orange Cyberdefense

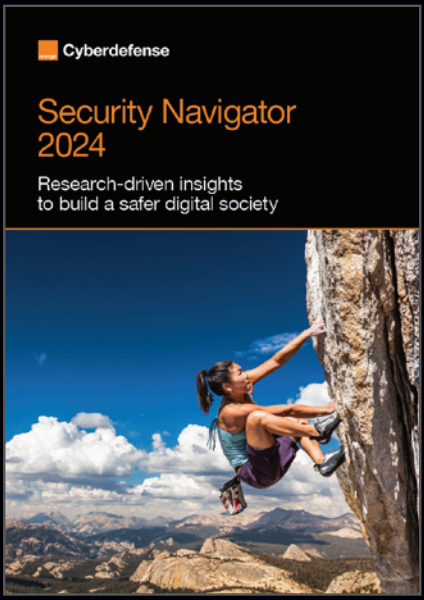
Security Navigator 2024

Executive Summary

- **We are proud to share this year the 5th edition of our Security Navigator. The past five years allowed us to consolidate our analysis methods as well as put underlying threat trends into perspective. This report aims to help CISOs and security experts to refine their security strategy.**

- **Orange Cyberdefense has built proprietary cyber threat intelligence capabilities over several years, leveraging its own and partner sources across 160 countries. Our security operations centers detected 129,395 potential incidents, of which 25,076 were confirmed breaches.**

- **This Executive Summary is a synthesis of the complete Security Navigator 2024 report, providing insights into the major cyber security trends of the year.**



Cyberdefense

Security Navigator 2024

Research-driven insights to build a safer digital society

Funnel: 129,395 incidents ▶ 25,076 confirmed security incidents

Cyber threats: the world in tension

The dynamics of current geopolitical crises have amplified the effects of globalization on cyber security. The lasting state of war at the gates of Europe, the risks of polarization of the conflict between Hamas and Israel and the rise in tensions in the Indo-Pacific region remind us that security remains - and will increasingly be in the future - at the heart of human and technological development strategies for organizations, governments and society at large.

Disruptions which combine geopolitical, economic and social dimensions are intensified by the accelerated digitalization in our lives and work – for instance, remote working. Our environment has become more unstable and less predictable. Cyber threat actors leverage this environment to seize and develop all attack opportunities for espionage, influence or extortion.

Our precise cyber threat insights allow our customers to measure the extent to which vulnerabilities pose a risk - from moderate to major - on their business-critical activities, their reputation, their people and their customer data.

The better organizations can anticipate and detect threats, the more cyber crises can be avoided or at least reduced via timely reaction and incident response. However, while hackers have embarked on an endless race to search for vulnerabilities to exploit, many organizations do not yet have the capabilities to identify, prioritize and appropriately patch vulnerabilities on an ongoing basis. This is despite an increased cyber security awareness by organizations.

Key Learnings from the Security Navigator 2024

We see four major points emerge, some of which confirm trends that Orange Cyberdefense had already identified, and others which highlight new ones.

1. **Cyber Extortion (Cy-X) remains the most prominent form of cyberattack.** In the last 12 months, the number of Cyber Extortion victims increased by 46%, affecting 3,400 organizations of all sizes and countries. Smaller organizations represent a quarter of victims of this type of attack. We observe a geographic lateralization of attack targets, with the largest increase in victims seen in India (97%), Oceania (73%) and Africa (70%). Cyber criminals are opportunistic in their approach, targeting the weakest link: nearly 40% of incidents are linked to an internal source.

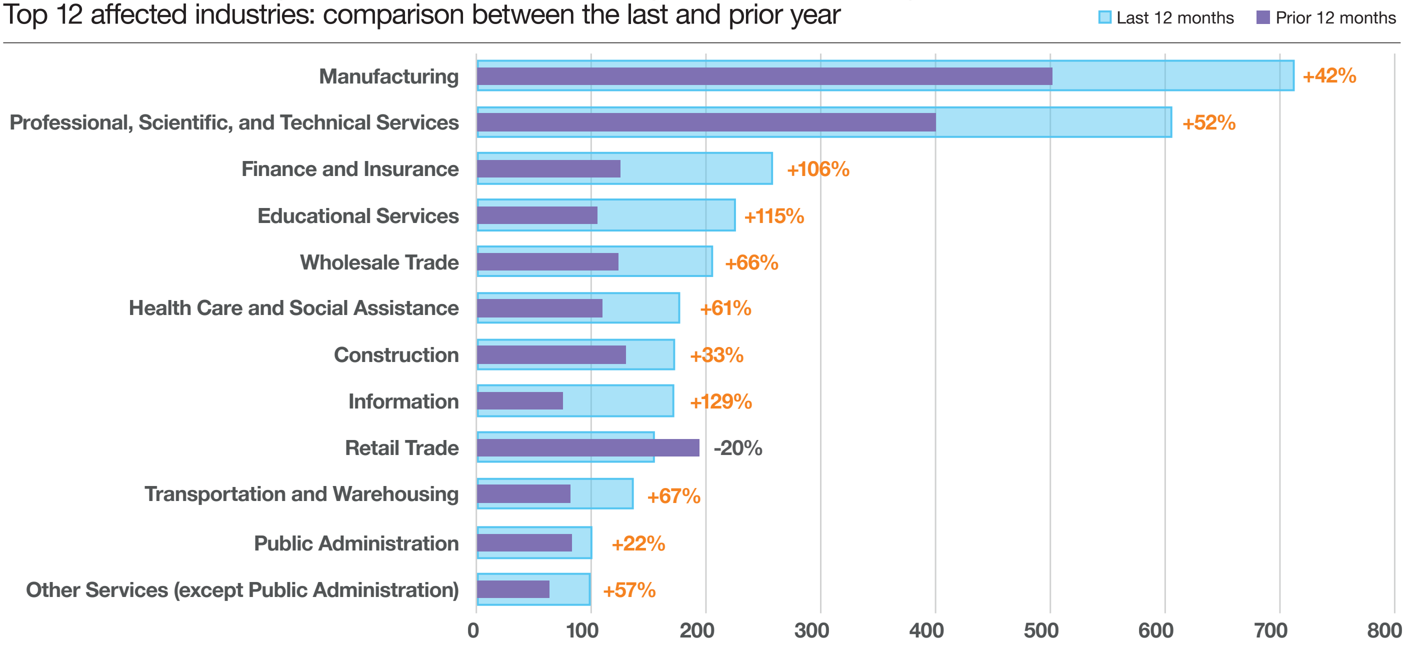
2. **Large organizations continue to have the largest share of incidents in our CyberSOC data (83% of incidents), in alignment with our customer base.** However, we see an increasing volume of incidents in small and medium businesses as well. Though total detected incidents this year increased by 25% vs the previous report, it is encouraging that there was a decrease in confirmed breaches by 19%. The main sectors affected this year, with over 75% of all incidents, are Manufacturing followed by Retail, Professional, Scientific and Technical Services and Finance and Insurance.

3. **The line between nation-state, cyber-hacktivists and criminal actors is increasingly blurry.** Though already prominent over the last two years, hacktivism to support political and social demands has exploded recently, exacerbated by the war against Ukraine. Ukraine itself, Poland and Sweden were the main victims of pro-Russian hacktivists. Other geopolitical events also contributed to this dynamic – in 2023, Europe was the target of 87% registered attacks, followed by North America and the Middle East. The Hamas-Israel war already amplifies this trend. A major mobilization of hacktivist groups has been observed globally. The majority of them are pro-Palestinian groups targeting Israeli and European entities with low-sophistication attacks such as Distributed Denial-of-Service (DDoS).

4. **The decompartmentalization of personal and professional generates new threats.** On one hand, our mobile devices are increasingly targeted by cyber actors in order to access personal and professional data stored or transiting in them. On the other, attackers target company personnel – now the source of 7% of incidents – in order to corrupt them or penetrate their organization's networks.

Shift in Cy-X victims by industry

Top 12 affected industries: comparison between the last and prior year



Our recommendations:

Prevention remains the best weapon to reduce the effects of an attack. This involves sensitizing as many people as possible to cyber threats and their consequences for the organization and employees: at all levels in the company, including senior leadership, but also at the level of each individual in their personal and professional digital usage. Security hygiene, in particular in the security of personal mobile devices and the general public is becoming a major issue for everyone, including businesses.

Cyber risk must be reinforced as the central element to an organization's risk management strategy, regardless of its size. Equally, the security function must be continuously assessed vs. the protection provided to the organization, its people, infrastructure, customer and partner data. This must be complemented by a planned cyber crisis management capability driven at the highest level of the organization.

A trusted partnership allows organizations to define and implement cyber risk management strategies adapted to the specific threats to their business interests. The intersection between cyber security and business expertise needs to be orchestrated at all levels in the organization – from individual employees to the CISO to the Board - to identify the company's critical assets, protect its vital interests and to build a tailor-made strategy that complies with regulations that will continue to impose themselves.

This partnership should increasingly allow the organization to dynamically adjust their security and comply with new regulatory requirements.

It is necessary to stay ahead of technological innovations to maintain an appropriate level of security. Artificial or post-quantum intelligence are both opportunities and risks for businesses: we need to build flexible local models to continually invest in innovative security services.

Read the full story! Get your free copy of the Security Navigator on:
orangecyberdefense.com/navigator/

Orange Cyberdefense Threat Research

Orange Cyberdefense has structured its threat analysis around data from multiple sources. We develop our assessment by cross-referencing data from our security operational centers (SOCs and CyberSOCs) with data from our OSINT research, data from our ethical hackers and CERT and our partners. We also benefit from analytical support provided by Orange, the telecommunications operator.

These analyzes and their results are then integrated into the services we provide to organizations, and shared with the cyber community through various publications, events and repositories (GitHub). Intelligence is also published daily, highlighting the vulnerabilities identified by Orange Cyberdefense, as well as the associated indicators of compromise. Other reports combining current technical and geopolitical approaches are shared monthly or annually, such as the Security Navigator.

About Orange Cyberdefense

Orange Cyberdefense is the Orange Group's entity dedicated to cybersecurity. It has 8,700 customers worldwide. As Europe's leading cybersecurity service provider, we strive to protect freedom and build a safer digital society. Our services capabilities draw their strength from research and intelligence, which allows us to offer our clients unparalleled knowledge of current and emerging threats. With 25 years of experience in the field of information security, 3,000 experts, 18 SOCs and 14 CyberSOCs spread around the world, we know how to address the global and local issues of our customers. We protect them across the entire threat lifecycle in more than 160 countries.

For more information check www.orangecyberdefense.com