The evolution of the cyber threat landscape

Uroš Žust, CISA, CISM, CISSP, PMP, aPRIS

26 February 2025

forvis mazars

Introduction
Why the sudden hype?

The reason for Cyber threats being such a hot topic

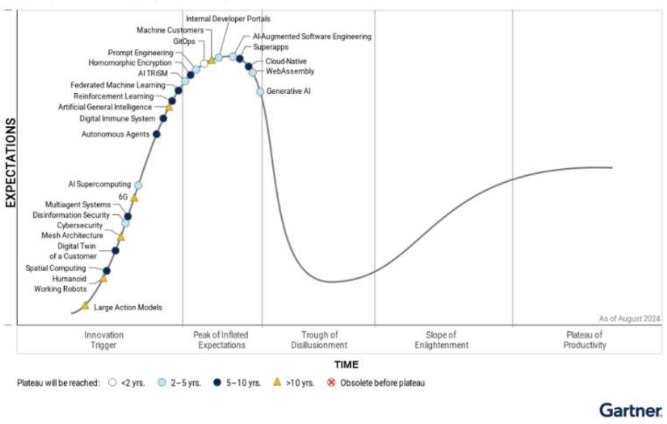
- Cyber incidents are continuously on the rise.
- Cyber actors are evolving and improving over time
- Crime in cyberspace is now a business - lower risk and higher reward
- Companies are increasing their reliance on technology as technology represents a competitive advantage and has an impact on all business processes
- Remote work is now a common commodity
- The trend of digitalization will not only continue, but is predicted to increase in the future
- New technologies are constantly being introduced, and they bring a new set of threats along

Introduction
Emerging Technologies

Gartner Hype Cycle for Emerging Technologies 2024

- Impossible to predict all potential technologies that may impact the business environment of the future.
- We see rapid changes in predictions every year.
- Some key emerging areas include:
  - **Autonomous AI:** AI systems that can operate with minimal human oversight, improve themselves and become effective at decision-making in complex environments (multiagent systems, large action models, machine customers, humanoid working robots, autonomous agents, and reinforcement learning).
  - **Boost Developer Productivity**: more than writing code quickly (AI-augmented software engineering, cloud-native, GitOps, internal developer portals, prompt engineering and WebAssembly).
  - **Empower With Total Experience**: strategy that creates superior shared experiences by intertwining customer, employee and user experience practices (digital twin of a customer, spatial computing, superapps and 6G).
  - **Deliver Human-Centric Security and Privacy**: building resilience by using security and privacy techniques that create a culture of mutual trust and awareness of shared risks between teams (AI TRiSM, cybersecurity mesh architecture, digital immune system, disinformation security, federated machine learning and homomorphic encryption).

Figure 1. Hype Cycle for Emerging Technologies, 2024



Introduction
Important Organizations

Some organizations active in the space of cybersecurity

- **The European Union Agency for Cybersecurity (ENISA)** - contributes to EU cyber policy and helps prepare EU countries for future cyber challenges.
- **The European cyber crisis liaison organisation network (EU CyCLONe)** - cooperation network for EU national authorities in charge of cyber crisis management
- **Cybersecurity and Infrastructure Security Agency (CISA)** – US operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience
- **ISACA** – international organization focused on focused on IT governance.
- **International Organization for Standardization (ISO)** - international standard development organization composed of representatives from the national standards organizations of member countries, responsible for ISO 27XXX standards
- **The Center for Internet Security (CIS)** – nonprofit organization, responsible for the CIS Controls and CIS Benchmarks, globally recognized best practices for securing IT systems and data
- **National Institute of Standards and Technology (NIST)** – US institute, responsible for NIST Cybersecurity Framework, an important framework for addressing the cybersecurity challenges
- …

Threat Landscape
Top technical threats

CISCO Cyber Threat Trends Report

Top Threats (based on threat categories of blocked domains):

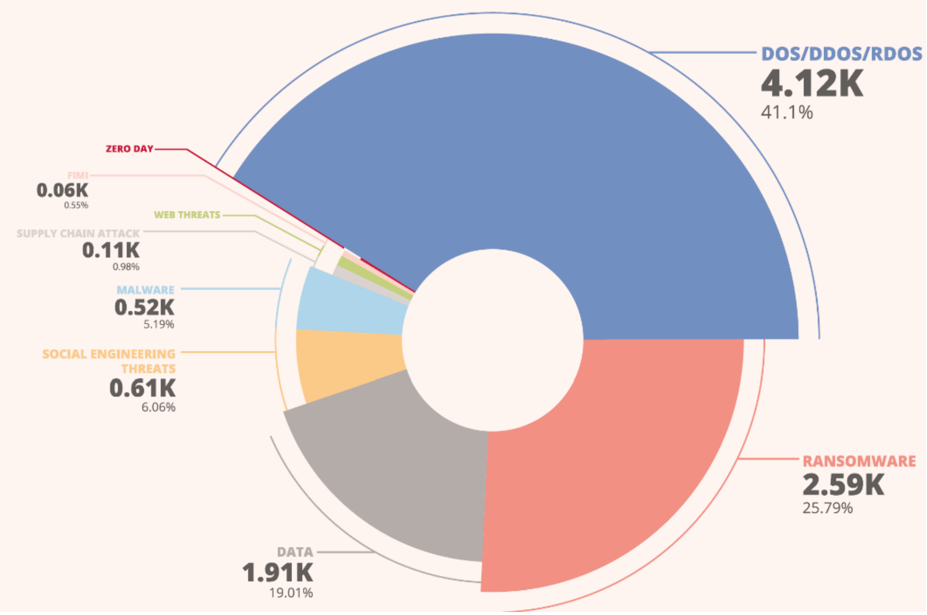
1. **Information stealer** – malicious programs designed to collect various kinds of personal and financial information
2. **Trojan** – malware that mislead users of their true intent establishing backdoor access to systems
3. **Ransomware** – malware that encrypts the files on a victim’s computer or network resulting in ransom payment demands
4. **RAT (Remote Access Trojans)** – malware that provide a backdoor for administrative control over the targeted computer
5. **APT** – complex, sophisticated threats that target specific entities to steal information or disrupt operations
6. **Botnet** – network of infected computers, known as bots, which are controlled by a threat actor
7. **Dropper** – malware designed to install other malwares onto a target system
8. **Backdoor** – method by which unauthorized users can bypass normal authentication and gain remote access

Threat Landscape
Top threats of 2024

ENISA Threat Landscape 2024 Report

- Throughout the latter part of 2023 and the initial half of 2024, there was a notable escalation in cybersecurity attacks, setting new benchmarks in both the variety and number of incidents, as well as their consequences.
- The 7 prime cybersecurity threats in 2024:
  1. Threats against availability: Denial of Service
  2. Ransomware
  3. Threats against data (breaches, leaks)
  4. Social Engineering
  5. Malware
  6. Supply chain attacks
  7. Information manipulation and interference

Incidents by threat type (July 2023 to June 2024)



Threat Landscape
Trends observed in 2024

ENISA Threat Landscape 2024 Report

- Threats against availability (DDoS) and Ransomware ranked at the top for another year.
- Advancements in defensive evasion techniques (LOTL, LOTS) .
- There has seen a sharp increase in Business Email Compromise (BEC) incidents.
- Emergence of AI tools specialised for cyber criminals.
- Recent surge in mobile banking trojans has been observed.
- Malware-as-a-Service (MaaS) offerings are evolving.
- Supply chain compromises through social engineering are emerging.
- DDoS-for-Hire allows large-scale attacks.
- Geopolitics continued to be a strong driver for cyber malicious operations.
- Information manipulation continues to be a key element of modern warfare.

Threat Landscape
Motivation and actors for cybersecurity incidents or targeted attacks in 2024

ENISA Threat Landscape 2024 Report

Four main types of threat actors have been identified:

- **State-nexus actors;** objective is primarily espionage and disruption, sometimes directed by the military, intelligence or state control apparatus of their country;
- **Cybercrime actors and hacker-for-hire actors;** objective is mostly financial gain or profits in general;
- **Private Sector Offensive actors (PSOA);** commercial entities that engage in the cyber-surveillance industry, they specialize in developing and selling cyberweapons, including "zero-day" exploits and malicious software;
- **Hacktivists;** often fuelled by strong motivations, their objectives often involve disruption, and they use hacking to affect some form of political or social change.
- **Insider Threat Actor** is not on the list, but suspected that should be as organisations remain reluctant to share these kind of details

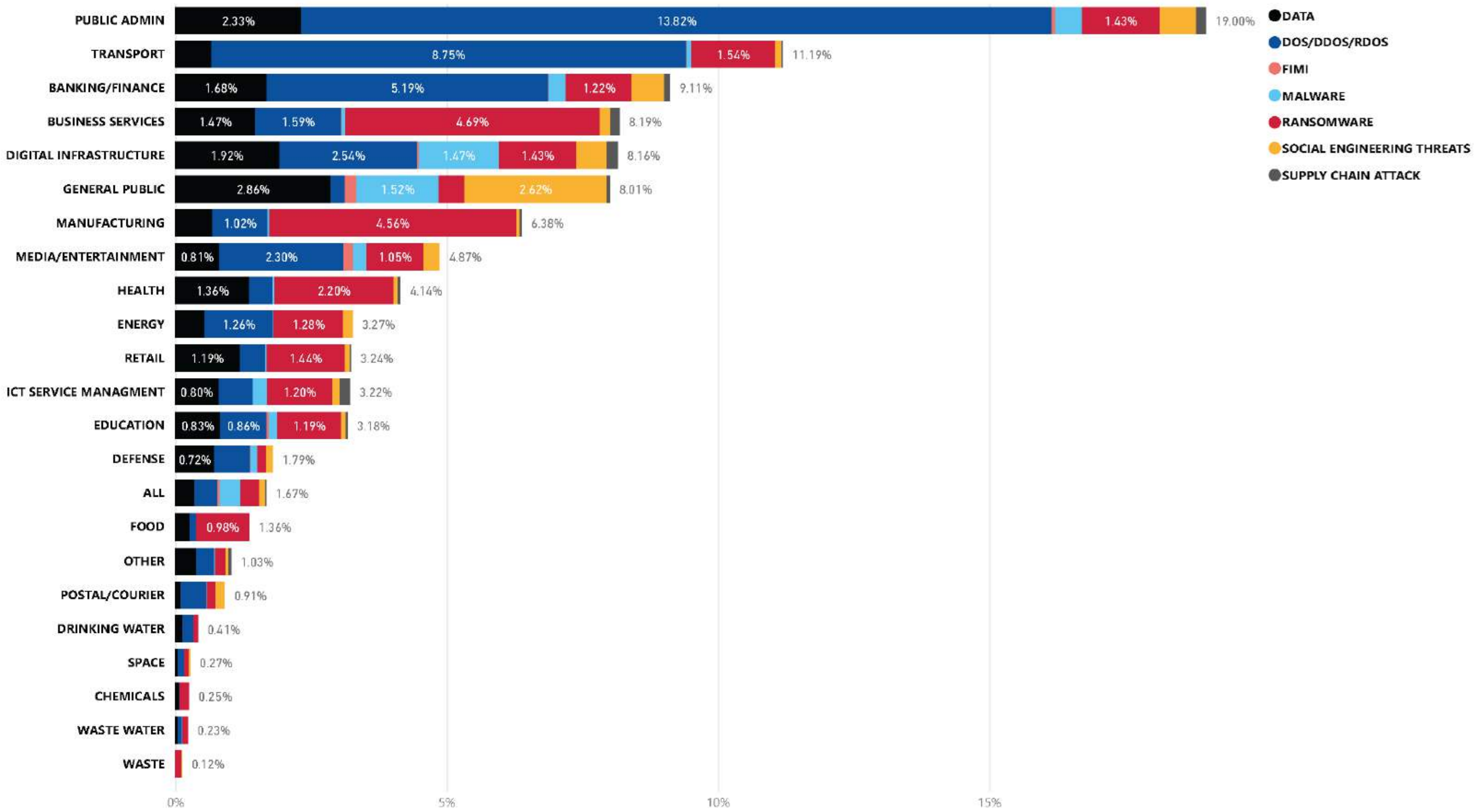
Five distinct kinds of motivation that can be linked to threat actors have been defined:

- **Financial gain**: any financially related action (carried out mostly by cybercrime groups);
- **Espionage**: gaining information on IP (intellectual property), sensitive data, classified data (mostly executed by state-sponsored groups);
- **Destruction**: any destructive action that could have irreversible consequences;
- **Ideological**: any action backed up with an ideology behind it (such as hacktivism).
- **Unknown**: unclear what the motivation was.

Threat Landscape

Threats per sector in 2024

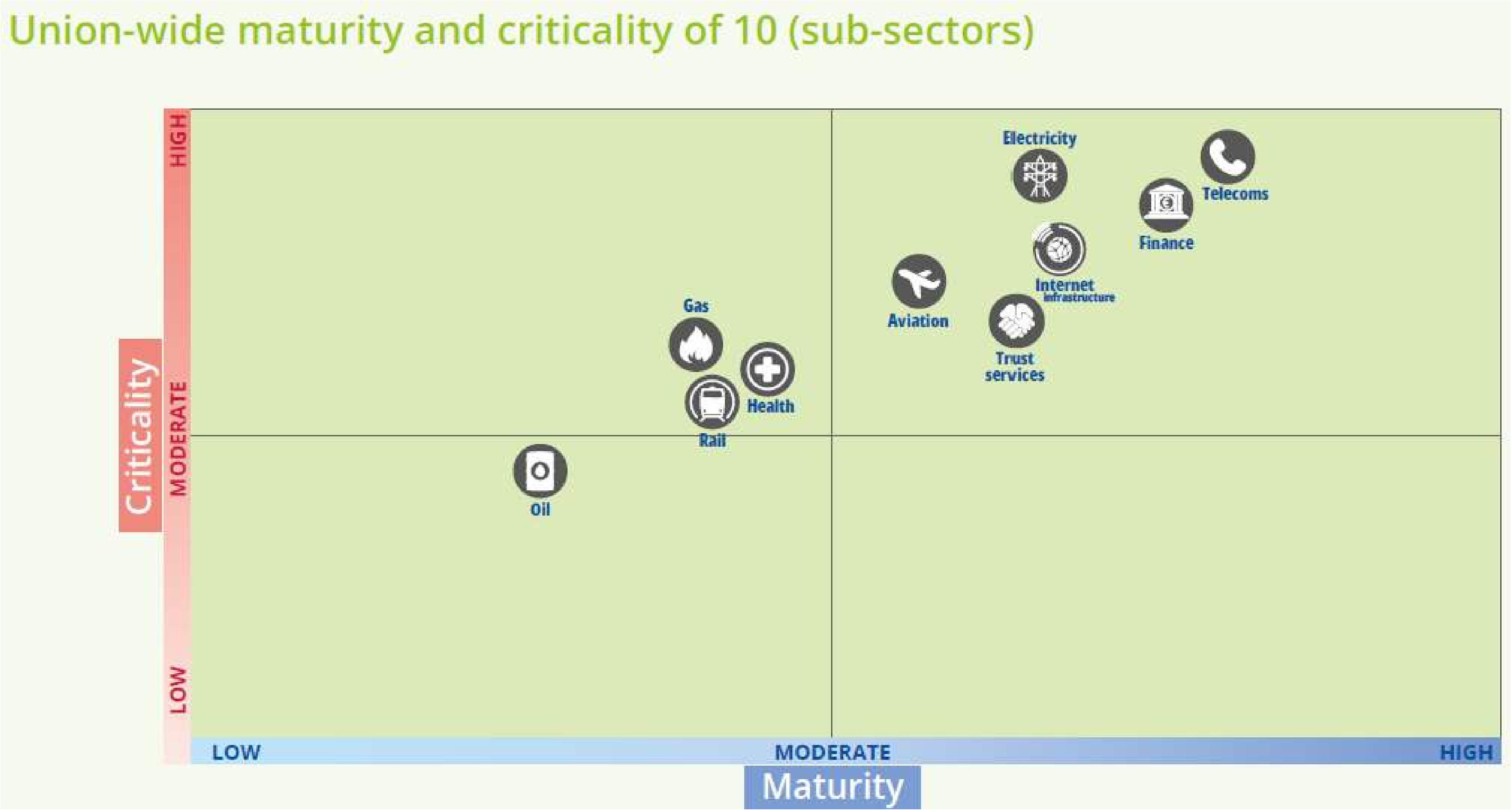
ENISA Threat Landscape 2024 Report



Threat Landscape

Criticality of sectors

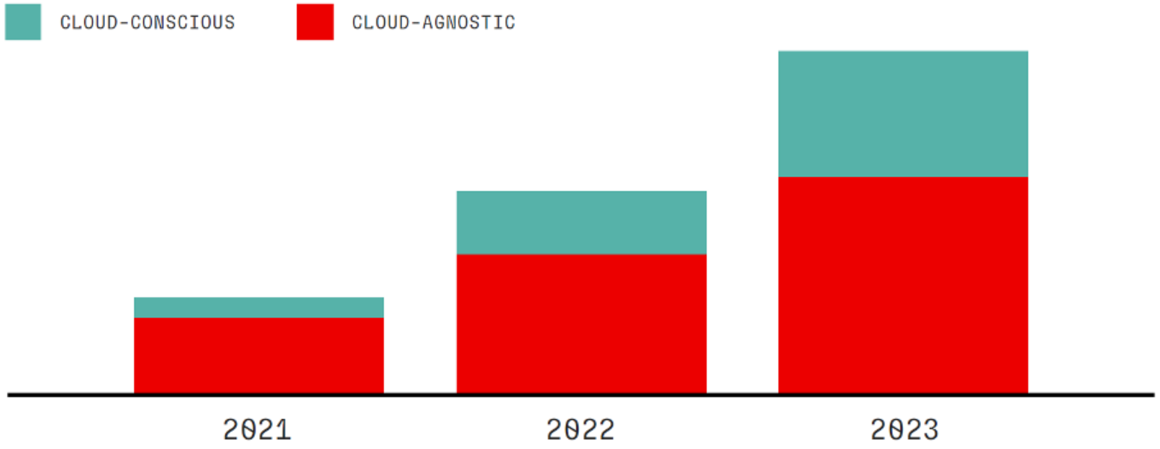
ENISA State of Cybersecurity in EU 2024 Report



Threat Landscape
Intrusions in 2024

CrowdStrike 2024 Global Threat Report

INCIDENTS IN THE CLOUD



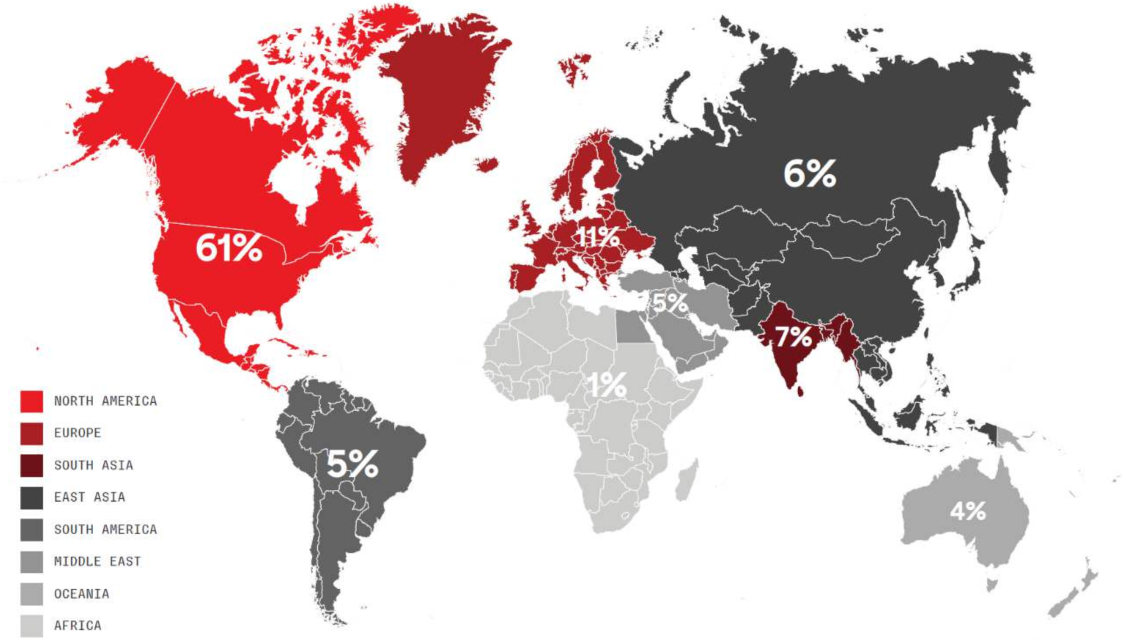
▲ **110%** **CLOUD-CONSCIOUS CASES**

ACTORS ARE AWARE THEY GAINED ACCESS TO A VICTIM-OWNED CLOUD ENVIRONMENT AND USE THEIR ACCESS TO ABUSE THE VICTIM-OWNED CLOUD SERVICE

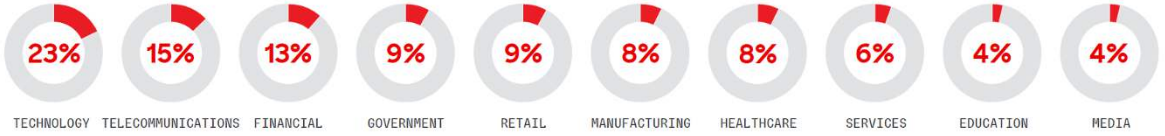
▲ **60%** **CLOUD-AGNOSTIC CASES**

ACTORS EITHER WERE NOT AWARE THEY HAD COMPROMISED A CLOUD ENVIRONMENT OR DID NOT TAKE ADVANTAGE OF CLOUD FEATURES

Interactive Intrusions by Region



Interactive Intrusions by Industry



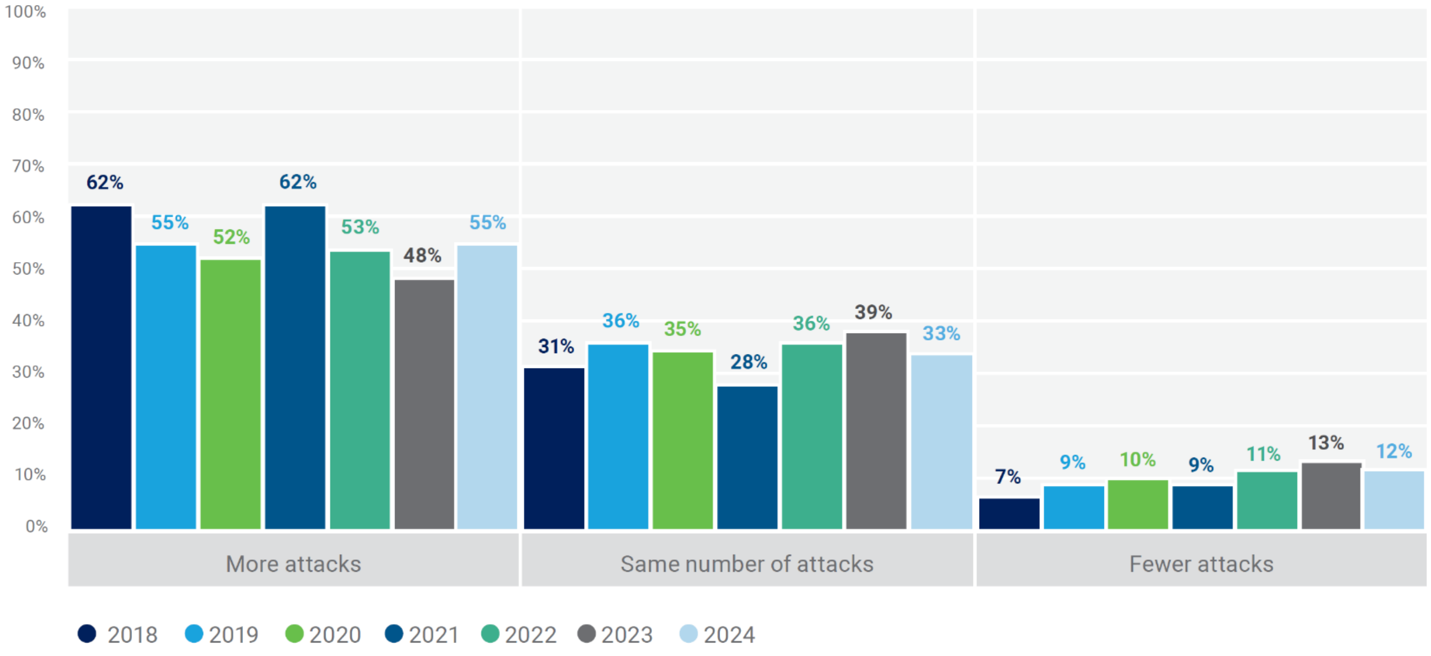
Threat Landscape

Cybersecurity Threats

ISACA State of Cybersecurity 2024 Report

- Data show a significant drop in cybersecurity funding levels
- Increasing numbers of attacks and threats do not correlate with increasing cybersecurity budgets
- Insiders still remain an important threat actor (21% of cases) with malicious insiders (12%) overtaking non-malicious insiders (9%)
- ISACA lists Social Engineering as the predominant attack type (19%)

FIGURE 31: Year Over Year Comparison of Cybersecurity Attack Reporting[12]

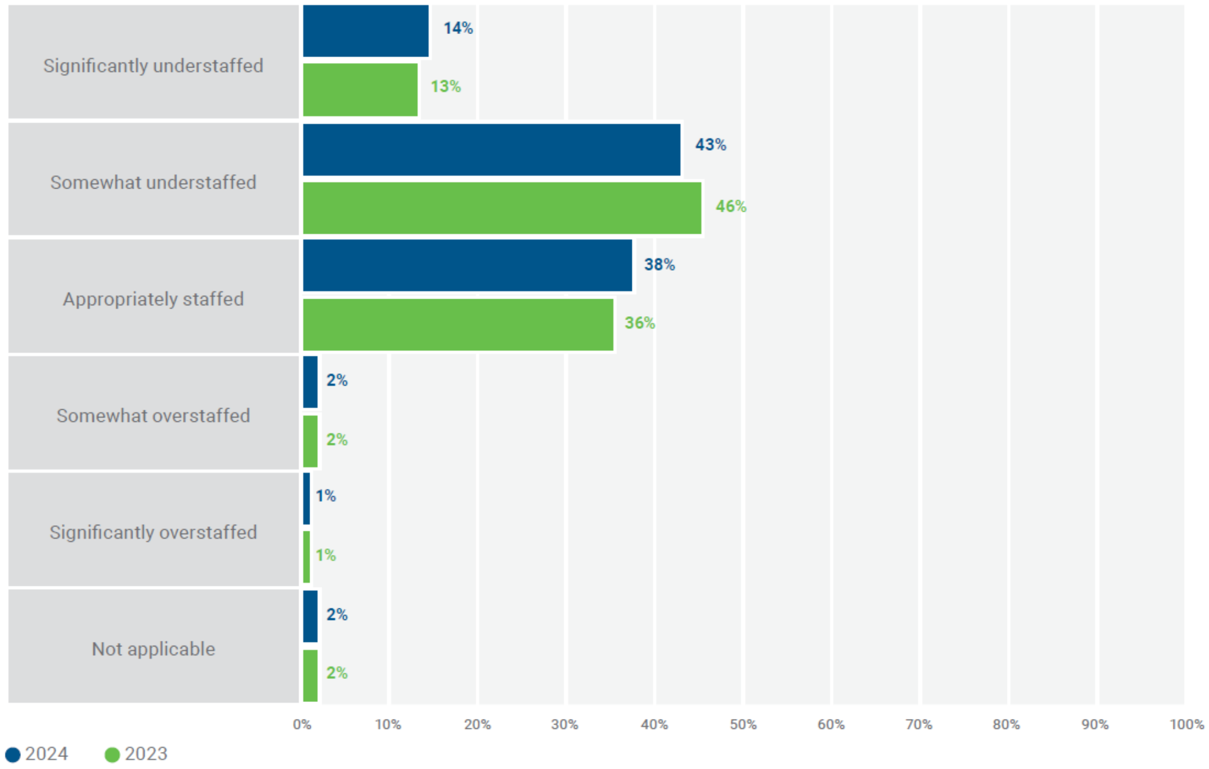


Threat Landscape
Cybersecurity staffing

ISACA State of Cybersecurity 2024 Report

- The current staffing in Cybersecurity remains a problem.
- The aging workforce is growing.
- 66 percent of respondents report that occupational stress is much higher than five years ago.
- 81 percent of respondents attribute the higher stress to an increasingly complex threat environment.
- Leveraging training to allow interested non-security professionals to move into security roles and increased use of contractors or consultants remain the primary mitigations for the cybersecurity technical skills gaps.

How would you describe the current staffing of your organization's cybersecurity team?



Threat Landscape
The Crime/Fraud Perspective

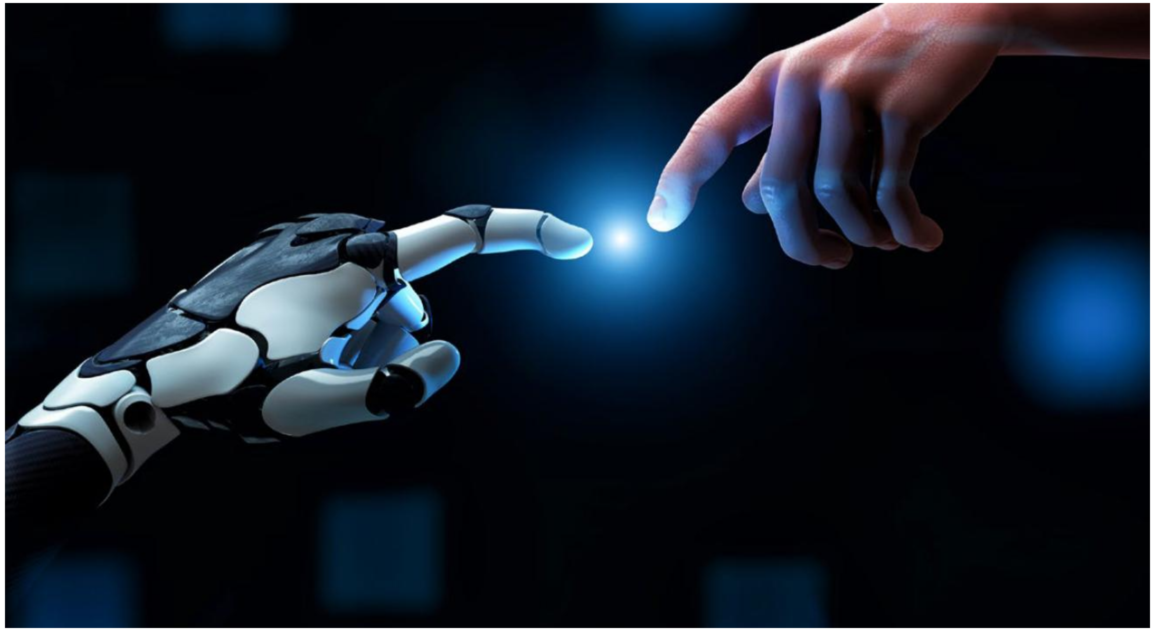
IOCTA 2024 Internet Organised Crime Threat Assessment

Main Threats:

- Investment fraud
- Business email compromise
- Romance fraud
- Growing volume of online child sexual abuse material

Issues:

- New technologies and widening use of digital infrastructure enable easier entry into the cybercriminal market
- Darkweb enables cybercrime, providing knowledge sharing and tools
- Fraud as a service is on the rise
- Cryptocurrencies enable cybercrime due to anonymity



Threat Landscape
Future predictions

IOCTA 2024 Internet Organised Crime Threat Assessment

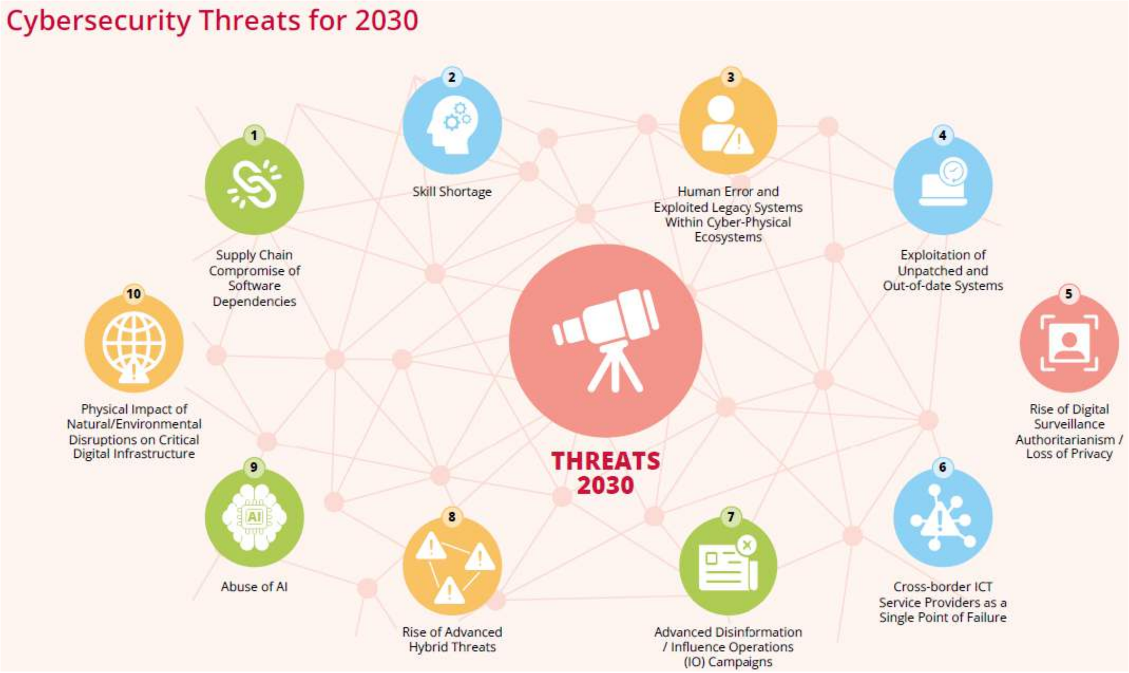
- AI-assisted cybercrime has only just begun
- Abusing technologies (E2EE, Crypto, etc.)
- Emergence of new RaaS brands
- Protecting EU payment systems (PSD2/3, PCI DSS, etc.)
- Bolstering the EU against illicit content online (EU Digital Services Act, ordinals)
- The future of crypto (higher adoption, higher exposure)
- Renewed focus on offender prevention (COP)

Threat Landscape
What does the future hold?

ENISA Foresight Cybersecurity Threats for 2030 Report

Top threats for 2030:

1. Supply Chain Compromise of Software Dependencies
2. Skill Shortage
3. Human Error and Exploited Legacy Systems Within Cyber-Physical Ecosystems
4. Exploitation of Unpatched and Out-of-date Systems within the Overwhelmed Cross-sector Tech Ecosystem
5. Rise of Digital Surveillance Authoritarianism / Loss of Privacy
6. Cross-border ICT Service Providers as a Single Point of Failure
7. Advanced Disinformation / Influence Operations (IO) Campaigns
8. Rise of Advanced Hybrid Threats
9. Abuse of AI
10. Physical Impact of Natural/Environmental Disruptions on Critical Digital Infrastructure


Cybersecurity Threats for 2030
THREATS 2030
1 Supply Chain Compromise of Software Dependencies
2 Skill Shortage
3 Human Error and Exploited Legacy Systems Within Cyber-Physical Ecosystems
4 Exploitation of Unpatched and Out-of-date Systems
5 Rise of Digital Surveillance Authoritarianism / Loss of Privacy
6 Cross-border ICT Service Providers as a Single Point of Failure
7 Advanced Disinformation / Influence Operations (IO) Campaigns
8 Rise of Advanced Hybrid Threats
9 AI
Abuse of AI
10 Physical Impact of Natural/Environmental Disruptions on Critical Digital Infrastructure

forvis mazars

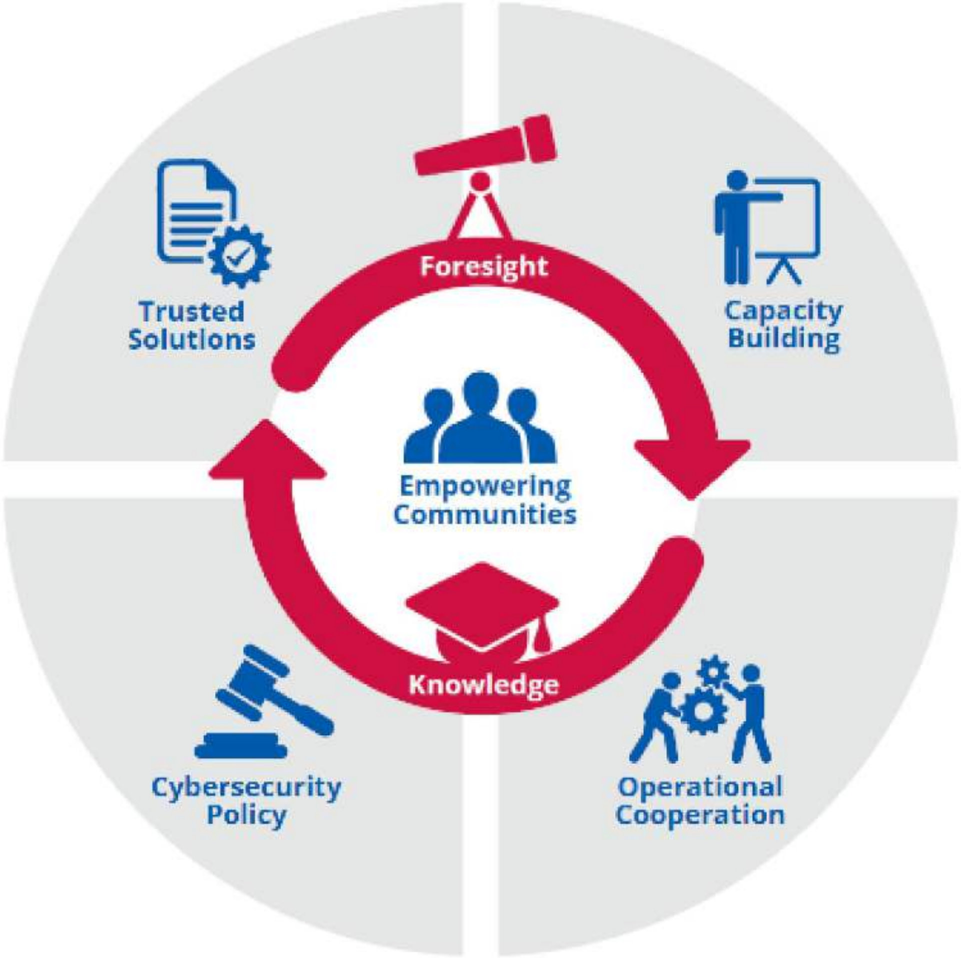
Response

How do we prepare?

ENISA Foresight Cybersecurity Threats for 2030 Report

ENISA Strategic Objectives:

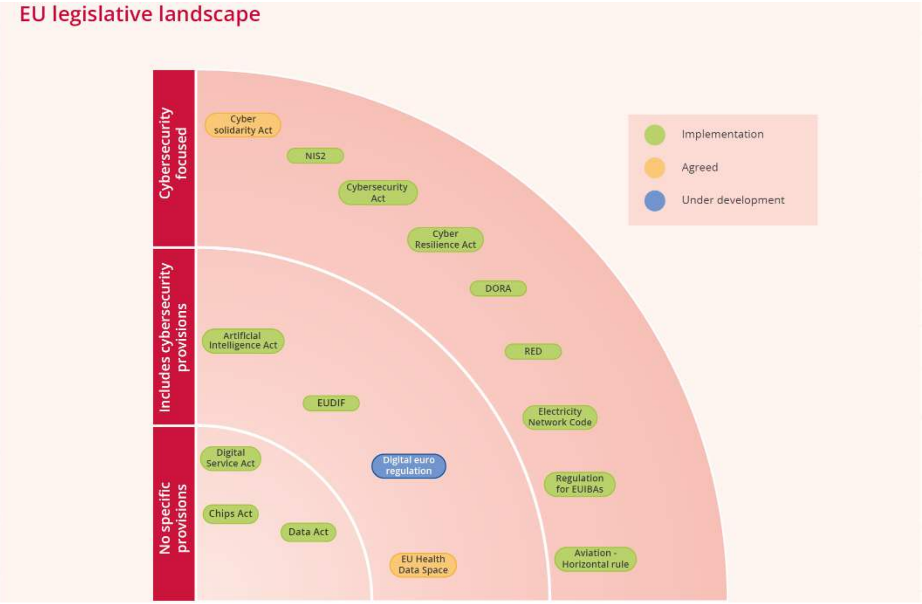
1. Empowered and engaged communities across the cybersecurity ecosystem.
2. Cybersecurity as an integral part of EU policies.
3. Effective cooperation amongst operational actors within the Union in case of massive cyber incidents.
4. Cutting-edge competencies and capabilities in cybersecurity across the Union
5. High level of trust in secure digital solutions.
6. Foresight on emerging and future cybersecurity challenges.
7. Efficient and effective cybersecurity information and knowledge management for Europe.



Response
EU Regulatory requirements and considerations

Acts and regulations related to cybersecurity and resilience in the EU area

- **The Cyber Resilience Act** – regulation on cybersecurity requirements for devices with digital elements (more secure hardware and software)
- **Cybersecurity Act**– primarily focused on strengthening the role of ENISA as the central authority for operational cooperation and crisis management in the EU and for the certification of ICT products, processes and services
- **Cyber Solidarity Act** – A joint effort to improve cyber risk response within the EU, focusing on the European Cybersecurity Shield and the Cyber Emergency Mechanism, all with the intention to provide better methods of defending against cyber risks.
- **NIS 2 Directive** – focused on ensuring a common high level of cyber resilience assurance for essential and critical organisations
- **Critical Entities Resilience (CER) Directive** – a directive connected to NIS 2, focused mainly on the physical aspect of security
- **Digital Operational Resilience Act (DORA)** – Financial sector-specific regulation intended to make financial systems more resilient to cyber threats. It focuses on improving ICT risk management, incident reporting, operational resilience testing and the involvement of external providers.
- …



Response

What is the solution?

- Focus on employees (users) with adequate training
- Performing regular assessments will help identify vulnerabilities before hackers do and prioritize actions
- Utilizing security frameworks is incredibly important
- Implementing MFA needs to become a baseline standard
- Patching needs to be a diligent activity
- Cloud environments will need enhanced protections
- Consolidation of security tools/platforms is necessary
- Supply chain will require extended attention
- A risk-based approach to cybersecurity needs to shift an enterprise's strategy from being reactive to proactive

Summary

- Advances in AI tools have already enabled new types of fraud and will continue to do so in the years to come.
- Deepfake forgery technologies are expected to be very important.
- Despite all the new developments, ransomware remains one of the biggest threats.
- Intrusions into hybrid and cloud environments are an important new challenge for information security.
- Cyber regulation is trying to help raise the security standard.
- It‘s important to cover both the basics (security governance) as well as the details (implementation).
- User awareness remains key.

Contact

Forvis Mazars

Verovškova ulica 55A
1000 Ljubljana
Slovenia

Uroš Žust

CISA, CISM, CISSP, PMP, aPRIS
Partner, IT Assurance & Advisory

+386 41 395 386
uros.zust@mazars.si

Follow us

LinkedIn:

www.linkedin.com/company/Forvis-Mazars-Slovenia
www.linkedin.com/company/ForvisMazarsGroup

X:
www.twitter.com/ForvisMazarsGroup

Facebook:

www.facebook.com/Forvis.Mazars.Slovenija
www.facebook.com/ForvisMazarsGroup

Instagram:

www.instagram.com/Forvis.Mazars.Slovenia
www.instagram.com/ForvisMazarsGroup

More on **www.forvismazars.com**

Forvis Mazars Group SC is an independent member of Forvis Mazars Global, a leading professional services network. Operating as an internationally integrated partnership in over 100 countries and territories, Forvis Mazars Group specialises in audit, tax and advisory services. The partnership draws on the expertise and cultural understanding of over 35,000 professionals across the globe to assist clients of all sizes at every stage in their development.

The contents of this document are confidential and not for distribution to anyone other than the recipients. Disclosure to third parties cannot be made without the prior written consent of Forvis Mazars Group SC.

forvis
mazars