Aalto-yliopisto
Aalto-universitetet
Aalto University

Cybersecurity Management

Managing and developing cyber capabilities

Lecture 1: Frameworks Overview for Cybersecurity Management

Euroopan unionin rahoittama – NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

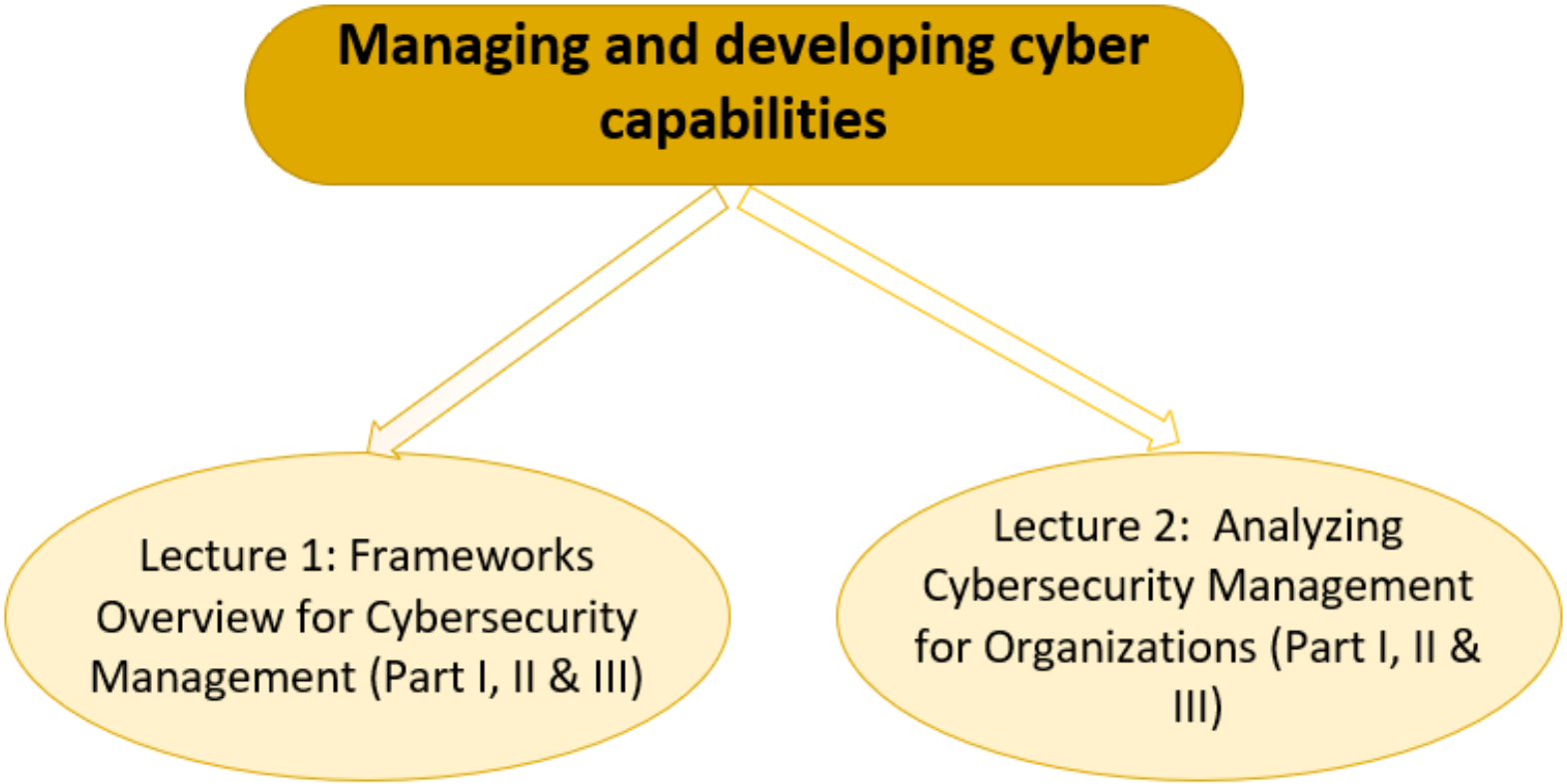
Cybersecurity Management

Dr. Tanesh Kumar

Staff Scientist,
Department of Information and
Communications Engineering, Aalto University

Email: **tanesh.kumar@aalto.fi**

Lecture Distribution



Outline: Lecture 1

- Lecture 1 is divided in three parts:
  - **Part I: Introduction to Cybersecurity Management Frameworks**
    - **What is cybersecurity management?**
    - **Need of cybersecurity management.**
    - **Cybersecurity design principles.**
    - **Need of cybersecurity framework.**
  - Part II: NIST Cybersecurity Framework
  - Part III: ISO/IEC-20071, CIS controls and others

Aalto-yliopisto
Aalto-universitetet
Aalto University

Cybersecurity Management

Managing and developing cyber capabilities

Lecture 1: Frameworks Overview for Cybersecurity Management

Part-I

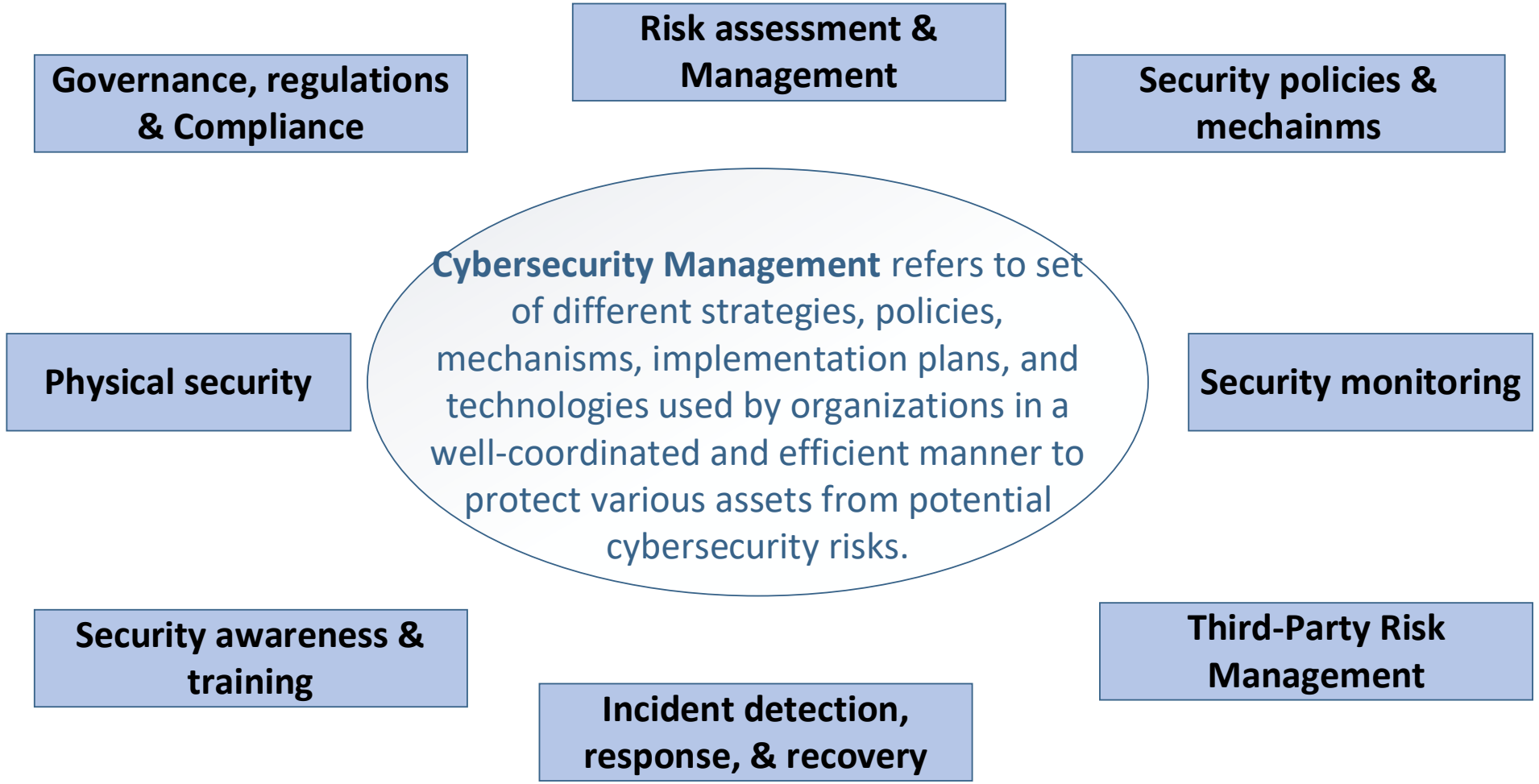
Introduction to Cybersecurity Management Frameworks

Euroopan unionin rahoittama – NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

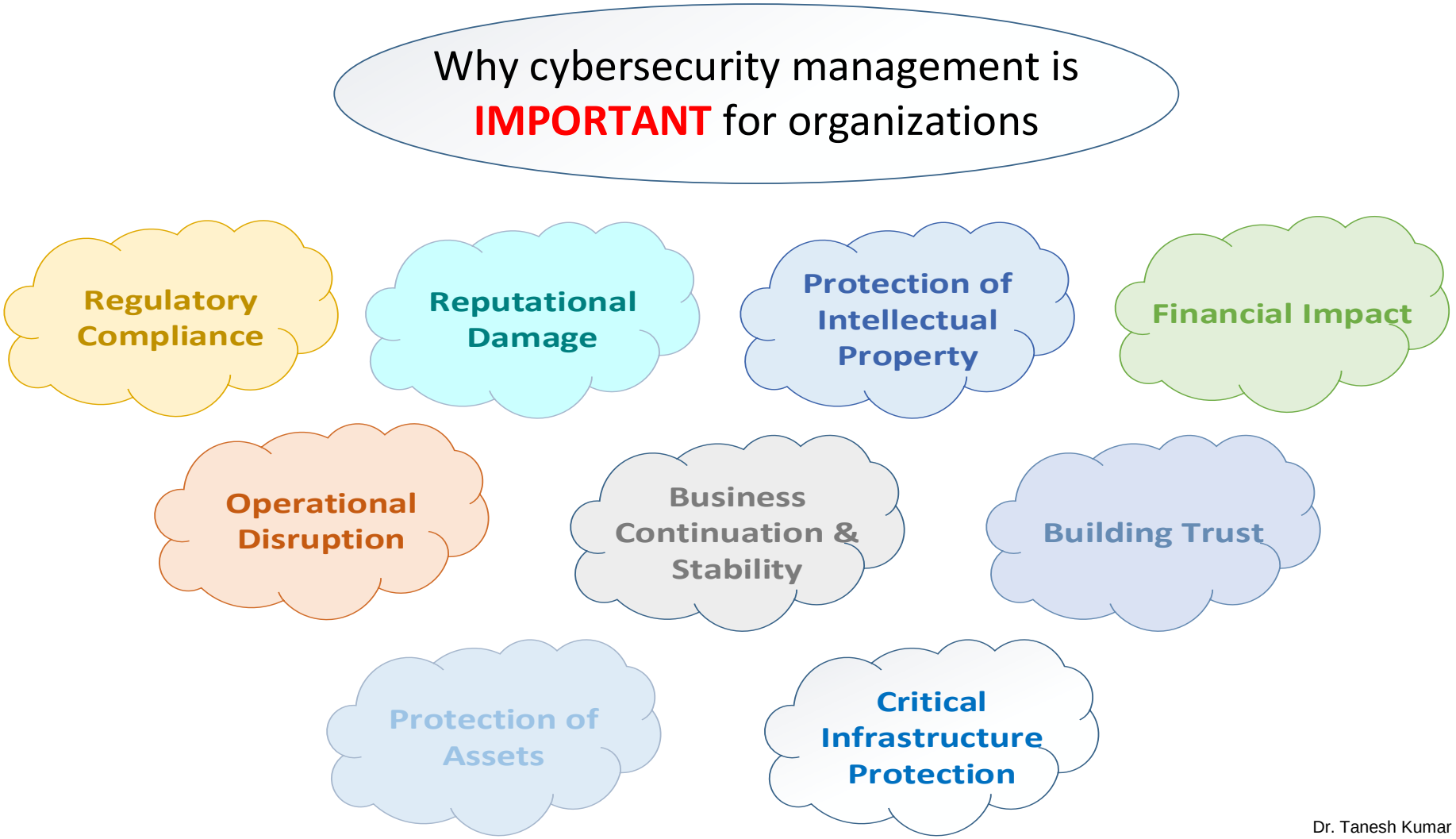
What is CYBERSECURITY MANAGEMENT?

Cybersecurity Management



NEED of Cybersecurity Management

Cybersecurity Management: *NEED*

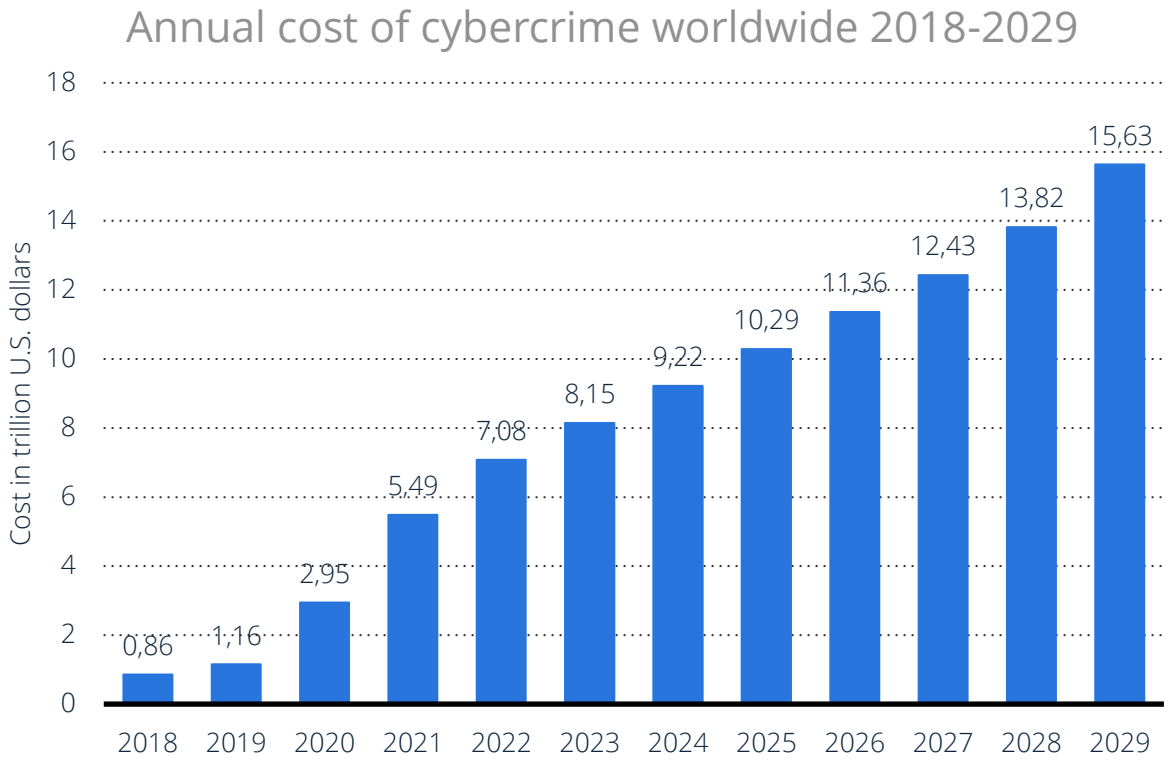


Cybersecurity Management: *NEED*

Estimated cost of cybercrime worldwide 2018-2029 (in trillion U.S. dollars)

- The 'Estimated Cost of Cybercrime' indicator in the cybersecurity market is projected to experience a consistent rise, reaching a total of 6.4 trillion U.S. dollars between 202 and 2029.

- Significantly, the 'Estimated Cost of Cybercrime' indicator in the cybersecurity market has been steadily increasing in recent years.



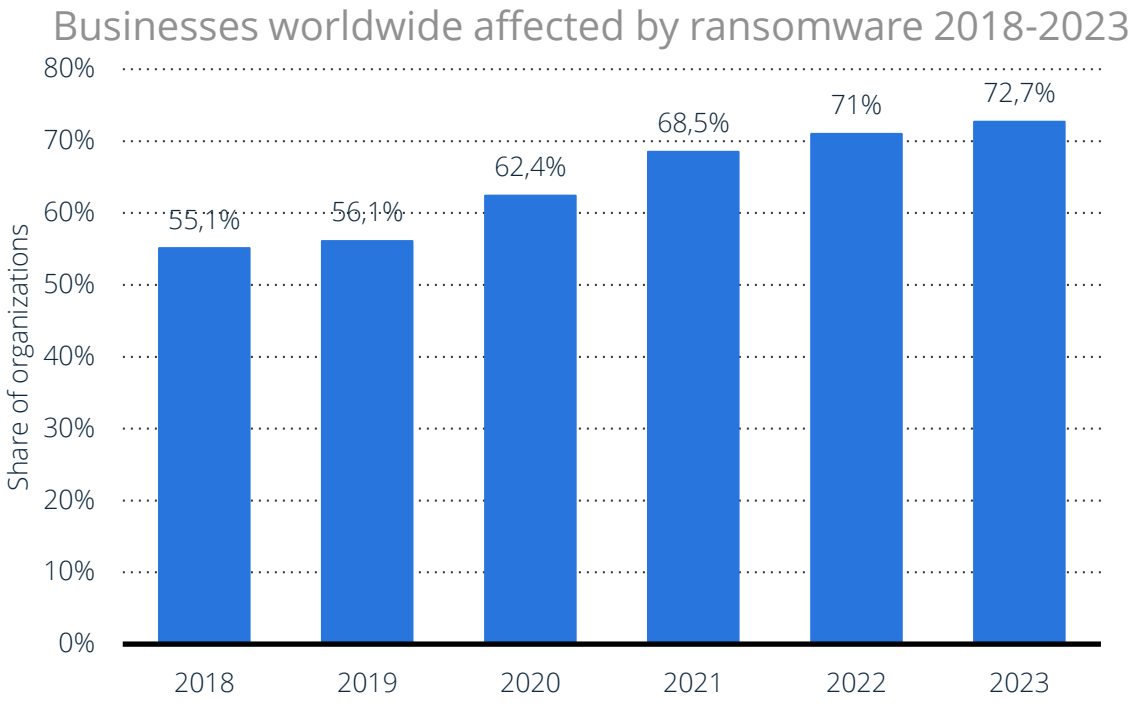
Note(s): Worldwide; 2018 to 2029
Further information regarding this statistic can be found on page 8.
Source(s): Statista; Statista Technology Market Insights; ID 1280009

Source: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

Cybersecurity Management: *NEED*

Annual share of organizations affected by ransomware attacks worldwide 2018 to 2023

- In 2023, ransomware attacks impacted more than 72 percent of businesses globally.
- In each year since 2018, over half of the survey respondents reported that their organizations had fallen victim to ransomware.



Note(s): Worldwide; 2018 to 2023; 1,200 respondents; IT security professionals and practitioners; all from organizations with more than 500 employees
Further information regarding this statistic can be found on page 8.
Source(s): CyberEdge; ID 204457

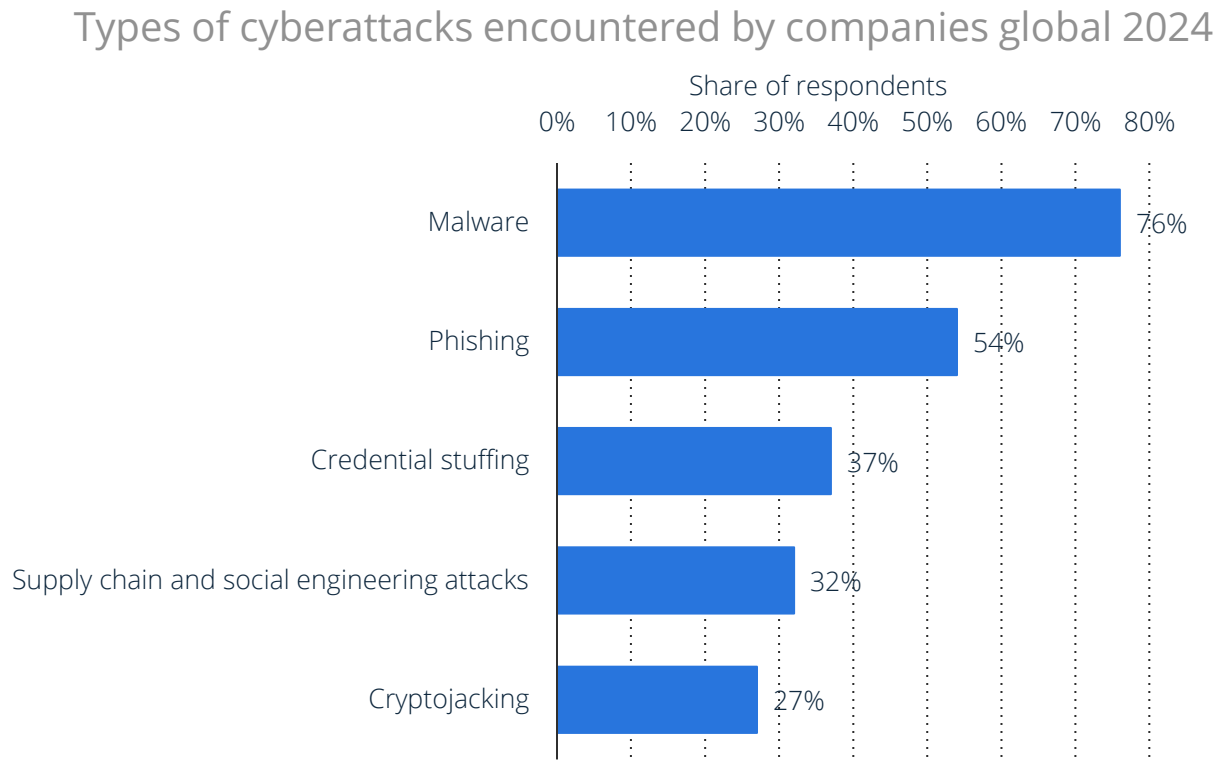
Source: https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

Cybersecurity Management: *NEED*

Types of cyberattacks experienced by organizations worldwide as of February 2024

- In February 2024, malware remained the most common cyberattack encountered by companies globally, with approximately three out of four organizations experiencing malware incidents.

- Phishing ranked as the second most common cyber threat, impacting 54% of companies globally.



Note(s): Worldwide; January and February 2024 ; 8,136 respondents
Further information regarding this statistic can be found on page 8.
Source(s): Cisco Systems; ID 1474819

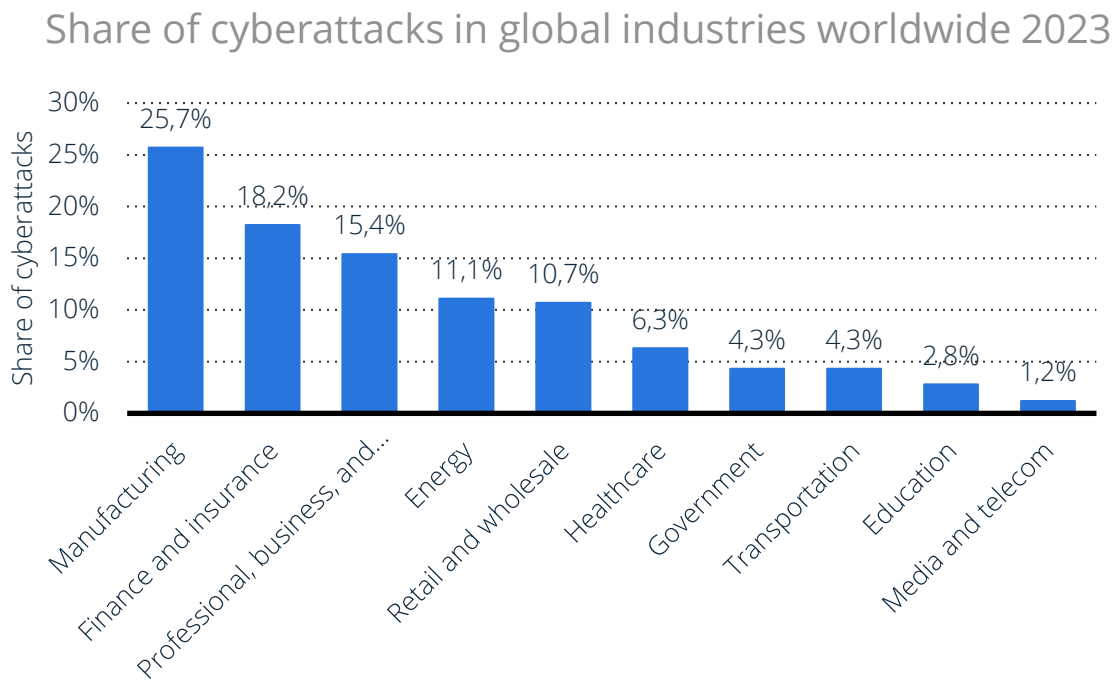
Source: https://www.statista.com/statistics/1474819/cyberattacks-by-businesses-worldwide-by-type/

Cybersecurity Management: *NEED*

Distribution of cyberattacks across worldwide industries in 2023

- In 2023, the manufacturing sector experienced the highest proportion of cyberattacks compared to other major industries globally.

- In this particular year, manufacturing companies faced close to 25% of all cyberattacks..



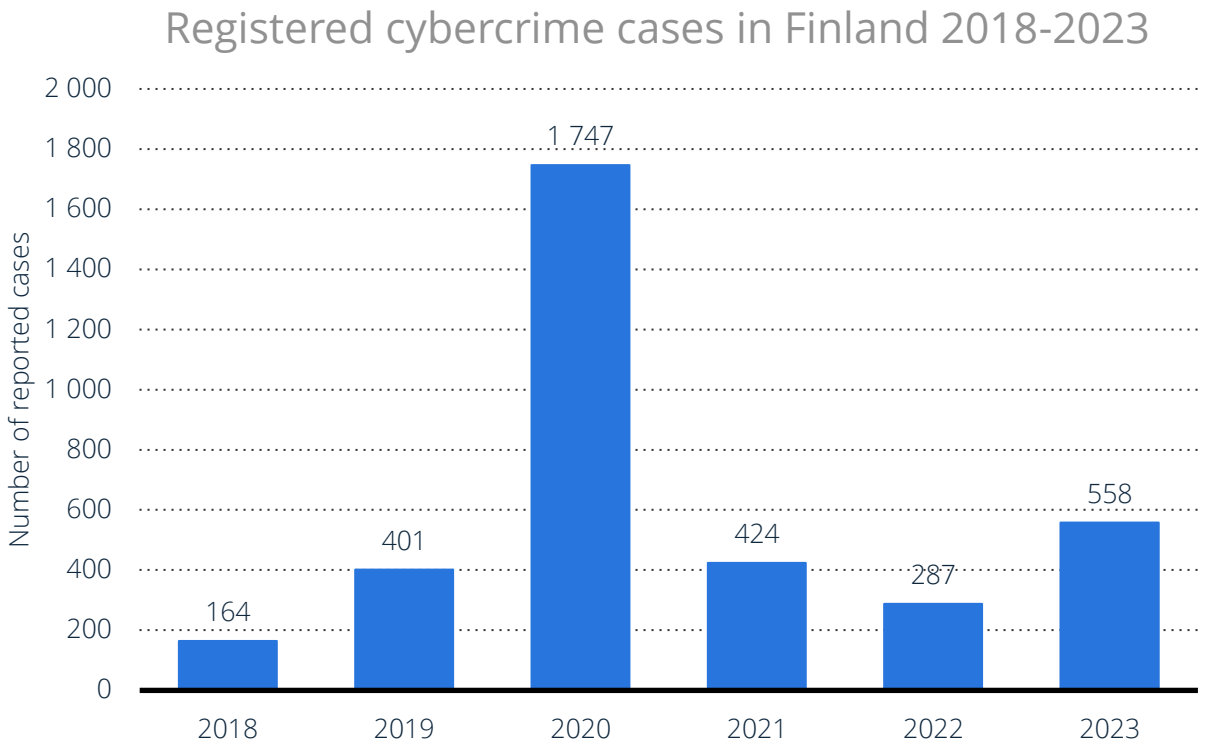
Note(s): Worldwide; 2023
Further information regarding this statistic can be found on page 8.
Source(s): IBM; ID 1315805

Source: https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide//

Cybersecurity Management: *NEED*

Number cybercrime cases registered in Finland from 2018 to 2023

- In 2023, Finland reported 558 instances of cybercrime.
- The highest number between 2018 and 2023 was recorded in 2020.
- The country reported a total of 1,747 incidents of cybercrime in the same year.



Note(s): Finland; 2018 to 2023
Further information regarding this statistic can be found on page 8.
Source(s): Statistics Finland; ID 1474911

Source: https://www.statista.com/statistics/1474911/cybercrime-cases-finland/

Cybersecurity DESIGN PRINCIPLES

Design Principles: The CIA Triad

- **Confidentiality:** Protection of information and disclosed to the authorized entities only
  - ***Example:*** Criminal steals customers' usernames, passwords, or credit card information

- **Integrity:** Ensuring accuracy of information, no unauthorized entity can change/alter information.
  - ***Example:*** Someone modify payroll information or a product design.

- **Availability:** Ensuring/Enabling the availability of information, data, and resources.
  - ***Example:*** Customers are unable to access online digital services

Design Principles: The CIA Triad: *Use Case*

Example: Banking/ATM Machine

- **ATMs (Automated Teller Machines)** serves be appropriate example of the CIA Triad because of their key role in handling sensitive financial transactions.

- ***Confidentiality:*** Two-factor authentication (ATM Card and PIN Code)
- ***Integrity:*** Ensure that transactions are accurately processed and recorded.
- ***Availability:*** ATMs are deployed in public places and can be accessed even if the banks are closed.

Need of Cybersecurity FRAMEWORK

Frameworks for Cybersecurity Management

- Digital transformation and advancements in technologies are changing the overall organization setting, business models/operation and customers interactions.
- Along with immense benefits, the increase integration of technology in the business creates huge threats landscape for organizations.
- Cyberthreats/incidents can cause massive damage to any company/organization, e.g., reputation, trust, and revenue.
- It is essential for every organization to take measures to protect the data, assets and infrastructures from potential cyber-threats
- Important to align cybersecurity approaches with the business goals.
- Highly vital for organizations to have cybersecurity education/training and culture.

Frameworks for Cybersecurity Management

- ‘Cybersecurity Framework’ provides voluntary recommendations for managing/minimizing cybersecurity risks based on existing standards, structured guidelines and best practices.
- Systematic and structured methods of managing and reducing cybersecurity risks.
- Popular categories of cybersecurity framework includes programs, controls and risks.
- Different organizations adopt frameworks to create a shared language with both internal stakeholders, customers and external third-parties.
- There isn’t any one common accepted cybersecurity framework that fits for all.
- Selecting an appropriate framework depends on various aspects, e.g., company size, threat scenario, business objectives, regulatory requirements.
- Numerous options of cybersecurity frameworks are already available, and organization can create their own customized based on their needs/requirements.

Framework for Cybersecurity Management

- Following are some of the well-known cybersecurity framework:
  - **NIST CSF** (Cybersecurity Framework)
  - **ISO/IEC 27001**
  - **CIS Critical Security Controls** (Center for Internet Security (CIS))
  - **COBIT** (Control Objectives for Information and Related Technologies)
  - **PCI-DSS** (Payment Card Industry Data Security Standards)
  - **SOC2** (Service Organization Control)
  - **GDPR** (General Data Protection Regulation)
  - **HIPAA** (Health Insurance Portability and Accountability Act)

Kiitos
aalto.fi