CyberGrant
SECURITY MADE EASY

WHITE PAPER

Cybersecurity Guide:

Threats, Sectors, Regulations, and Opportunities

Index

The current cybersecurity landscape

The threat ecosystem

In today's hyperconnected world, cybersecurity is a strategic necessity. As of 2025, we are navigating a threat landscape shaped by:

- **Expanding Attack Surface** – The widespread adoption of IoT, cloud computing, and remote work has drastically increased the exposure of digital environments.
- **Greater Attack Sophistication** – Threat actors now leverage AI to automate, scale, and personalize attacks with unprecedented precision.
- **Ransomware Surge** – Double and triple extortion ransomware campaigns are escalating, causing both operational disruption and reputational damage.
- **Supply Chain Threats** – Supply chain attacks have emerged as a particularly dangerous trend.
- **Cyber Talent Shortage** – The global skills gap continues, with millions of cybersecurity roles unfilled worldwide.

2024 Cybersecurity data highlights

According to the **IBM "Cost of a Data Breach 2024"** report, the average **cost of a breach has exceeded $4.5 million**. Detection and containment now average more than 280 days.

The **CLUSIT 2025 Report** (Italian National Cybersecurity Association) identified **12,732 publicly disclosed cyber incidents** between January 2020 and December 2024.

$4.5 million

average cost of a breach

12.732

cyber incidents in 4 years

+27%

2024 alone saw 3,541 incidents, the highest annual total ever recorded, up 27% from 2023.

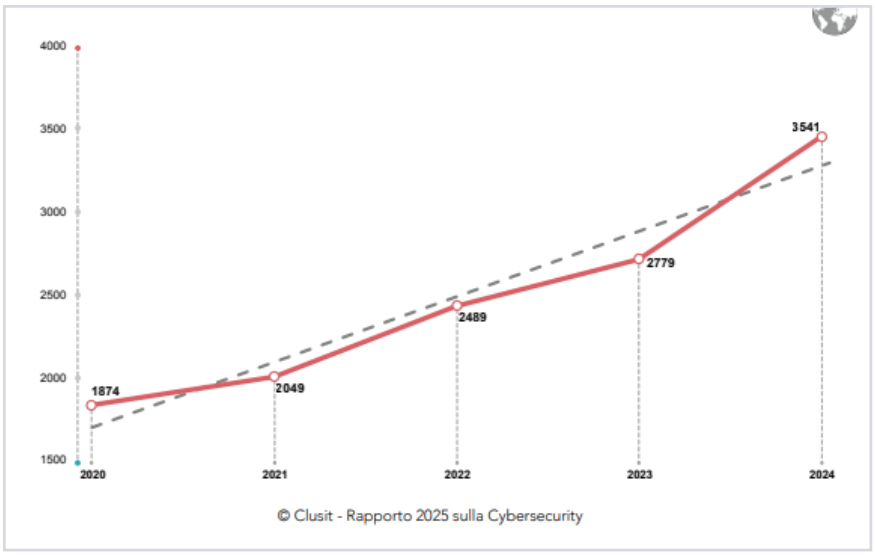


Image source: CLUSIT Report 2025 – Number of Known Global Incidents (2020–2024)

The rise of cybercrime

Cybercrime was the leading cause (86% of incidents), demonstrating the profitability of digital crime and the proliferation of cybercrime-as-a-service models.

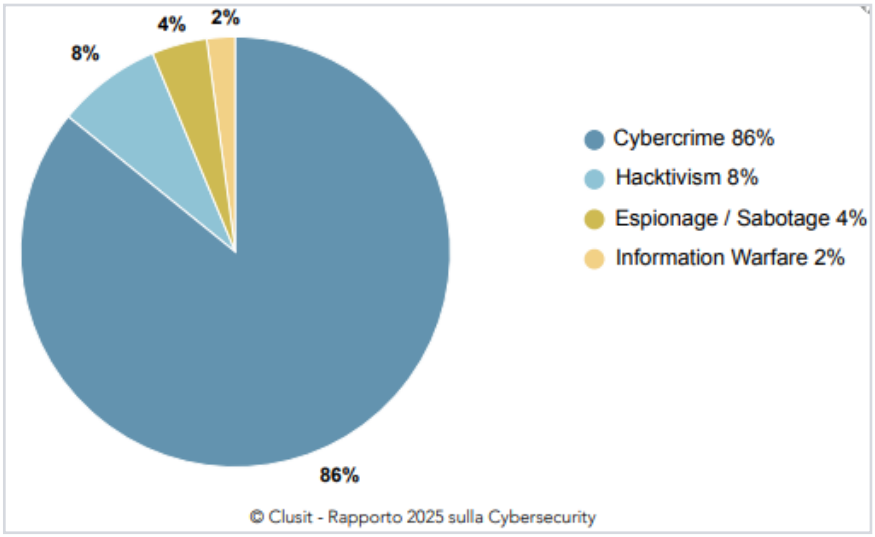


Image source: Clusit Report 2025 – Types and distribution of attackers in 2024

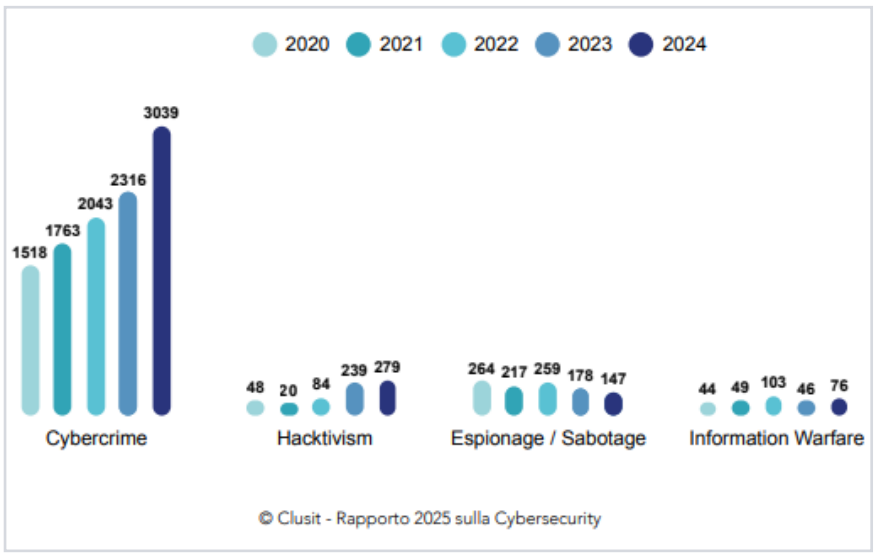


Image source: CLUSIT Report 2025 – Threat Actor Distribution (2020–2024)

Noteworthy trends include:

- **Hacktivism up 16%**
- **Information warfare nearly doubled**
- **Espionage/sabotage down 20%, the only category to decline**

Victims of attacks in 2024

Top targeted sectors in 2024 included:

- **Multiple Targets: 18%**
- **Government / Military / Law Enforcement: 13%**
- **Healthcare: 13%**

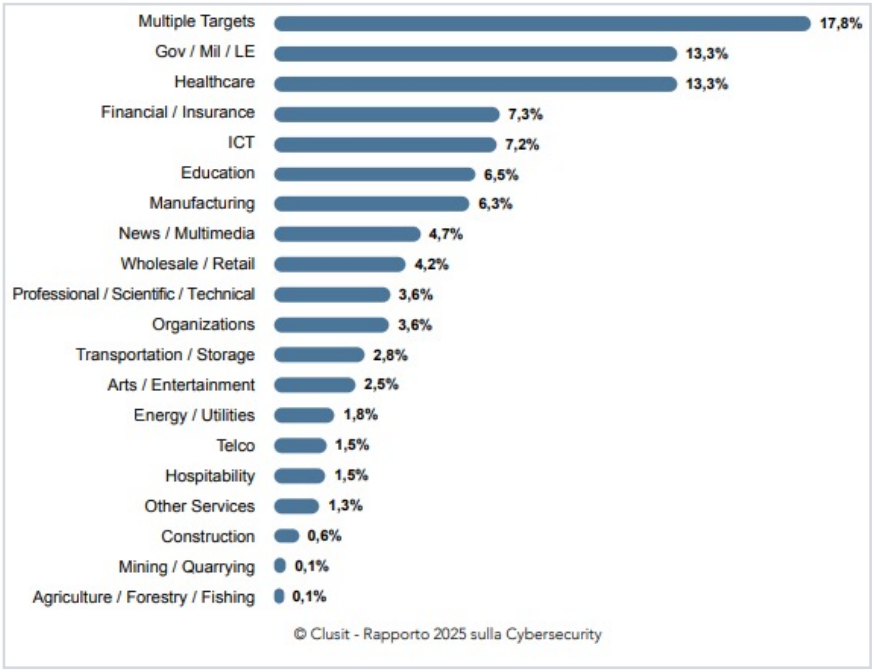


Image source: CLUSIT Report 2025 – Victim Types and Distribution (2024)

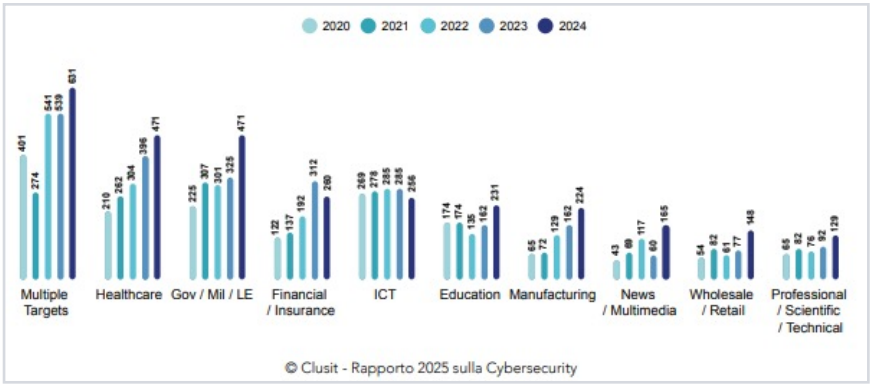


Image source: CLUSIT Report 2025 – Top Ten Victim Categories (2020–2024)

Growth in attacks compared to 2023:

- **Government / Military / Law Enforcement: +45%**
- **Healthcare: +18.9%**
- **Multiple Targets: +17%**

The financial and ICT sectors saw a decline, likely due to stronger compliance (e.g., DORA regulation) and improved defenses. Conversely, several sectors experienced significant growth:

- **Education: +43%**
- **Manufacturing: +38%**
- **Professional / Scientific / Technical: +40%**
- **News / Multimedia: +175%**
- **Wholesale / Retail: +92%**

Global distribution of victims

Over 65% of incidents occurred in the Americas and Europe, reflecting the maturity of disclosure regulations such as GDPR, DORA, and NIS2.

- **Europe saw a 67% increase in incidents**, fueled by stricter notification requirements.
- **Oceania experienced a 228% spike**, due to new local regulations and increased threat actor focus.

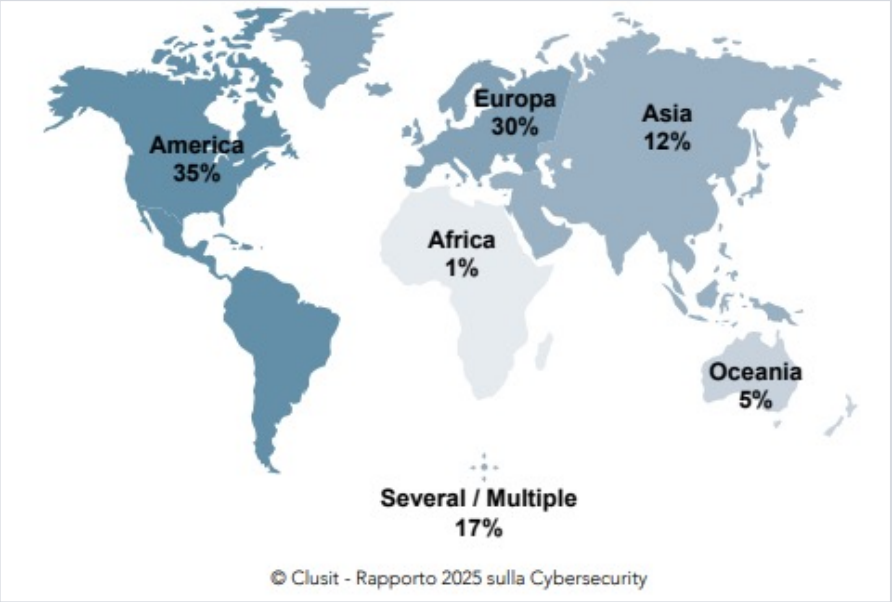


Image source: CLUSIT Report 2025 – Victim Geography (2024)

Key threats and challenges

Ransomware & extortion campaigns

Modern ransomware involves:

- Data encryption
- Data exfiltration and extortion
- DDoS attacks to intensify pressure
- Direct outreach to victims' clients, partners, and media

Ransomware-as-a-Service (RaaS) models from groups like Lockbit and ALPHV have lowered the barrier to entry.

Advanced persistent threats (APT)

APT groups, often state-sponsored, pursue:

- Cyber espionage
- Infrastructure sabotage
- Intellectual property theft
- Political interference

They operate stealthily, with prolonged system access and advanced exfiltration techniques.

Supply chain vulnerabilities

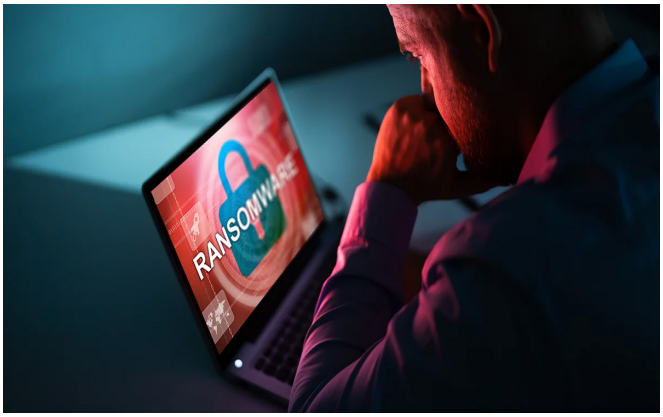
Attackers compromise software and hardware components before deployment, targeting:

- Open-source libraries
- Software update mechanisms
- Hardware backdoors
- Cloud and SaaS platforms

Phishing & social engineering

Evolving tactics include:

- Spear phishing
- Business E-mail Compromise (BEC)
- Deepfakes and voiceprinting
- AI-generated, highly convincing messages

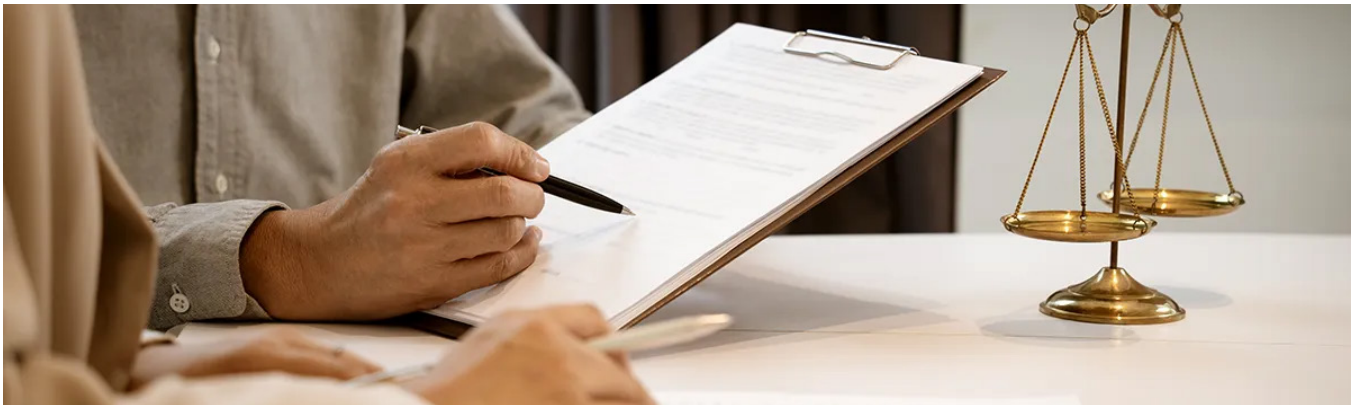


IoT Threats

IoT proliferation introduces risks such as:

- Insecure-by-design devices
- Limited patching options
- Entry points into corporate networks
- Botnet recruitment targets

Cybersecurity regulatory framework



Europe

- **NIS2 Directive** – Expands the scope of NIS1, enforces stricter controls, and broadens sectoral coverage, including digital service providers.
- **GDPR** – Global reference for personal data protection. Enforces 72-hour breach notifications and can impose fines up to 4% of global revenue.
- **DORA** – Targets the financial sector, requiring operational resilience testing and third-party IT vendor oversight.
- **Cyber Resilience Act** – Mandates cybersecurity controls for products with digital elements and introduces EU certification systems.

United States

The U.S. uses a sector-based approach:

- **Federal regulations:**
  - **CMMC** – Certification required for Department of Defense suppliers
  - **FISMA** – Security standards for federal agencies
  - **Executive Order on Cybersecurity** – Focuses on national strategy, public-private collaboration, AI security, and sanctions

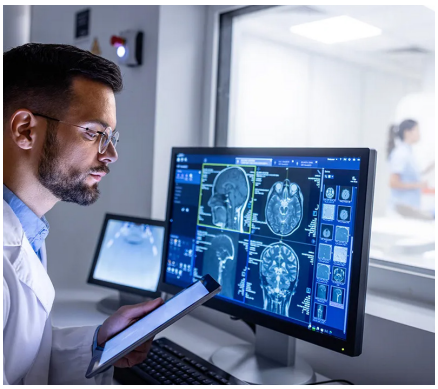
- **Industry-specific laws:**
  - **HIPAA** – Healthcare sector
  - **Gramm-Leach-Bliley Act** – Financial sector
  - CCPA/CPRA – California data privacy
  - Colorado and Virginia Data Protection Acts
- **SEC guidelines:**
  - Require cyber incident disclosure within 4 business days
  - Mandate detailed risk governance transparency

South america (selected highlights)

- **Argentina:** Data Protection Law, Law 26.388 on cybercrime
- **Brazil:** LGPD (GDPR-equivalent), PNCiber strategy
- **Chile:** Cybersecurity Framework Law 21663
- **Colombia:** National CONPES 3854 cybersecurity strategy
- **Mexico:** Federal Data Protection and Cybersecurity Laws
- **Uruguay:** National Cybersecurity Strategy 2024–2030
- **Venezuela:** No comprehensive data law, but some constitutional protections and cybercrime legislation

Cybersecurity by industry

Healthcare



Key threats:

Ransomware, data theft, medical device compromise, service disruption

Challenges:

Balancing access with privacy, securing legacy devices, interoperability, cross-border compliance

Opportunities:

- Zero Trust adoption
- Network segmentation
- Staff training
- Disaster recovery planning
- Blockchain for secure EHRs

Financial services

Key threats:

Payment infrastructure attacks, fraud, phishing, insider threats, DDoS

Challenges:

Payment resilience, fintech-security balance, global compliance, nation-state threats

Opportunities:

- AI-based fraud detection
- Strong MFA adoption
- Industry-specific SOCs
- Red teaming
- Regulator collaboration

Manufacturing

Key threats:

ICS attacks, IP theft, production sabotage, ransomware

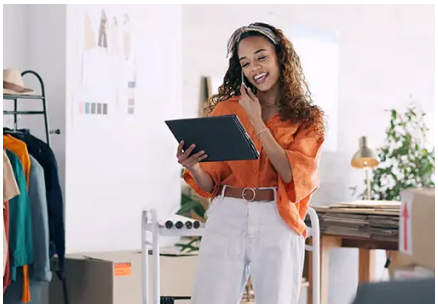
Challenges:

IT/OT integration, securing legacy systems, IP protection

Opportunities:

- Air-gapped networks
- ICS monitoring
- IEC 62443 adoption
- OT anomaly detection
- Operator security training

Retail & eCommerce



Key threats:

payment skimming, account theft, identity fraud, DDoS

Challenges:

Customer data protection, secure seasonal scaling, multichannel security

Opportunities:

- ML fraud detection
- PCI-DSS compliance
- Advanced WAFs
- Malicious code monitoring
- Anti-bot capabilities

Legal & administrative

Key threats:

Confidential data theft, e-mail compromise, ransomware, spear phishing

Challenges:

Professional secrecy, secure client communication, legal compliance

Opportunities:

- End-to-end encryption
- DLP solutions
- Phishing awareness training
- Secure client collaboration platforms

Consulting services

Key threats:

IP theft, credential compromise, digital supply chain risks, espionage

Challenges:

Securing multi-client data, privileged access control, safe consultant mobility

Opportunities:

- Secure onboarding/ offboarding
- CASB solutions
- Risk scoring frameworks
- PAM implementation
- Isolated client environments

Future outlook

Cybersecurity is no longer just a technical issue—it's a business imperative.

Key trends

- Zero Trust as the new standard
- Convergence of cybersecurity and operational resilience
- AI-driven automation to bridge the talent gap
- Enhanced public-private threat intel sharing
- Global regulatory harmonization

Strategic recommendations:

- Risk-based investment prioritization
- Company-wide security culture
- Ongoing employee training
- Comprehensive incident response planning
- Investment in AI and automation tools

How CyberGrant Can Help

CyberGrant Inc. delivers cutting-edge solutions to protect sensitive data, enforce compliance, and prevent cyber threats across industries.

FileGrant

A **secure document-sharing platform** that enables:

- **File protection** – Advanced encryption ensures compliance and safeguards sensitive data
- **Role-based access control (RBAC)** – Prevents unauthorized file access or modification
- **Document management** – Real-time collaboration, versioning, and post-download restrictions

RemoteGrant

An endpoint-focused **Data Loss Prevention (DLP) solution** offering:

- **Ransomware and cyberattack defense** – Blocks malware, secures network ports, and prevents RDP misuse
- **Phishing protection** – Blocks fraudulent websites and credential theft attempts
- **Secure access controls** – Restricts file access to authorized PCs and blocks USB and RDP copying

RemoteGrant simplifies compliance with global regulations by protecting source code, preventing tampering, and ensuring regulatory resilience.

Conclusion

Cybersecurity is a strategic pillar for every organization. The future lies in Zero Trust models, integrated resilience, intelligent automation, and a collaborative global defense ecosystem.

Partners like CyberGrant can empower your organization to protect its data, reduce risk, and comply with evolving regulations—transforming security from a cost into a competitive advantage.

A cura di **Federica Maria Rita Livelli**

www.cybergrant.net