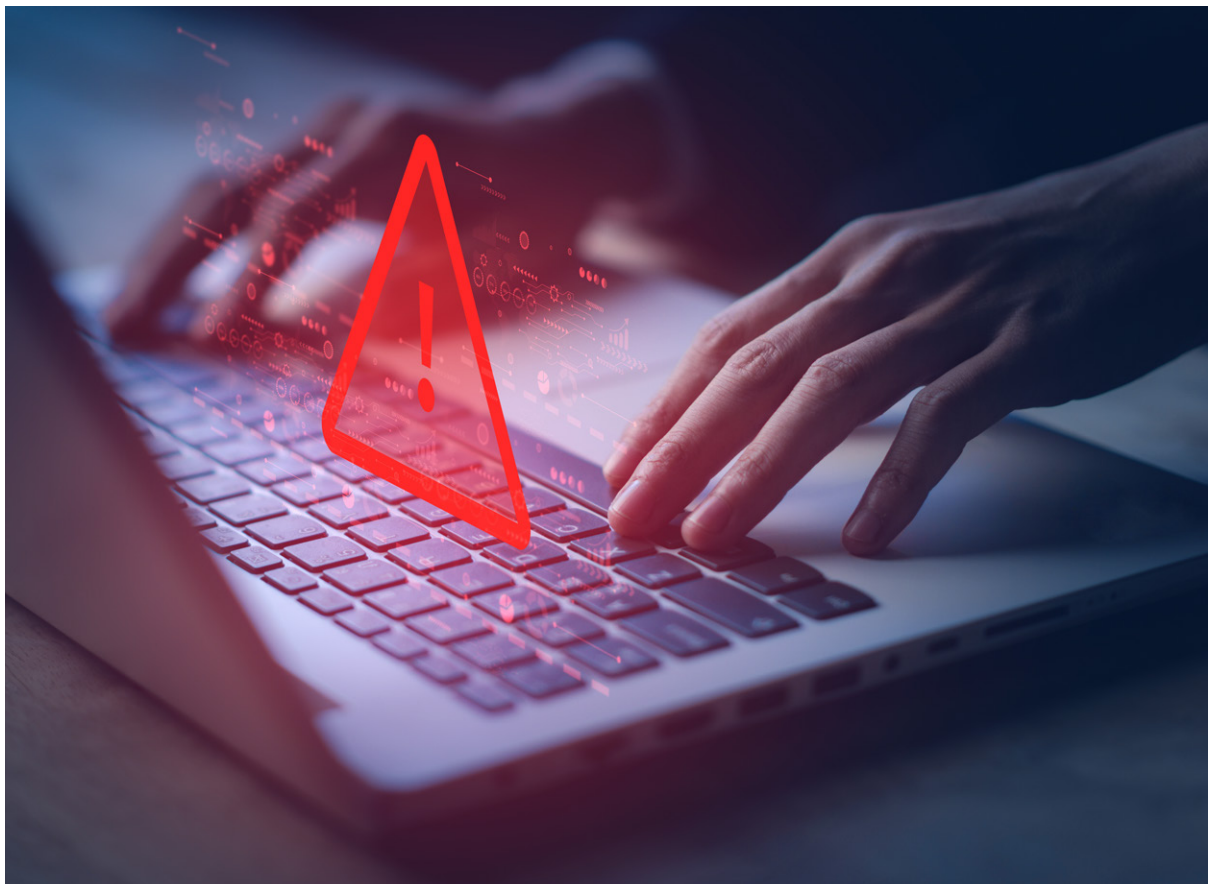
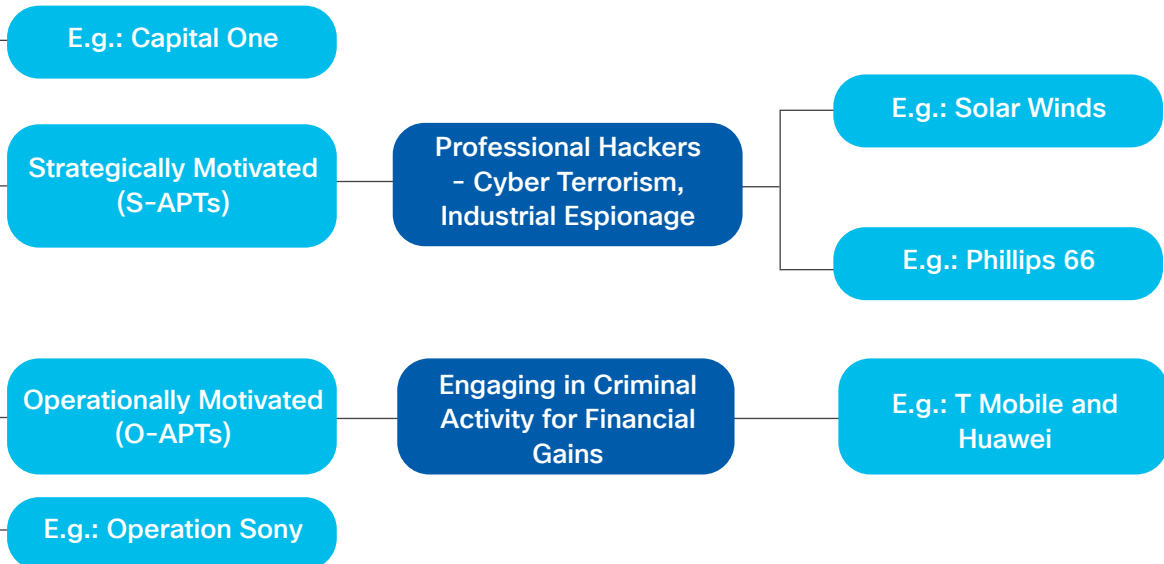


Figure 3: Cyber Threat Actors: Classification

Furthermore, the rapid expansion of the Internet of Things (IoT) has led to increased complexity and a surge in cyberattacks targeting sensitive data. IoT devices are vulnerable to various attack vectors, including user interface vulnerabilities, cloud service exploits, protocol-level attacks, and system interconnections. In 2021, there were 11.3 billion IoT gadgets present globally. By 2023, this figure is estimated to reach 15.1 billion<sup>16</sup>. With remote work becoming mainstream, threat actors now have multiple weak points to probe and launch attacks. Working from home is evolving into a new entry point for these cybercriminals to conduct alternative forms of data theft.

Data breaches can stem from different sources, including targeted attacks on specific organizations, opportunistic attacks on vulnerabilities discovered online, and inadvertent breaches resulting from mistakes or third-party failures. Organizations are now experiencing a 29 percent increase in ransomware attacks from 2018 to 2022<sup>17</sup>. The most common cyber attacks that result in data breaches are ransomware, phishing, malware, and illegal access<sup>18</sup>. The volatility in the geopolitical landscape is also contributing to the upsurge in Advanced Persistent Threats (APTs) driven by politically or ideologically motivated hackers and state-sponsored cyber incidents. Geographies across the globe are coming up with regulations to combat security breaches and establish cyber hygiene.





# The Impact of Geopolitics in Cyberspace



**86%** Cyber Leaders and 93% Business leaders agree that global geopolitical uncertainty will most likely or moderately lead to a cyber catastrophe in the next two years.

Source: (World Economic Forum; Global Cybersecurity Outlook 2023)

**74%** of organization leaders agree that global geopolitical instability has influenced their cyber strategy.

Source: (World Economic Forum; Global Cybersecurity Outlook 2023)

Cybersecurity and geopolitics are closely intertwined and are constantly reshaping the technological, legal, and regulatory landscape. The current geopolitical developments have profoundly impacted global cyber strategy and tactical cybersecurity operations. Leaders have realized that the impact of cybersecurity events are cascading from one business to another and across borders is beyond a single entity's control.

Geopolitics matter as it impact global organizations even if they aren't direct targets (Refer to case study 1). Geopolitical conflicts utilize cybersecurity as a weapon, leading to complex and persistent attacks. Economic interests

Cybersecurity and geopolitics are closely intertwined and are constantly reshaping the technological, legal, and regulatory landscape.

---

are affected by disruptions in trade and supply chains. Geopolitical factors shape

regulatory environments, international relations, and public trust.

### Case Study 1: Attacks on Energy Sector

***“Interconnected nature of the global economy means that a cyber-attack in one country can have far-reaching implications for organizations and individuals around the world.”***

The attack on the Indian critical establishments was reported to have taken place in 2019 by a North Korean hacking group. The attack involved malware that was found on the establishment’s administrative network. The malware was said to have originated from a phishing email that was sent to an employee. Once the employee clicked on the link in the email, the malware was able to infiltrate in the network and spread to other systems.

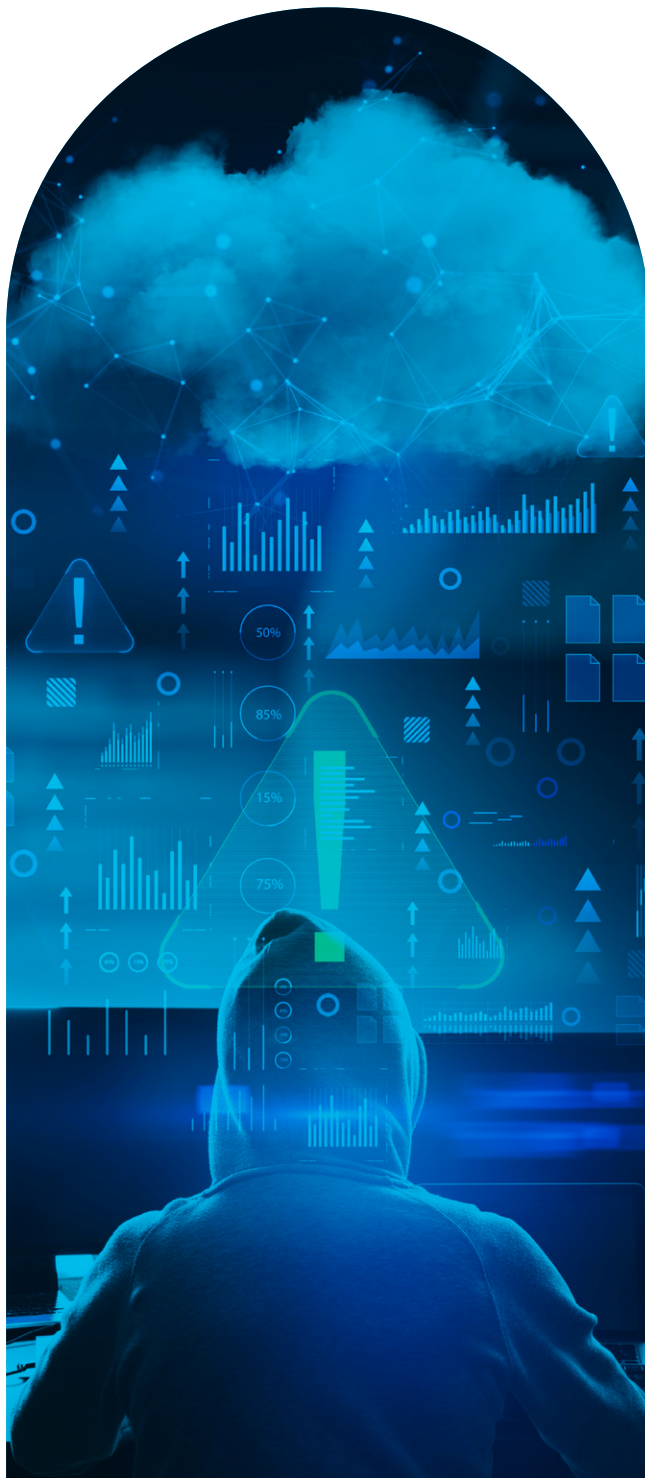
Geopolitical Implications: The attack did not result in any damage to the establishment operations, albeit, it raised concerns about the security of critical infrastructure in India and the potential impact on multinational organizations that rely on the establishment for their energy needs. Since the establishment is a joint venture between two nations, the incident highlighted the potential for cyber attacks to impact international partnerships and collaborations.

Building security, resiliency, and trust would require collaboration and cooperation across public and private sector players in charge of our shared digital infrastructure. Businesses need to improve their internal procedures and

policies and the efficiency of their third-party cybersecurity controls. Developing a clearer understanding of cyber dangers is necessary for long-term cyber resilience in order to integrate security into strategic business priorities.

# India's Cyber Threat Landscape

---



India's remarkable strides in digitalization are changing the way citizens and other state entities operate. In line with the G20's policy initiatives, India is quickly transforming its policy and administrative infrastructure to achieve this goal. Nevertheless, this transformation poses new risks and susceptibilities, particularly in terms of cyber threats from adversaries both inside and outside the country.

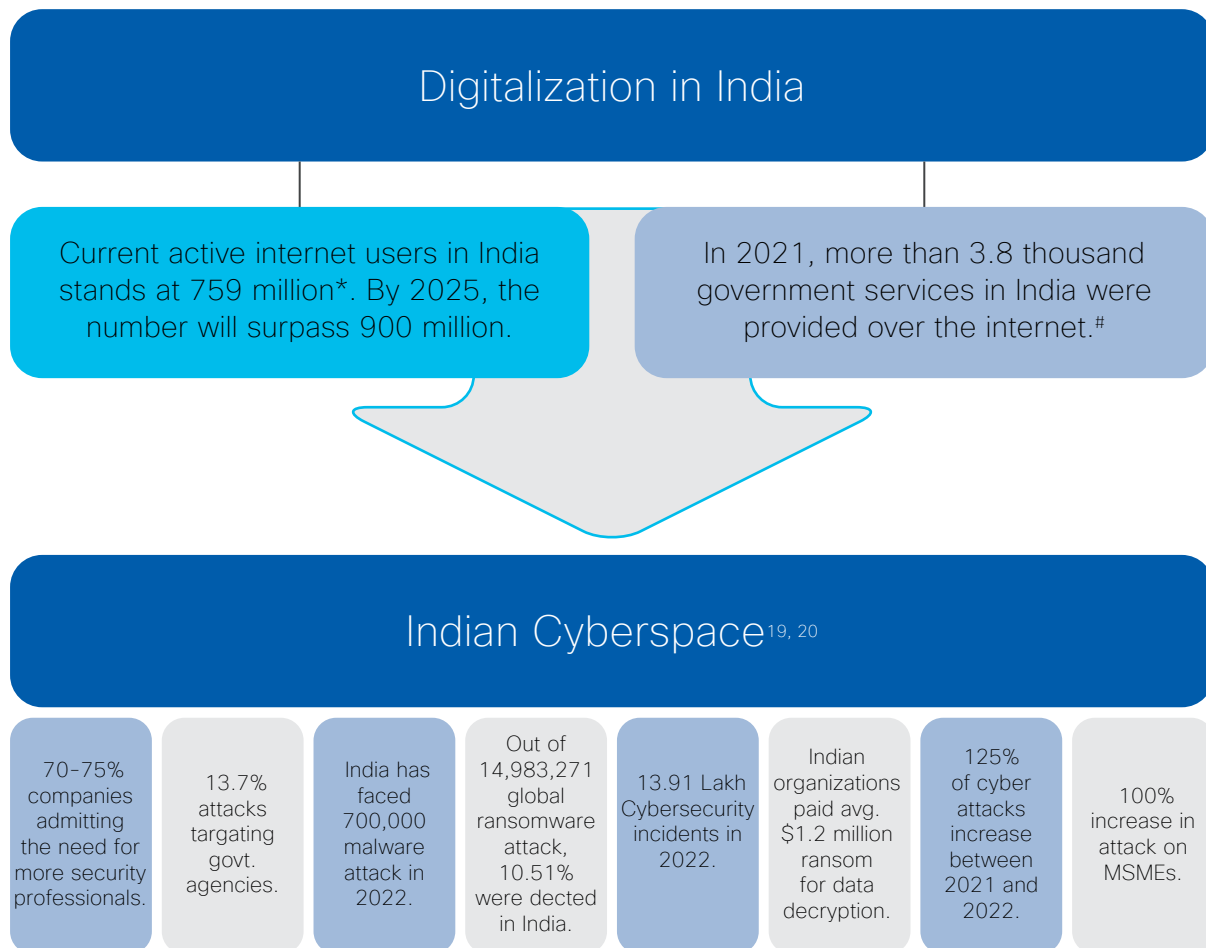


Figure 4: Indian Cyberspace

### 3.1 Vulnerabilities & Attacks in Indian Cyberspace

#### Attacks on Health Infrastructure

- Indian healthcare industry becomes the most targeted sector facing ~1.9 million cyberattacks in 2022.<sup>21</sup>
- Premium health institute became the prime target of ransomware attack compromising the data of millions of patients due to attack on its servers.
- Major pharmaceutical companies were targeted to steal critical information and data on vaccine research and trials across borders from Russia, China, North Korea, and Iran notably.

\*As on May 2023, Kantar & IAMAI Internet in India 2022 report.

†Statista. (2022, September 13). Number of online services provided by the government India FY 2016-2021.

### Attacks on Aviation Sector

- Top airlines in the countries are experiencing increasing cyber attacks (Ransomware, Phishing, DDoS, Data Breaches, and Cyber Espionage), compromising millions of customer records, including various degrees of Personal Identifiable Information (PII), including passport and credit card information.

### Attacks on Financial Sector

- Indian banks experienced 248 successful data breaches between March 2018 and June 2022, 41 from public sector, 205 from private sector, and 2 from overseas.<sup>22</sup>
- One of the leading India based payment company handling payments for tech giants and leading e-marketplaces suffered a databreach impacting 35 million customers.
- High risk of cybercrimes such as UPI frauds, debit or credit card cloning due to the lack of cybersecurity hygiene among a significant number of digital payment users.
- Around 40% of fraudulent activities in India are caused by digital and cyber-related problems in the fintech sector.

### Attacks on State & Critical Infrastructure<sup>21,22</sup>

- In 2017, Kolkata, Delhi, Bhubaneswar, Pune, and Mumbai got impacted due to the 'WannaCry' ransomware attack.
- Chinese hacker group 'RedEcho' caused power grid failure in Mumbai, disrupting traffic, stock market, and hospitals at the peak of the covid pandemic.
- The ransomware attacks on state-owned infrastructure are on rise. For eg, attack on Jawaharlal Nehru Port Container Terminal (JNPCT), etc.

## 3.2 Challenges in Indian Cyberspace

- Rising cases of cyber warfare.
- Lack of unified national-level architecture, despite setting up of the National Critical Information Infrastructure Protection Centre (NCIIPC).
- Harmonised supply chains increase threat of risk of tech hardware and embedded software; indigenisation & installation of trusted products key.
- Outdated India's National Cybersecurity Policy (2013); need to refresh to address the present-day technological and ecosystem realities.
- Lack of adequate trained cybersecurity professionals in the Indian workforce.
- Limited focus on promoting innovation & entrepreneurship; government and private R&D labs working in silos for in areas of national priorities.







# Cybersecurity Regulations

---



The increasing cybersecurity threats, the lack of preparedness of organizations, and the high cost of cyber incidents has propelled governments across the globe to come up with mandates to augment and strengthen Cybersecurity in the country. These efforts are materializing in the form of regulatory and compliance frameworks such as Cyber Emergency Response Team guidelines (India, Singapore, etc)<sup>23</sup> to proactively defend national and organizational Cybersecurity interests for the various stakeholders in the ecosystem. The table below lists down the cyber incident and breach notification timelines across jurisdictions.

Indian Computer Emergency Response Team (CERT-In) directions provide a structured approach to manage and respond to cyber incidents in India.

---

Geography/ Country <sup>24</sup>	Regulatory Body	Sectoral Regulatory Bodies	Governing Law/ Regulations	Timeframe for reporting Cyber Incidents (Within following hours*)	
India	CERT-In		IT Act, CERT-In Directions.	6 hours of noticing/ detecting such incidents. <sup>25</sup>	
		RBI (Reserve Bank of India)- Financial Institutions.	Cybersecurity Framework for Banks.	Within 2-6 hours of noticing/ detecting such incidents.	
		TRAI (Telecom Regulatory Authority of India) – Telecom Sector.		Reporting prescribed. Timelines not defined.	
		SEBI (Securities and Exchange Board of India) – Stockbrokers.	Cybersecurity & Cyber Resilience Framework.	Within 6 hours of noticing/ detecting such incidents.	
		IRDAI (Insurance Regulatory and Development Authority of India) – Insurance Sector.	Information and Cybersecurity Guidelines.	Within 6 hours of becoming aware of the incident. A copy of the report to be sent to IRDAI and other relevant regulators/authorities.	
Singapore	SingCERT		Personal Data Protection Act.	Personal Data Protection Commissioner.	3 days
				Individuals	As soon as practicable.
		Monetary Authority of Singapore (MAS)– Financial Services.		1 hours	
		Critical Infrastructure	Cybersecurity Act 2018	2 hours	
USA	US CERT: Cyberse- curity and Infrastruc- ture Secu- rity Agency (CISA).		Cyber Incident Reporting for Critical Infra- structure Act, 2022.	72 hours	

<sup>24</sup> Refer to annexure for detailed guide to cybersecurity regulation across jurisdictions.

Geography/ Country	Regulatory Body	Sectoral Regulatory Bodies	Governing Law/ Regulations	Timeframe for reporting Cyber Incidents (Within following hours*)		
Australia	Australian Cybersecurity Centre: AUS-CERT		SOCI (Security of Critical Infra- structure) Act		Verbal	Written
				Critical Asset	12 hours	84 hours
				Non- Critical Asset	72 hours	48 hours
United Kingdom	National Cybersecurity Centre: U.K CERT		NIS(Network and Information Security) Regu- lations	72 hours		
		FCA (Financial Conduct Authority)		As soon as of becoming aware.		
European Union	CERT E.U/ ENISA (Euro- pean Network and Informa- tion Security Agency)		NIS Directive, privacy Direc- tive	72 hours		

## 4.1 Data Breach and Incident Response - India

### CERT-In on Cyber Incidents:

Indian Computer Emergency Response Team (CERT-In) directions provide a structured approach to manage and respond to cyber incidents in India. The directions are designed to help organizations to identify, respond to, and recover from cyber incidents in a timely and effective manner.

- **Incident Reporting:** Organizations in India must report cyber incidents to CERT-In within six hours of being informed.
- **PoC Appointment:** Designation of a responsive Point of Contact (PoC) for communication with CERT-In is mandatory.

- **Log Maintenance & Time Synchronization:** Secure maintenance of ICT system logs for 180 days and synchronization of clocks with trusted NTP (Network Time Protocol) servers.
- **Customer Information:** Network service providers and other relevant entities must register and maintain accurate customer information for at least five years.
- **KYC Requirements:** Virtual asset providers and custodian wallet providers are required to retain Know Your Customer (KYC) information and financial transaction records for five years.

Intermediaries have a due diligence obligation to report security breaches to CERT-In, with template provided for incident reporting.<sup>26</sup>





## Expectations and Obligations from Organizations in Digitalization Context

---



Complying with country-specific directions can often be daunting for organizations grappling with limited manpower and escalating operational costs. Revamping technological capabilities is paramount to quickly identify incidents, reduce damage, and mitigate reputational damage.

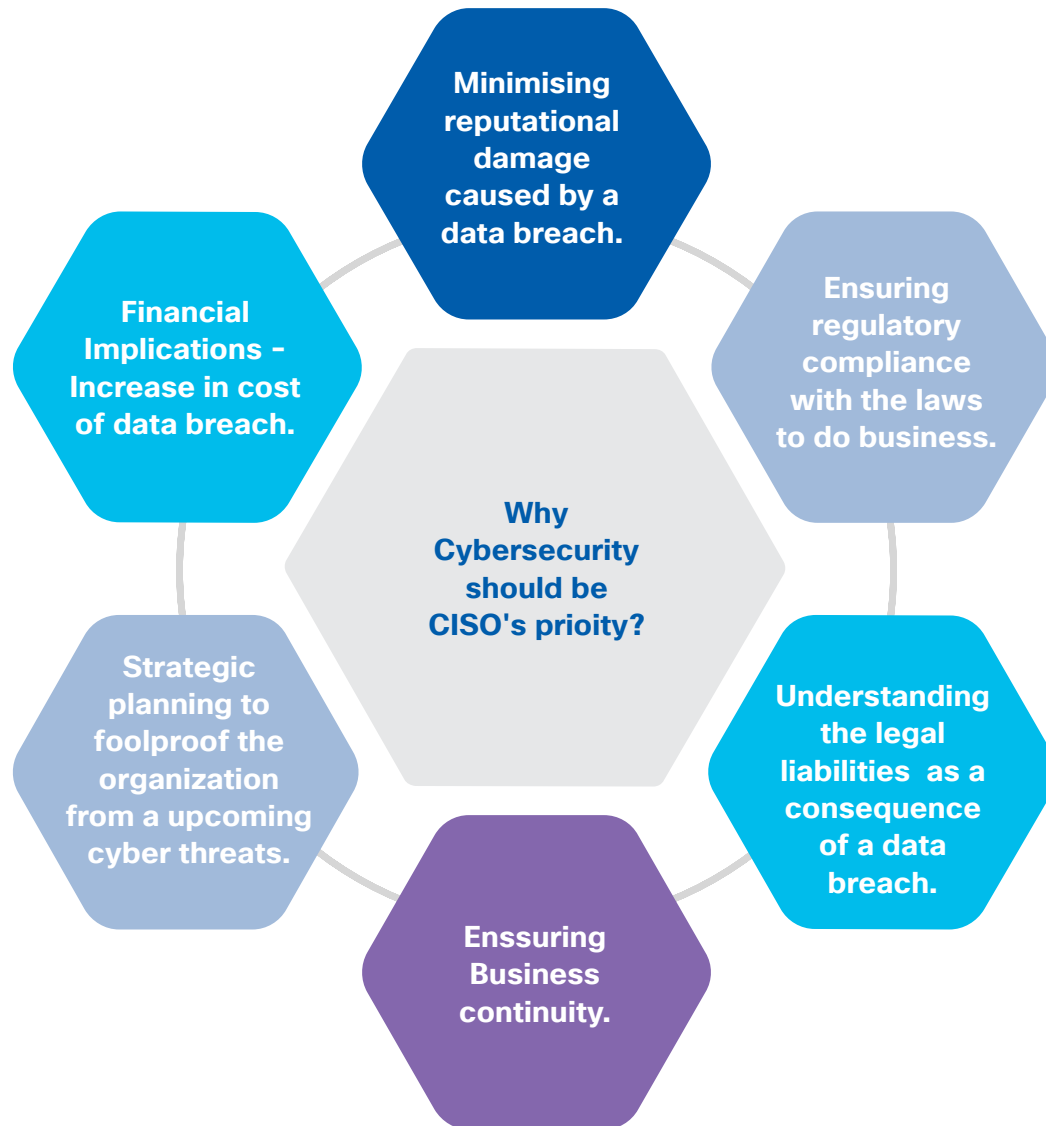
Organizations can better prepare themselves to respond to incidents effectively and efficiently by building internal capacities to complement their cyber incident strategy. This involves investing in the right tools, technologies, and equipping analysts with sufficient resources to maintain the security of networks, systems, and applications. Thus, enabling organizations to contribute to an overall security program by proactively remediating security incidents.

It is the responsibility of the CISO to maintain the security and integrity of the IT network and infrastructure

---

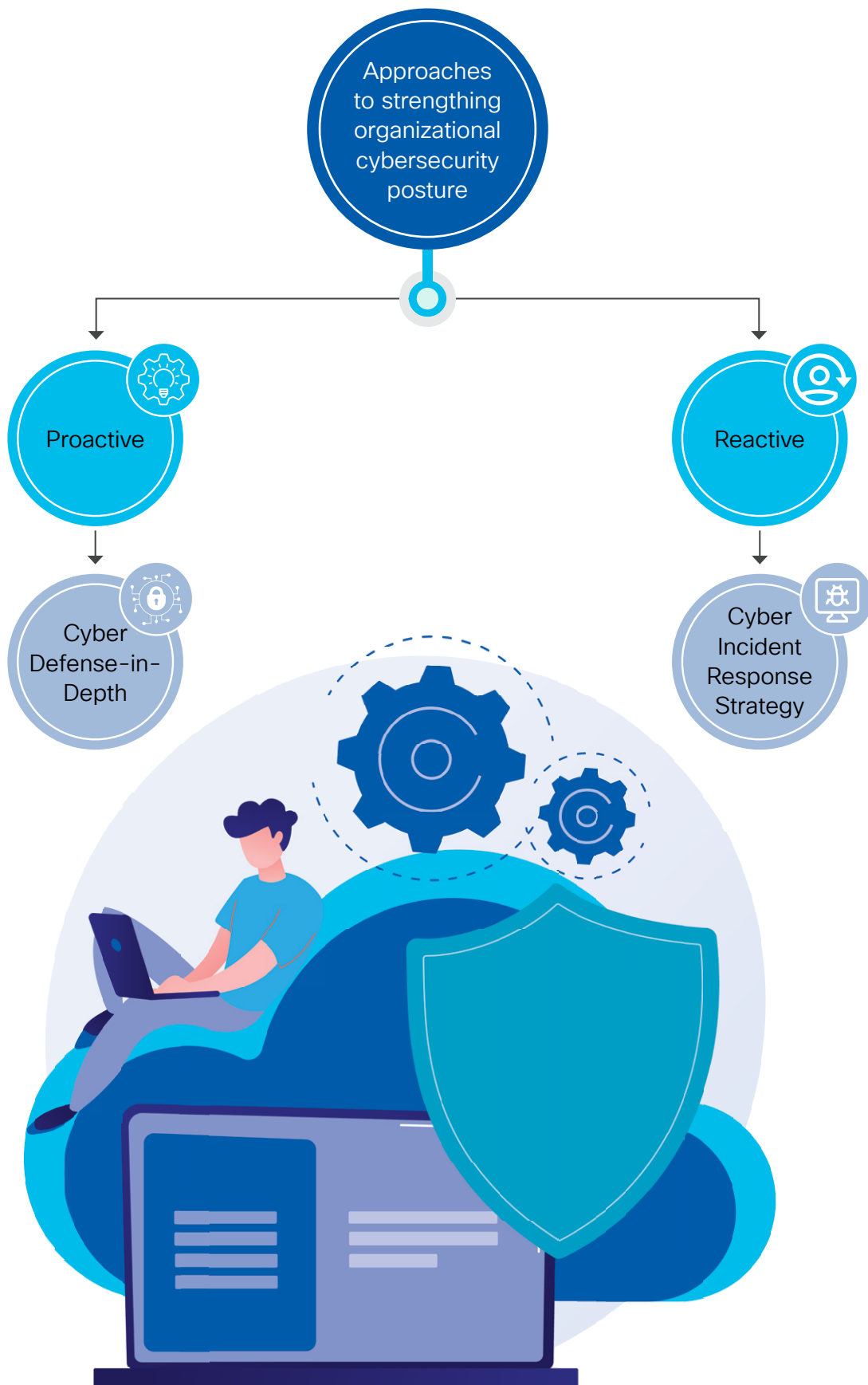


## 5.1 The CISO's Evolving Role & Responsibilities:



To ensure the success of Digital Transformation strategies, cybersecurity should be integrated into the design and implementation process instead of being an afterthought. It is the responsibility of the CISO to maintain the security and integrity of the IT network and infrastructure, including data and applications on-prem and in the cloud, using cutting-edge technologies.

Traditionally, the CISO team would work in isolation to protect the organization from cyber threats, but modern threats require a more agile and integrated approach. The security team should play a strategic role in the organization and use proactive and reactive measures to ensure business continuity and gain a competitive advantage.







# Towards Efficient Incident Response: Cyber Defense in Depth Strategy

---



Cyber defense in depth is a **proactive approach** to cybersecurity that aims to prevent attacks by layering multiple security controls. This includes both technical controls, such as firewalls and intrusion detection systems, and non-technical controls, such as employee training and security awareness.



- Physical Security
- Network Security
- Hardware Security
- Software Security
- Data

*Figure 5: Layers of Security in Defense in depth*

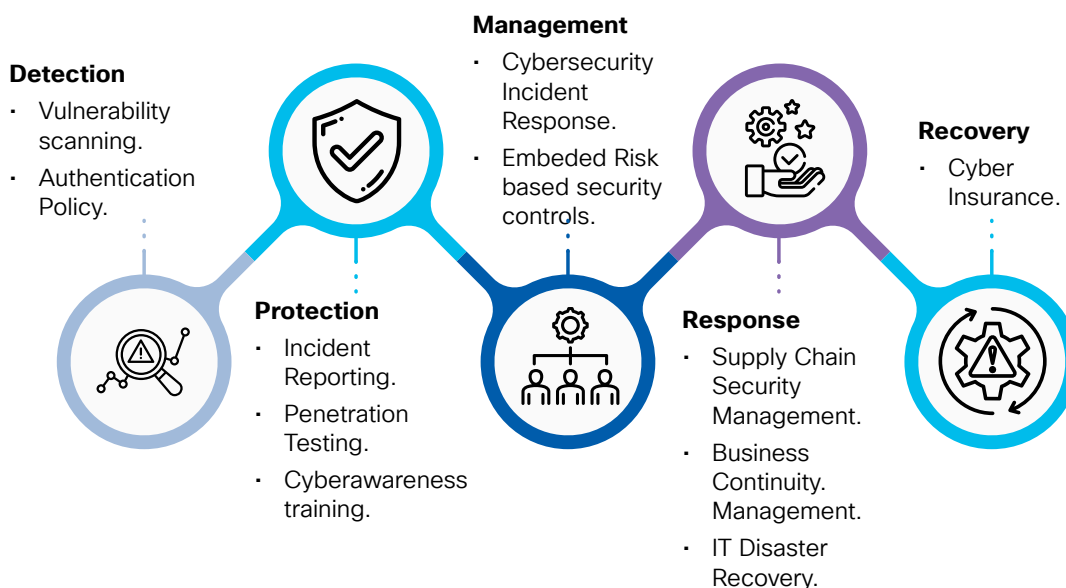


The concept of defense in depth, originally derived from military tactics, aims to impede and discourage attackers by slowing down their progress. In the realm of cybersecurity, this approach involves implementing counter measures to safeguard crucial assets and creating targeted protection mechanisms for areas that are identified as weak, vulnerable, or prone to attack. For defense in depth to be effective, it must encompass people, technology, and operations.

### Why is it important?

- **Increased Resilience:** Organization can ensure that even if one layer is breached, other layers can still provide some level of protection.
- **Deterrence:** The presence of multiple layers of defense can act as a deterrent to cyber criminals, who may be less likely to target an organization with strong defenses.
- **Better Detection:** An organization is more likely to detect cyber threats at an early stage thus minimizing damage.
- **Protection Against Advanced Threats:** Cyber defense in depth can provide additional protection against APTs by using a combination of technologies and strategies.
- **Compliance:** Many regulations and standards require organizations to implement multiple layers of defense to protect sensitive data.

## 6.1 Stages of Cyber Defense in Depth Strategy: Adopting a Risk-Based Approach



### 6.1.1 Detection

- Be aware of the potential dangers organizations may encounter and identify the areas of cyber defenses that are most susceptible to breaches.
- Conduct frequent vulnerability scanning and penetration testing to stay ahead of emerging threats.

### 6.1.2 Protection

- Empower your employees as a vital line of defense by providing them with security knowledge and responsibilities. While not all organizations require extensive security measures, implementing a fundamental level of security is indispensable.

- Showcase your commitment to cybersecurity excellence by obtaining certifications for security schemes.

### 6.1.3 Management

- Adopt a comprehensive approach to protect your organization against cyber threats, including risk-based security controls and supply chain oversight.
- Regularly conduct audits to ensure robust protection and adherence to security standards and compliance to regulations.
- Certifications, such as obtaining ISO 27001, serve as a tangible testament to customers, stakeholders, and employees that your organization adheres to and upholds the highest standards of information security best practices.

### 6.1.4 Response

- While implementing security measures can reduce the impact of a successful attack, having a response plan in place is crucial to containing the damage and minimizing associated costs.

**Data Breach Reporting:** This becomes even more critical in the event of personal data breaches, which must be reported to the relevant data protection authorities.

### 6.1.5 Recovery

- Recovering from a cyber-attack or data breach can prove more disruptive than anticipated. Though critical services can often be restored, returning to normal operations can take several months. To alleviate some of the associated concerns, having cyber insurance coverage can provide peace of mind. It ensures that your organization has the necessary financial support when it is most needed, facilitating a swift and efficient recovery process. Cyber insurance serves as a valuable safeguard, enabling your organization to rebound promptly from the impact of cyber incidents.

Defense in depth is structured to prevent and detect security incidents. However, if it fails to curtail the occurrence of cyber incident; incident is triggered. In such cases, effective incident management comes into play. This involves swiftly identifying the nature and the scope of the incident, containing its impact, eliminating the threat, and restoring affected systems to their normal state.


*Cyber defense in depth is about building a strong foundation of security controls to deter attacks, while cyber incident response strategy is about having a plan in place to deal with attacks that do occur.*





# Devising a Cyber Incident Response Strategy for your Organization

---



It is a **reactive approach** that involves a structured approach to identify, respond, and recover from cyber incidents effectively and efficiently. An incident response strategy typically includes processes, procedures, and protocols to detect, analyze, contain, eradicate, and recover from incidents. It involves a coordinated effort between various stakeholders within an organization, including incident response teams, IT personnel, legal and public relations departments, and external entities such as CERT. The goal of an incident response strategy is to minimize the damage caused by an incident, restore normal operations, and prevent future incidents by learning from the incident and implementing necessary improvements.



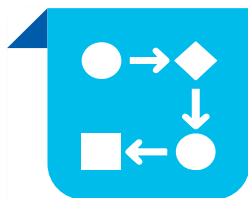
### Technology alone falls short

- Technology needs support from people and processes to address blind spots, misconfigurations, maintenance issues, and other challenges that can undermine its effectiveness.



### The people angle

- People are critical assets in incident response. They manage stakeholder expectations, make important decisions, think creatively, address blind spots and pain points.



### Vitality of processes

- Well-developed processes ensure consistency, muscle memory, documentation, and stress-tested actions. They facilitate effective coordination, communication, and decision-making during incidents.

Figure 6: The people, process, technology lens

The people, process, technology triad plays a crucial role in the incident response life cycle, ensuring a comprehensive and pragmatic approach to handling security incidents.

Here are some important considerations for each area:

#### People:

Responding to a security incident should not be viewed as solely a technical matter, and individuals from various departments beyond IT should be actively involved. To ensure an effective response, a well-defined management structure that is easy to implement and execute is necessary<sup>27</sup>.

The management schema for incident response typically includes the following roles:

#### 1. Incident Response Team (IRT):

The IRT is responsible for the overall management of the incident response

effort. This team typically includes members from the IT department, security team, and other relevant departments.

#### 2. Incident Response Coordinator:

The incident response coordinator is responsible for coordinating the response effort, ensuring that all necessary contacts are involved, and managing communication between the various parties.

#### 3. Technical Contacts:

Technical contacts are responsible for investigating and resolving the technical aspects of the incident. This may include members of the IT department, security team, or external security consultants.

#### 4. Legal Contacts:

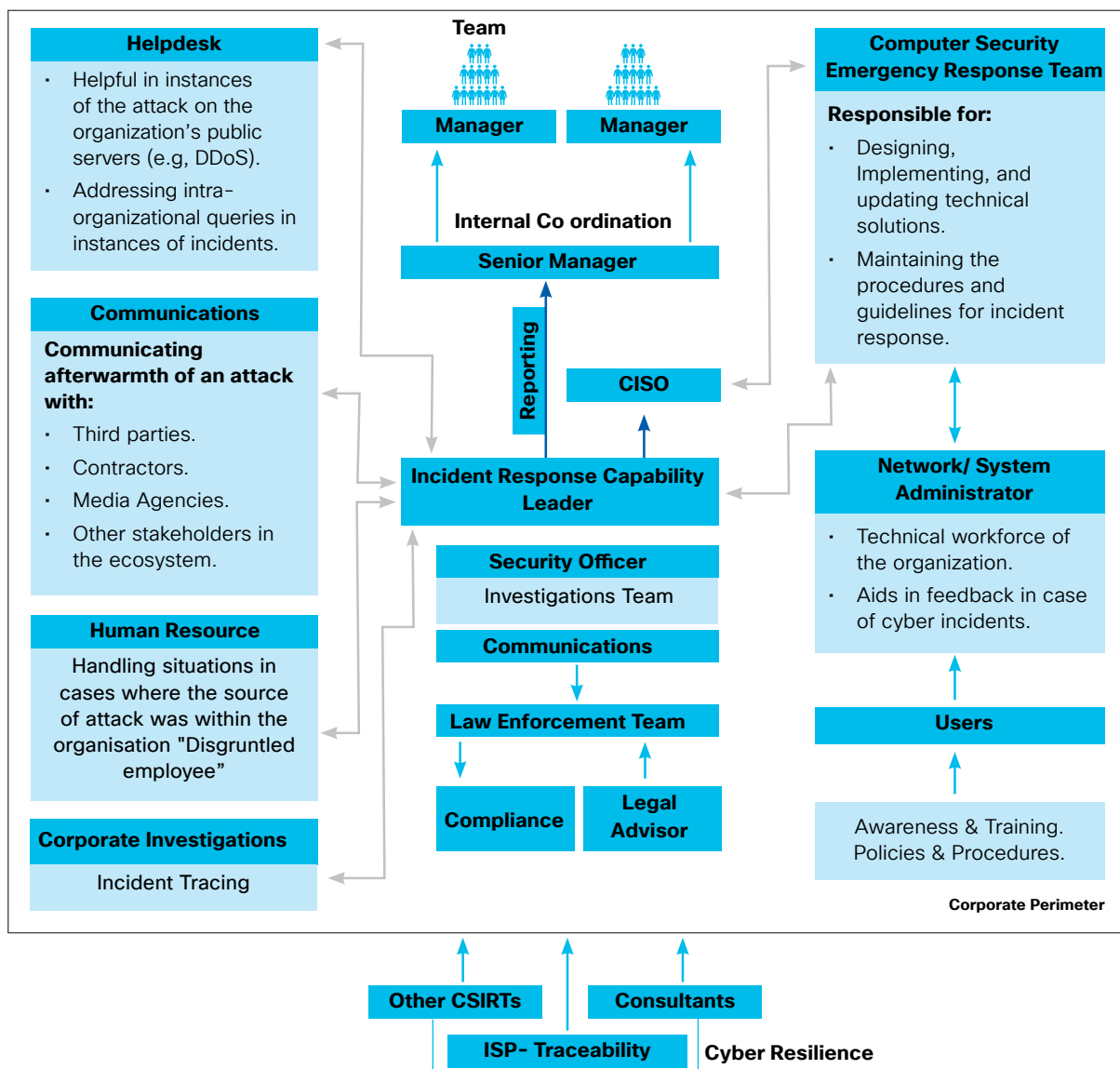
Legal contacts are responsible for managing legal aspects of the incident, such as compliance with regulations, reporting requirements, and potential legal liabilities.



5. **Public Relations Contacts:** Public relations contacts are responsible for managing the public relations aspects of the incident, including communicating with the media, customers, and other stakeholders.

Thus, by defining these roles and responsibilities and ensuring that all necessary parties are involved, organizations can respond to security incidents more effectively and minimize the impact of the incident on their operations, customers, and partners.

Figure 7: Management Schema of Incident Response



## Process:

1. Incident response plan: A comprehensive incident response plan should be developed, detailing the

steps that should be taken in the event of a security incident. The plan should be regularly updated and tested to ensure that it remains effective.

2. Communication procedures: Clear communication procedures should be established, detailing how information should be shared between the incident response team, executive leadership, employees, and external stakeholders.
3. Documentation and reporting: This procedures should be established to ensure that incidents are tracked and analyzed effectively, and that regulatory requirements are met.

### Technology:

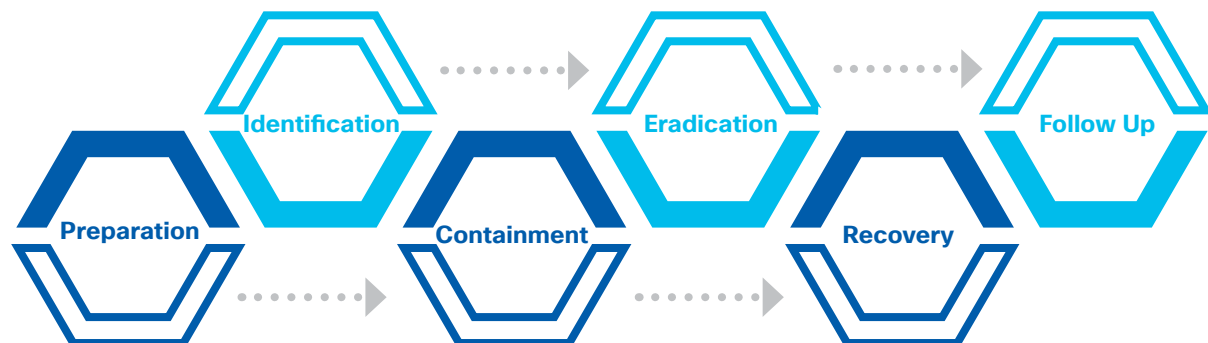
1. Security tools and technologies: The incident response team should have access to the necessary security tools and technologies, including network monitoring tools, endpoint protection

software, and forensic analysis tools.

2. System backups and disaster recovery: Regular system backups and disaster recovery procedures should be established to ensure that critical data can be restored quickly in the event of a breach.
3. Threat intelligence: The organization should have access to up-to-date threat intelligence to help detect and respond to emerging threats.

By focusing on these areas, organizations can build internal capabilities for cyber incident response, improving their ability to detect and respond to security incidents effectively and efficiently.

## 7.1 Phases of Incident Response:



### 7.1.1 Preparation

- An organization prepares for a potential cyber incident by developing an incident response plan, identifying the roles and responsibilities of the incident response team, and establishing communication channels for reporting and responding to incidents (Refer section: Devising a Cyber Incident Response Strategy for your Organization). This includes identifying critical assets, defining incident severity levels, and implementing technical controls to detect and prevent incidents.

Threats	Prevention Toolkits <sup>28</sup>
Malware, DDoS attack, hacking (ransom and extortion, espionage). Compromised sensitive information (malicious and accidental)	Anti-virus software
	Awareness trainings
	Encryption
	Anti DDoS and CDN measures
	Data loss prevention software
	Deploying approved scanning vendors
	Penetration testing

### 7.1.2 Identification

- The crucial stage in the process is the identification stage, where the starting point of an event is determined, and critical decisions must be made to categorize and respond to the event appropriately. If the procedures fail during this stage, the entire methodology can collapse.
- Once an incident is identified or suspected, evidence collection should begin immediately. However, determining whether abnormal activity is once in a while attack or an attack pattern can be difficult. Technology can assist with methods like intrusion detection and Real Time Threat Management Systems (RTTMS), but the human factor is typically the one with knowledge of abnormal activity in a specific corporate environment.
- Approaches for dealing with network incidents depending on their severity:
  - o Immediately close the attacker's point of entry and eliminate all possible access means.
  - o Remain "open" as long as possible to gather as much information as possible for use as evidence later.

Alert	Logs	Publically available Information	People
<ul style="list-style-type: none"> <li>• IDP/IPS</li> <li>• SIEM,XDR</li> <li>• Anti Virus software alerts</li> </ul>	<ul style="list-style-type: none"> <li>• Operating Devices</li> <li>• Operating Services</li> <li>• Applications</li> <li>• Network Devices</li> <li>• System flows</li> </ul>	<ul style="list-style-type: none"> <li>• Open Source Information</li> </ul>	<ul style="list-style-type: none"> <li>• Suspicious activity (User &amp; Admin)</li> </ul>

## Audit log collection, examination, and analysis

The information about an incident can be found at various sources (e.g. firewall(s), IDS Intrusion Detection System (s), router(s), etc.) a great amount of effort and time is required to correlate them before reaching trustworthy conclusions. The importance of having a central System Log Server that performs a log analysis is based on the observation that using one central system and applying filters can provide useful conclusions in a relatively short period of time.

## Detection Systems

Host and Network-Based Intrusion Detection Systems have a vast database of known attack patterns that can be helpful in identifying the type and source of an incident. If the incident matches a known attack pattern in the IDS database, then the system in question should be checked for the vulnerability that caused the incident. If the system has the appropriate countermeasure, such as a software patch, then the incident is logged for future reference. However, if the incident is a new and unknown; the security gateway audit logs, usually the firewall logs, should be analyzed to gather more information. If the affected system is found to be vulnerable, it should be isolated to prevent the incident from infecting other systems and networks.

**Considerations:** Collecting and correlating data from various sources, including logs, network traffic, cloud infrastructure, and endpoints, to identify potential threats and incidents helps responders to quickly understand the scope and impact of an incident and take appropriate actions. Thus, providing a cross-layer visibility into the network, cloud, and endpoints.

When an incident is detected, it should be classified into one of three security levels

based on its impact on the organization's financials, manufacturing, sales, corporate image, or customer trust. The extent of the impact will determine the initial response to the incident.

Developing the risk matrix which maps impact of the incident to the urgency with which it should be addressed will help in prioritizing the further course of action.

## Incident reporting and assessment

This categorization is part of the Incident Reporting form, which documents all relevant information about the incident. The Incident Reporting Form is crucial since it contains valuable information that is reviewed later during a forensic analysis or follow-up phase. Examples of information include; the date and time of reporting, the date and time of incident discovery, the system in which the incident was first identified, possible affected systems and networks, system configuration, host applications, criticality, and the name and credentials of the person completing the form.

## 7.1.3 Isolation & Containment

The subsequent step involves promptly implementing remedies, which restrict the scope of the incident and allow the attack to operate only to the desired extent. However, some attacks may need to continue to allow for computer forensics analysis for certain reasons. Standard approaches to addressing the situation involve making patch installations and configuration modifications to critical perimeter, public, and internal systems.

## Preventive Measures:

- Deactivation of particular system services.
- Alteration of access and authentication systems and deactivation of accounts.

- Disconnection of the affected system from the network.
- Temporary suspension of the compromised system.
- Recovery of the compromised system.

#### 7.1.4 Eradication

This phase pertains to the solutions that need to be implemented on the affected systems in the medium and long term to eliminate any potential avenues for the specific attack to reoccur. Possible measures during this stage consist of verifying policy compliance, conducting independent security audits, and updating policies, among others.

##### Preventive Measures

- Altering access and authentication systems in all compromised systems.
- Completely removing intruder access and identifying any possible alterations,
- Fully reinstalling the compromised systems and rebuilding the system.

#### 7.1.5 Recovery

Once all the prior steps have been carried out effectively, the process of system recovery and enhancement of security mechanisms should commence to restore the entire system to operation without any open security vulnerabilities. This may involve actions such as rebuilding the entire system, retrieving data from backup media, installing additional security mechanisms, and so on. Prior

to reintroducing compromised systems into operation, it is recommended to conduct a vulnerability assessment or penetration test to reveal any potential existing vulnerabilities.

##### Preventive Measures

- Rebuilding the system from the ground up.
- Restoring user data from reliable backups.
- Conducting an audit of system configurations.
- Reviewing the protective and detective mechanisms to ensure that they are functioning properly.

#### 7.1.6 Follow-Up Phase

It is crucial to document all actions and information related to the incident and to disseminate electronic evidence for analysis by experts in a forensically sound manner. In addition, a post-incident meeting with senior management should be held to evaluate the damage, the strengths and weaknesses of policies, and the necessary procedures to be followed. The aftermath of an incident may require updates to security policies, procedures, and guidelines to prepare for future attacks. Once the incident analysis is complete, changes to system configurations should be documented, and the inventory of systems and network assets should be updated to reflect these changes.





# Supplementing Organizational Incident Response

---



**Establishing Linkages with Cyber Attack Kill Chain:** Understanding the steps of the 'Cyber Attack Kill Chain' provides insights into intrusion detection and adversary tactics. Mapping these steps against preventive controls helps with investment decisions, defensive strategies, and real-time response to cyber attacks<sup>29</sup>.

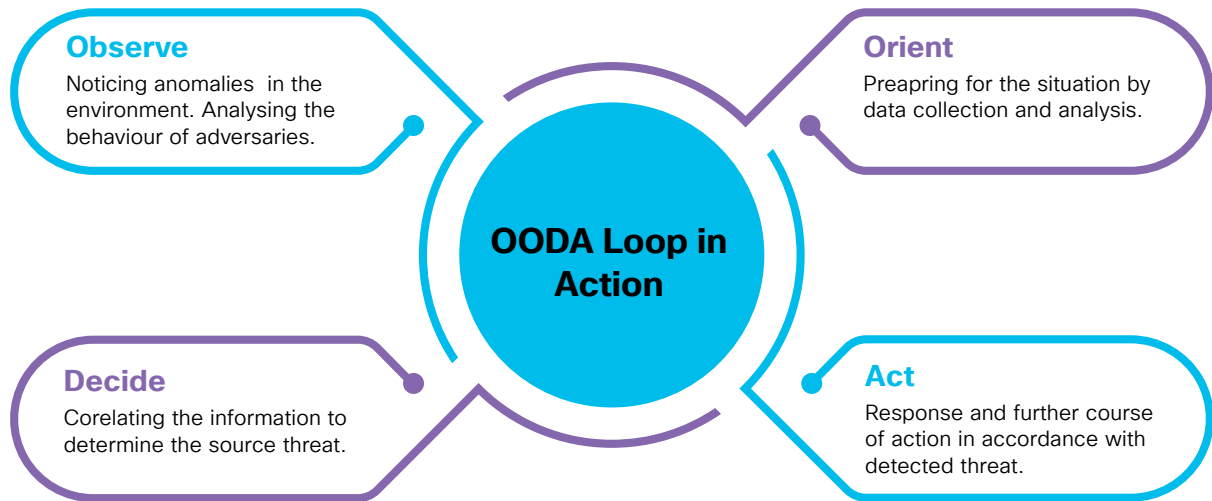
The ability to act promptly is critical during a cybersecurity breach. The OODA loop comprises of four phases, namely Observe, Orient, Decide, and Act, which are repeatedly iterated.

---

<sup>29</sup> Refer to annexure for more details.



## OODA Loop in Action: Proactive Steps for Timely Data Breach Mitigation



The ability to act promptly is critical during a cybersecurity breach. The OODA loop comprises four phases, namely Observe, Orient, Decide, and Act, which are repeatedly iterated. OODA loop serves the purpose of assisting individuals in making informed decisions and prompt action instead of succumbing to

inactivity. At its core, it is a framework for recognizing and evaluating an individual's thought process, actions, reactions, and ability to adjust to stimuli. This approach can be extremely beneficial to an information security professional and has diverse applications in both offensive and defensive contexts<sup>30</sup>.



# Achieving Regulatory Compliance:

## Recommendations for Organizations

---



- Acknowledge your baseline and establish clear cybersecurity policies and procedures aligned with regulations. This means understanding your organization's most critical assets and the risks they face, and then developing policies and procedures that will help to mitigate those risks.
- Conduct regular risk assessments to quickly identify vulnerabilities and prioritize actions. This will help organizations to identify areas where security posture is weak.
- Training employees on cybersecurity policies, their roles and responsibilities. Employees are often the weakest link in an organization's cybersecurity defenses. By training employees on how to identify and report suspicious activity.
- Engage in third-party risk management to ensure compliance throughout the supply chain. This means assessing the cybersecurity risks of your third-party vendors and taking steps to mitigate those risks.

- Identify all devices on your network, including those forgotten devices. This will help you to get a complete picture of your network and to identify any potential security vulnerabilities.
- Develop and test an incident response plan for effective handling of security incidents. This plan should outline how your organization will identify, contain, and eradicate security incidents.
- Regularly assess and improve cybersecurity controls and practices. The threat landscape is constantly evolving, so it is important to regularly review your security controls and make changes as needed.
- Seek guidance of legal and compliance professionals on regulatory requirements.
- Stay informed about evolving regulations and engage with regulatory bodies. Cybersecurity regulations are constantly changing, so it is important to stay updated. Engaging with regulatory bodies to understand their expectations and to get feedback on your compliance efforts.

By following these recommendations, organizations can effectively address the compliance implications associated with cybersecurity regulations and demonstrate their commitment to cybersecurity, accountability, and transparency.

# Solutions Enabling End-To-End Security to Enterprises

---



Only 15% of global organizations have a mature cybersecurity posture to defend against the risks of the hybrid world<sup>31</sup>.

---

To ensure comprehensive end-to-end security, it is crucial to establish strong connections between securing the end user, remote users on the cloud, and the network. This can be achieved by implementing several key measures. Firstly, deploying robust endpoint security solutions helps protect individual devices and fortify the first line of defense. Secondly, implementing secure remote access and cloud security measures ensures encrypted communication channels and secure connectivity for remote users. Thirdly, strengthening network security through firewalls, intrusion prevention systems, and network segmentation helps protect against unauthorized access and network attacks.



Let's explore some key solutions that enable end-to-end security in cyberspace.

- **Endpoint Security Solutions:** Endpoint security focuses on protecting individual devices, such as desktops, laptops, and mobile devices, from threats and unauthorized access. It involves deploying robust antivirus software, firewalls, encryption techniques, and intrusion detection systems to secure endpoints. Advanced solutions like Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) provide enhanced threat detection, real-time monitoring, and rapid response capabilities.
- **Network Security Solutions:** Network security solutions play a crucial role in safeguarding the communication channels and infrastructure within an organization. These solutions include firewalls, secure gateways, Intrusion Prevention Systems (IPS), Virtual Private Networks (VPNs), and Network Access Controls (NAC). They help protect against unauthorized access, data breaches, network attacks, and malware propagation across the network.
- **Cloud Security Solutions:** Cloud security solutions involve implementing strong access controls, encryption, Data Loss Prevention (DLP) measures, and continuous monitoring of cloud environments. Additionally, cloud providers often offer security services such as cloud-based firewalls, threat intelligence, and security incident response to enhance overall cloud security.
- **Security Information and Event Management (SIEM):** SIEM solutions aggregate and analyze security event data from various sources to provide real-time threat detection,

incident response, and compliance management. SIEM systems collect logs, monitor network traffic, and generate alerts, enabling organizations to proactively identify and respond to security incidents.

- **Identity and Access Management (IAM):** IAM solutions are crucial for managing user identities, authentication, and access rights across different systems and applications. By implementing strong authentication mechanisms, Multi-Factor Authentication (MFA), and Role-Based Access Controls (RBAC), organizations can mitigate the risk of unauthorized access and improve overall security.

## 10.1 Securing the Cyberspace: Exploring Solutions

Security measures implemented by organizations to protect their digital assets falls into network, endpoint and logs. To mitigate the possibility of an undetected threat actor persisting in the network for an extended duration, it is crucial to incorporate all these elements in establishing a comprehensive Security Operations Centre (SOC) Visibility Triad. This triad employs a proactive methodology aimed at reducing the risk and ensuring early detection.

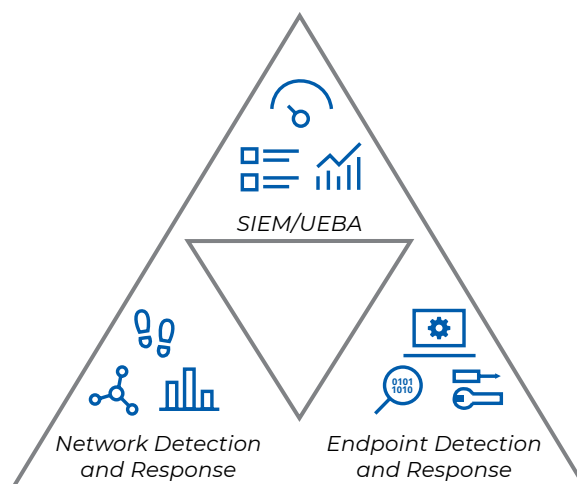


Figure 8: SOC Visibility Triad (Source: Gartner)

- **Endpoint-centric measures:**

1. Tools: Endpoint Detection and Response.
2. Limitation: Lack visibility across networks, servers, and cloud workloads.

- **Log-based measures:**

1. Tools: Security Information and Event Management (SIEM), User and Entity Behaviour Analytics (UEBA) tools, Cloud Access Security Brokers (CASB).
2. Limitation: SIEM tools primarily focus on threat detection by gathering data from various sources, conducting analysis, and providing

actionable signals. However, they often face challenges in providing comprehensive visibility and context for detecting and responding to advanced threats.

- **Network-based measures:**

1. Tools: Network Traffic Analysis (NTA), Network Detection and Response (NDR) solutions.
2. Limitation: Lack endpoint visibility.

These approaches create siloes of disjointed toolsets resulting in lack of understanding what is critical, no incident prioritization and reduced speed to response that are leveraged by threat actors to intrude in the network.

## 10.2 Addressing the Gaps- Inadequate Integration and Siloed Security Tools:

**51%** express concerns about the capabilities of their existing tools to effectively detect and investigate advanced threats.

**36%** of professionals aren't satisfied with their existing tools' capability to efficiently correlate alerts.

32

Organizations often depend on security tools from different vendors to build their security infrastructure. However, the lack of integration or shared telemetry among these tools poses significant concerns. To address these challenges effectively, it is crucial to integrate threat detection tools across endpoint, network, and log-based security measures. By doing so, organizations can overcome the following issues:

- Overreliance on disconnected security tools.
- Insufficient data integration across vendors hampers seamless integration with analysis tools, resulting in analysis paralysis. Organizations lack a unified

and comprehensive view of the overall security landscape.

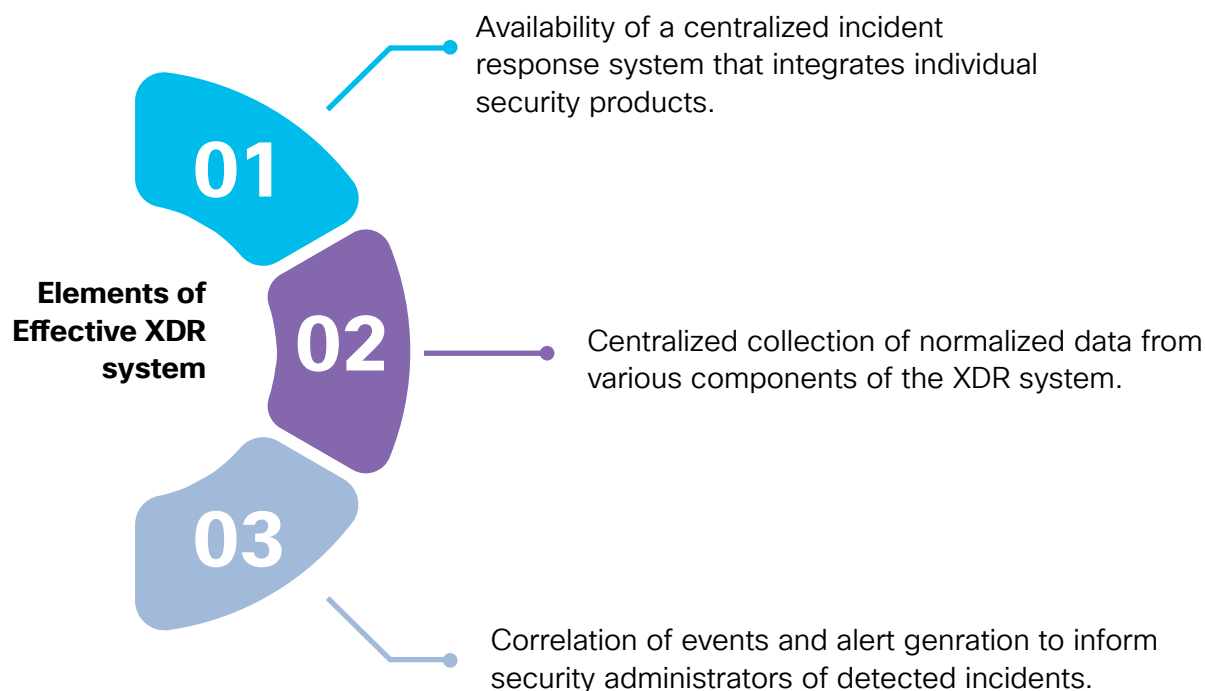
- Lost time and effort spent switching between different tools.
- Lack of coordination among the various tools, leading to complex security operations and impeding the effectiveness of incident response capabilities.
- Insufficient return on investment (ROI) for the organization's existing security investments.

## 10.3 XDR as an Approach

*XDR encompasses three core aspects. Firstly, it involves gathering telemetry from diverse sources. Secondly, it*

*applies analytics to the collected telemetry to identify malicious activities. Finally, XDR emphasizes*

*not only the detection but also the response and remediation of these malicious elements. IDC.*



### How XDR Empowers First Line of Response.

SOC analysts are facing challenges in prioritizing the increasing volume and complexity of security alerts. It is crucial to find a balance between identifying relevant threats and prioritizing them based on contextual awareness.

#### The XDR Advantage

- **Improved Threat Detection:** XDR integrates multiple security controls for comprehensive threat detection, reducing false positives.
- **Advanced Analytics and Correlation:** XDR uses analytics and correlation techniques to prioritize and consolidate related alerts.
- **Contextual Insights:** XDR leverages both local telemetry data and global threat intelligence to provide contextual insights into security events. This helps SOC analysts understand the significance and potential impact of alerts, enabling them to focus on critical threats and ignore noise.
- **Automated Response and Remediation:** XDR automates predefined response actions, reducing manual effort for SOC (Security Operations Centre) analysts.
- **Unified Management and Investigation:** XDR provides a centralized console for managing and investigating security events. It allows SOC analysts to view alerts, events, and incidents from multiple sources in a centralized location. This unified approach streamlines the investigation process, enables efficient collaboration, and reduces the time spent on navigating disparate systems.

- **Integration with Existing SOC Components:** XDR integrates with SIEM and SOAR (Security Orchestration, Automation, and Response.) tools, enhancing the overall effectiveness of the SOC infrastructure.

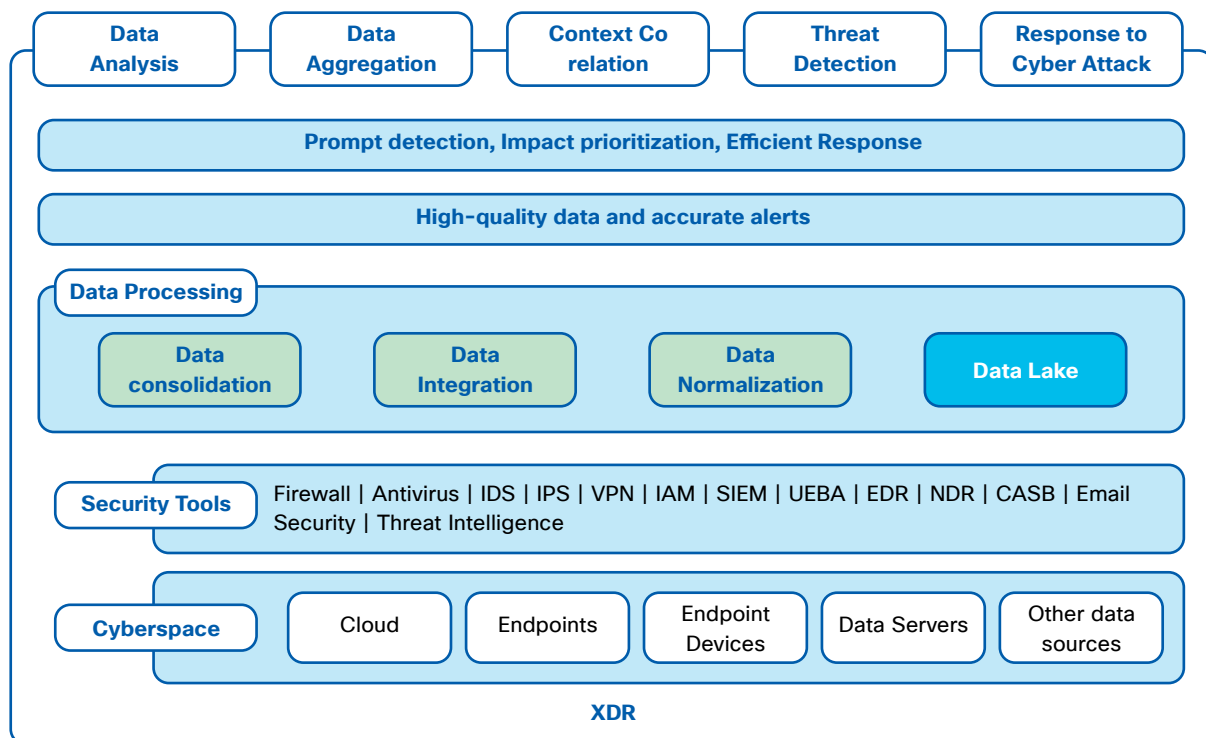
### How does XDR work?

XDR systems integrate multiple tools into a unified platform for the detection and response to security incidents. By collecting historical and real-time data from various levels of the enterprise infrastructure, including access points,

network layers, sandboxes, vulnerability scanners, cloud environments, mail traffic, access control systems, and DLP systems, XDR provides comprehensive control over potential attacks.

The collected information undergoes several stages:

Normalization based on predefined parameters, storage in a Data Lake, correlation, response, and, if needed, investigation. This streamlined process simplifies operations and enables efficient management of security incidents.



In the XDR framework, network security encompasses the monitoring, analysis, and response to network traffic to identify and address suspicious or malicious activities. It involves collecting and analysing network telemetry, such as network flow data, packet captures, and logs, in conjunction with endpoint telemetry to thoroughly detect and investigate security incidents.

By leveraging network visibility and telemetry data, XDR solutions have the

capability to uncover network-based attack patterns, lateral movement within the network, and command-and-control communications that may not be apparent when focusing solely on endpoint data. This expanded scope enhances the overall effectiveness of threat detection in XDR, enabling organizations to respond more efficiently to network breaches.

Recognizing the importance of both endpoint and network security, the



integration of these two components within XDR allows organizations to adopt a more comprehensive and robust approach to threat detection and response.

XDR harnesses the synergy of human reasoning and machine capabilities to make accurate and sophisticated decisions. It combines the functionalities ideally expected of SIEM tools such as telemetry integration, alert correlation, incident prioritization, as well as SOAR

tools such as automated triaging, investigation and response. Additionally, XDR integrates with underlying focussed detection and response platforms like EDR and NDR.

It's important to note that XDR does not replace existing security platforms such as SIEM or EDR; instead, it brings together multiple security products into a unified incident-response platform to up-level a SOC analyst.

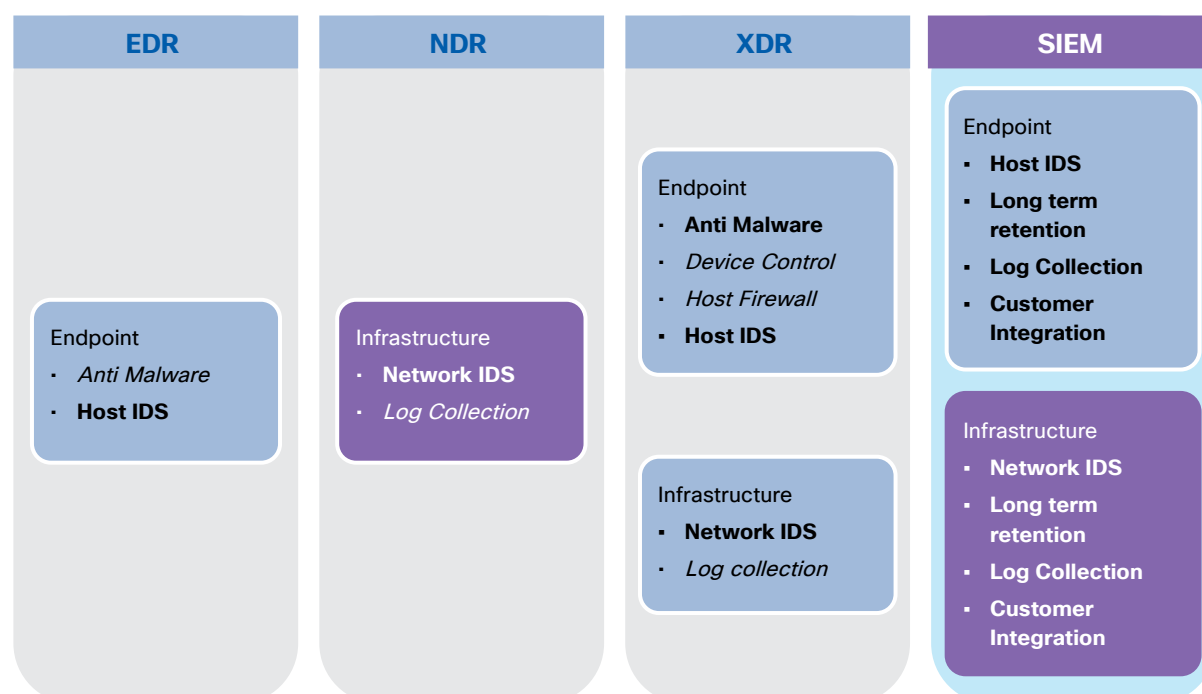


Figure 9: Primary elements of each toolset mapping similarities amongst them. Core components are emphasised, while additional features observed are indicated in italics across Endpoint (Servers & Systems) and Network (Cloud & Network)

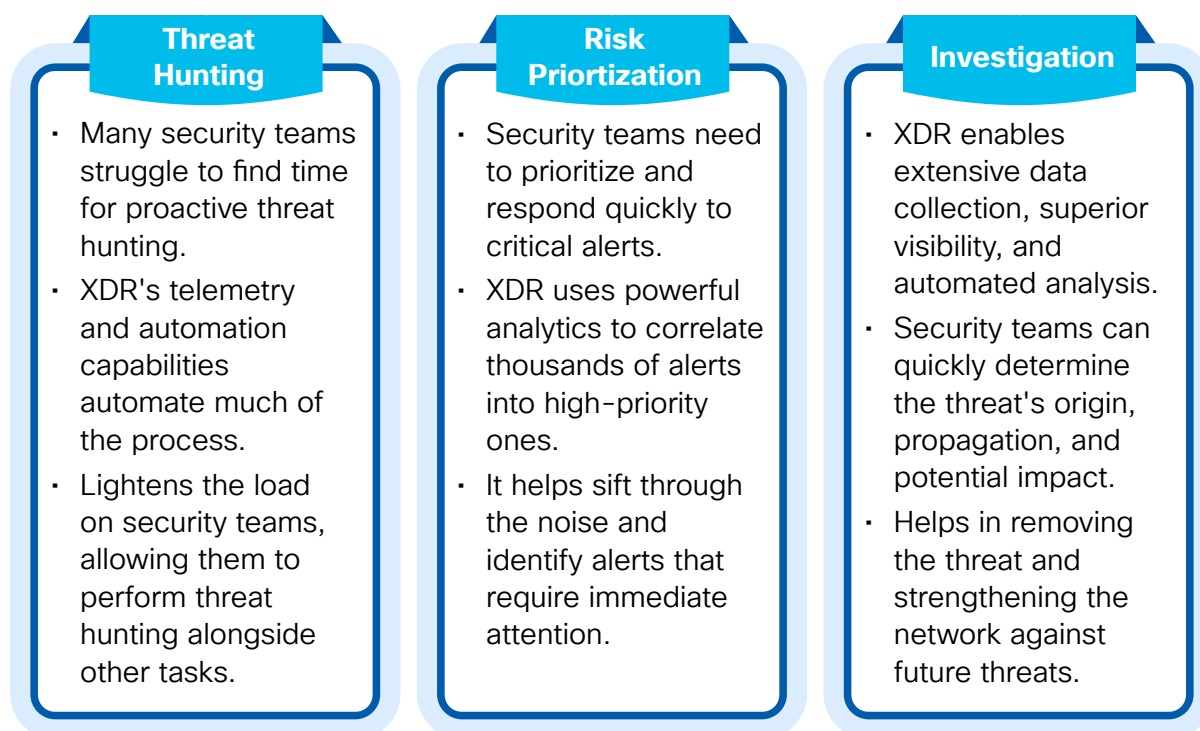
Traditional detection and response models are not enough to defend against sophisticated threats. Over 80% of organizations leverage more than 10 data sources for their security operations<sup>33</sup>. These models rely on individual security solutions that are often siloed and difficult to manage. This can lead to missed threats and slow response times.

SIEM and SOAR solutions have been developed to address these challenges, but they have not fully solved the problem. SIEM solutions can unify data from multiple sources, but they can be complex and difficult to use. SOAR solutions can automate security operations, but they can be expensive and require a lot of manual configurations<sup>33</sup>.

XDR is a new approach to threat detection and response that aims to bridge the gap between traditional models and SIEM/SOAR solutions. XDR provides comprehensive visibility across multiple

data sources and enables cohesive security operations. This allows security teams to quickly and confidently respond to threats.

### 10.3.1 XDR Use Cases



### 10.4 Market Considerations

XDR solutions are currently offered by security solution providers that offer a range of infrastructure protection products under a unified management platform, including EDR and network protection. However, there are market considerations and challenges that need to be addressed:

- **Deployment challenges:** Organizations currently rely on multiple point tools for different security aspects, which leads to a fragmented approach. For the long-term vision, the security teams need to embrace the emerging technologies and solutions for a unified approach to cybersecurity.
- **Integration with SOC:** Integration with existing security infrastructure can be

challenging for large enterprises that have already invested in establishing a SOC. Collaboration and integration with existing SOC components are more beneficial than competing with them.

- **MDR/MSSP services:** As threat detection and response become more complex, organizations are seeking external vendors to manage the entire process. XDR providers have the potential to complement their products by offering Managed Detection and Response (MDR) or Managed Security Service Provider (MSSP) services. They may also collaborate with existing MDR/MSSP services to provide a comprehensive security solution to organizations.



# Conclusion

---



The rapidly evolving ICT-driven world presents significant cybersecurity challenges, driven by the migration to the cloud and increased reliance on technology. These developments have created opportunities for organizations, but they have also heightened the risks of cyber threats. The shortage of skilled cybersecurity professionals further compounds the problem, leaving organizations vulnerable to attacks. The rise of connected devices and the shift to a hybrid workforce introduce additional weak points for cybercriminals to exploit. Geopolitical conflicts and the global landscape have also contributed to the increase in cyberattacks.

In the Indian context, digitalization efforts have brought remarkable progress but have also exposed vulnerabilities to cyber threats. Establishing efficient incident response capabilities and adopting a proactive approach to cyber defence is paramount to function in a cyber compliant environment. Adhering to these regulations and investing in technological capabilities are



necessary steps. The role of the Chief Information Security Officer (CISO) is particularly important in maintaining network security, developing cybersecurity strategies, and establishing incident response plans to foster a culture of cyber resilience.

XDR offers a comprehensive security approach that extends beyond endpoints, safeguarding the entire enterprise infrastructure. This includes network layers, virtual devices, and hybrid clouds, providing robust protection against the complexities.

XDR's multifunctional analytical engine and investigation tools enhance its

effectiveness in detecting and responding to incidents. Integration with other systems like SIEM, SOAR, DLP, IAM/IDM, UEBA, SASE, and CASB further enriches XDR's capabilities. The integration of machine learning and automation within XDR systems lightens the workload of security administrators, leading to improved overall efficiency.

The future of XDR looks promising as it aligns with the global trend of centralizing and consolidating security tools for efficient operations. Building upon the foundation of EDR products, XDR represents a logical progression in the ever-evolving security landscape.

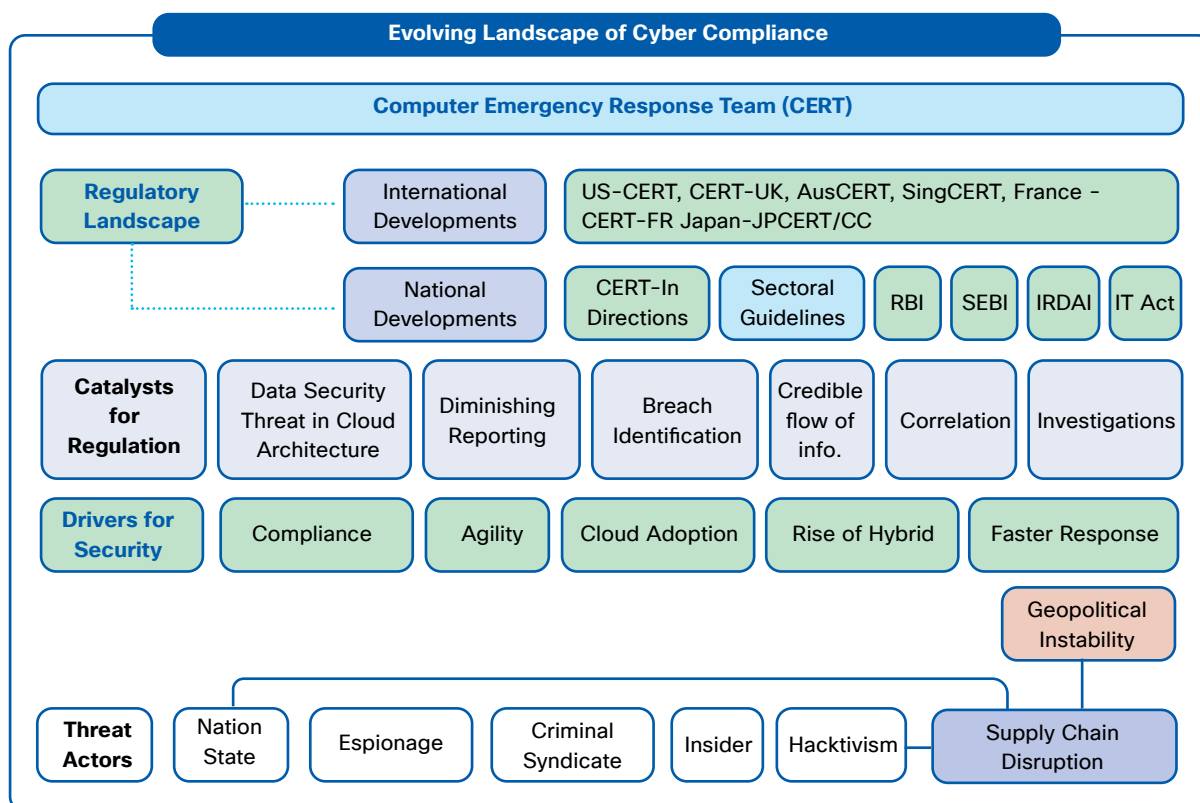


# Encapsulate

The figure below provides an overview of the evolving landscape of cyber compliance. The lower layer of the framework focuses on the rise of sophisticated cyber threat actors amid growing geopolitical instability, leading to supply chain disruptions. Building upon this, the framework emphasizes the drivers that propel organizations to enhance their capabilities in key areas like threat intelligence, risk assessment, visibility, and threat analysis to strengthen their defence.

This transformation is fuelled by the urgent need for agility and prompt response.

On top of these layers, there are factors that drive the necessity for regulations. The framework outlines the cybersecurity regulations introduced by governmental bodies globally to enhance their cybersecurity posture and ensure greater compliance with established cybersecurity standards. It calls for approaches to build effective cyber incident response capabilities.



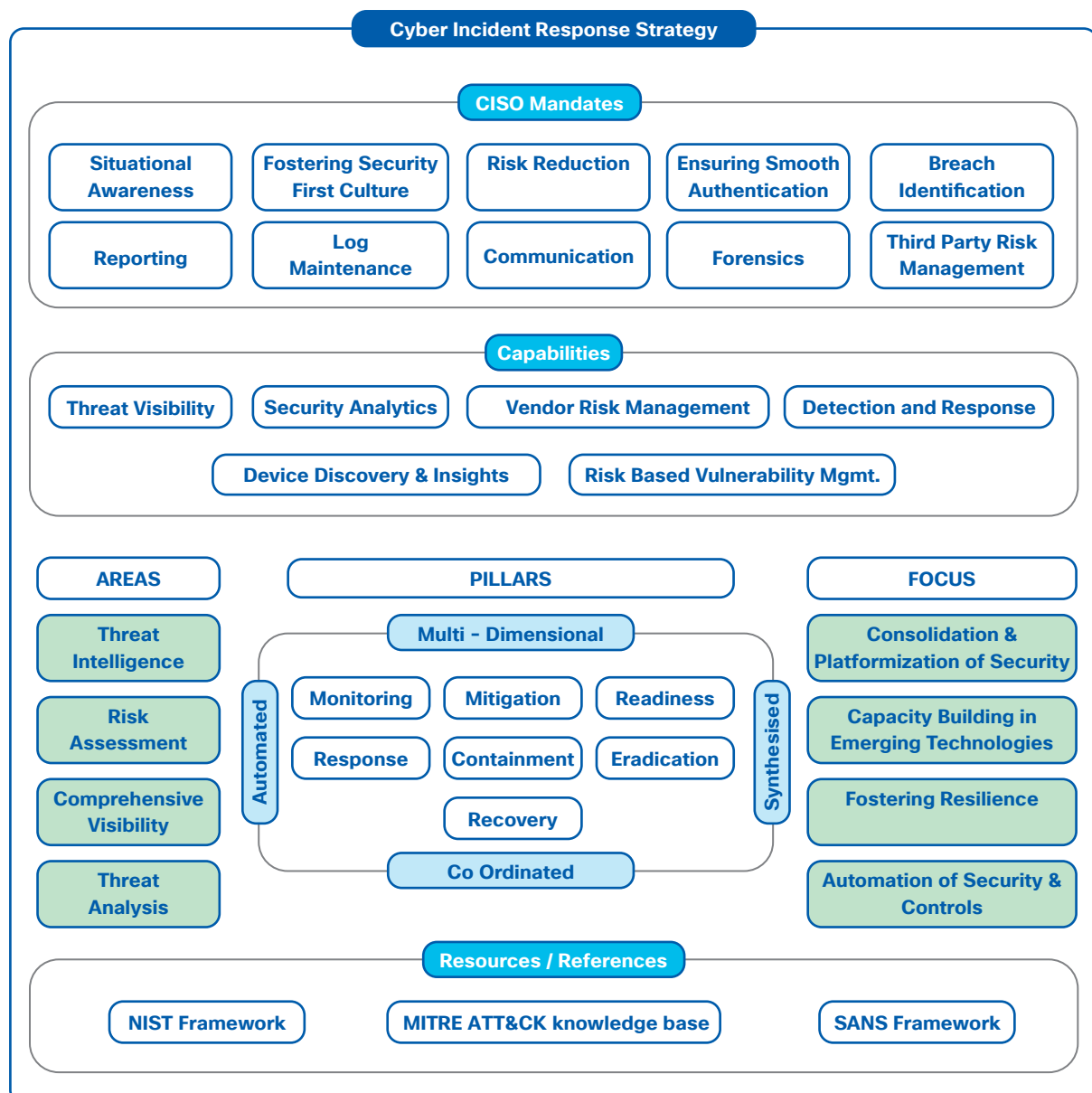
## Cyber Incident Response Strategy

The proposed encapsulate provides a comprehensive framework for cyber incident response strategy offering a deeper and overarching understanding of the theme. It serves as a valuable resource for enterprises seeking to enhance their incident response capabilities.

The framework consists of three layers. The top layer highlights the CISO mandates in navigating the ever-changing cybersecurity landscape. The second layer outlines the essential capabilities that

organizations should possess to effectively mitigate the repercussions and aftermath of cyber incidents. The bottom layer identifies key areas that require the CISO's attention and focus for strengthening their competencies.

At the core of the encapsulate lies the pillars of a robust cyber incident response plan: multi-dimensional, synthesized, automated, and coordinated response. These pillars form the foundation for an effective and efficient incident response strategy.



# Annexure

---

## 13.1 Cyber Kill Chain [Phases of Cyber Attack]

The seven steps of the Cyber Kill Chain are an intelligence-driven approach to intrusion detection. In the case of an incident, an adversary must move through every phase of the attack lifecycle to be successful and exploit vulnerabilities to install malware and take active control of the system.

The dissection of the stages provided by the Cyber Kill Chain improves the visibility of an incursion and aids security teams in comprehending the strategies, tactics, and practices of an adversary. The steps come together to produce a chain-like integrated end-to-end process and are conceptualized to reveal the active state of a data breach. As each stage requires

specific instrumentation to detect cyber attacks, effective coordination between people, processes, and technology is indispensable to prevent the cyber-attack life cycle.

Mapping each step involved in the cyber kill chain against the preventive controls can help organisation to:

- Make optimal investment decisions to prepare, plan, recover, and reconstitute their assets in the case or aftermath of an attack.
- Mapping the organization's defensive tools and capabilities across the cyber-attack lifecycle while adopting a threat-based strategy.
- Effectively respond to a cyber-attack on a real-time basis.

The steps come together to produce a chain-like integrated end-to-end process and are conceptualized to reveal the active state of a data breach.

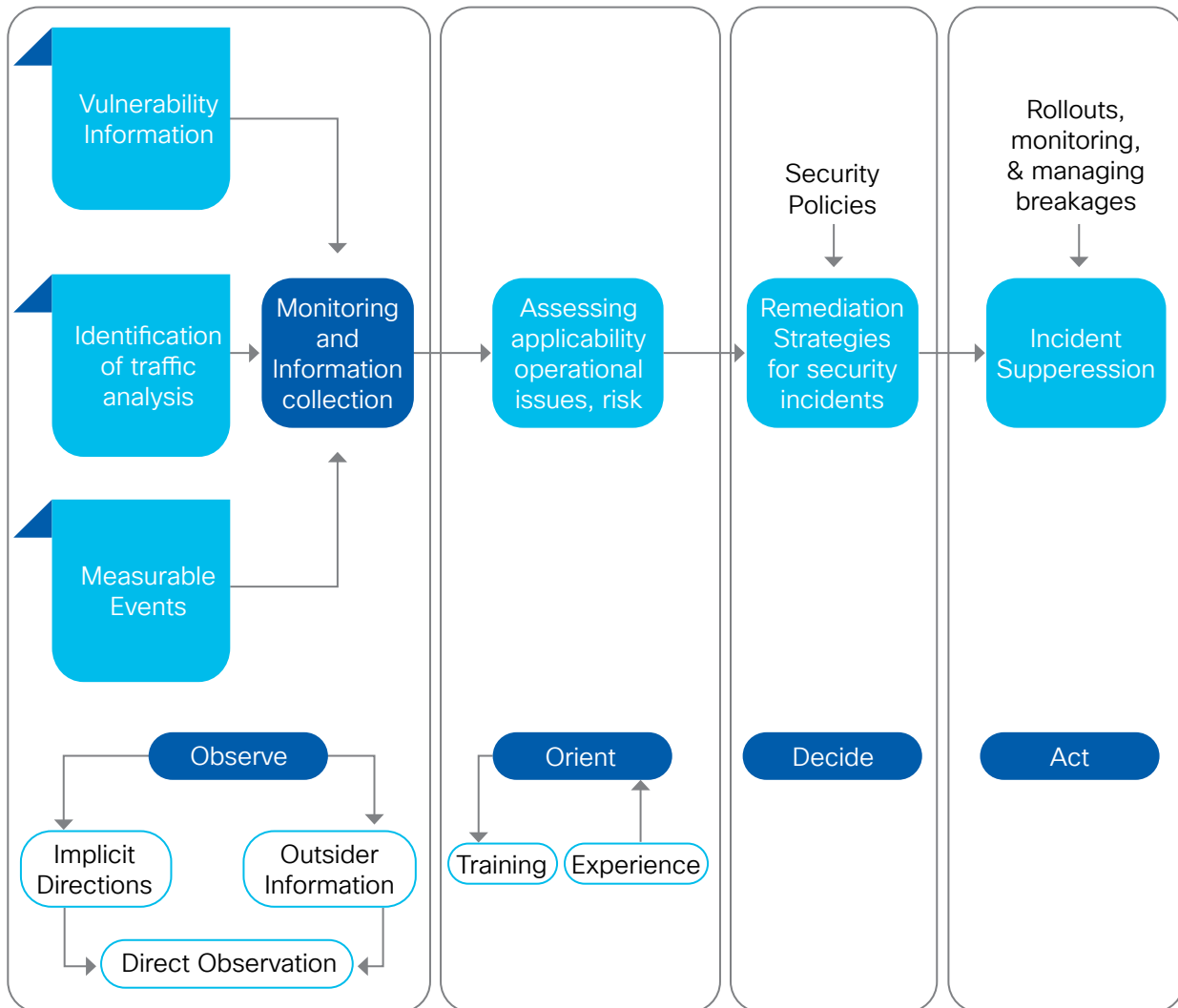
---



Stage	Prevention Controls	Security Controls
<p><b>1. Reconnaissance:</b></p> <p>Gathering information about the target.</p> <ul style="list-style-type: none"> <li>▪ <b>Passive Reconnaissance:</b></li> </ul> <p>Information gathered by indirect and publicly available sources.</p> <ul style="list-style-type: none"> <li>▪ <b>Active Reconnaissance:</b></li> </ul> <p>Active interaction with the target. The cyber adversary initiates to scrutinize the network for open ports and maps the vulnerabilities for exploitation from a system and human perspective.</p>	<p>Implementing strong access controls, monitoring network activity for suspicious behaviour, host sweeps and using web filtering to block access to known malicious sites.</p>	<p><b>Detect:</b> Web Analytics, Threat Intelligence, NIDS</p> <p><b>Deny:</b> Information sharing policy, Firewall ACLs</p>
<p><b>2. Weaponization: "Exploiting the weakness."</b></p> <p>The hacker creates strategies to enter the target's network using the previously collected information.</p> <p>Distribution of spear phishing emails, creation of "watering holes" for transmission of malware is observed as a common practice.</p>	<p>Using advanced threat detection tools to identify and block weaponized payloads.</p> <p>Using email security filters to block malicious attachments and implementing software and application whitelisting to prevent unauthorized software from executing.</p>	<p><b>Detect:</b> Threat Intelligence, NIDS.</p> <p><b>Deny:</b> NIPS.</p>
<p><b>3. Delivery</b></p> <p>The attacker determines the pathway to transmit malicious payloads or weapons based on the reconnaissance phase.</p> <p>They may use automated tools like exploit kits, spear phishing attacks using malicious links or attachments, and malvertising as some of their techniques.</p>	<p>Creating user awareness, inducting security training, and conducting phishing campaigns that introduce best security practices.</p> <p>Establishing security controls against perimeter breaches by blocking malicious or risky websites via URL filtering.</p>	<p><b>Detect:</b> Endpoint malware protection.</p> <p><b>Deny:</b> Change. Management, Application Whitelisting, Proxy Filter, HIPS.</p> <p><b>Disrupt:</b> Inline AV.</p> <p><b>Degrade:</b> Queuing.</p> <p><b>Contain:</b> Router ACLs, App aware firewall, trust zones, Inter-zone NIPS.</p>
<p><b>4. Exploitation</b></p> <p>The hacker starts to reap the benefits of preparing and delivering the attack. It can sprout as SQL injection, buffer overflow, malware, etc.</p> <p>The hacker investigates the targeted network to understand better its traffic patterns, the systems connected to it, and potential vulnerabilities.</p>	<p>Once the attacker has breached the host, there are very few defence mechanisms. As the final line of security against exploit attempts, techniques like data execution prevention and anti-exploit are leveraged.</p> <p>Tools used after an infection rely on defence mechanisms like sandboxes to find already-used exploits.</p>	<p><b>Detect:</b> Endpoint malware protection, HIDS.</p> <p><b>Deny:</b> Secure password, Patch management.</p> <p><b>Disrupt:</b> DEP.</p> <p><b>Contain:</b> App aware firewall, trust zones, Inter-zone NIPS.</p>

Stage	Prevention Controls	Security Controls
<b>5. Installation</b> The attacker ensures continued access to the network.	Preventive controls at this stage include using antivirus and endpoint protection tools to detect and block malware, implementing application and software whitelisting to prevent unauthorized software from executing, and monitoring network activity for suspicious behaviour.	<b>Detect:</b> Endpoint malware protection, HIDS. <b>Deny:</b> Privilege Separation, strong passwords, multi-factor authentication. <b>Disrupt:</b> Router ACLs. <b>Contain:</b> App aware firewall, trust zones, Inter zone NIPS.
<b>6. Command and Control</b> Once malware has been installed, the attackers control the connection between the compromised machine and their malicious infrastructure. To communicate and transfer data between the infected devices and their own infrastructure, the attackers will set up a command channel.	Block upload of files and data patterns as well as outgoing command-and-control connections. Use internal sinkholes to divert malicious outward communication in order to locate and shut down compromised hosts. Deploy URL filtering to prevent outbound communication to known dangerous URLs. Compile a list of nefarious domains to ensure widespread detection and prevention via DNS monitoring. Implementing granular application control to enable only authorized applications can prevent attackers from moving laterally with unidentified tools and scripts.	<b>Detect:</b> NIDS, HIDS. <b>Deny:</b> Network Segmentation, Firewall ACLs. <b>Disrupt:</b> HIPS. <b>Degrade:</b> Tarpit. <b>Deceive:</b> DNS Redirect. <b>Contain:</b> Trust Zones, DNS Sinkholes.
<b>7. Action on the objective</b> The adversaries act as per their motivations to accomplish their purpose as they have control, persistence, and ongoing contact. This could be done to extort money, exfiltrate data, destroy vital infrastructure, deface web property, or incite terror.	To implement the proper prevention-based controls, create links between the Network Operations Centre (NOC) and the Security Operations Centre (SOC). Implementing data loss prevention tools to prevent exfiltration of sensitive data, monitoring network activity for suspicious behaviour, and regularly backing up critical data to ensure its availability in the event of a cyber attack.	<b>Detect:</b> Endpoint malware protection. <b>Deny:</b> Data at rest (Encryption). <b>Disrupt:</b> Endpoint malware detection. <b>Degrade:</b> Quality of service <b>Deceive:</b> Honeypot. <b>Contain:</b> Incident Response.

## 13.2 OODA Loop In Cyber Incident Response



## Observe

The Observe phase of the OODA loop involves ongoing monitoring and data collection of computer networks and information systems. This includes identifying vulnerabilities, analysing network traffic, identifying hosts, and observing measurable events like intrusion detection alerts. The monitoring process utilizes security monitoring tools to identify unusual behaviour that may necessitate further investigation.

**Tools:** Log Analysis, SIEM Alerts, IDS Alerts, Traffic Analysis, Netflow tools, vulnerability analysis, and Application performance monitoring, among others, can be utilized to document observations

about network and business operations for efficient defence and response.

## Orient

The Orient phase of the OODA loop is considered the most crucial stage. During this phase, data is analyzed and synthesized through alert correlation and other methods. A comprehensive visualization of the network situation can be highly beneficial for human analysts. This information can then be utilized to tailor defence strategies against the latest attack tools and tactics.

**Tools** such as Incident Triage, Situational Awareness, Threat Intelligence, Security, and Research, can help gain insight into the attacker's mindset.

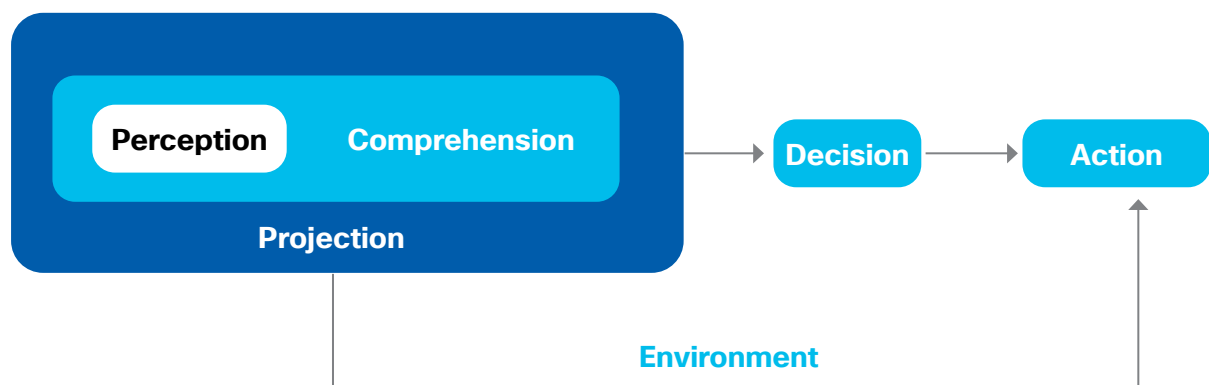


Figure 10: Three level model of situational awareness

**Considerations:** It is vital to ensure that Threat Intelligence feeds security monitoring tools, providing the right information and context for effective threat detection and response.

## Decide

The initial two stages of the OODA loop aim to position the analyst appropriately to prepare for the decide phase. This phase involves making a decision by weighing the need for prompt action against the

requirement for informed choices based on the data collected in the Observe and Orient stage.

During the Decide phase, the observations and context gained from the previous stages guide the decision-making process. It is essential to document all aspects of the Incident Response process, with attention given to communication regarding data collection and decision-making procedures.



**Tools:** Organisation's security policies and documentation.

## Act

Taking immediate action after making a decision is essential within the OODA loop framework. The objective of this approach is to enable rapid decision-making and confuse the adversary. If too much time is spent analysing a decision before acting, it increases the likelihood that the adversary will act swiftly and make the decision irrelevant. Therefore, quick action and a return to the Observation phase is necessary to learn about the adversary based on reactions to previous actions.

After taking the action, remediation and recovery are essential, and it is critical to improve the incident response procedures based on lessons learned. Constantly improving the ability to act effectively during incidents is key to success.

**Tools:** Data capture tools, forensics analysis tools, system backup and recovery tools, patch management, and other systems management tools can aid in this process.

**Considerations:** It is crucial to understand that the iteration through the OODA loop is a mental process that should be performed by a human operator. Therefore, the toolset is designed to assist the operator, not replace the decision-making process. The tools provide information and enable actions, but the incident handler retains responsibility for the decisions and actions taken.

## 13.3 Cybersecurity Incident Guidelines Across Geographies

### India

#### IT Act (2008): Origin & Extensions

**Section 70B:** It mandates all organizations and businesses to report any cyber

incident or breach that affects their computer resources to the Indian Computer Emergency Response Team (CERT-In) in a timely manner. This reporting requirement applies to all organizations (service providers, intermediaries, data centres, bodies corporate and government organisations), whether they are owned by the government or private entities. The CERT-In directions are an extension of the IT Act.

#### CERT-In Directions:

**Scope of Applicability:** Service providers, intermediaries, data centres, body corporate, Virtual Private Servers (VPS), cloud service providers, Virtual Private Network Service (VPN) providers, and government organizations, are subject to these regulations.

The regulations apply to all types of ICT environments, whether they are on-premises systems or systems managed by third-party providers, hosted on the cloud, or located in data centres.

#### Directions:

- **Incident Reporting:** It is mandatory for organizations to report cyber incidents within 6 hours of being informed about them. If requested, organizations should also provide information about the steps taken to protect and prevent further incidents.
- **PoC Appointment:** Organizations are required to provide a Point of Contact (PoC) for communication with CERT-In, who should be available and responsive to ensure prompt and effective incident response.
- **Log Maintenance & Time synchronization:** Organizations must maintain logs of all ICT systems securely for 180 days and connect to NTP server of the NIC or NPL, or NTP

servers that can be traced back to these servers, to synchronize the clocks of all ICT systems. This is to ensure that the logs can be correlated consistently & reliably.

- **Customer information:** Network service providers, data centres, VPS providers, cloud service providers, and VPN service providers are required to register precise details of authenticated subscribers/customers and maintain it for at least five years after cancellation or withdrawal of the registration.
- **KYC Requirements:** Virtual asset exchange providers, virtual asset service providers, and custodian wallet providers must keep all information collected during the Know Your Customer (KYC) process, including financial transaction records, for a period of five years.

**Intermediaries:** *It mandates intermediaries to report any security breaches to CERT-In as part of their due diligence obligations. CERT-In provides templates for reporting cybersecurity incidents on its website, which includes various details such as the time of occurrence, the type of incident, impacted systems or network information, symptoms observed, technical systems deployed, actions taken, and other pertinent information.*

### Sector specific regulations:

#### RBI: “Cybersecurity Framework for Banks”

- Requires prompt reporting of any cybersecurity incident, successful or attempted, within 2-6 hours, with details in a standard template.
- RBI prescribes measures such as incident reporting mechanisms, cyber crisis management plan, system

surveillance, and customer data protection to be established to mitigate risks.

- Payment aggregators under the “Guidelines on Regulation of Payment Aggregators and Payment Gateways” must have a board-approved information security policy in place to secure payment systems.
- Banks must have a written incident response program, Cybersecurity policy, and crisis management plan to handle cyber threats, with mandatory reporting of cyber-breach incidents within 2-6 hours.
- RBI mandates the appointment of a CISO and security steering committee to report incidents to the head of risk management.
- Periodical vulnerability assessment and penetration testing exercises are required for all critical systems in banks.
- RBI prescribes conducting due diligence, audits, and regular monitoring of vendors and service providers.
- Board of directors to be held accountable for the overall information security governance framework.
- Appropriate training and awareness of cybersecurity policies and programs must be provided to human resources.

#### Telecom Sector: Telecom Regulatory Authority of India

Every telecommunication licensee is required to create a monitoring facility to detect intrusions, attacks, and frauds on their technical systems within a year of authorization. They must also report any such occurrences to the Department of Telecommunications.

## **SEBI- “Cybersecurity & Cyber Resilience Framework”**

The framework proposes a five-step approach to manage Cybersecurity risks related to IT assets, processes, networks, and systems:

- Identify critical IT assets and associated risks.
- Protect assets with suitable controls and measures.
- Detect incidents, anomalies, and attacks with monitoring tools/ processes.
- Respond promptly to incidents, anomalies, or attacks.
- Recover from incidents using incident management, disaster recovery, and business continuity framework.

Stockbrokers and depository participants are required to ensure that records of user access to critical systems are identified and logged for audit and review purposes, and the logs should be maintained and stored in a secure location for a period of not less than two years.

SEBI has also established deadlines (within 6 hrs) for reporting cyber attacks and requested that portfolio managers submit quarterly reports on cyber incidents, breaches, and mitigation measures taken within 15 days of the end of each quarter.

## **Insurance Sector: IRDA “Guidelines on Information and Cybersecurity”**

The guidelines are applicable to all insurers, insurance intermediaries, and other entities regulated by IRDAI. Regulated entities are obligated to promptly report any cyber incidents to CERT-In within six hours of their detection. Additionally, they are required to submit the relevant information regarding these

incidents to the authority within 24 hours of being notified. Furthermore, if any subsequent forensic analysis uncovers additional findings, these details must be updated and submitted to the authority within 24 hours of their availability.

Alongside these reporting requirements, the guidelines specify that registered insurance companies must maintain security logs for a minimum of six months, implement an incident management system that includes incident reporting and recording, and establish an incident response plan.

## **Consequences of Non-Compliance [Under IT Act]:**

- **Section 43A of the IT Act, 2000:** Any company that fails to protect sensitive personal information from unauthorized access or disclosure may be liable to pay compensation to the affected individuals. The compensation may extend up to 5 crore (approximately USD 675,000) or more, depending on the damages suffered.
- **Section 72A of the IT Act, 2000:** Any person or entity that discloses personal information in breach of a lawful contract or without the consent of the individual concerned may face imprisonment up to 3 years or a fine up to 5 lakh (approximately USD 6,700) or both.
- **Section 70B of the IT Act, 2000:** Provides for the punishment of a person who fails to comply with CERT-In. Any person who contravenes the provisions of this section shall be punished with imprisonment for a term which may extend to one year or with a fine which may extend to one lakh (approximately USD 1,350), or both.

In addition to the legal penalties, non-compliance with CERT-In may also result in reputational damage and loss of trust from customers and partners.

**Table 2: Comparison of Sectoral Cyber Incident Guidelines in India**

Guidelines	RBI	SEBI	IRDA
Establishment of Incident Response Plan/ Mechanisms	✓	✓	✓
CISO Appointment to oversee cyber incidents	✓	✓	✓
Audit Mechanisms, Due Diligence & Monitoring of Vendors	✓	✓	✓
Maintenance, Monitoring & Audit log analysis	✓	✓	✓
Conduction of vulnerability assessment and penetration testing exercises	✓	✓	✓
Need or board-approved cybersecurity policy	✓		✓
Training and awareness of cybersecurity policies for human resources	✓		✓

## Power Sector

The Ministry of Power has established a Computer Emergency Response Team (CERT) to address cybersecurity risks within power systems. Additionally, four subsidiary CERTs have been created to work with power utilities in transmission, thermal, hydro, and distribution coordination. It require intermediaries to notify CERT-In of any cyber incidents.

### Singapore

In case of a data breach which is not contained within the organization involving personal data and has caused/may cause significant harm involving/likely to involve more than 500 people mandates a notification to Singapore Personal Data Protection Commissioner as soon as practicable and within 3 calendar days and as soon as practicable to the individuals under s26D (5) PDPA (Personal Data Protection Act).

Singapore Computer Emergency Response Team (SingCERT) has established incident reporting timelines for organizations to follow when reporting cybersecurity incidents.

### Financial Sector- Monetary Authority of Singapore:

Financial institutions operating in Singapore are required to inform the Monetary Authority of Singapore (MAS) within **one hour** of discovering a severe incident that has a widespread impact on their operations or materially affects their customers, regardless of when the incident occurred.

### Critical Infrastructure:

Companies identified as critical information infrastructure providers are obliged to report any prescribed cybersecurity incident to the Commissioner of Cybersecurity **within two hours** of becoming aware of it, under section 7 of the Cybersecurity Act 2018.



**Other Establishments:** All entities are also required to report data breaches that are likely to result in significant harm or scale to Singapore's Personal Data Protection Commission in **24 hours**.

**Consequences of Non-Compliance:** It can lead to organizational fines of up to \$1 million SGD or 10% of the organization's annual turnover in Singapore (whichever is higher).

### United States of America-CIRCI

The Cyber Incident Reporting for Critical Infrastructure Act, 2022 (CIRCI) is a significant legislation similar to the CERT-In Rules 2022. It mandates owners of critical infrastructure<sup>34</sup> to inform the Cybersecurity and Infrastructure Security Agency (CISA) about cyber attacks that result in unauthorized access or disruption of business or industrial operations. CIRCI requires covered entities to report certain types of cyber incidents to CISA within 72 hours of reasonably believing that the incident has occurred. In the case of ransomware payments, they must be reported within **24 hours** of payment being made.

### Australia - SOCI Act

The Security of Critical Infrastructure Act 2018 (SOCI Act) in Australia categorizes various assets as critical. Regulated entities are required to report Cybersecurity incidents to the Australian Cybersecurity Centre (ACSC).

- **Critical Assets:** If a regulated entity experiences a critical cybersecurity incident that has had or is likely to have a relevant impact on its assets, it must verbally notify the ACSC within **12 hours** of becoming aware of the incident, followed by a written report within **84 hours**.
- **Non-critical assets:** For cybersecurity incidents, the reporting timeline is

within **72 hours** of becoming aware of the incident, with a written record following verbal notification within **48 hours**.

- **Consequences of Non-Compliance:** If an organization fails to report eligible data breaches or comply with the requirements related to notifying individuals and the Australian Information Commissioner (OAIC), they may face civil penalties of up to AUD 2.1 million per breach.

### United Kingdom - NIS Regulations

Digital service providers such as online search engines, online marketplaces, and cloud computing services have an obligation to report cyber incidents that have a significant impact to the Information Commissioner's Office (ICO) within **72 hours**, including data breaches. This reporting requirement applies to all entities.

**Financial sector:** Entities under the regulation of the Financial Conduct Authority (FCA) must report material cyber incidents to the authority as soon as they become aware of them. The determination of material cyber incidents is based on specific criteria, and if they meet these criteria, they must be reported immediately\* to the FCA.

**Consequences of Non-Compliance:** Under the General Data Protection Regulation (GDPR), organizations can face fines of up to £17.5 million or 4% of their annual global turnover (whichever is greater) for failing to report a data breach within the prescribed timelines.

### European Union: GDPR/ CERT-EU

General Data Protection Regulation (GDPR) mandates data controllers must report personal data breaches to the supervisory authority within **72 hours** of becoming aware of the breach.

*\*"Immediate" is subjective and depends on the nature and severity of the incident.*

CERT-EU (Computer Emergency Response Team for the European Union) is responsible for handling cybersecurity incidents that affect the IT systems and networks of the EU institutions, agencies, and bodies. However, it does not impose reporting timelines for other organizations.

**Consequences of non-compliance:**

Under the General Data Protection

Regulation (GDPR), organizations can face fine of up to €20 million or 4% of the global annual turnover, whichever is greater, for failing to report a personal data breach or for delaying reporting without a valid reason. Additionally, failing to comply with the NIS Directive can result in administrative fines or penalties imposed by national authorities.

# References

---

- <sup>1</sup> Drew Todd, 'Ponemon Institute: Cost of Data Breach Hits Record High' <<https://www.secureworld.io/industry-news/cost-of-a-data-breach>>
- <sup>2</sup> 'Cost of a Data Breach 2022 | IBM' <<https://www.ibm.com/reports/data-breach>>
- <sup>3</sup> 'Cost of a Data Breach 2022 | IBM'
- <sup>4</sup> Compliancy Group, 'How to Limit the Cost of Data Breaches', Compliancy Group, 2019 <<https://compliancy-group.com/how-to-limit-cost-of-data-breach/>>
- <sup>5</sup> '2022 Data Breach Investigations Report', Verizon Business <<https://www.verizon.com/business/resources/reports/dbir/>>
- <sup>6</sup> 'Incident-Response-Planning-Infographic.Pdf' <<https://www.cisco.com/c/dam/en/us/products/collateral/security/incident-response-planning-infographic.pdf>>
- <sup>7</sup> 'CISCO\_Security\_eBook\_Digi.Pdf' <[https://www.cisco.com/c/dam/m/en\\_be/offers/security/CISCO\\_Security\\_eBook\\_Digi.pdf](https://www.cisco.com/c/dam/m/en_be/offers/security/CISCO_Security_eBook_Digi.pdf)>
- <sup>8</sup> 'Cost of a Data Breach 2022 | IBM'
- <sup>9</sup> 'India Witnessed 13.9 Lakh Cybersecurity Incidents In 2022: Govt' <<https://inc42.com/buzz/india-witnessed-13-9-lakh-cybersecurity-incidents-in-2022-govt/>>
- <sup>10</sup> 'Global Average Cost of a Data Breach 2022', Statista <<https://www.statista.com/statistics/987474/global-average-cost-data-breach/>>
- <sup>11</sup> Business Standard, 'Cost for Data Breaches Averaged Rs 17.6 Cr in 2022, Highest Ever: IBM Study', 2022 <[https://www.business-standard.com/article/companies/cost-for-data-breaches-averaged-rs-17-6-cr-in-2022-highest-ever-ibm-study-122072701127\\_1.html](https://www.business-standard.com/article/companies/cost-for-data-breaches-averaged-rs-17-6-cr-in-2022-highest-ever-ibm-study-122072701127_1.html)>
- <sup>12</sup> '(ISC)2 2022 Cybersecurity Workforce Study' <<https://www.isc2.org:443/Research/Workforce-Study>>
- <sup>13</sup> Urvi Malvania and Veena Mani, 'Shortage of Cybersecurity Professionals Triggers Fight for Talent', The Economic Times, 30 March 2023 <<https://economictimes.indiatimes.com/jobs/mid-career/shortage-of-cybersecurity-professionals-triggers-fight-for-talent/articleshow/99116296.cms?from=mdr>>
- <sup>14</sup> 'Cyber Attacks: Cyber Attacks Triple in Last Three Years, but Security Funds Underutilised - The Economic Times' <<https://economictimes.indiatimes.com/tech/technology/cyber-attacks-triple-in-last-three-years-but-security-funds-underutilised/articleshow/95981111.cms?from=mdr>>
- <sup>15</sup> 'Products - XDR Buyer's Guide - Cisco' <<https://www.cisco.com/c/en/us/products/collateral/security/securex/xdr-buyer-guide.html>>
- <sup>16</sup> 'IoT Connected Devices Worldwide 2019-2030', Statista <<https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/>> [accessed 1 December 2022].
- <sup>17</sup> 'IBM X-Force Threat Intelligence Index 2022', SecurityHQ <<https://www.securityhq.com/reports/ibm-x-force-threat-intelligence-index-2022/>>
- <sup>18</sup> Refer to the figure for the detailed bifurcation of cyber threat actors.
- <sup>19</sup> 'India: Number of Online Services Provided by the Government 2021 | Statista' <<https://www.statista.com/statistics/1170639/india-number-of-online-services-provided-by-the-government/>>

<sup>20</sup> 'India: Number of Active Internet Users 2025 | Statista' <<https://www.statista.com/statistics/1257929/india-number-of-active-internet-users/>>

<sup>21</sup> 'Cyber Attacks on Healthcare Sector Rising', BusinessLine, 2022 <<https://www.thehindubusinessline.com/opinion/cyber-attacks-on-healthcare-sector-rising/article66278678.ece>>

<sup>22</sup> Business Standard, 'Private Banks Reported Most Data Breaches in 2018-22: Parliament Told', 2022 <[https://www.business-standard.com/article/companies/private-banks-reported-most-data-breaches-in-2018-22-parliament-told-122080201419\\_1.html](https://www.business-standard.com/article/companies/private-banks-reported-most-data-breaches-in-2018-22-parliament-told-122080201419_1.html)>

<sup>23</sup> Refer to table below for the Cyber incident and breach notification timelines across jurisdiction

<sup>24</sup> Refer to annexure for detailed guide to cybersecurity regulation across jurisdictions.

<sup>25</sup> 'Cert-In - Home Page' <<https://www.cert-in.org.in/SecurityIncident.jsp>>

<sup>26</sup> Refer annexure for a detailed view for the CERT-In directions along with the sectoral regulations.

<sup>27</sup> Considerations: Employee awareness and training: All employees should receive training on cybersecurity best practices and should be aware of their role in incident response procedures. This can help ensure that incidents are detected and reported quickly, reducing the potential impact of a breach.

<sup>28</sup> Indicative

<sup>29</sup> Refer to annexure for more details.

<sup>30</sup> Refer to annexure for more details.

<sup>31</sup> 'Cybersecurity Readiness Index', Cisco <[https://www.cisco.com/c/m/en\\_us/products/security/cybersecurity-reports/cybersecurity-readiness-index.html](https://www.cisco.com/c/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index.html)>

<sup>32</sup> Jon Oltsik, 'ESG Research Report: SOC Modernization and the Role of XDR' <<https://www.esg-global.com/research/esg-research-soc-modernization-and-the-role-of-xdr>>

<sup>33</sup> Oltsik.

<sup>34</sup> CIRCIA's definition of "covered critical infrastructure" is broad and encompasses businesses that may not perceive themselves as providers of critical infrastructure.



## Authors:

- Vinayak Godse, CEO, DSCI.
- Aditya Bhatia, Senior Consultant, DSCI.
- Neha Mishra, Associate, Technical Research, DSCI.

## Acknowledgement:

- K.P.M. Das, National Cybersecurity Officer, Cisco.
- Aditya Raghavan, Cybersecurity Solutions Architect, Threat Detection & Response APJC, Cisco.
- Bhishm Narayan Sharma, Technical Solutions Architect, Cisco.

[illegible]





Cisco (NASDAQ: CSCO) is the worldwide technology leader that securely connects everything to make anything possible. Our purpose is to power an inclusive future for all by helping our customers reimagine their applications, power hybrid work, secure their enterprise, transform their infrastructure, and meet their sustainability goals. Discover more on The Newsroom and follow us on Twitter at @Cisco.

Cisco offers an industry-leading portfolio of technology innovations. With networking, security, collaboration, cloud management, and more, we help to securely connect industries and communities. Read more about our products and services here.



Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by nasscom, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI brings together governments and their agencies, industry sectors including ITBPM, BFSI, telecom, industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit [www.dsci.in](http://www.dsci.in)

## DATA SECURITY COUNCIL OF INDIA

Nasscom Campus, Fourth Floor, Plot. No. 7-10, Sector 126, Noida, UP - 201303

☎ +91-120-4990253 | ✉ [research@dsci.in](mailto:research@dsci.in) | 🌐 [www.dsci.in](http://www.dsci.in)

🐦 DSCI\_Connect    **f** dsci.connect    📺 dsci.connect    **in** data-security-council-of-india    **YouTube** dscivideo

All Rights Reserved © DSCI 2023