



***ENGAGE.  
INNOVATE.  
SCALE.***

***MCR HRD***



# Top 10 Global Risks - Allianz Risk Barometer

CYBERSECURITY CENTRE of EXCELLENCE  
A joint initiative of DSCI & Government of Telangana

## TOP 10 Risks 2021 – NEW PRIORITIES



2019: 37% (2)  
**Cyber incidents**  
(e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)



2019: 37% (1)  
**Business interruption**  
(incl. supply chain disruption)



2019: 27% (4)  
**Changes in legislation and regulation**  
(e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)



2019: 28% (3)  
**Natural catastrophes<sup>1</sup>**  
(e.g. storm, flood, earthquake)



2019: 23% (5)  
**Market developments**  
(e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)



2019: 19% (6)  
**Fire, explosion**



2019: 13% (8)  
**Climate change**  
/increasing volatility of weather



2019: 13% (9)  
**Loss of reputation or brand value**



2019: 19% (7)  
**New technologies**  
(e.g. impact of Artificial Intelligence, autonomous vehicles, 3D printing, Internet of Things, nanotechnology, blockchain)



**NEW**  
**Macroeconomic developments**  
(e.g. monetary policies, austerity programs, commodity price increase, deflation, inflation)



# Our Story



The Cybersecurity Centre of Excellence (CCoE) is a joint initiative of Data Security Council of India (DSCI) and the Government of Telangana.

The CCoE is created to accelerate the cybersecurity and privacy momentum and create a conducive cybersecurity and privacy ecosystem which *nurtures innovation, entrepreneurship and capability building*.

It aims to provide a secure and resilient cyberspace to fulfil the needs of the digital economy and society by creating a **GLOCAL** cluster of cybersecurity organizations.

# Pillars of CCoE

Empowered with the vision to elevate and scale the cybersecurity ecosystem, CCoE collaborates with organizations under each of these pillars to bridge the areas of gap, enable market access and encourage innovation.



## Industry

Large Enterprises, SMEs,  
Start-ups



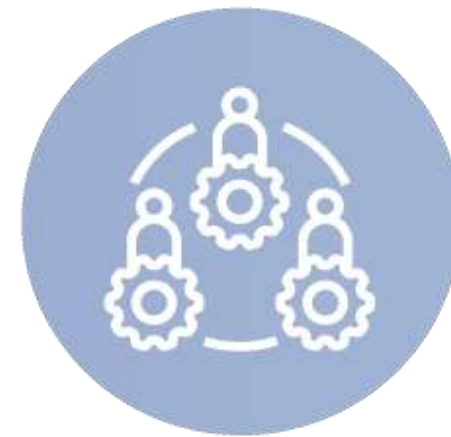
## Government

Central & State govt departments  
and agencies



## Academia and R&D centres

Universities & technical  
institutions



## User groups

User Industries like banking, pharma,  
finance, retail, FMCG, manufacturing,  
defence etc.



## Collaborations

With Local, National & Intl. industry  
bodies, incubators,  
Accelerators, NGOs and Trade &  
Investment Divisions



# Contents

How Cyber Attacks Affect the Industry

Impact and Severity of Cyber Attacks

Who's Behind these Data Breaches

Threats Involved, and Consequences of Getting Hacked

Real-Time Security Breaches

Security and Privacy Implications

Preventive Measures

Effective Incident Response

Risk Management

NIST Risk Management Framework

ENISA Risk Management Standards Framework

CISO Best Practices

Third Party Risk - Supply Chain Security

Data Privacy Laws

Security Audit Frameworks

Vendor Risk Management Best Practices

International Law for Cyber Crime

International Trends in Cyber Security

Cyber Security Regulations

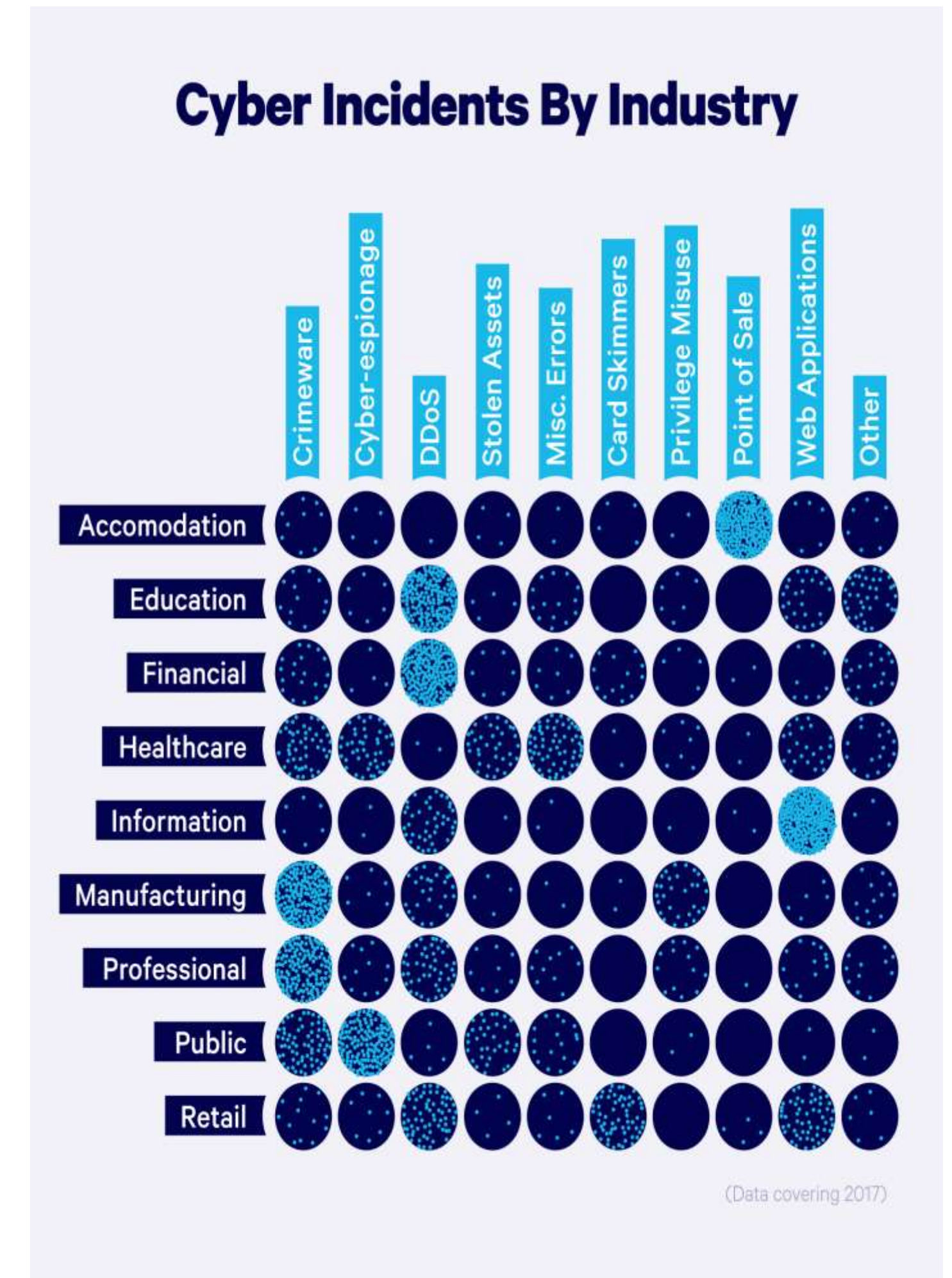
National Cyber Security Policy Strategies

Tools to Mitigate Cyber Risk



# How Cyber Attacks Affect the Industry

- Cybercriminals can penetrate 93 percent of company networks due to Insufficient security measures.
- 43% of all data breaches involve small and medium-sized businesses.
- 83% of small and medium-sized businesses are not financially prepared to recover from a cyber attack.
- One in five small companies does not use endpoint security, and 52% SMBs do not have any IT security experts in-house.
- Only 14% of small businesses consider their cyber-attack and risk mitigation ability as highly effective.
- 2021 saw 50% more cyber attacks per week on corporate networks compared to 2020.





# Impact and Severity of Cyber Attacks

Cyber attacks can impact an organization in many ways — from minor disruptions in operations to major financial losses.

Below are five areas where your business may suffer:

- Financial losses
- Loss of productivity
- Reputation damage
- Legal liability
- Business continuity problems

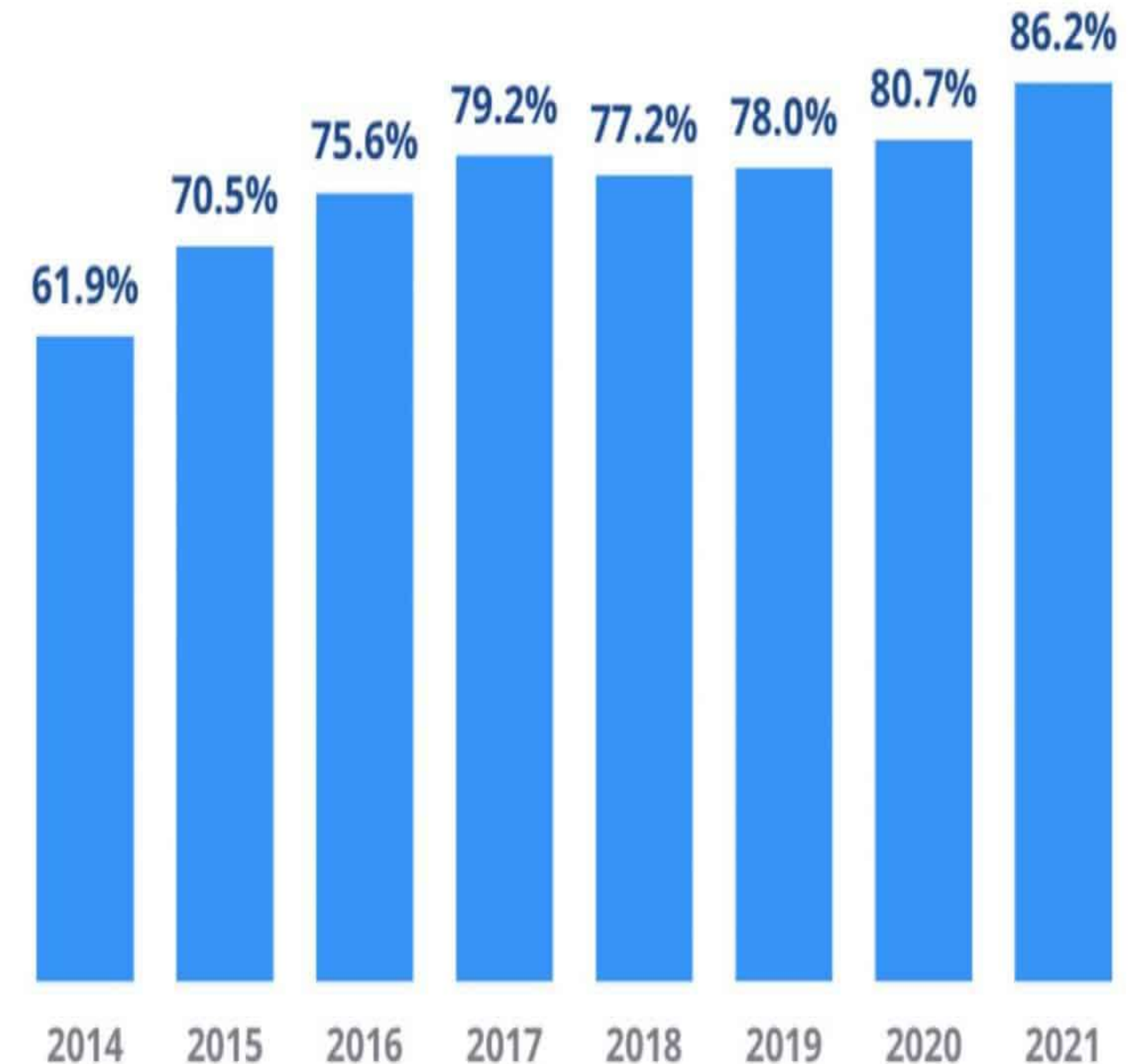
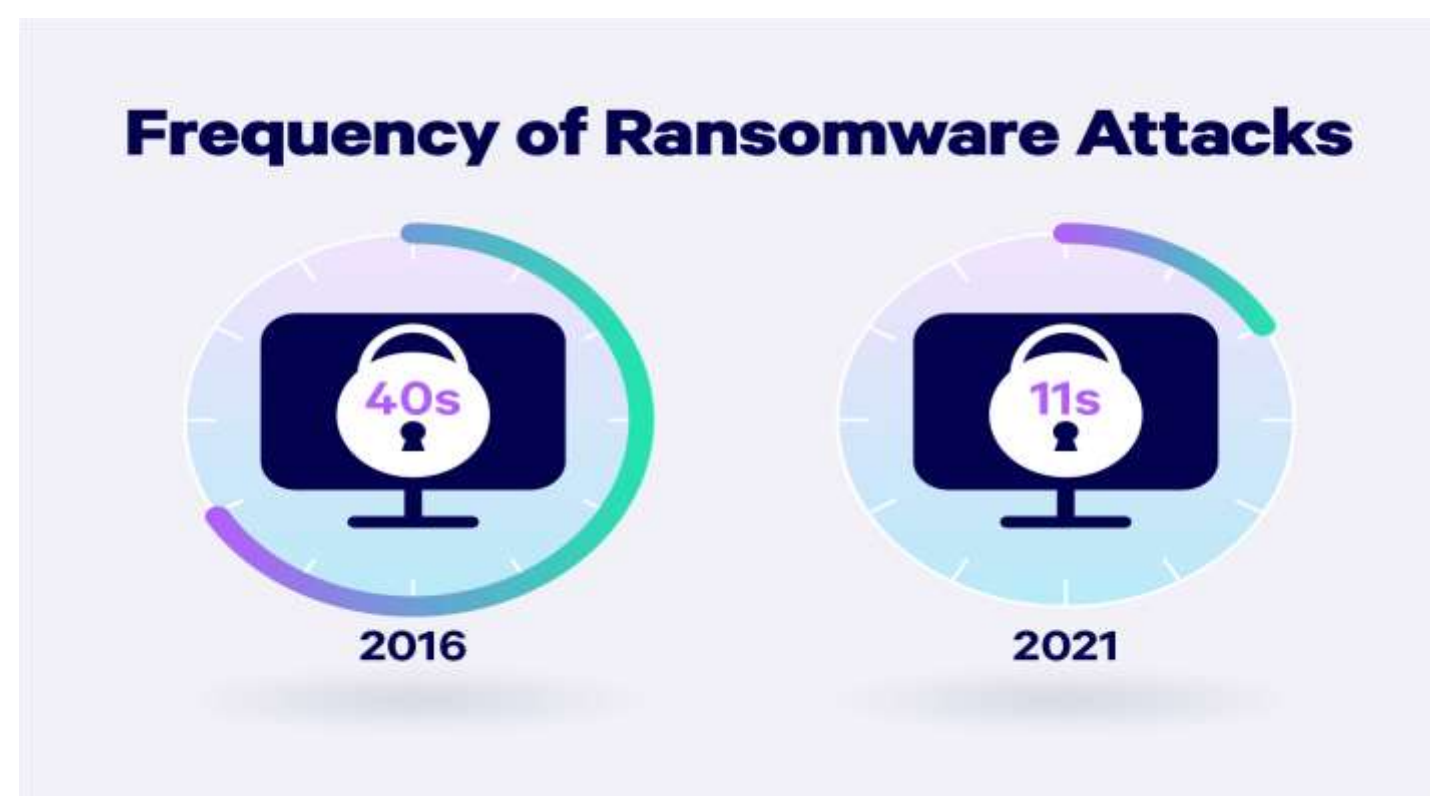
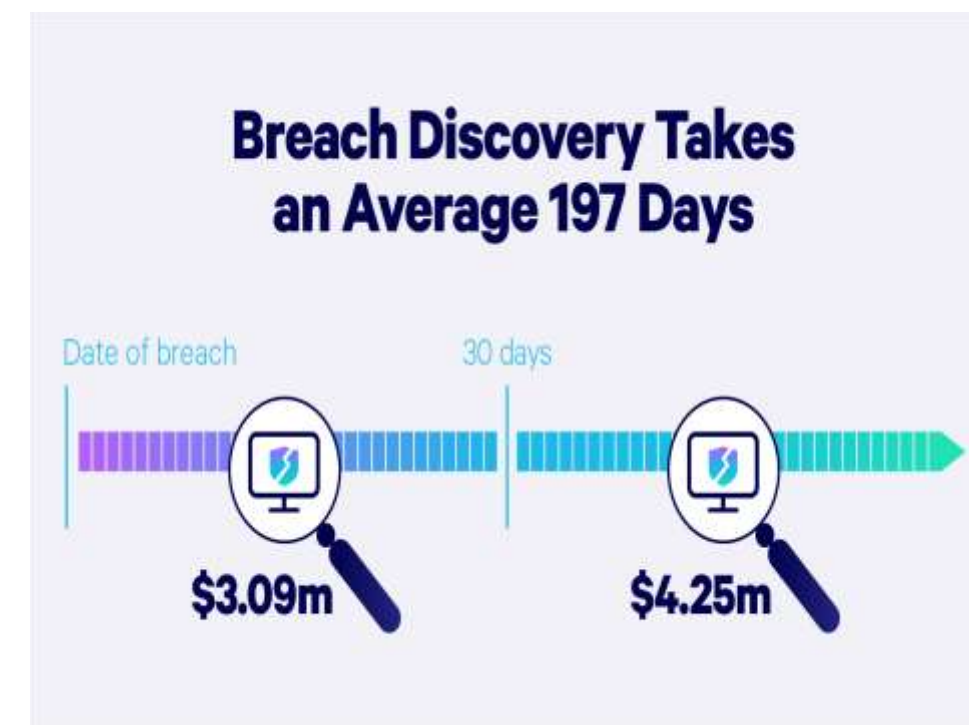


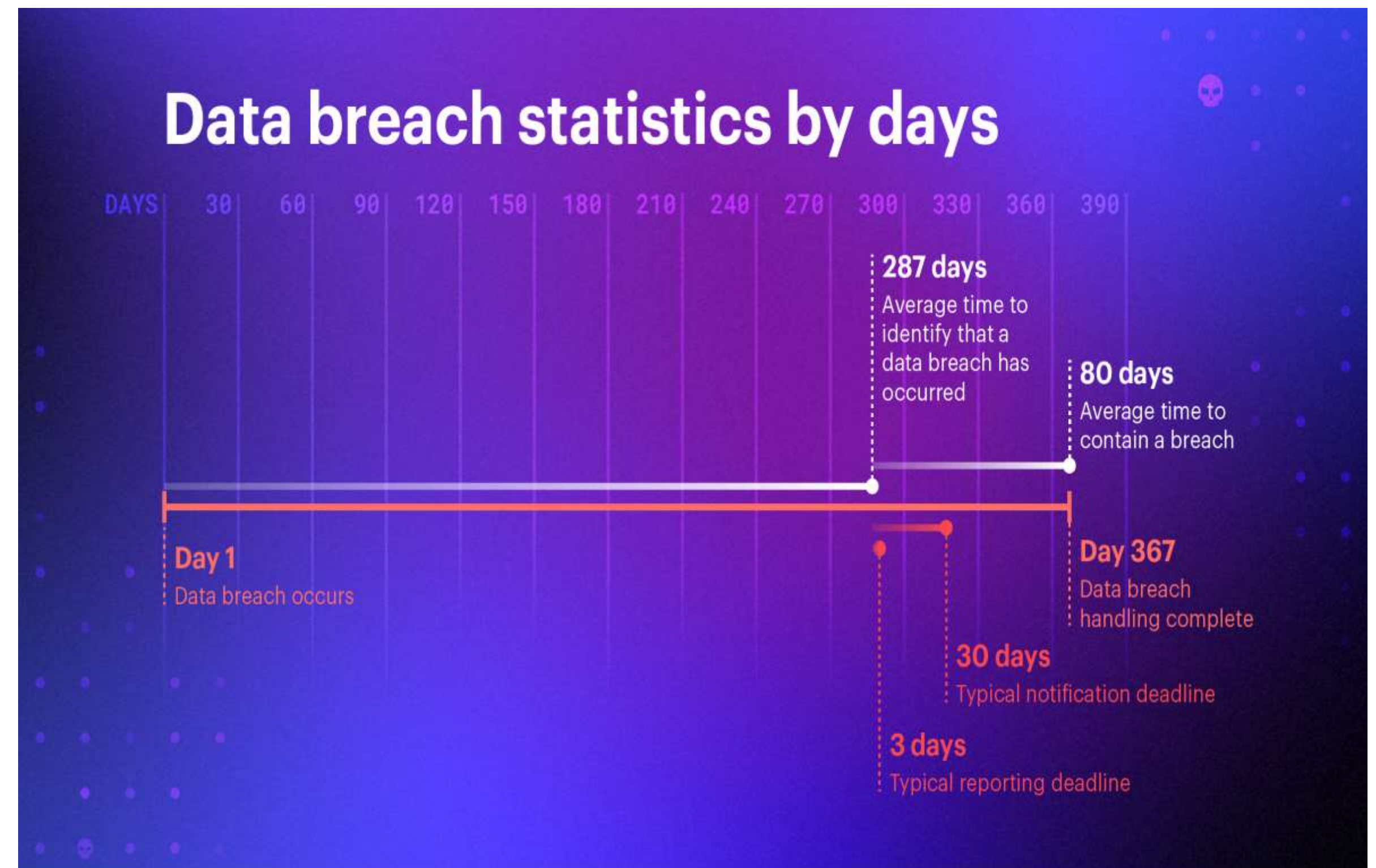
Figure 2: Percentage of organizations compromised by at least one successful attack.



# Who's Behind the Data Breaches?

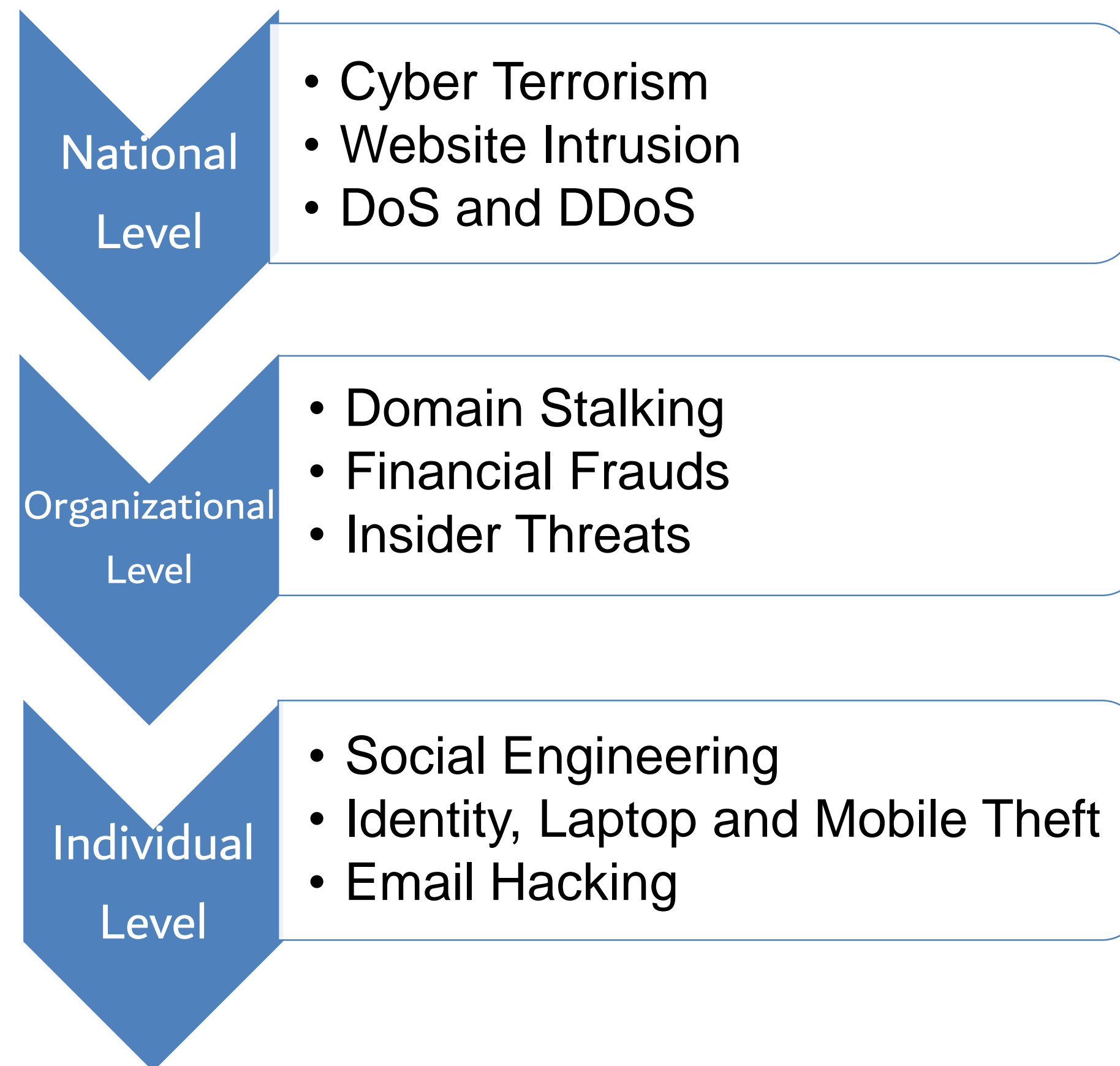
A data breach is any incident in which confidential or sensitive information has been accessed without permission.

- Outsiders
- Organized Criminal Groups
- Internal Actors
- State-Affiliated Actors
- Multiple Parties
- Partners





# Threats Involved, and Consequences of Getting Hacked



Hacks on an individual or an organization leads to:

- Data theft
- Damage to physical equipment
- Suspension of accounts
- Website crash
- Heavy financial losses
- Emotional toll on the victims



# Real-Time Security Breaches

## **Web:**

- Equifax: Online portal got hacked through a known vulnerability in Apache Struts
- Panera Bread: Customer details are displayed in plain text
- Rail Europe: Skimming software over the web

## **Network:**

- Coinrail: Hacked the storage servers that contains the coins information
- Target: Malware read the information from POS systems
- Yahoo: Unauthorized access to accounts without password through hacking of the Complete source code
- JP Morgan: Hackers gained access to 29 servers using the programs running in those servers

## **Mobile:**

- British Airways: Malware in Mobile app payment systems
- Under Armor: Data Breach through Mobile App
- T Mobile: Data Breach In Tmobile

## **Cloud:**

- Deloitte: A sophisticated hack of the email server which is hosted on Microsoft Azure cloud
- National Electoral Institute of Mexico: 93 Million voters data compromised due to purely configured database hosted on Amazon cloud.



# Security and Privacy Implications

- Loss of Data – Personal, Financial, Proprietary etc.
- Loss of Business
- Loss of Business
- Loss of Customer's Trust
- Loss of Share Value
- Money Spent in Forensic Investigation
- Money Spent on Support Staff
- Regulatory and Compliance Fines





# Preventive Measures

- Access only trusted and secure websites
- Strong password for login
- Regular patching and updating
- Provide the data only on need basis
- Anti-Malware
- Security Controls like WAF should be in place
- Document the survival of an attack
- The defender needs to think like an attacker
- Adopt attacker mindset while developing and deploying security systems
- Outsource protection for MSMEs



# Effective Incident Response

## A few alarming statistics:

- 41% of respondents in a survey of business owners had a cybersecurity mishap related to COVID-19
- 94% of executives say their firms have experienced a business-impacting cyber-attack or compromise within the past 12 months.
- 47% of businesses reported experiencing five or more attacks in the last 12 months.
- 78% of respondents said they expect an increase in cyber-attacks over the next two years
- 63% of security leaders admit it's likely their systems suffered an unknown compromise over the past year
- 21% of companies have adopted formal, enterprise-wide security response plans
- 74% have ad-hoc plans or no plans at all for any type of incident
- Only 39% of organizations with a formal, tested incident response plan experienced an incident, compared to 62% of those who didn't have a plan
- Having a tested incident response plan can save 35% of the cost of an incident.



## Incident Response:

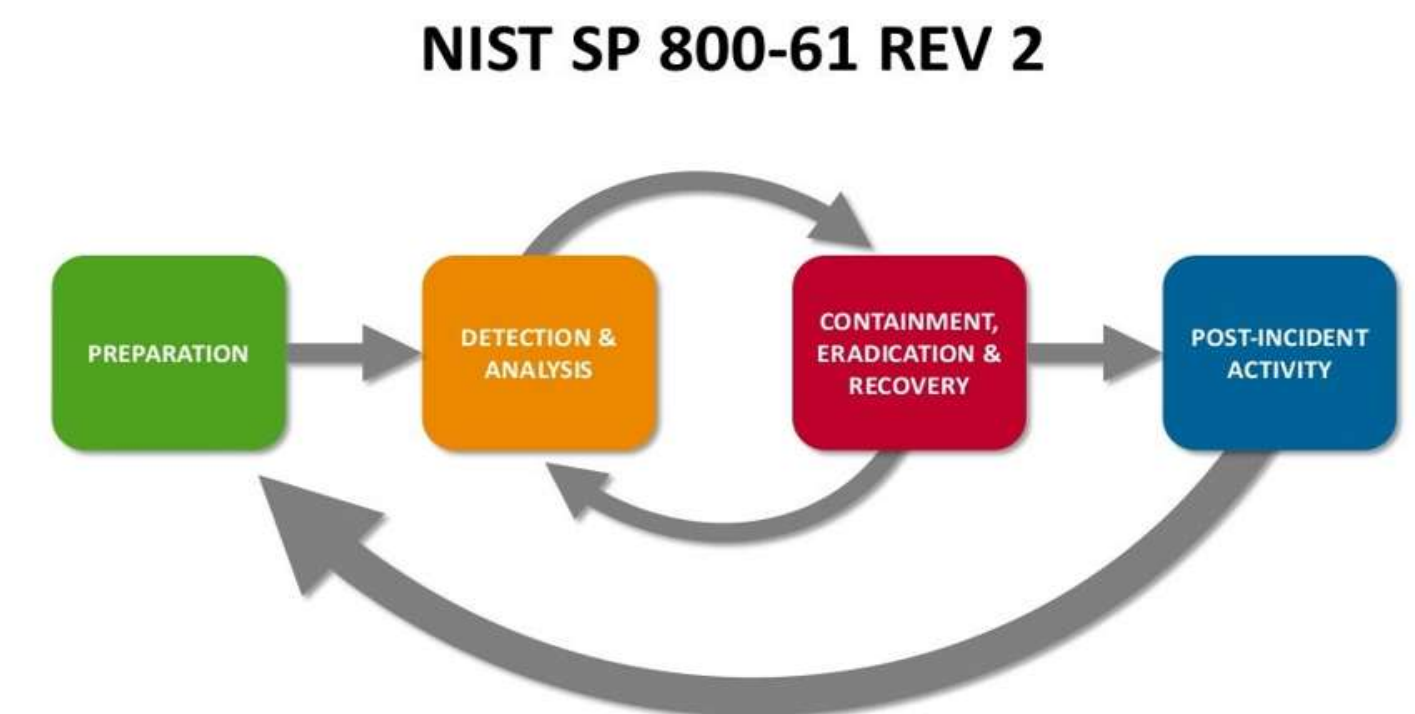
“Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.” — [NIST](#)

The NIST Incident Response Lifecycle contains four steps:

- . Preparation
- . Detection and Analysis
- . Containment, Eradication, and Recovery
- . Post-Incident Activity

## Emergency Preparedness:

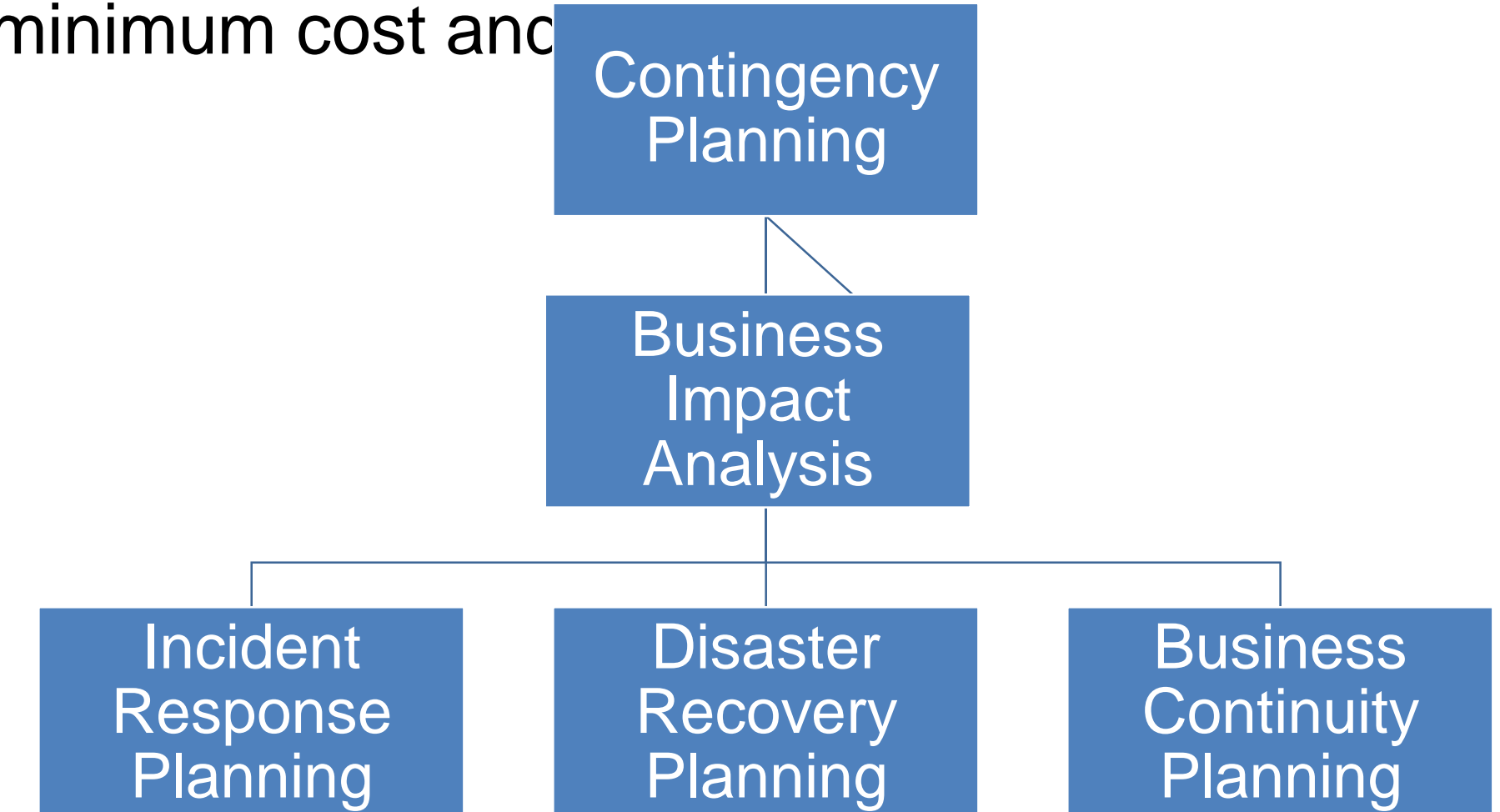
- Emergency preparedness is essential for smooth emergency response – and the faster you respond to an emergency, the better.
- The speed with which an organization can recognize, analyze, prevent, and respond to an incident will limit the damage done and lower the cost of recovery.





## Contingency Planning:

- The overall planning for unexpected events is called contingency planning (CP).
- It is how organizational planners position their organizations to prepare for, detect, react to, and recover from events that threaten the security of information resources and assets.
- The main goal is the restoration to normal modes of operation with minimum cost and disruption to normal business activities after an unexpected event.
- CP comprises of:
  - Business Impact Analysis
  - Incident Response
  - Disaster Recovery
  - Business Continuity plan



# Risk Management

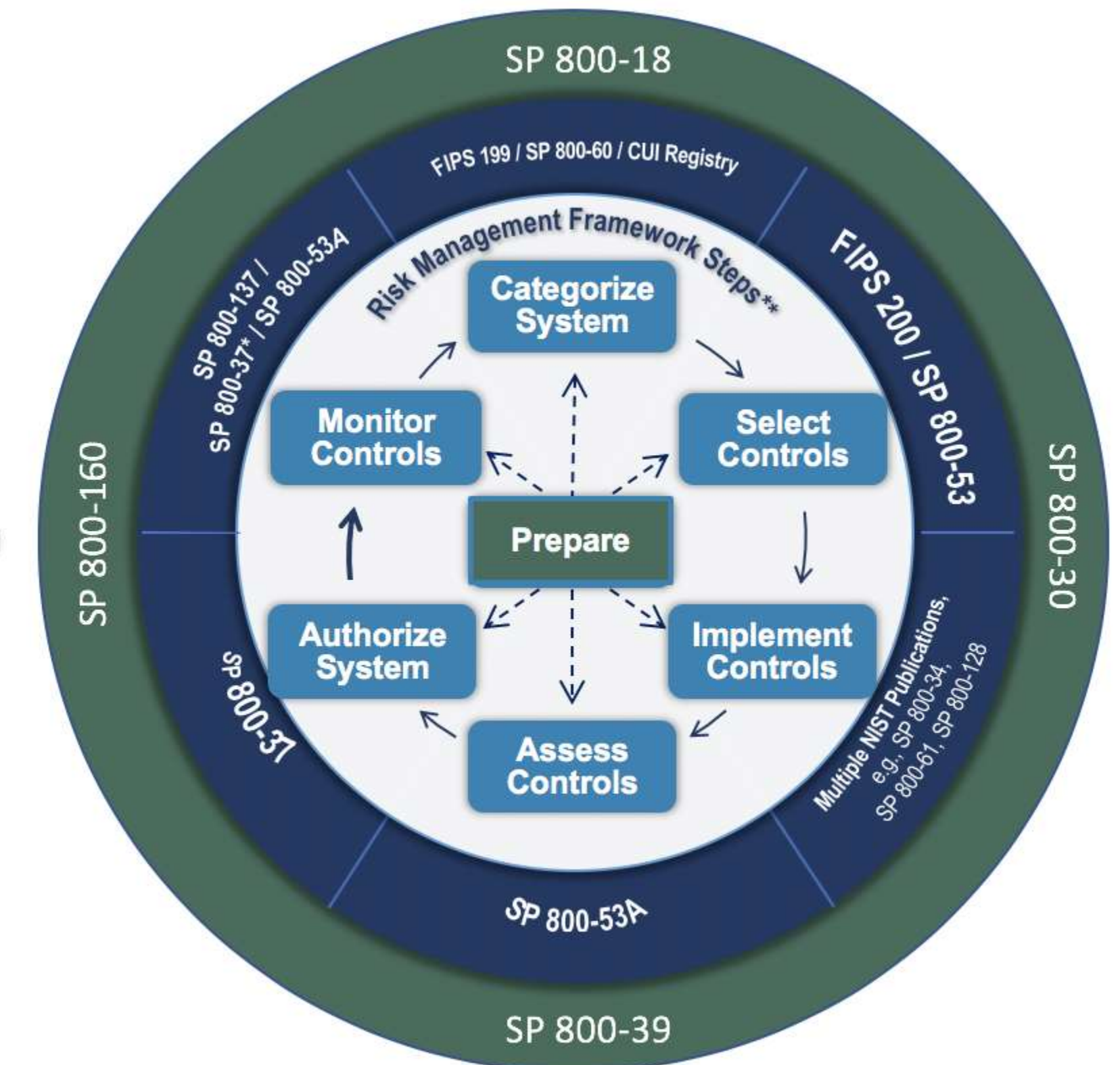
- An effective risk management process is an important component of a successful IT security program. The principal goal of an organization's risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets.
- Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.
- Risk management consists of the following steps:
  1. Identification of threats
  2. Evaluation of threats
  3. Evaluation of risk
  4. Mitigation of risk
  5. Evaluation and assessment of risk controls





# NIST Risk Management Framework

- Risk Management Process:
  - The risk management process is the individual way in which an organization addresses the concept of risk and the relevant types of risk within itself.
  - Risk management may address individual types of risks, such as enterprise risk, market risk, credit risk, operational risk, project risk, development risk, supply chain risk, infrastructure risk, component risks, etc..
- Risk management encompasses three processes:
  1. Risk assessment,
  2. Risk mitigation, and
  3. Evaluation and assessment

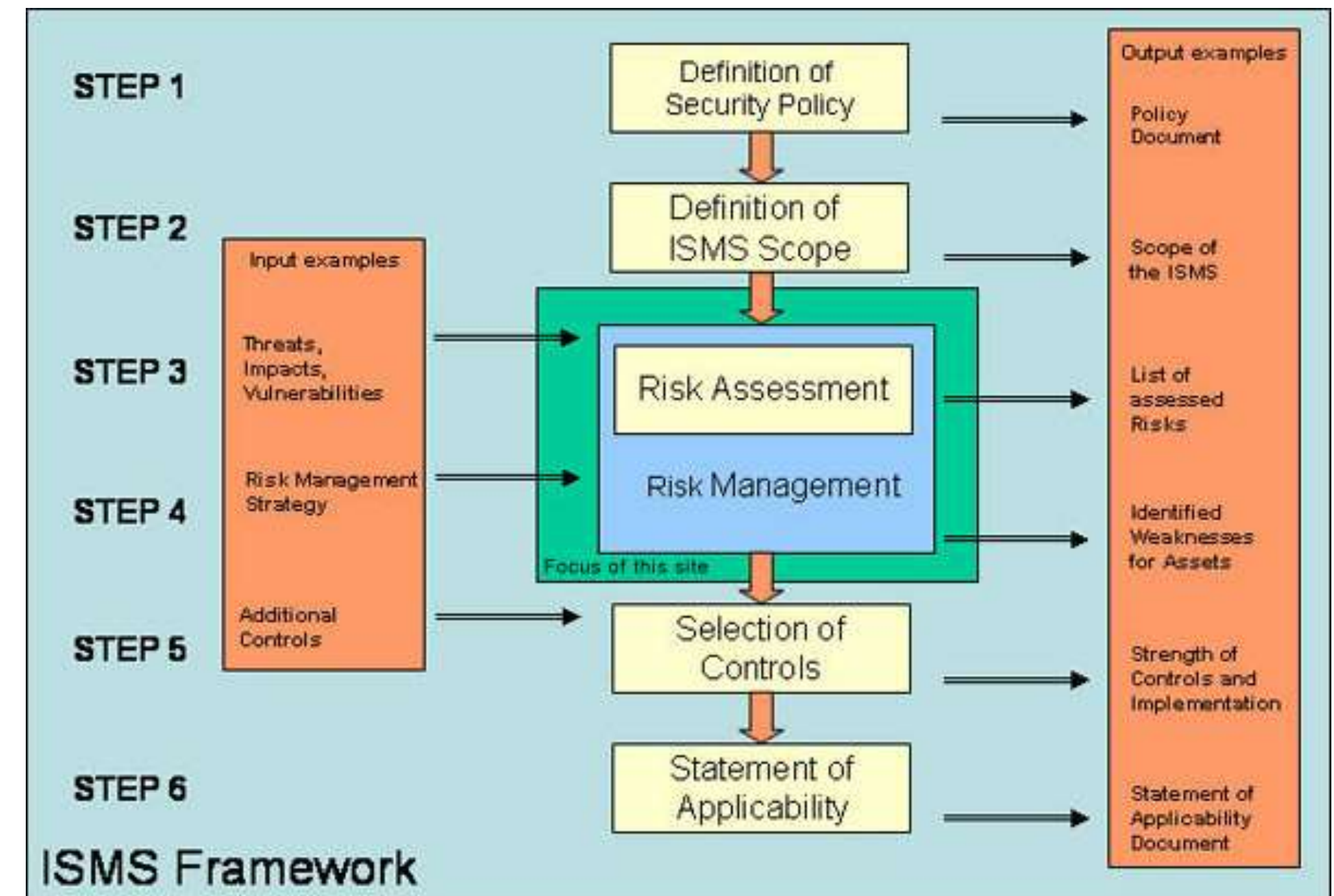




# ENISA Risk Management Standards/Framework

Risk management standards and methodologies can be used for several purposes in an entity:

- Setting up or reinforcing a management process for the digital risk within an organisation,
- Assessing and treating the risks relating to a digital project, in particular with the aim of security accreditation,
- Defining the level of security to be achieved for a product or service according to its particular uses and the risks to be countered, from the perspective of certification or accreditation for example.





# CISO Best Practices

Chief Information Security Officers (CISOs) are a relatively new addition to the C-suite. In the current version of this role, CISOs are now expected to possess business acumen along with security expertise.

## 1. Failure to Obtain Leadership Buy-In

- Executive buy-in is crucial to ensure the financial and human resources needed to keep your organization safe.
- Two of the most common roadblocks to leadership buy-in are finances and a misplaced sense of invincibility, or “This can’t happen to us.” To overcome these obstacles, you must clearly define the organization’s risk appetite and speak in terms that the C-suite understands. It is helpful to translate risk into expenses and lost revenues.

## 2. Balancing Operations with Cybersecurity and Compliance

- To ensure leadership buy-in over the long term, cybersecurity must be a partner to the business, not an impediment.
- Regular security assessments and regulatory gap assessments are necessary to ensure that cybersecurity processes do not interfere with business operations and are effective.

## 3. Not Having Insurance, or Relying on Insurance Too Heavily

- Cyber insurance policies, just like health, auto, and homeowners’ policies, have coverage limitations and loopholes.
- For example, cyber policies generally do not cover breaches due to “employee negligence.” This may sound reasonable, but some policies consider an employee clicking on a phishing link to be “negligence,” and phishing attacks account for over 80% of security incidents.

#### 4. Lacking Visibility Across the Entire Data Environment


- Regular security assessments in combination with timely log and event monitoring will help you keep tabs on the users, applications, and devices connecting to your network.
- Regulatory gap assessments will identify how closely your organization is following industry and monitored SIEM and MDR solution will defend against cyberattacks in near real-time standards and regulations, such as ISO 27001.
- A managed and monitored SIEM and MDR solution will defend against cyberattacks in near real-time

#### 5. Lacking a Clearly Defined Security Policy

At a minimum, a security policy should include password security rules:

- An acceptable use policy for email, internet browsing, and social media
- Rules regarding access and control of proprietary data and client data
- Rules regarding access to company data from remote locations or on personal devices, and
- What to do in the event of a suspected security breach or data loss

#### 6. Lack of Employee Cybersecurity Training

- Often, an organization's biggest cybersecurity risk is its own people.
  - Employee cybersecurity training must be ongoing and include real-world exercises and tests, such as phishing simulations, which are critical to helping your employees avoid falling for social engineering schemes.
  - An outside security consultant can help you devise and implement appropriate cybersecurity training.
- 



# Third Party Risk - Supply Chain Security

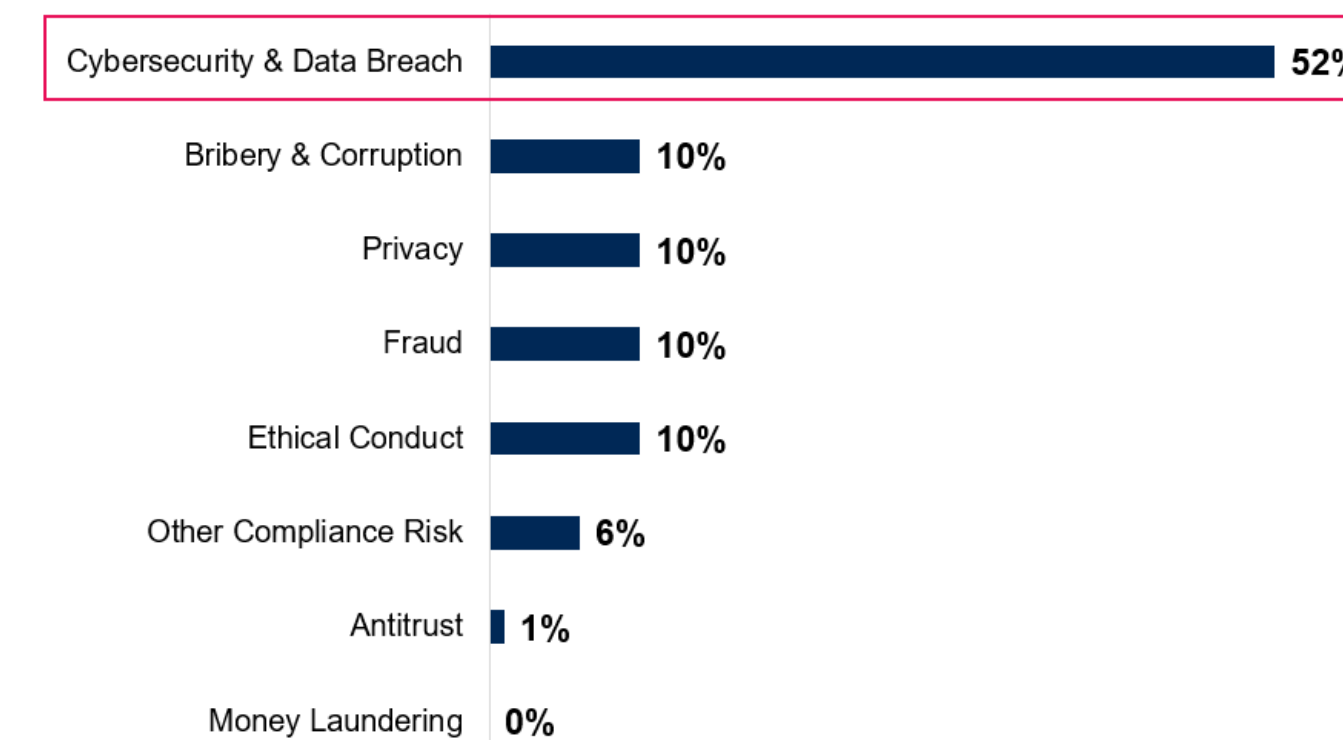
“**Third-party risk**” is the potential threat to organizations originating from the external parties which they knowingly (and unknowingly) rely on.

- Whether the threat is an attacker leveraging a compromised software component to attack your organization directly, a breach in a third-party that handles your data, or some other specific manifestation, the business impact of such risks can be grouped into three categories:
  - Financial and reputational: Risks that incur costs, harm revenue, or damage your reputation
  - Legal and regulatory: Risks that may lead to legal consequences and/or that negatively impact your compliance with legislation or regulations
  - Operational: Risks that disrupt your operations, leading to service interruptions, production downtime, and other costly scenarios

# Third Party Risk - Supply Chain Security (contd.)

- In a research conducted by SpiceWorks, respondents indicated that third-party breaches resulted in:

- disrupted operations (27%)
- increased operational complexity and cost (52%)
- reputational damage (19%), and
- financial losses and penalties (26%)



With many third parties also relying on a newly remote workforce, most compliance leaders are worried about cybersecurity risks resulting from practices such as using unsecure networks.

n=145

Source: Gartner's COVID-19's Impact on Third-Party Risk Management Webinar Poll; 14 April 2020

- **Managing third-party risk:**

## a) **Policies: Minimize**

1. Define supply chain policies
2. Develop due diligence tools
3. Establish periodic validation
4. Raise security awareness
5. Encourage improvement

## b) **Prevention: Measure**

1. Identify assets and obligations
2. Define risk appetite
3. Conduct risk assessments
4. Analyze results and risks
5. Define defensive requirement

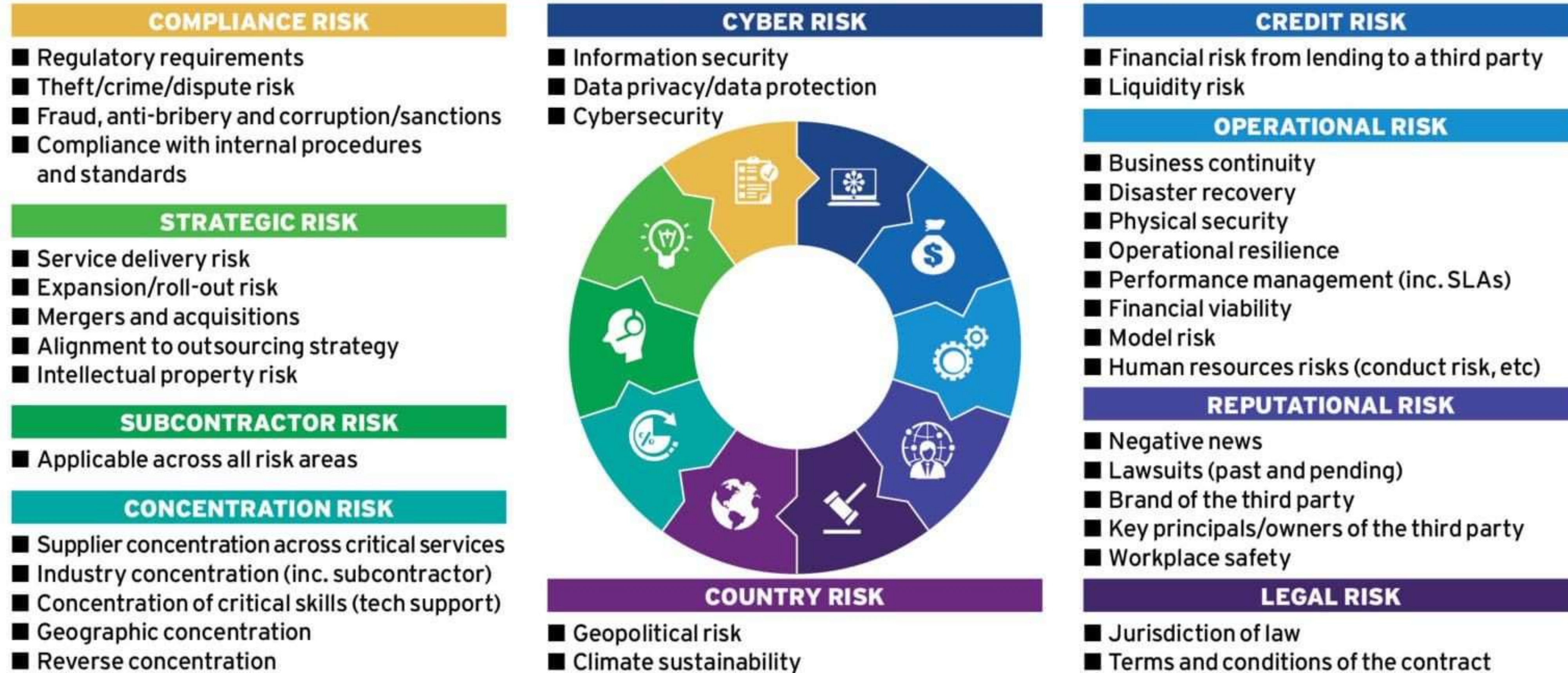
## c) **Promises: Mitigate**

1. Contractual obligations
2. Define responsibilities
3. Establish minimum standards
4. Document notifications
5. Representations/Warranties



# Third Party Risk - Supply Chain Security (contd.)

**FIGURE 2: RISK ASSESSMENT PROCESS - WHAT ARE THE POTENTIAL AREAS OF THIRD PARTY RISK?**

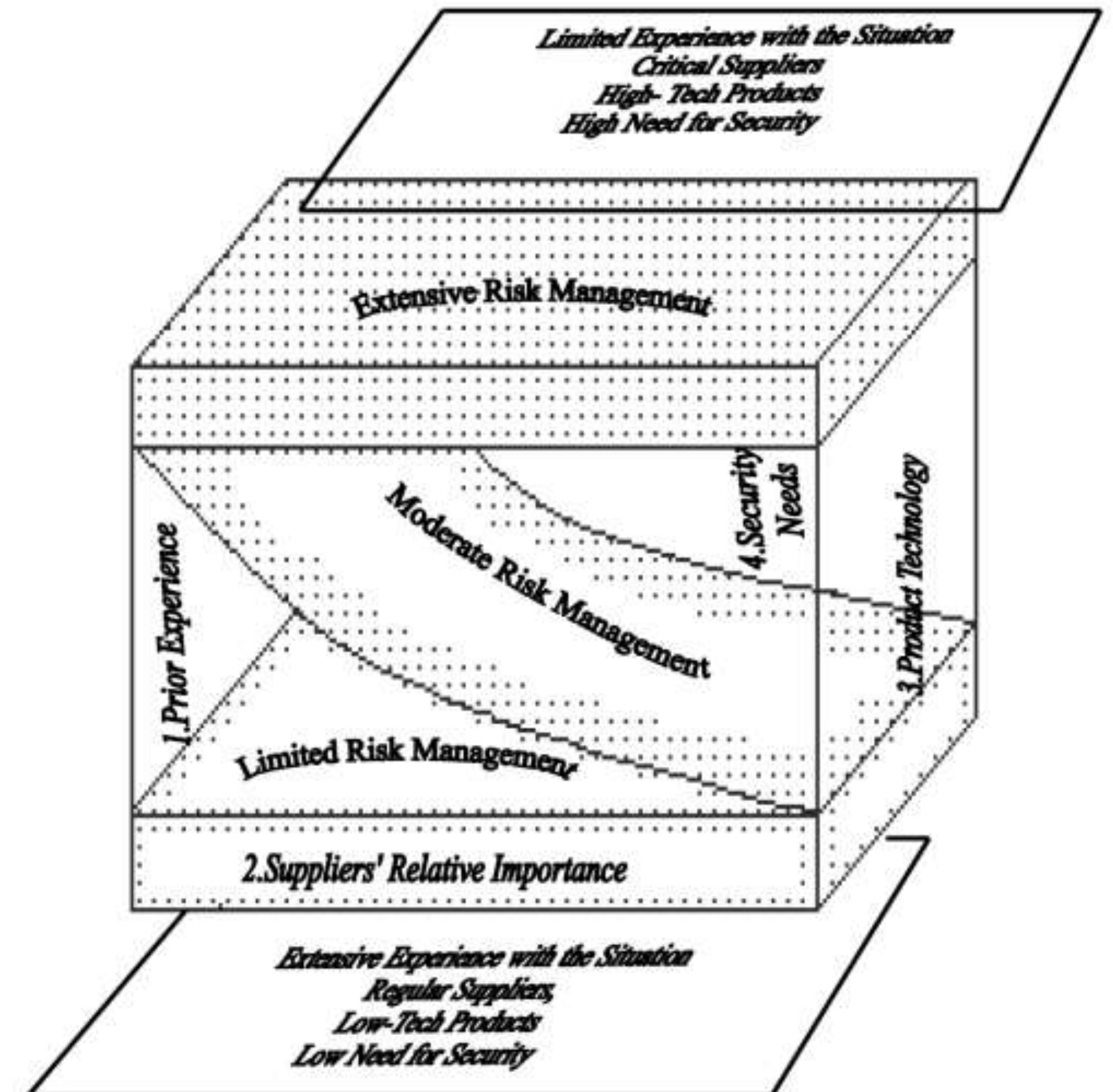




# Third Party Risk - Supply Chain Security (contd.)

Four dimensions that determine the extent of supply chain risk management needs are the:

- (1) degree of product technology involved in the item purchased (high-tech vs low-tech products);
- (2) need for security in handling, packaging and transporting the product (high vs low);
- (3) importance of the supplier (regular vs critical suppliers);  
and
- (4) purchasers' prior experience with the situation whether it is a new item, new supplier, or both (limited vs significant experience)







# Data Privacy Principles

- 1. Lawfulness, Fairness, and Transparency**
- 2. Purpose Limitation**
- 3. Data Minimization**
- 4. Accuracy**
- 5. Storage Limitation**
- 6. Integrity and Confidentiality**
- 7. Accountability**



# Data Privacy Laws

## 1. The General Data Protection Regulation (GDPR)

- The most important data protection legislation enacted to date is the General Data Protection Regulation (GDPR).
- It governs the collection, use, transmission, and security of data collected from residents of any of the 28 member countries of the European Union.
- The law applies to all EU residents, regardless of the entity's location that collects the personal data.
- Some important requirements of the GDPR include:
  - a) Consent
  - b) Data Breach Notification

### Bigger Responsibility, Bigger Repercussions





# Data Privacy Laws

## 2. California Consumer Privacy Act (CCPA)

- The California Consumer Privacy Act of 2018 (“CCPA” or “the Act”) became effective on January 1, 2020, and is codified at §§1798.100-199 of the Civil Code.
- It enables residents of the Golden State to know what data companies and websites collect about them.
- Similar to EU’s GDPR

### → Businesses that CCPA Covers

- Business has gross annual revenues exceeding \$25 million;
- Buys, receives, or sells the personal information of 50,000 or more consumers, households, or devices;
- Derives 50 percent or more of annual revenues from selling consumers’ personal information.



- UPDATE YOUR PRIVACY POLICY**  
Make sure your privacy policy will be in compliance with the CCPA requirements. Companies often follow the strictest standard that applies to them, and CCPA may be one of the strictest.
- CREATE ACCESSIBILITY METHODS**  
Establish a means for customers to be able to request access, change, and data deletion. We recommend at a minimum a toll-free phone number.
- INTRODUCE A VERIFICATION SYSTEM**  
An identity verification system will be apart of the new CCPA compliance regulations. If people can verify their identity, they can access their rights to their personal information on their own.
- DATA GOVERNANCE**  
Prepare data maps, records, inventories, etc. of California residents' personal data so you are ready to allow them to exercise their rights dictated by the CCPA.
- "OPT OUT" BUTTON / LINK**  
Citizens of California have the right to opt-out of the sharing of their personal information. This way you can be compliant without the extra hassle of manually updating that customer.
- OBTAIN CONSENT FROM MINORS**  
Create a method for obtaining consent from parents of minors under 13 years old and direct consent from those aged 13-16 years. Minors under 16 cannot automatically consent under CCPA.



# Data Privacy Laws

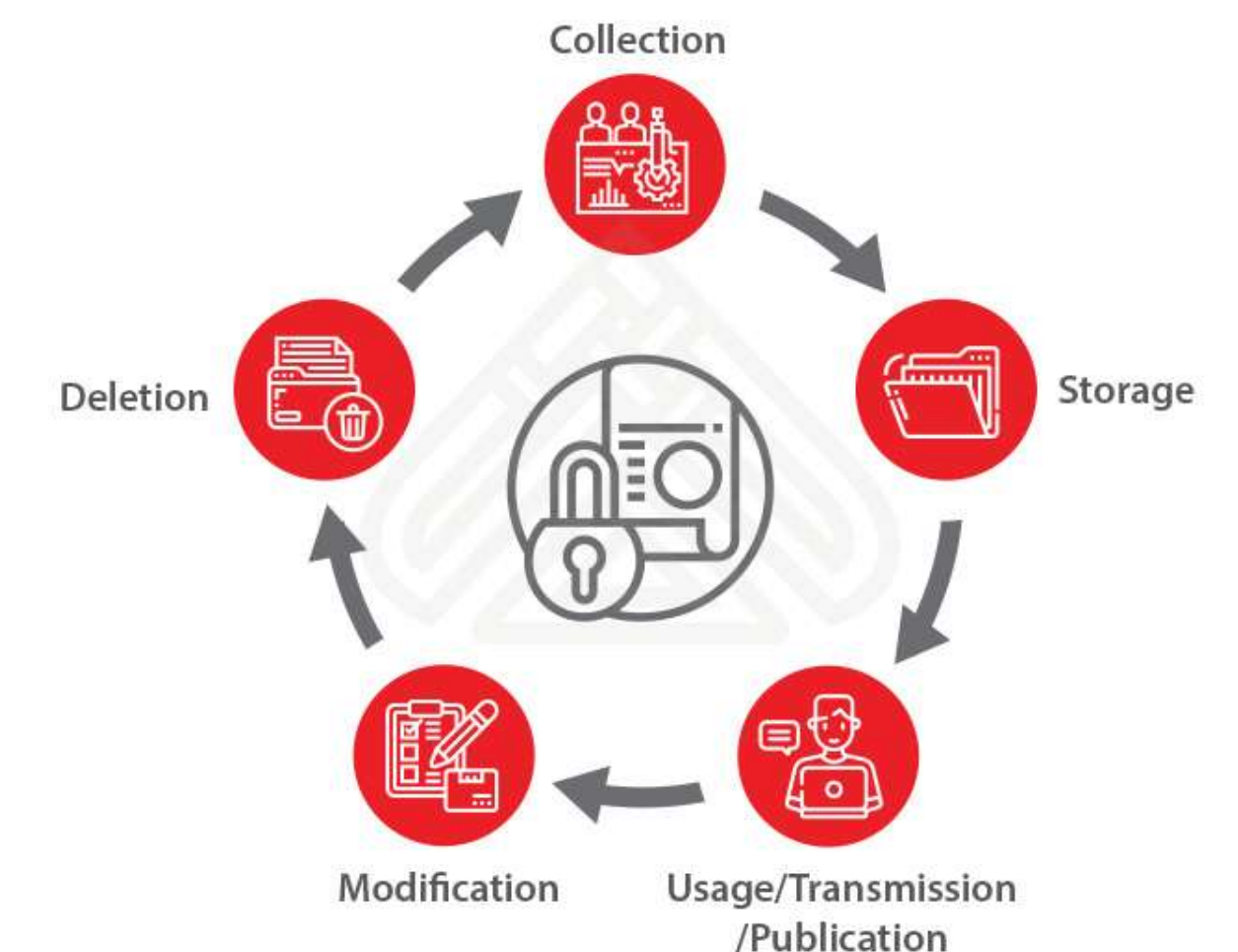
## 3. China's Personal Information Protection Law

- China's first comprehensive legislation regulating the protection of personal information
- Modeled after the European Union's GDPR
- The PIPL is not only applicable to organizations and individuals who process personally identifiable information (PII) in China, but also those who process data of China citizens' PII outside of China.

### China's PIPL: 7 Processor Obligations

- Formulate internal management systems and operating procedures.
- Implement classified management of personal information protection.
- Adopt technical security measures such as encryption and de-identification.
- Reasonably determine the operational authorizations for personal information and provide regular training and security education for operational staff.
- Formulate and carry out response plans when security incidents related to personal information occur.
- Carry out regular compliance audits.
- Adopt other security measures laid out in laws and regulations.

Processing Under the Context of Personal Information Protection





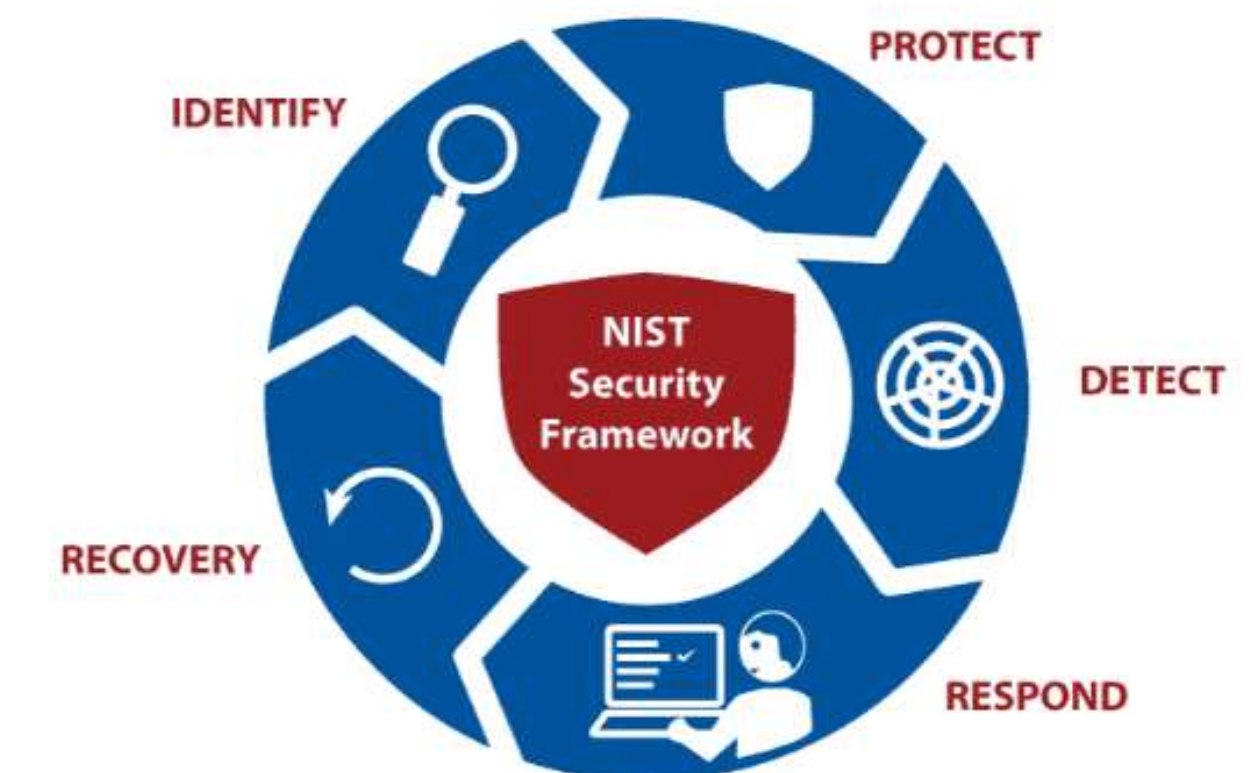
# Security Audit Frameworks

## 1. NIST Cybersecurity Framework

A gold standard for assessing cybersecurity maturity, identifying security gaps, and meeting cybersecurity regulations.

Its core material is divided into five major functions:

- 1. Identify:** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- 2. Protect:** Develop and implement appropriate safeguards to ensure delivery of critical services.
- 3. Detect:** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- 4. Respond:** Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- 5. Recover:** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.



# SOC 2

## 2. SOC (System and Organization Controls) 2

- SOC 2 is a voluntary compliance standard for service organizations, developed by the American Institute of CPAs (AICPA).
- There are two types of SOC 2 reports:
  - a. Type I** describes the organization's systems and whether the system design complies with the relevant trust principles.
  - b. Type II** details the operational efficiency of these systems.
- Basic SOC 2 compliance checklist, which includes controls covering safety standards:
  - a. Access controls**—logical and physical restrictions on assets to prevent access by unauthorized personnel.
  - b. Change management**—a controlled process for managing changes to IT systems, and methods for preventing unauthorized changes.
  - c. System operations**—controls that can monitor ongoing operations, detect and resolve any deviations from organizational procedures.
  - d. Mitigating risk**—methods and activities that allow the organization to identify risks, as well as respond and mitigate them, while addressing any subsequent business.

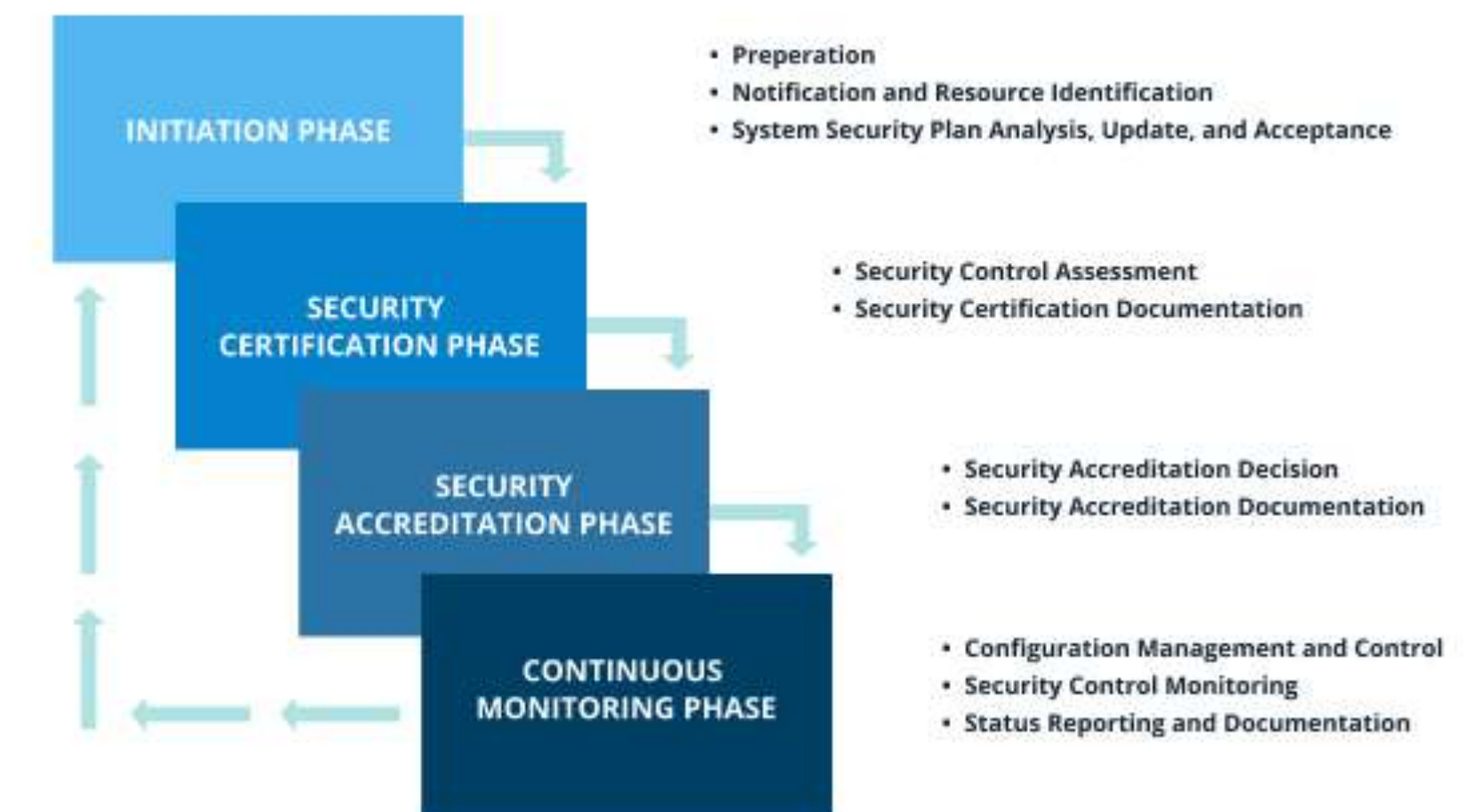




# FISMA

## 3. FISMA

- Federal Information Security Management Act
- A United States legislation that defines a framework of guidelines and security standards to protect government information and operations.
- Specifically, FISMA requires federal agencies, and others it applies to, to develop, document and implement agency-wide information security programs.
- **FISMA compliance best practices**
  1. To ensure compliance with FISMA, here are some best practices to follow:
  2. Stay up to date with any new FISMA standards or NIST guidelines.
  3. Keep a record of FISMA compliances. Keeping any detailed records on steps taken to maintain compliance should help with any audits regarding FISMA.
  4. Classify data based on its level of sensitivity when it's created. This will ensure sensitive data is treated securely.
  5. Encrypt sensitive data automatically. A tool can be used to do this automatically, based on classification levels.



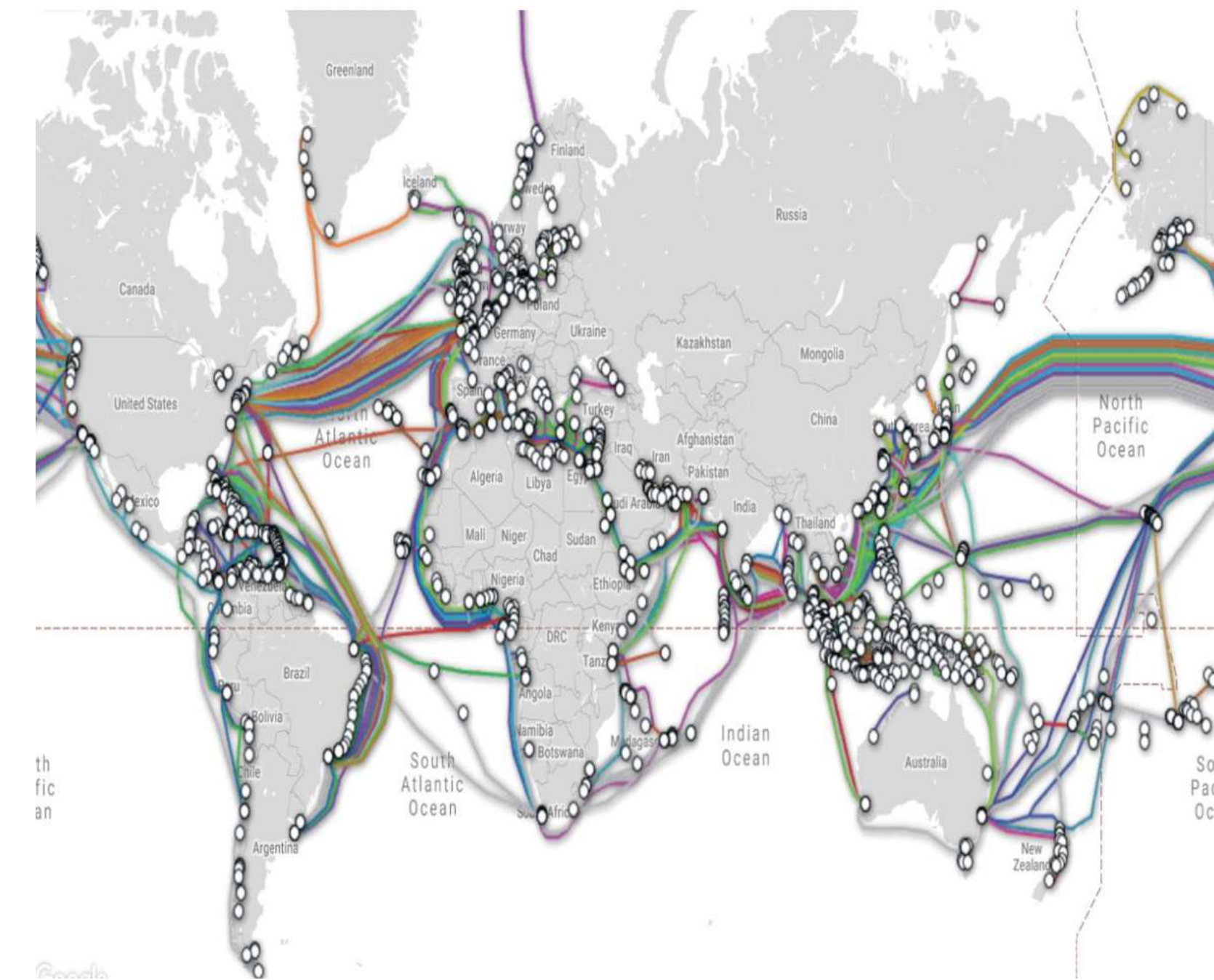
# Vendor Risk Management Best Practices

1. Take inventory of all third-party vendors your organization has a relationship with.
2. Catalog cybersecurity risks that the counterparties can expose your organization to.
3. Assess and segment vendors by potential risks and mitigate risks that are above your organization's risk appetite.
4. Develop a rule-based system to assess future vendors and set a minimum acceptable hurdle for the quality of any future third-parties in real-time by reviewing data security and independent reviews.
5. Establish an owner of vendor risk management and all other third-party risk management practices.
6. Define three lines of defense including leadership, vendor management and internal audit.
7. The first line of defense – functions that own and manage risk.
8. The second line of defense – functions that oversee or specialize in risk management and compliance.
9. The third line of defense – functions that provide independent assurance, above all internal audit.
10. Establish contingency plans for when a third-party is deemed below quality or a data breach occurs.



# International Law for Cyber Crime

- Cybercrime is "international" that there are 'no cyber-borders between countries'.
- The complexity in types and forms of cybercrime increases the difficulty to fight back.
- Fighting cybercrime calls for international cooperation.
- Various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a regional and on an international scale.





# International Trends in Cyber Security

There are several emerging international trends of cybercrime:

- Platform switch
- Social engineering scams
- Highly targeted
- Dissemination and use of malware
- Intellectual property theft (IP theft)





# Cybersecurity Regulations

A Cyber Security Regulation comprises directives that safeguard information technology and computer systems.

## **Health Insurance Portability and Accountability Act (HIPAA)**

- was enacted by the 104th United States Congress and signed by Bill Clinton in 1996 in his presidency.
- was created primarily to modernize the flow of healthcare information.

## **The Federal Information Security Management Act (FISMA)**

- Is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107–347, 116 Stat. 2899).
- The act recognized the importance of information security to the economic and national security interests of the United States.
- The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems.

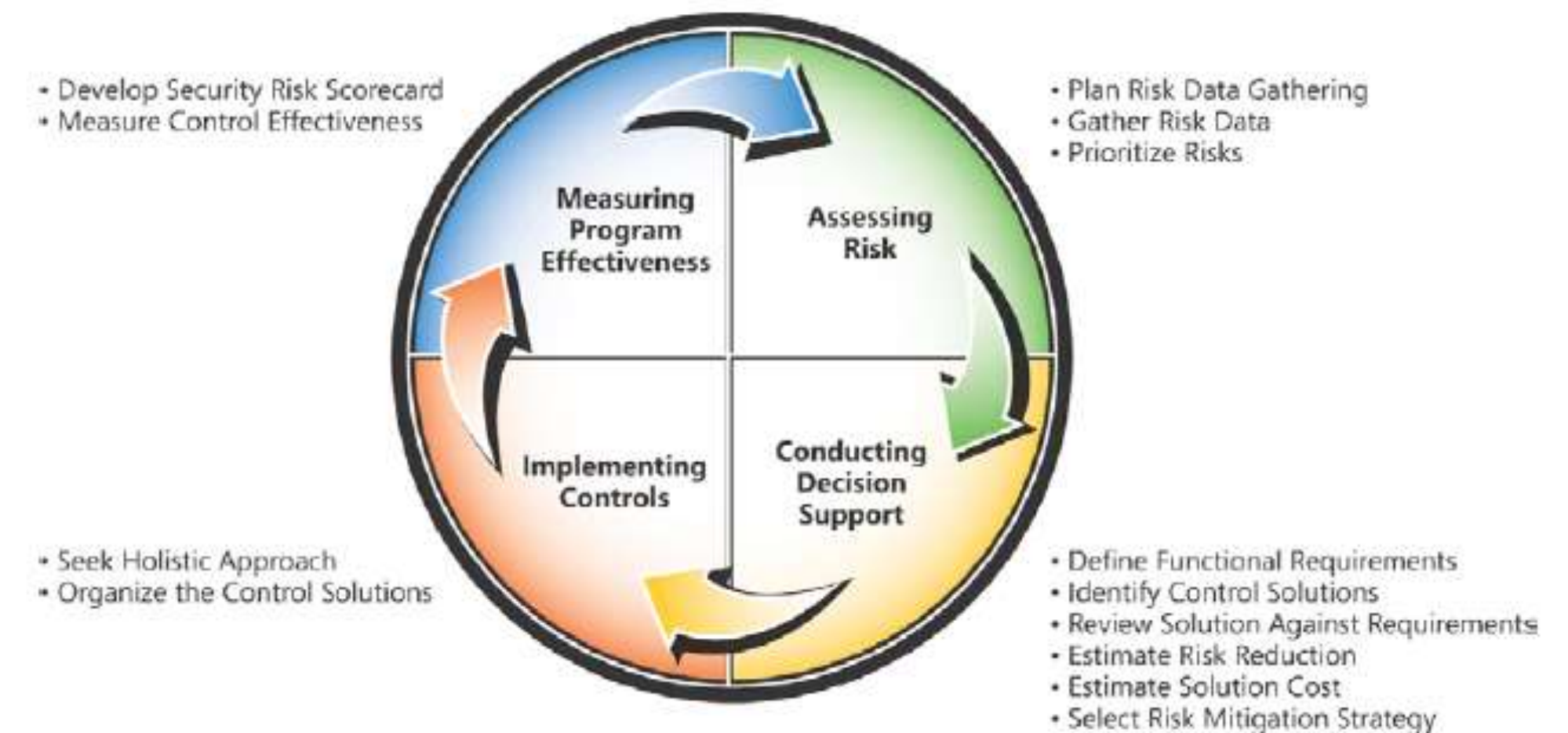
# GBLA

## The Gramm–Leach–Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999

- An Act to enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, and other financial service providers, and for other purposes.

## **The Privacy Regulations Under GLBA :**

- The Privacy Regulations govern the treatment of non public personal information about consumers by a financial institution.
  - Require a financial institution to provide notice to customers about its privacy policies and practices;
  - Describe the conditions under which a financial institution may disclose nonpublic personal information about consumers to third parties; and
  - Provide a method for consumers to prevent a financial institution from disclosing that information to the most non affiliated third parties by “opting out” of that disclosure subject to certain exceptions.





# National Cyber Security Policy Strategies

- Creating a Secure Cyber Ecosystem
- Creating an Assurance Framework
- Encouraging Open Standards
- Strengthening the Regulatory framework
- Creating Mechanisms For Security Threat Early Warning, Vulnerability Management and Response to Security Threats
- Securing E-governance Services
- Protection and Resilience Of Critical Information Infrastructure
- Promotion of Research & Development in Cyber Security
- Reducing Supply Chain Risks
- Human Resource Development
- Creating Cyber Security Awareness
- Developing effective Public Private Partnerships
- Information Sharing and Cooperation
- Prioritized Approach for Implementation

# Tools to Mitigate Cyber Risk

## a. Vulnerability Assessment Tools

- OpenVAS
- Nexpose Community
- Nikto
- Tripwire IP360
- Wireshark

## b. Breach and Attack Simulation Tools

- CyCognito
- Mandiant
- FireMon
- Qualys
- Rapid7

## c. Vendor-Provided Tools

- Cisco
- Skout
- Cyberfish
- KnowB4
- Azure

- The suggested tools, mitigation strategies, and preventive measures can be employed to safeguard your organizations from impending threats.
- It is always suggested to understand and follow best practices to maintain a secure cyber hygiene.



# Contact Us

<https://ccoe.dsci.in/>

Stay updated for upcoming events

[youtube.com/user/dscivideo](https://www.youtube.com/user/dscivideo)

Subscribe us on YouTube

[facebook.com/ccoe.hyd/](https://www.facebook.com/ccoe.hyd/)

Follow us on Facebook

[linkedin.com/company/ccoehyd/](https://www.linkedin.com/company/ccoehyd/)

Get updates from our LinkedIn

[twitter.com/ccoe\\_hyd](https://twitter.com/ccoe_hyd)

Follow us on Twitter

## Reach us

Phone : 9703587766

Email : [marketing.ccoe@dsci.in](mailto:marketing.ccoe@dsci.in)

Web : <https://ccoe.dsci.in/>



***THANK YOU!***

