The evolution of the cyber threat landscape

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

27 November 2024

forvis mazars

Introduction
Why the sudden hype?

The reason for Cyber being such a hot topic

- Cyber incidents are 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
- Technology represents a competitive advantage and has an impact on all business processes
- New technologies are constantly being introduced, and they bring a new set of threats along
- Remote work is now a common commodity
- The trend of digitalization will not only continue, but is predicted to increase in the future

forvis mazars

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
  4. Social Engineering
  5. Malware
  6. Supply chain attacks
  7. Information manipulation and interference

Threat Landscape
Trends observed in 2024

ENISA Threat Landscape 2024 Report

- Threats against availability (DDoS) and Ransomware ranked at the top during the reporting period for another year.
- Advancements in defensive evasion techniques.
- 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

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

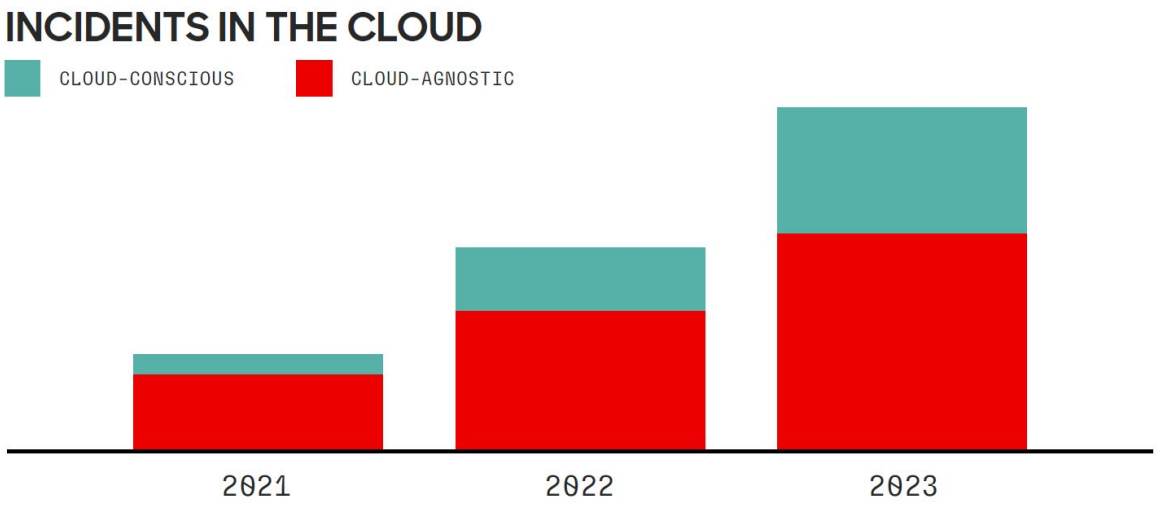
- **Financial gain**: any financially related action (carried out mostly by cybercrime groups);
- **Espionage**: gaining information on IP (intellectual property), sensitive data, classified data (mostly executed by state-sponsored groups);
- **Destruction**: any destructive action that could have irreversible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

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.

Threat Landscape
Intrusions in 2024

CrowdStrike 2024 Global Threat Report

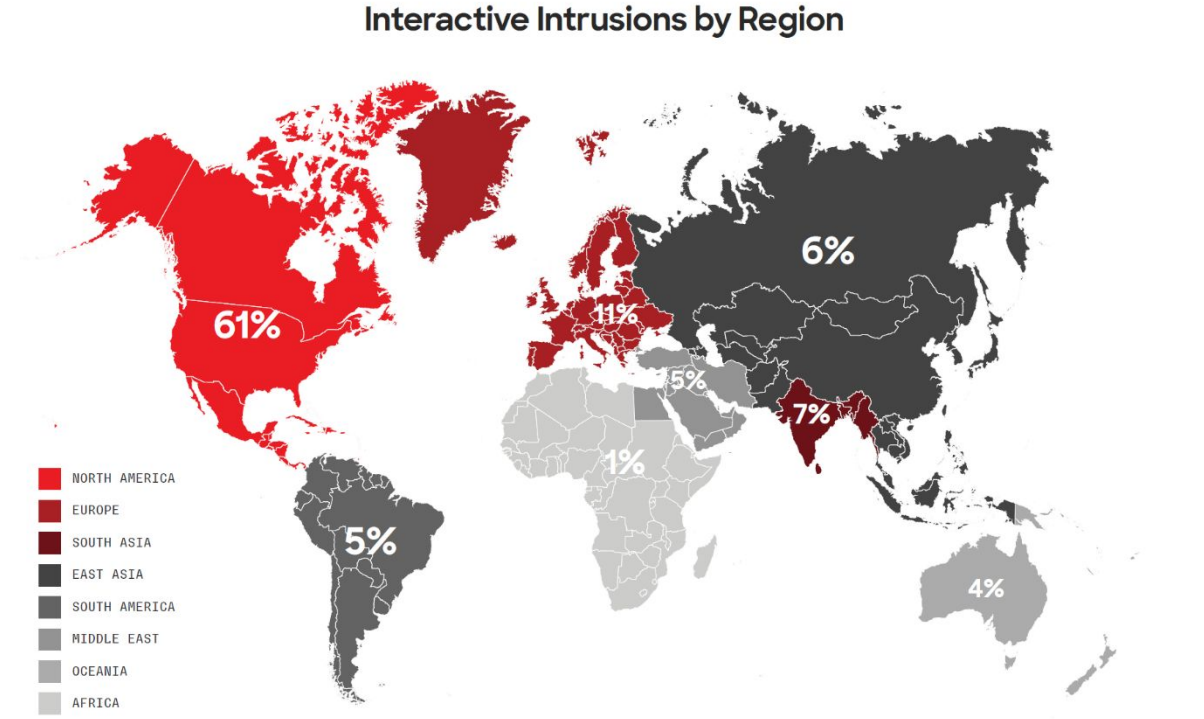


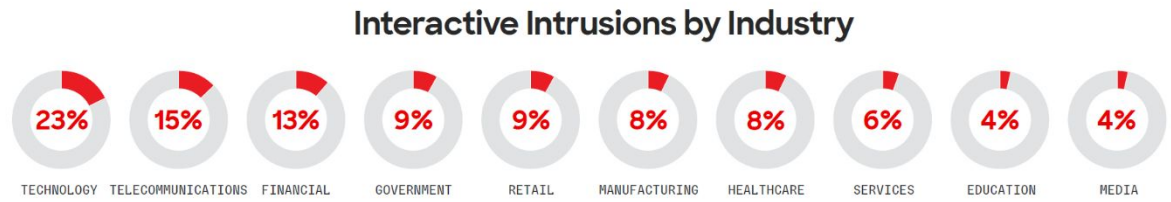
▲ 110% CLOUD-CONSCIOUS CASES

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

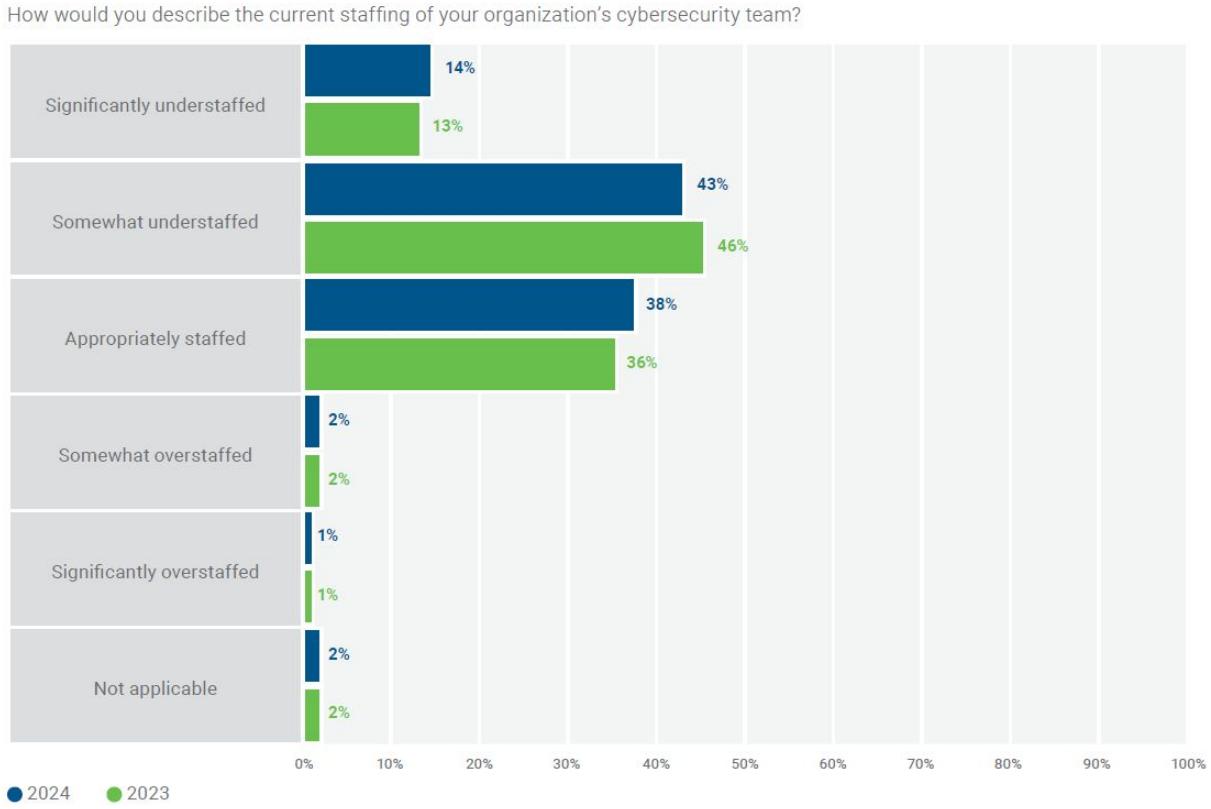




Threat Landscape
Cybersecurity staffing

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.



Regulatory requirements and considerations
EU

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.
- **General Data Protection Regulation (GDPR)** – focused on data and information protection
- …

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, 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)

Summary

- Advances in AI tools have already enabled new types of fraud and will continue to do so in the years to come.
- Deep 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.
- Selection or modification of a suitable framework is highly encouraged
- Start with the basics (security governance) and move down
- User awareness remains key.
- Performing regular assessments will help you identify vulnerabilities before hackers do

forvis mazars

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**