Session 21

CYBER RISK & DATA BREACH

Business Losses to Cybercrime Data Breaches to Exceed $5 Trillion by 2024

https://www.securitymagazine.com/articles/90806-business-losses-to-cybercrime-data-breaches-to-exceed-5-trillion-by-2024

A report from Juniper Research found that the cost of data breaches will rise from $3 trillion each year to more than $5 trillion in 2024, an average annual growth of 11%.

This will primarily be driven by increasing fines for data breaches as regulation tightens, as well as a greater proportion of business lost as enterprises become more dependent on the digital realm.

Cybercrime is increasingly sophisticated; the report anticipates that cybercriminals will use AI which will learn the behavior of security systems in a similar way to how cybersecurity firms currently employ the technology to detect abnormal behavior.

The research also highlights that the evolution of deep fakes and other AI-based techniques is also likely to play a part in social media cybercrime in the future.

Juniper Research expects that security awareness training will become an increasingly important part of enterprise cybersecurity practice. The gains that can be made by increasing human awareness of cybersecurity can make more efficient use of cybersecurity spending.

The Future of Cybercrime & Security: Threat Analysis, Impact Assessment & Mitigation Strategies 2019-2024

Jessica Davis

February 12, 2020 - The FBI estimates that cybercrime cost individuals and US businesses $3.5 billion in losses last year, as estimated in the 2019 Internet Crime Report **published** by the FBI Internet Crime Complaint Center (IC3). The most expensive complaints were **caused** by business email compromise.

In 2019, the FBI received 467,361 complaints, up from its average 340,000 complaints it receives each year. In fact, there were more incidents were reported to the FBI than any previous year.

Since its foundation in May 2000, the IC3 has received more than 1,200 complaints each day for the last five years, or a total of 4.88 million in the last decade. The total number of recorded losses for the last five years was $10.2 billion.

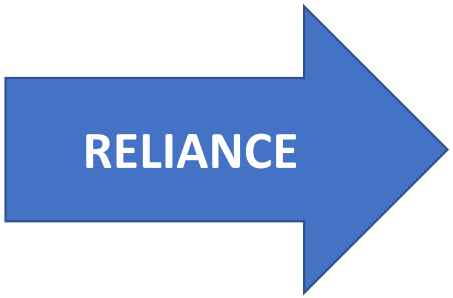
The FBI noted that despite increased awareness around the country, cybercrime continues to boom given that hackers are improving upon previously successful campaigns with new techniques and tactics.

Email continues to be a common entry point, but these fraud attempts are also being launched through text messages or even fake websites.

Cyber Risk

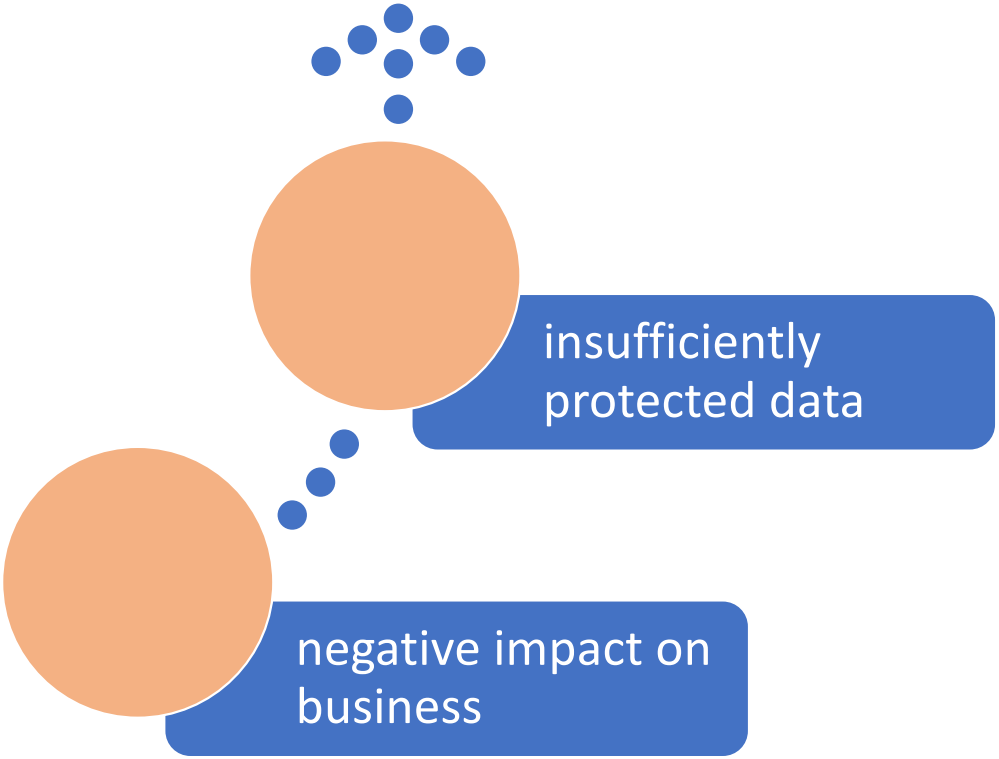
- probability of exposure or loss resulting from a cyber attack or data breach on your organization
- potential loss or harm related to technical infrastructure, use of technology or reputation of an organization

Threatens more and more organizations



- computers
- networks
- programs
- social media

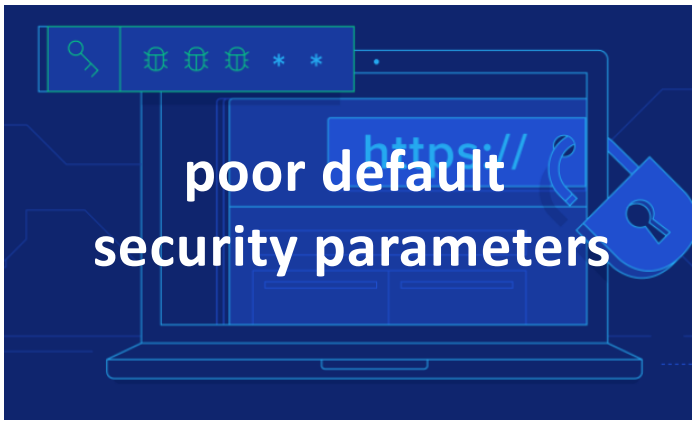
Data breaches

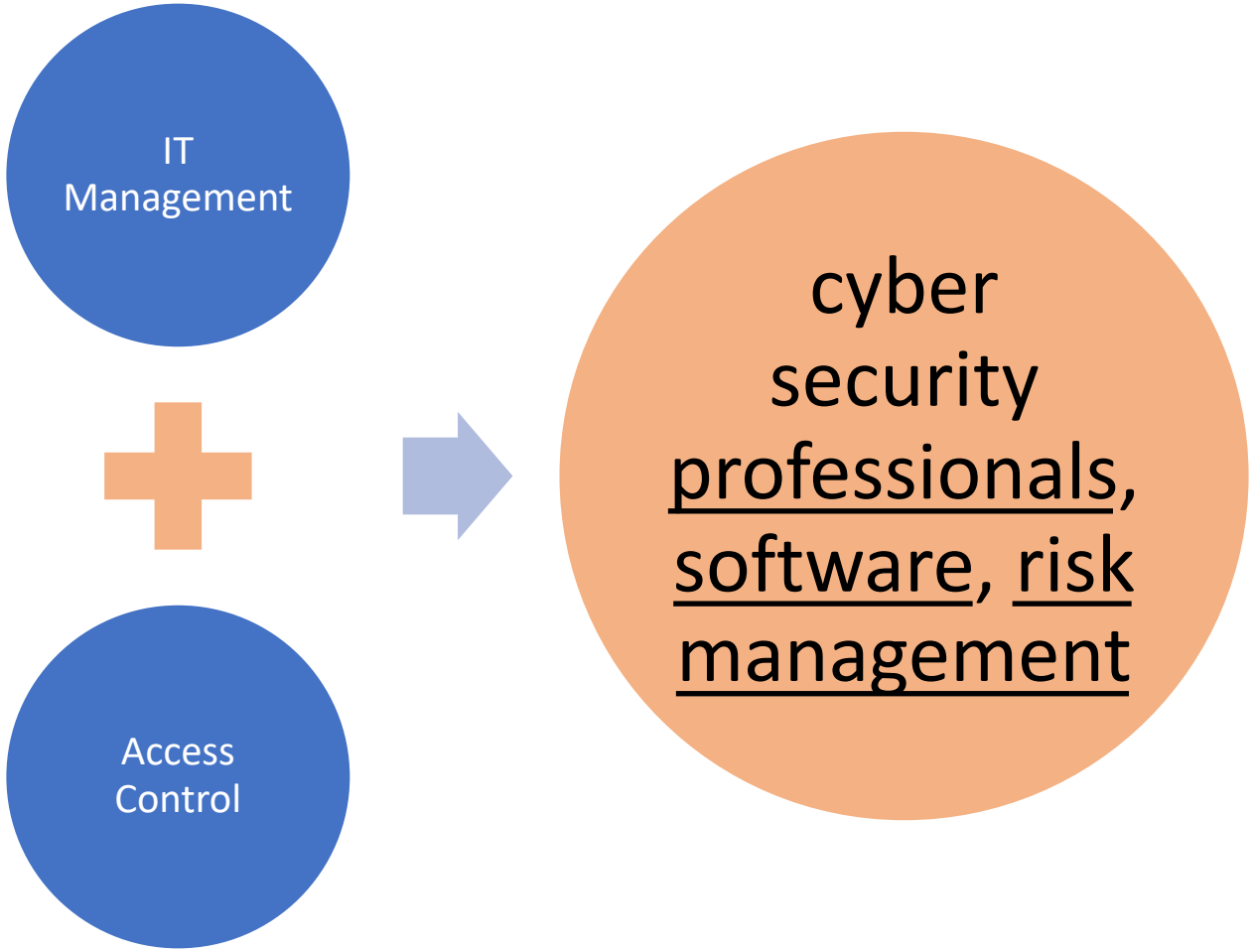


Risk is increasing

Global connectivity

increasing use
of cloud services




IT Management
Access Control
cyber security professionals, software, risk management

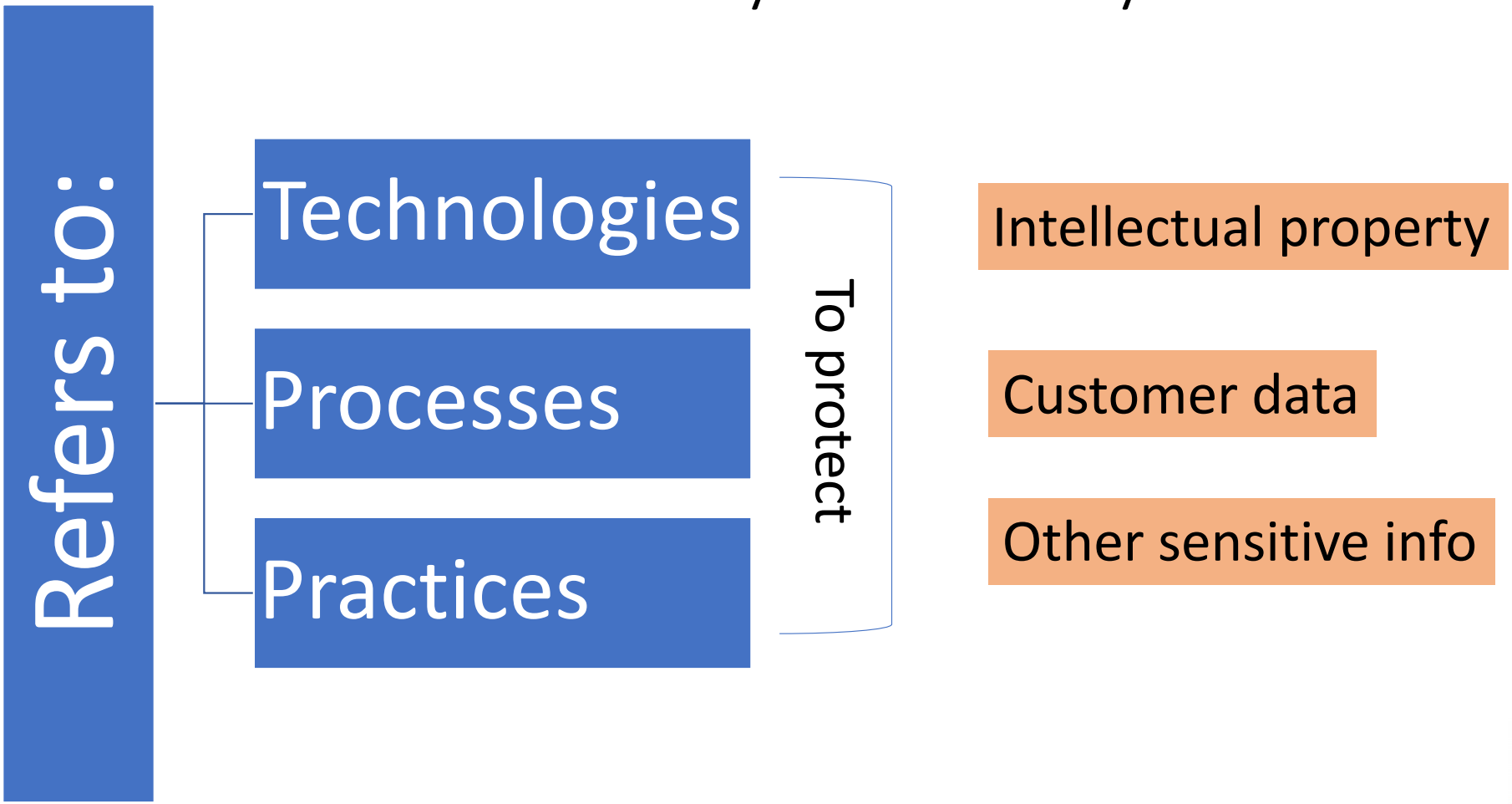

traditional information technology
security controls


threat intelligence tools
security programs

Out in place


1
Risk assessment
2
Risk mitigation
3
Incident Response Plan

What Is Cybersecurity?



frequency

severity

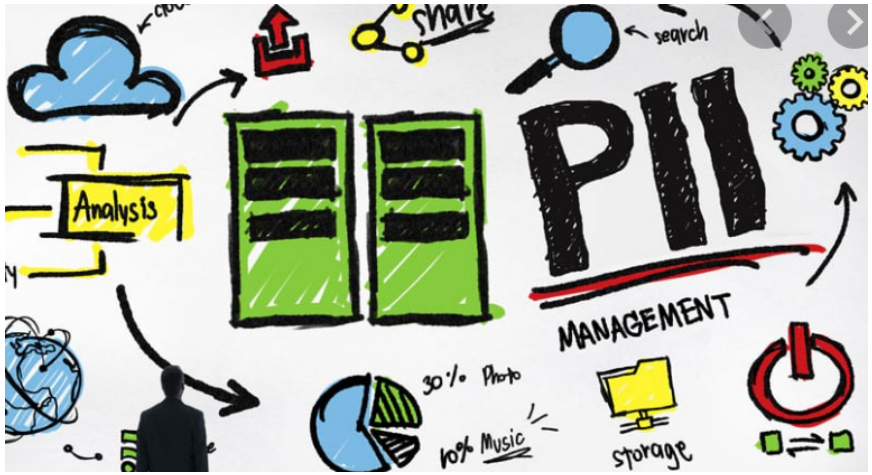
*need for improved cybersecurity risk management

What Is the Business Significance of Cyber Attacks?

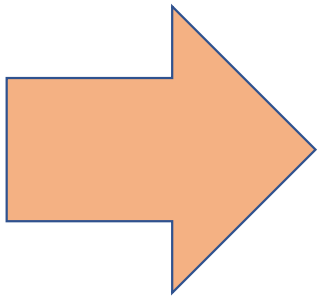
- Security controls are useful but insufficient to provide protection against cyber attacks.
- Technology enables more unauthorized access to your organization's information than ever before.

What Is the Business Significance of Cyber Attacks?

- Third-parties are increasing provided with information.
- Organizations are increasingly storing large volumes of Personally identifiable information (PII) on external cloud providers



- increasing number of devices that are always connected in data exchange
- the web of employees, customers and third-party vendors is getting bigger
- need for instant and real-time access to information from anywhere



exponentially increase the attack surface for malware, vulnerabilities, and all other exploits.

Cyber threats can come from

- ✓ hostile foreign powers
- ✓ competitors
- ✓ organized hackers
- ✓ third-party vendors
- ✓ poor configuration
- ✓ insiders

becoming increasing complex

SOFTWARE

- manage their third-party vendors
- continuously monitor for data breaches

Cyberattacks are committed for a variety of reasons including

financial fraud, information theft, activist causes, to deny service, disrupt critical infrastructure and vital services of government or an organization.

Cybersecurity is relevant to all systems that support an organization's business operations and objectives, as well as compliance with regulations and laws. An organization will typically design and implement cybersecurity controls across the entity to protect the integrity, confidentiality and availability of information assets.

Cyberattacks are committed for a variety of reasons including

- ✓ financial fraud
- ✓ information theft
- ✓ activist causes to deny service
- ✓ disrupt critical infrastructure and vital services

Potential targets to cyber criminals

- ✓ Customer data
- ✓ Employee data
- ✓ Intellectual property
- ✓ Third and fourth party vendors
- ✓ Product quality and safety
- ✓ Contract terms and pricing
- ✓ Strategic and operations plans
- ✓ Financial data

Who Should Own Cybersecurity Risk?

Chief Information Security Officer (CISO)

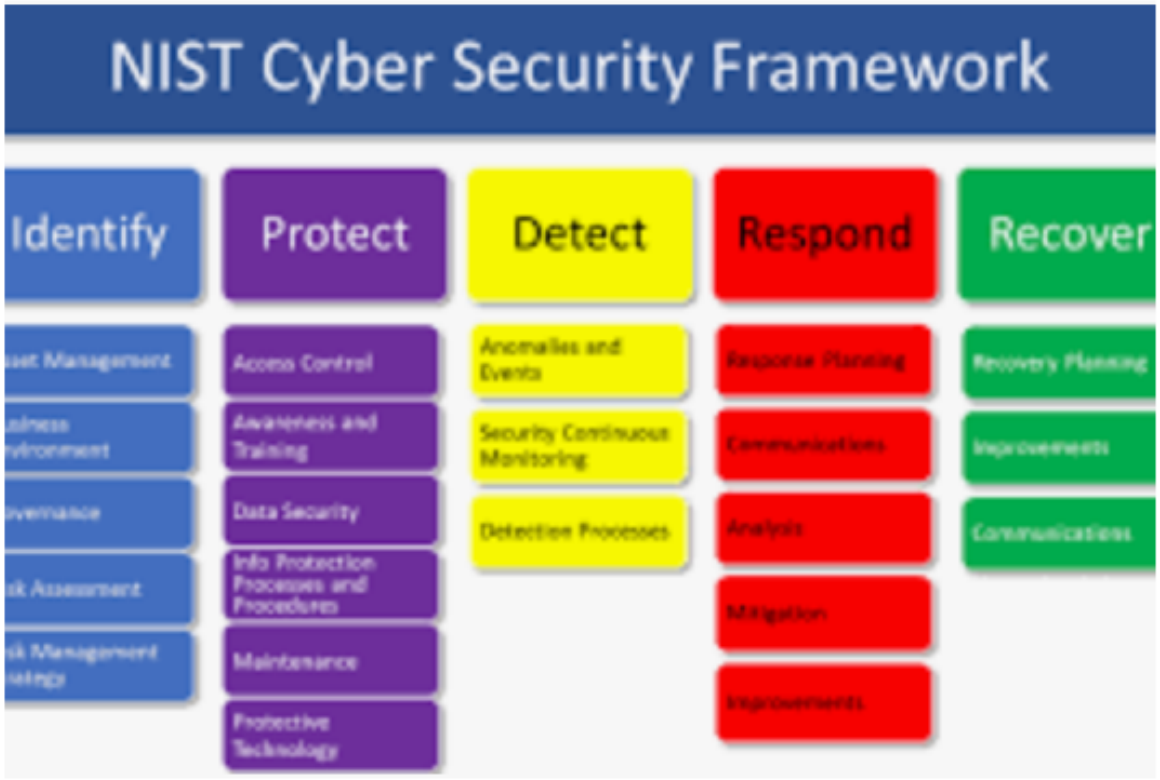
"Responsible for establishing and maintaining the enterprise vision, strategy and program to ensure information assets and customer data is adequately protected."

Common cyber defence activities

- ✓ Administering security procedures, training and testing
- ✓ Maintaining secure device configurations, up-to-date software, and vulnerability patches
- ✓ Deployment of intrusion detection systems and penetration testing
- ✓ Configuration of secure networks that can manage and protect business networks

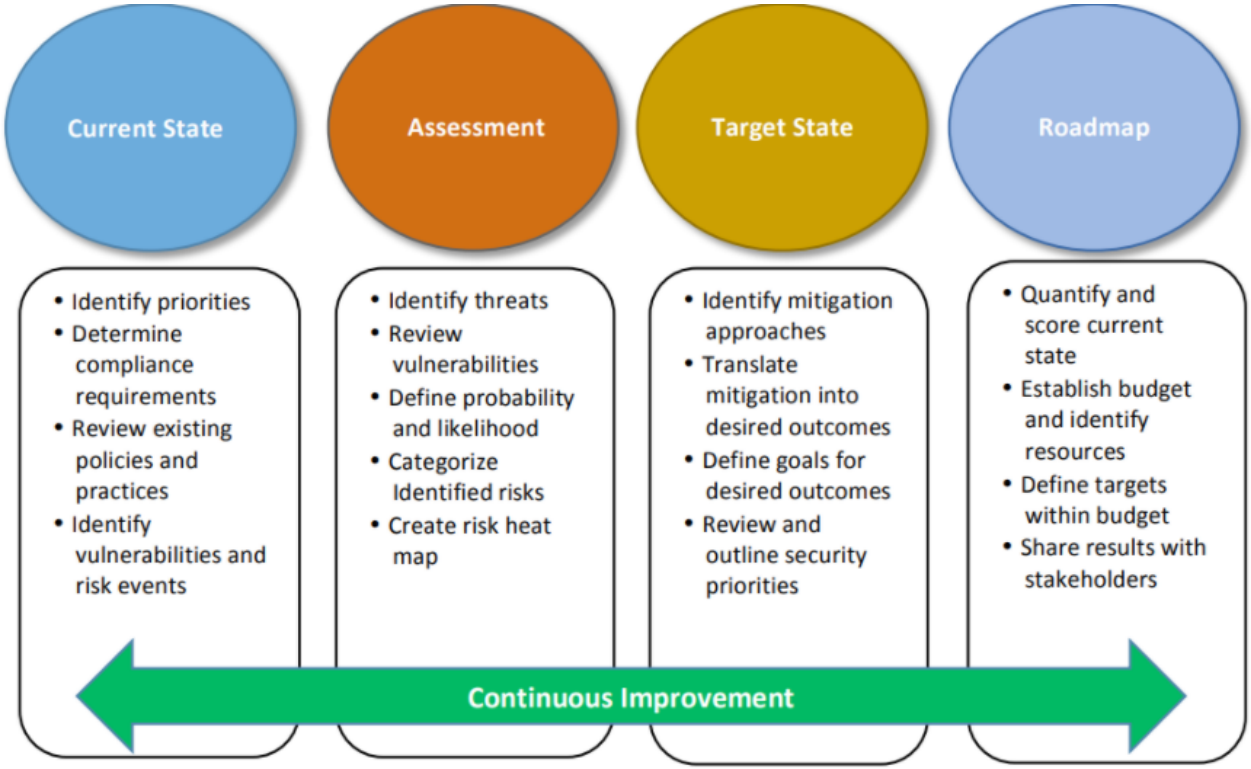
Common cyber defence activities

- ✓ Deployment of data protection and loss prevention programs and monitoring
- ✓ Restriction of access to least required privilege
- ✓ Encryption of data where necessary
- ✓ Proper configuration of cloud services
- ✓ Implementation of vulnerability management with internal and third-party scans
- ✓ Recruitment and retention of cybersecurity professionals



**NIST – National Institute of Standards and Technology*

Implementation Framework



Key Points

- The importance of identifying, addressing and communicating a potential breach outweighs the preventive value of traditional, cyclical IT security controls.
- Data breaches have massive, negative business impact and often arise from insufficiently protected data.
- External monitoring through third and fourth-party vendor risk assessments is part of any good risk management strategy.
- Without comprehensive IT security management, organizations are vulnerable to financial, legal, and reputational risk.

"Your organization can never be too secure. Cyber attacks can come from any level of your organization, so it's important to not pass it off to IT and forget about it."