Operationalizing the Cyber Threat Landscape: Key Considerations and Challenges in Developing a Specific Organizational Program

Costel CIUCHI, PhD
Assoc. Prof., Faculty of Electronics, Telecommunications and Information Technology,
National University of Science and Technology POLITEHNICA Bucharest, Romania
costel.ciuchi@upb.ro

Abstract

The landscape of cyber threats is multifaceted, encompassing a wide array of attack vectors, including distributed denial of service (DDoS) attacks, phishing, man-in-the-middle attacks, password-based intrusions, remote exploitation, privilege escalation, and malware deployment. As the sophistication of cyber threats continues to advance, coupled with the development of increasingly sophisticated evasion techniques, traditional security mechanisms - such as firewalls, intrusion detection systems, antivirus software, and access control lists - are proving less effective in identifying and mitigating these complex threats. This underscores the urgent need for the development and implementation of innovative, more robust solutions to counteract the growing prevalence of cyber-attacks. The objective of this proposal is to examine the ENISA Cybersecurity Threat Landscape Methodology and explore potential advancements that integrate traditional decision-making frameworks with emerging cybersecurity technologies. As concerns over cyber warfare continue to escalate, nations must adopt adaptable cyber frameworks and methodologies capable of preventing cyber crises. Furthermore, these frameworks should foster greater international collaboration and participation in the ongoing global discourse on cybersecurity.

Index terms: risk & vulnerability management, threat landscape, cyber threat intelligence, defence strategies, incident response, intrusion detection, frameworks and methodologies

1. Introduction

The digital threat landscape constantly evolves, with malicious actors launching more sophisticated attacks daily. Organizations must keep up with the latest cybersecurity frameworks to stay ahead of this dynamic threat environment. The frequent questions from stakeholders and political level related to cybersecurity: How secure we are? What is the status of cybersecurity?

Several factors led to the development of legislation, policies and guidance, but not limited to, the growing cyber threat landscape, technological advancement, increase in emerging risks, insufficient implementation of the Directives in the national legislative framework, increased dependency on digital and supply chain risks, evolving European cybersecurity policy, and the need to strengthen the developments in domain.

Cybersecurity Threat Landscape (CTI) represent the knowledge and understanding of actual or perceived threats that conduct organizations' security decision-making. The intelligence typically relates to the threat actor's goals, intentions, strategies, capabilities, limitations, and vulnerabilities. It is used in organizational planning, analysis, situation awareness, and prediction of future events related to cybersecurity to support business operations and managerial decisions.

The practice of threat intelligence comes from the military area [1], where decision-makers and experts, collect, process, and disseminate intelligence to other upper levels of decisions and stakeholders.

CTI represent a subset of cyber intelligence (CI) that relates to threats and threat actors [2]. By implementing a CTI Program, organizations can transform generic cyber practices from being "reactive and undirected" to being "proactive, anticipatory, and dynamic" [3].

2. Threat Landscape

The **threat landscape** is the entirety of potential and identified cyber threats affecting a particular organization, sector, group of users, or time period [4].

The threat landscape is typically conceptualized as encompassing the vulnerabilities, malicious software, and distinct categories of threat actors along with their methodologies that pose risks within a particular context.

This implies that it is essential to consider the specific characteristics of an organization, sector, or even an individual, which may include, but are not limited to, the following factors [5]:

- the sensitive or valuable data targeted by attackers;
- the security state, cost and frequency of cyber-attacks;
- geopolitical influences, as certain threats focus on entities located in specific countries or regions.

The threat landscape evolves both over time and in response to events that have a substantial impact on the organization, people, or sector for which the threat landscape is defined. A recent example of this is the rise in attacks targeting remote-access tools, which have become prominent within the threat landscapes of numerous organizations.

Several factors, shape and influence the evolution of the threat landscape [6, 7], including:

- identification and disclosure of vulnerabilities that open opportunities for cybercriminal exploitation;
- release of updated software versions introducing additional functionality and potential security risks;
- development of new hardware platforms, and innovative data processing methodologies, such as cloud computing and edge computing;
- global events, such as the COVID-19 pandemic, have forced organizations to make major changes to their infrastructure, often expanding the attack surface.

Understanding the current threat landscape is crucial, as conducting a comprehensive analysis allows for the identification of potential information security risks confronting a specific entity - whether a company, individual, or entire sector.

This proactive approach enables the implementation of preventive measures, thereby enhancing the entity's ability to anticipate and mitigate emerging threats to information security.

3. Current Cyber Threat Landscape

The current cybersecurity threat landscape is marked by growing complexity and rapid evolution. Organizations are exposed to a wide spectrum of threats, ranging from simple, low-tier attacks to sophisticated, highly coordinated campaigns launched by nation-state actors.

According to the ENISA Threat Landscape 2024 report [8], which covers the period from July 2023 to June 2024 and was released in September 2024, seven primary cybersecurity threats were identified:

- Ransomware
- Malware

- Social Engineering
- Threats against data
- Threats against availability: Denial of Service
- Information manipulation and interference
- Supply chain attacks

Fig. 1. ENISA Threat Landscape 2024 - Prime threats [8]

The ENISA Threat Landscape (ETL) 2024 report is derived from a combination of open-source data, primarily of a strategic nature, as well as ENISA's own Cyber Threat Intelligence (CTI) capabilities. The report follows the methodology outlined in the ENISA Cybersecurity Threat Landscape (CTL) framework [9].

According to the CrowdStrike 2024 Global Threat Report [10], several key emerging trends and evolving threats are currently shaping the cybersecurity landscape, including:

- **Ransomware -** remains a persistent and high-impact threat, with threat actors employing increasingly advanced tactics to target organizations of all sizes. The primary method of monetization for ransomware attacks continues to be the encryption of critical data, followed by extortion demands for decryption keys or the threat of public data leakage;
- **Supply Chain Attacks -** involve the compromise of third-party vendors or software providers to gain unauthorized access to a target organization’s systems. These attacks are primarily aimed at data exfiltration and optimization of extortion tactics, often leveraging trusted relationships to bypass traditional security measures;
- **Business Email Compromise (BEC) -** a form of social engineering in which attackers impersonate senior executives or other trusted individuals to deceive employees into transferring funds or disclosing sensitive information. BEC attacks often result in substantial financial losses for organizations globally, exploiting human trust and organizational communication channels;
- **IoT vulnerabilities** - the growing number of Internet of Things (IoT) devices presents an attractive target for threat actors, as many of these devices are deployed with inadequate security measures. Exploiting these vulnerabilities allows attackers to gain unauthorized access to corporate networks or use compromised devices as launching points for attacks on other systems or organizations;
- **State-Sponsored Attacks -** nation-state actors remain a critical threat, conducting cyber espionage, intellectual property theft, and targeting critical infrastructure for disruption. Geopolitical tensions often escalate these activities, resulting in highly targeted intrusions and an increase in hacktivist-driven cyber operations. Such attacks are expected to persist

as key drivers of cyber conflict, with both strategic and ideological motivations shaping the threat landscape;

- **Generative Artificial Intelligence (AI) - t**hreat actors are leveraging AI technologies to enhance the sophistication and precision of cyberattacks. AI-driven attacks can automate social engineering tactics, refine malware to evade detection and optimize attack strategies, making them more adaptive and harder to mitigate. This increasing use of AI poses significant challenges for traditional defence mechanisms;
- **Malvertising and SEO Poisoning** - **Malvertising** involves the creation of malicious advertisements that serve as vectors for cybercriminal activities, often leading to malware infections or data breaches. **SEO Poisoning** involves manipulating search engine optimization (SEO) techniques to artificially elevate malicious websites in search engine results. This tactic exploits the common user perception that top-ranked search results are the most credible, increasing the likelihood of users visiting and interacting with compromised sites.

Global reports emphasize several critical trends that must be considered when assessing the current cyber threat landscape. These include:

- **Increasing Role of Artificial Intelligence (AI)**: AI technologies are increasingly being utilized in both cyberattack execution and the enhancement of cybersecurity defences. Attackers leverage AI to automate and refine attack strategies, while defenders use it to improve threat detection, response times, and overall security posture;
- **Emerging Security Regulations**: Governments and regulatory bodies are enacting new and **evolving** cybersecurity laws, compliance standards, and data protection frameworks. These regulations are significantly shaping how organizations manage data security, privacy, and risk mitigation, with a growing emphasis on compliance and accountability;
- **Critical need for cyber resilience:** as cyber threats become more persistent and sophisticated, organizations must focus on building resilience to ensure rapid recovery, business continuity, and minimal disruption in the event of a successful cyberattack, thereby maintaining operational stability even during a breach.

4. Implement a Cyber Threat Landscape Program

Based on the three pillars of cybersecurity - **people**, **process**, and **technology** [11] - an organizational cyber threat landscape program must incorporate a strategy that is tailored to the specific needs of the business and aligned with its objectives. This approach should be designed to enhance the organization's ability to perform securely and effectively. To achieve this, all three pillars should be guided by five key directions:

- **Prevention (education, policy development, and security best practices)**
- **Protection (defence mechanisms, block malicious activity and mitigate risks).**
- **Detection (monitoring tools, anomaly detection, and behavioural analytics identifying attacks in real-time).**
- **Response (incident response planning, containment strategies, and communication protocols.**
- **Cooperation (sharing information and collaborating with internal and external sources)**

By integrating these five directions into the core pillars of people, process, and technology, organizations can develop a robust, adaptive cybersecurity program that aligns with business goals and responds effectively to the evolving threat landscape.

Developing a cyber threat landscape assessment [12] based on proposed program pillars represents a more comprehensive evaluation of an organization's digital security posture. It involves

systematically identifying, analysing, and prioritizing potential new possible cyber threats that could impact the organization.

This assessment helps organizations understand the range of risks they face, the likelihood and potential impact of those threats, and the effectiveness of existing security controls. By gaining insights into current vulnerabilities and emerging threats, organizations can develop targeted strategies, policies, and procedures, to enhance their cybersecurity defences and improve overall risk management.

Conducting a ***cyber-threat landscape assessment*** provides several key benefits for organizations that are using classical cybersecurity approaches. These benefits include (Table 1):

Table 1. Benefits for organizations

Directions	***Domain***	***Benefits***
Prevention	*vulnerabilities*	• *classification of vulnerabilities based on the organization technologies, processes, and personnel;* • *identify cross-domain vulnerabilities.*
Protection	*risk mitigation*	• *helps prioritize the most significant threats and vulnerabilities based on the potential impact on the organization;* • *ensure effective risk reduction by prioritizing risk mitigation efforts.*
Detection	*enhanced threat intelligence*	• *better understanding of potential cyber threats and attackers, and associated risks;* • *develop more effective incident response plans, detect and prevent malware infections, and identify emerging attack techniques.*
Response	*improved incident response and recovery*	• *identify potential breaches and security incidents, allowing organizations to develop a proactive incident response plan;* • *effectively respond to a security incident with a plan, minimizing the impact on their operations.*
Compliance	*compliance with regulations and standards*	• *ensure an organization complies with these regulations and standards;* • *identify potential compliance gaps or factors such as insufficient access controls or inadequate security training.*
Cooperation	*collaboration and intelligence sharing*	• *collaboration with external partners, such as threat intelligence networks, industry groups, or local authorities lead to a stronger collective defence.*

5. Program actions to protect against the Threat Landscape

Organizations must establish a robust and proactive cybersecurity framework to safeguard against the dynamic and constantly evolving threat landscape. A comprehensive cyber threat landscape program should incorporate several critical components, including the four primary workflows:

- **Establish Programs - Supply Chain Security program, Threat Monitoring program, Change Management program;**
- **Implement Plans - Regular Security Assessments plan, Incident Response plans, Disaster Recovery plans;**
- **Conduct - regular Employee Training, regular Cyber Exercises, and regular Software and System Updates;**
- **Control - Implementing rigorous verification, monitoring, and control mechanisms across all the aforementioned activities (regular audits, performance tracking, and the use of automated tools)**

A critical starting point for organizations is to adopt the ENISA Cybersecurity Threat Landscape (CTL) methodology [9] as part of their organizational culture. This approach provides a structured framework for understanding and managing cyber threats. Organizations should then develop a

tailored cybersecurity framework that focuses on effectively managing cybersecurity risks, mitigating vulnerabilities, and enhancing overall digital defence mechanisms. This framework should integrate threat intelligence, risk assessment, and proactive security measures to address evolving threats and safeguard the organization's assets.

Also, adopting a methodology (ENISA Cybersecurity Threat Landscape - CTL), including high management leadership and oversight, legal considerations will develop a cybersecurity governance framework that will ensure an organization's cybersecurity practices are well-coordinated, consistently applied, and capable of adapting to an ever-changing threat landscape.

By strategically investing in human resources, addressing skills gaps, leveraging advanced technologies, enhancing risk management practices, and fostering improved communication and collaboration, organizations can significantly bolster their security posture and mitigate potential cybersecurity risks.

Additionally, the continuous development and refinement of existing frameworks and methodologies will serve as critical enablers for capacity building, empowering organizations to effectively navigate the increasingly complex and dynamic cybersecurity landscape.

To strengthen their cybersecurity defences, organizations should take several specific actions. First, they must develop and implement proactive recruitment strategies to attract and retain skilled cybersecurity professionals, offering competitive salaries, benefits, and opportunities for professional development. Additionally, investing in training and development programs is essential to upskill existing staff, bridging skills gaps through online webinars, corporate training events, and mentoring initiatives.

Organizations should also explore the potential of artificial intelligence (AI) to automate routine tasks, enhance threat detection and response capabilities, and improve overall security posture. Conducting regular cyber risk assessments is critical for identifying vulnerabilities and developing strategies to mitigate the likelihood and impact of cyberattacks.

Furthermore, organizations must ensure comprehensive cyber insurance coverage, understanding the terms of their policies to ensure they provide adequate protection against potential risks. Finally, fostering effective communication and collaboration across security teams, leadership, and other departments is vital. Breaking down silos and sharing information, insights, and best practices will help strengthen the organization's collective cybersecurity efforts.

Also, for a successful program in the cybersecurity threat landscape, employees must prioritize staying informed about the latest threats and trends by regularly updating their knowledge and skills through professional development, certifications, and online resources.

In addition to technical expertise, developing strong soft skills such as communication, collaboration, critical thinking, and problem-solving is essential for effective performance, as these skills facilitate teamwork and strategic decision-making. Given the constantly evolving nature of the cybersecurity landscape, embracing a mindset of continuous learning is crucial.

By committing to lifelong learning, individuals can remain adaptable, stay ahead of emerging threats, and maintain their professional edge in an increasingly complex field.

6. Conclusion

Developing and adopting robust, adaptable cybersecurity frameworks is essential for mitigating the risks posed by evolving threats. These frameworks should incorporate risk management strategies, continuous monitoring, and collaboration across sectors and borders. International cooperation will be critical to address threats that span multiple countries and jurisdictions.

The evolution of cyber threats presents significant challenges to the security and stability of modern societies. As cyber threats become more advanced, widespread, and complex, traditional defence mechanisms are increasingly inadequate. To effectively combat these threats, it is essential

to adopt an approach that integrates innovative technological solutions, robust frameworks, continuous collaboration, and enhanced cybersecurity education. Only through these combined efforts can we hope to mitigate the risks posed by the rapidly evolving landscape of cyber threats.

Integrating traditional decision-making frameworks, established standards, and senior management with emerging cybersecurity technologies presents a powerful opportunity to enhance an organization's security posture, improving both effectiveness and agility. Several advancements can be leveraged in this integration, such as Data-Driven Decision-Making with AI and Machine Learning, which enables real-time threat detection and predictive risk modelling. Automated Threat Intelligence Integration can streamline the analysis of threat data, ensuring timely and informed responses to evolving cyber risks.

Adaptive Risk Management Models facilitate continuous, real-time risk assessments, empowering organizations to dynamically adjust their security strategies as new vulnerabilities emerge. The use of Blockchain for Secure Decision-Making and Audit Trails ensures the integrity, transparency, and immutability of security-related decisions, providing a verifiable record for compliance and accountability. Additionally, Cybersecurity Decision Support Systems (DSS) can assist senior management in making data-driven, strategic decisions by aggregating threat intelligence, simulating attack scenarios, and offering predictive insights into the organization's cybersecurity risks.

These advancements enable organizations to navigate the increasingly complex cybersecurity landscape with greater precision, responsiveness, and foresight. This fusion enables a more proactive, data-driven, and transparent approach to managing cybersecurity risks, ensuring that organizations are better equipped to respond to the rapidly evolving threat landscape.

Operationalizing the cyber threat landscape is essential for organizations seeking to build a resilient and adaptive cybersecurity program. While there are numerous key considerations, including integrating threat intelligence, adopting risk-based strategies, and ensuring continuous monitoring, organizations also face significant challenges such as resource constraints, skill shortages, and the complexity of managing evolving threats. Addressing these challenges requires a holistic approach, involving strong leadership, cross-functional collaboration, and a commitment to continuous improvement and adaptation in the face of a rapidly changing cybersecurity landscape.

References

[1]. Sean Barnum. 2012. Standardizing cyber threat intelligence information with the structured threat information expression (STIX). Mitre Corporation 11(2012), 1-22.

[2]. Donald Gerwin & J. Stephen Ferris, 2004. "Organizing New Product Development Projects in Strategic Alliances," Organization Science, INFORMS, vol. 15(1), pages 22-37, February.

[3]. Bongsik Shin, Paul Benjamin Lowry, A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished, Computers & Security, Volume 92, 2020.

[4]. Fortinet Training Institute, Introduction to the Threat Landscape, https://training.fortinet.com/local/staticpage/view.php?page=library_introduction-to-the-threat-landscape

[5]. Top Cybersecurity Statistics for 2024, https://www.cobalt.io/blog/cybersecurity-statistics-2024

[6]. Expert Insights Podcast, John Grancarich On the Evolution of the Threat Landscape, How Security Providers Need To Pivot, https://podcasts.apple.com/gb/home

[7]. Antonio de Lucas Ancillo, Sorin Gavrila, María Teresa del Val Núñez, Workplace change within the COVID-19 context: The new (next) normal, Technological Forecasting and Social Change, Volume 194, 2023, ISSN 0040-1625.
[8]. ENISA Threat Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
[9]. ENISA Cybersecurity Threat Landscape (CTL) methodology, July 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology
[10]. CrowdStrike 2024 Global Threat Report, https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf
[11]. I.C. Mihai, C. Ciuchi, and G. Petrică, "Current challenges in the field of cybersecurity - the impact and Romania's contribution to the field", Ed. Sitech, 2018.
[12]. I.C. Mihai, G. Petrică, C. Ciuchi, L. Giurea, "Cybersecurity challenges and strategies", Ed. Sitech, 2015.