Charter
of Trust

HYBRID THREATS

AN EXPERT'S PLAYBOOK ON CYBERSECURITY

14 February 2025

Chief Information Security Officers and Chief Cyber Security Officers of Charter of Trust Partners

Contributors: AES, Allianz, Atos, Bosch, Danfoss, IBM , Infineon, Siemens, TÜV SÜD

aes

Allianz

Atos

BOSCH

Danfoss

IBM

Infineon

Microsoft

MITSUBISHI
HEAVY INDUSTRIES

SIEMENS

TÜV SÜD

Founding
Partner

msc

Charter
# of Trust

TABLE OF CONTENTS

1

THE RISE OF HYBRID THREATS: A NEW STRATEGIC CHALLENGE

In the digital era of the 21st century, the concept of power is evolving. Cyber power has become a defining factor in international politics, alongside soft and physical means of power. Meanwhile, the security landscape is being shaped for decades to come by the emergence of hybrid threats – a sophisticated fusion of conventional, unconventional, and cyber capabilities.

For multinational corporations, the stakes are bigger than ever. Companies may be directly targeted or become collateral damage in attacks aimed at states, governments or societies, concedes Morten Pors Simonsen, Chief Information Security Officer (CISO) at Danfoss. In the face of complex threats in the digital and physical realm, it is no longer sufficient to deploy a reactive strategy or to increase cybersecurity investments.

To keep pace with this changing threat landscape, the Charter of Trust – a non-profit alliance of leading global companies – calls for a more comprehensive "whole-of-society" approach that integrates innovation, strategy, foresight, collaboration, transparency, and talent development as well as continuous training.

DEFINING HYBRID THREATS – THE INTERSECTION OF PHYSICAL AND DIGITAL CONFLICT

The Charter of Trust partners and their CISOs have experienced hybrid threat attacks firsthand. Paul Bayle, Group CISO at Atos, regards cyberspace "as the terrain on which the battle is fought, rather than on the streets or the fields." Cyberattacks have become part of hybrid warfare which is defined as subtle and covert ways to pursue geopolitical objectives, often blurring the lines between war and peace. Raphael Otto, CISO at Infineon, highlights the ambiguity of these tactics, "making it challenging to respond."

The ambiguity of hybrid threats makes it difficult to attribute actions or even to identify whether an attack has occurred. Key characteristics of such hybrid warfare attacks include

1. Blurred lines between civilian and military targets,
2. Deniability, and
3. Synchronization across multiple domains.

Hybrid threat’s “whole-of-society” approach mobilizes state and non-state actors to exploit societal vulnerabilities, undermining trust in democratic institutions. This necessitates a similar response, where the private sector plays a vital role. In the cyber realm, this translates into forward-looking and comprehensive strategies from multinational companies to maintain stability in an interconnected world.

DEFENDING CRITICAL INFRASTRUCTURE AND THE ROLE OF MULTINATIONAL CORPORATIONS

In the cyber domain of hybrid threats, multinational corporations, particularly those managing critical infrastructure, are pivotal defenders and prime targets. Private companies own most of the critical infrastructure, rendering them essential partners in national defense. For instance, the Nord Stream pipeline sabotage led NATO to establish an Undersea Infrastructure Coordination Cell, enhancing public-private cooperation. Similarly, the European Commission’s contractual Public-Private Partnership (cPPP) with the European Cyber Security Organisation (ECSO) demonstrates collaborative efforts.

In practice, the private sector contributes to cyber resilience by mitigating threats and shielding critical infrastructure with advanced in-house cyber intelligence and 24/7 defense operations. Particularly through information sharing, incident response and proactive security measures, corporations can enhance efficient cooperation with governments.

> » *Hybrid warfare may involve disruptions in global supply chains, affecting businesses and organizations that rely on imports and exports for their operations. This can cause supply shortages, disruptions and financial losses. Other tactics like spreading disinformation can affect public opinion, harming the reputation and brand image of organizations. Businesses as well as public institutions need to adopt a holistic approach and take joint action to successfully address these challenges.* «

Natalia Oropeza

Global Chief Cybersecurity Officer at Siemens

aes
TÜV SÜD
Allianz
SIEMENS
Atos
Charter of Trust
MITSUBISHI HEAVY INDUSTRIES
BOSCH
Microsoft
Danfoss
infineon
IBM

The Charter of Trust and its current members

THE CHARTER OF TRUST'S ROLE IN THE NEW THREAT LANDSCAPE

In the Charter of Trust, leading companies collaborate to share expertise and insights, playing a vital role in mitigating the negative impacts associated with hybrid threats. We create comprehensive overviews of key cybersecurity regulations worldwide and offer guidance on managing the complexities introduced by AI and quantum computing. Additionally, we establish industry best practices to strengthen the resilience of supply chains against cyber threats amidst shifting geopolitical landscapes.

By raising awareness about cyber threats, promoting best practices, and providing training opportunities for individuals, students, and organizations globally, the Charter of Trust ensures a proactive approach to cybersecurity. Furthermore, it fosters public-private dialogue, advocates for greater international alignment and reciprocity in cybersecurity regulations and advises regulators on practical implementation strategies.

2

IMPACT ON CORPORATIONS: RIPPLE EFFECTS

ATTACKS AND ACTORS

The proliferation and diversity of threat actors have significantly expanded, creating a highly challenging cybersecurity landscape. While cybercrime was once the domain of a small, highly skilled elite, the emergence of AI and other advanced technologies has democratized cybercrime[1].

The rise of hacktivist groups, Cyber Crime-as-a-Service (CaaS), and alliances among threat actors have further magnified the scale and complexity of threats, enabling even unsophisticated individuals to orchestrate impactful attacks.[2] Norbert Vetter, CISO at TÜV SÜD, confirms that "the emerging multipolar world has amplified the threats facing multinational enterprises."

Between 2000 and 2023, the European Repository of Cyber Incidents (EuRepoC) database recorded 2,506 politically motivated cyber-attacks, of which China accounted for 12 percent, followed closely by Russia at 11.6 percent. However, the majority of these harmful incidents – 45 percent – remain unattributed.[3] The ENISA Threat Landscape Report 2024 also underscores the inherent difficulty in attributing the origin of attacks, stating that in one of three attacks, the threat actor was unknown.[4]

> » *Around the globe, we see a continued rise in reporting of financially motivated crime utilizing ransomware and supply chain threat vectors. In addition, we believe that hacktivist individuals and organizations will use cyber-attacks to advance their political causes.* «

Kyle Oetken

Director
Cyber Defense
at AES

CHARTER OF TRUST MEMBERS TRACK ATTACKS AND HELP BRING CLARITY IN THE COMPLEX THREAT LANDSCAPE

Natalia Oropeza, Siemens Global Chief Cybersecurity Officer, observes that the most common types of incidents, which Siemens has addressed over the past five years, involve malicious activities targeting employees:

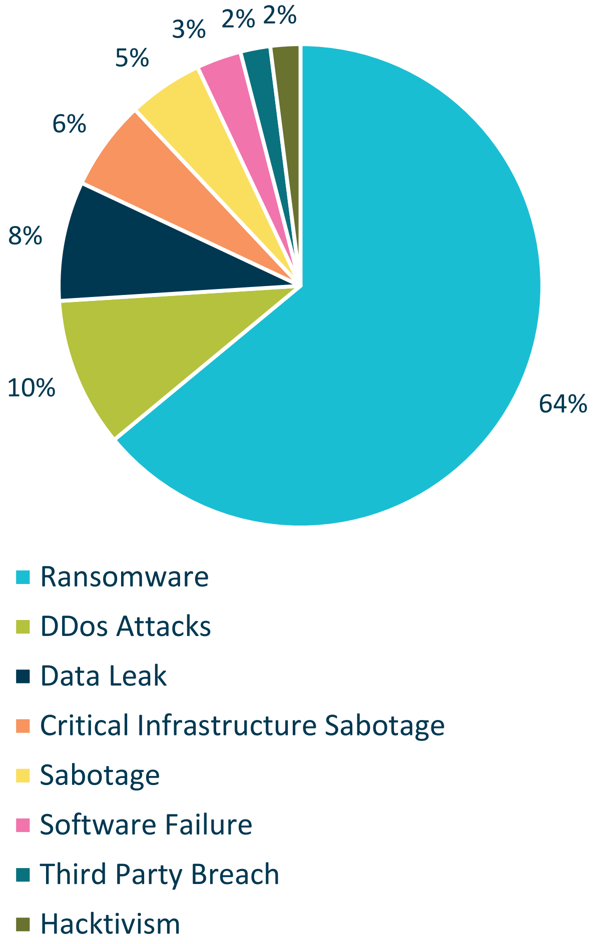
1. Credential Leaks,
2. Malware, and
3. Social Engineering.

Credential leaks, frequently linked to differnet types of social engineering attacks (e.g. phishing), have overcome malware attacks over the last years.

According to Siemens and Danfoss, ransomware attacks continue to pose the greatest threat. Morten Pors Simonsen emphasizes that “this is not due to the risk of data leaks, but for the damage on the IT infrastructure and the resulted unavailability.”

Additionally, Siemens highlights nation-state actors might be a significant concern, particularly due to sabotage attacks targeting critical infrastructure.

Cybersecurity events impacting relevant sectors for Siemens in 2024



> » *Danfoss has experienced DDoS attacks on country-specific websites that we suspect are linked to hybrid warfare, mostly with the intent to create FUD (Fear, Uncertainty, and Doubt).* «
>
> **Morten Pors Simonsen**
>
> *Chief Information Security Officer at Danfoss*

Multinational corporations manage vast digital infrastructures that often intersect with critical national systems. Cyberattacks targeting these corporations can trigger cascading effects on national economies and public infrastructure. “There is currently an increasing number of hybrid attacks not only addressed to exfiltrating and stealing intellectual property and industrial knowledge, but also to indirectly causing damage to countries by damaging infrastructures deployed or operated by these corporations,” explains Natalia Oropeza, Global Chief Cybersecurity Officer at Siemens.

Additionally, Raphael Otto, CISO & CSI at Infineon, notes that hybrid threat tactics can result in economic pressure and trade disruptions, affecting supply chains and leading to increased costs and operational challenges. These factors often translate into severe financial implications for companies, including expenses related to remediation, legal fees, regulatory fines, and loss of revenue.

THREAT ACTORS BLUR LINES WITH CYBERCRIME AND PSYCHOLOGICAL TACTICS

Alongside the rise in technical attacks, hybrid threats have increasingly adopted psychological tactics. Paul Bayle, Group CISO at the Charter of Trust partner ATOS, indicated that “the most notable incident linked to hybrid warfare was the false allegations published by a Russian-affiliated group of cybercriminals in December 2024, claiming they had successfully compromised Atos.”

Paul Bayle highlights that “their false allegations caused significant concern, even though this group had not even attacked Atos at all. Few clients reacted immediately, with some even disconnecting their networks’ gateways.” He underscores that incidents like this demonstrate “the powerful impact of such malicious claims, even when no actual data was stolen, and no system was breached.”

Raphael Otto, CISO & CSO at Infineon, similarly highlights the evolving nature of cybercrime, noting that it can be “perpetrated by both financially motivated threat actors, such as organized crime groups, and nation-state affiliated actors engaged in cyber espionage.”

He further explains that the “distinction between these two types of threat actors is becoming increasingly blurred due to their collaboration and evolving motives, as well as the utilization of services like malware as a service, which further impedes attribution between actor groups.” This blending of motives and methods, combined with advanced psychological tactics, makes identifying and combating these actors increasingly complex.

> » *Hybrid threats and hybrid warfare are multifaceted and can encompass cyber security risks, economic challenges, geopolitical instability, and operational disruptions. Adapting to these complex threats requires a comprehensive approach that integrates cyber security, geopolitical risk analysis, and robust business continuity planning.* «
>
> **Raphael Otto**
>
> *Chief Information Security Officer at Infineon*

MULTINATIONAL COMPANIES CANNOT ESCAPE THE THREAT EXPOSURE

Such attacks significantly impact an "enterprise's digital infrastructure, especially communication networks, and brand reputation, disrupting operations and eroding customer trust", reflects Raphael Otto, Infineon CISO & CSO. Similarly, Siemens Global Chief Cybersecurity Officer Natalia Oropeza emphasizes the growing prevalence of disinformation and reputational campaigns, particularly as a result of geopolitical conflicts.

The challenges posed by these campaigns are further compounded by the increasing frequency and sophistication of ransomware attacks.

For industries that depend on system availability, such as manufacturing, the unavailability of critical systems due to ransomware can lead to catastrophic ripple effects. Speaking on this issue, Danfoss CISO Morten Pors Simonsen emphasized that "for a manufacturing company like Danfoss, the availability of our critical systems is of utmost importance."

3

THE FUTURE OF HYBRID THREATS: KEY CHALLENGES

The evolution of hybrid threats indicates a significant escalation in the precision and scale of cyberattacks. The emergence of post-quantum computing could introduce unprecedented vulnerabilities, underscoring the urgent need for corporations to implement forward-looking security measures.

According to the Allianz Risk Barometer, cyber incidents remain the top global risk for 2025, marking the fourth consecutive year in this position – and likely remaining in this ranking in the near future.

The experiences of Charter of Trust partners underscore the growing significance of hybrid threats and the merging of political and corporate spheres in the realm of cybersecurity. To maintain vigilance, partners have identified several key threat drivers in the cyber domain and developments that will demand focused attention in the coming decade.

ADVANCED PERSISTENT THREATS (APTS) AND STATE-SPONSORED ATTACKS

» *While AI will contribute to more effective and efficient cyber defense in the future through consistent integration into defense frameworks, attackers currently benefit more. This is partly because the validation and verification of (non-trivial) AI systems is not yet systematically solved, and securing these systems is very complex. As an attacker, the advantages of generative AI are much easier to exploit.* «

Christoph Peylo

Chief Cyber Security Officer at Bosch

APTs are expected to focus on prolonged, clandestine access to sensitive information, aiming to disrupt operations and gain strategic advantages. Increasing geopolitical tensions are likely to drive a surge in such covert activities targeting critical infrastructure and key industries. Similarly, the frequency of cyberattacks involving nation-states is projected to grow.

Bosch Chief Cyber Security Officer (CCSO) Christoph Peylo predicts "a rise in sophisticated, state-sponsored attacks" alongside an intensification of "espionage campaigns targeting intellectual property and sensitive data related to critical infrastructure." He further notes that these attacks, potentially originating from both state-sponsored actors and industrial competitors, will "leverage advanced persistent threats (APTs) designed to evade detection and exfiltrate valuable information."

AI AND CYBER THREATS

The integration of AI into cyber threats is poised to reshape the threat landscape. Adversaries are expected to harness AI to execute more precise and scalable attacks, including automated disinformation campaigns and highly sophisticated phishing schemes – making such tactics accessible even to those with limited resources or expertise.

Looking to the future, Paul Bayle, Group CISO at Atos, highlights that "advanced information manipulation tools," particularly through AI, will present a pervasive challenge.

» *Today's quantum computers are rapidly progressing toward 'cryptographic relevance' while cybercriminals may be stealing and storing data, a practice known as 'harvest now, decrypt later' hoping to access sensitive data. Organizsations should accelerate post-quantum cryptography planning today.* «

Koos Lodewijkx

Vice President and Chief Information Security Officer at IBM

EXPLOITATION OF EMERGING TECHNOLOGIES

Emerging technologies like quantum computing offer groundbreaking opportunities but also introduce new vulnerabilities. Quantum computing, for example, has the potential to compromise current encryption protocols, leaving critical data more vulnerable to breaches.

This timeline is no longer speculative; it has become a pressing reality that requires immediate action. The replacement of existing algorithms in critical industries is urgent but faces a significant challenge, as modifications to products and systems often take decades to implement. It is essential to begin preparations for replacing these algorithms, particularly in industries where such changes are both complex and time intensive.

SUPPLY CHAIN VULNERABILITIES

Supply chains continue to represent a critical vulnerability, as adversaries increasingly exploit interconnected networks to disrupt operations. The complexity of global supply chains makes it difficult to monitor and secure every link, underscoring the need for robust risk management strategies and collaboration among stakeholders.

Christoph Peylo, CCSO at Bosch, emphasizes that “disruptive attacks, including ransomware and distributed denial-of-service (DDoS) attacks, will likely increase, potentially disrupting supply chains and essential services.” He further highlights that this risk is exacerbated by the “interconnectedness of European industries and critical infrastructure with global networks.”

» *The interconnected nature of supply chain disruptions are critical risks, as cyber incidents often overlap with other critical risks such as business interruption and geopolitical tensions. This interconnectedness requires multinational companies to adopt a holistic approach to risk management, integrating cyber resilience into their broader strategic framework.* «

Haydn Griffiths

Chief Information Security Officer at Allianz Commercial

4

SOLUTIONS: THE CHARTER OF TRUST PLAYBOOK

Addressing the multifaceted challenges of hybrid warfare requires collective action. Just a few years ago, companies often operated in secrecy regarding security breaches, fearing reputational damage or competitive disadvantage. However, the scale and sophistication of modern cyber threats have reshaped this mindset, revealing a critical truth: no organization, regardless of size or industry, can face these challenges alone.

TO THIS END, CHARTER OF TRUST PARTNERS HIGHLIGHT POTENTIAL SOLUTIONS:

1. Collaboration as a Foundation

Intra-sectoral collaboration has become a critical defense strategy in cybersecurity. By working together, companies within the same sector can identify patterns in attack vectors, anticipate vulnerabilities specific to their shared infrastructure, and implement more cohesive defenses. Christoph Peylo, CCSO at Bosch, emphasizes that “investing in cybersecurity resilience and actively collaborating with international partners are crucial steps in safeguarding European industry and national security in this challenging geopolitical environment.”

Equally vital is inter-sectoral collaboration, as cyber threats frequently span multiple industries and exploit interconnected systems. Cybercriminals and state-sponsored actors do not confine their activities to a single sector, making the lessons learned in one field essential for protecting another.

> » *Over the past five years, our cybersecurity approach has been continually evolving. We strive to maintain an adaptive security posture, recognizing that attackers constantly update their techniques. It is a matter of survival to do the same. We regularly review top risks and implement transformation projects to mitigate them, ensuring our cybersecurity measures remain robust and responsive.* «

Paul Bayle

Head of Security and Chief Information Security Officer at Atos

Natalia Oropeza, Siemens Global Chief Cybersecurity Officer, highlights this challenge: “All of these attacks have undesirable international effects; some countries are resorting to protectionist policies: They show reluctancy to share threat intelligence information or they are producing regulation that hinders cross-country collaboration. This strategy put in place by some countries does not seem to consider the fact that hacking ‘industry’ does not know frontiers.”

Engaging in collaboration is crucial for private companies to establish a unified defense strategy against modern cyber threats. The Charter of Trust underscores the power of collaboration in a field where information-sharing is often constrained by competitive concerns and the sensitive nature of cyber incidents.

Haydn Griffiths, CISO at Allianz Commercial, highlights the EU Digital Operational Resilience Act as an example of increasing regulatory demands, accentuating the importance of readiness and robust responses to information security incidents. Ultimately, fostering a comprehensive and transparent strategy is crucial to collaboratively develop shared threat intelligence, identify sector-specific vulnerabilities, and implement unified defense mechanisms. This also entails engagement with the public sector, industry peers and jointly fostering an environment of resilience. Such collaboration not only strengthens individual corporate defenses but also enhances collective resilience.

2. Advanced Cybersecurity Measures and AI for Threat Detection

As Koos Lodewijkx, CISO of IBM, explains, effective cyber defense ultimately relies on the ability to detect and isolate intruders quickly – and AI plays a pivotal role in intercepting attacks at early stages. AI-driven threat detection systems enable real-time identification and mitigation of sophisticated attacks, while Zero Trust architecture restricts access and minimize vulnerabilities.

As Charter of Trust partner IBM revealed in their latest *Cost of a Data Breach Report,* two out of three organizations stated that they are deploying security AI and automation across their security operations center and saw a 10% jump from the prior year. When

> » *The importance of collaboration across different sectors, but also within individual sectors, cannot be overstated. While there is a reluctance to discuss security measures in public, within these collaborative frameworks, significant knowledge is gained through the sharing of experiences, as all parties are confronted with similar challenges.* «

Norbert Vetter

Chief Information Security Officer at TÜV SÜD deployed extensively across prevention workflows, organizations averaged USD 2.2 million less in breach costs compared to those with no AI use in prevention workflows.[5]

Beyond AI, Infineon takes a structured approach to quantifying risks, evaluating them as a combination of threat actor capabilities, defense capabilities, and the potential impact of security events. According to Infineon CISO & CSO Raphael Otto, these quantified risks are used to prioritize security investments. By leveraging this approach, Infineon can identify risks and gaps in its defenses, allowing the organization to address them proactively.

Organizations must adopt proactive safeguarding measures against complex threats. Key steps include developing multi-vendor strategies, regularly optimizing incident response plans, and conducting cyber simulation exercises to prepare for potential incidents.

3. Education and Talent Management

Technological solutions alone are insufficient to mitigate risks. As Atos Group CISO Paul Bayle emphasizes, "raising awareness and providing training on cybersecurity, alongside fostering critical thinking, will be essential for executives to make informed decisions and mitigate the impact of hybrid warfare." Efforts like the implementation of secure-by-default principles for critical infrastructure and IoT technologies must go hand in hand with consistent employee training to counter human vulnerabilities, stresses Koos Lodewijkx, CISO at IBM.

Echoing this, TÜV SÜD CISO Norbert Vetter says that the "key to success is to prioritize and support your cyber defense experts. Paired with powerful AI-driven technologies, these defenders form the backbone of any effective cyber defense strategy. In an era of government-backed hacking, the threat level has never been more critical." By explaining cybersecurity in terms of business impacts and aligning it with broader organizational goals, companies can bridge the gap between technical measures and executive decision-making, ultimately fostering awareness and a culture of security. Charter of Trust partners are actively engaged in education. They set out to raise awareness about cyber threats, promote best practices, and provide comprehensive training opportunities to individuals, students and organizations across the world.

Discovering and fostering talents in the field of cybersecurity is of utmost importance if one sets out to navigate the evolving threat landscape successfully as a company, organization, and society. One example, which Charter of Trust partners engage in, is the Cyber Talent Academy, which provides accelerated, high-quality training and GIAC Certifications to effectively launch careers in cybersecurity. This free program enables participants to pass industry-recognized certification exams, equipping them with skills that will make a difference in the field from day one.

By providing this training, the Charter of Trust is bridging the digital skills gap globally. The Cyber Talent Academy trains and offers job opportunities to underrepresented groups, which in turn helps companies to find and hire much-needed cybersecurity talents and develop them into experts.

4. Acknowledging Regional Cultural Differences - Fostering Collaboration

According to Bosch CCSO Christoph Peylo, Germany and Europe, although making progress, still lag behind Asia and America in robust cybersecurity knowledge sharing and seamless public-private collaboration. Cultural factors, such as a strong emphasis on data privacy and a traditionally cautious approach to information sharing, contribute to this gap. Additionally, the fragmented nature of the European legislatures – where national authorities interpret European regulations and enforce varying security postures – creates significant challenges to achieving cohesive collaboration.

Bosch CCSO Christoph Peylo also highlights those distributed responsibilities, such as those inherent in Germany's federal structure, further exacerbate fragmentation and complexity. He stresses that overcoming entrenched cultural factors and breaking free from path dependency is essential for progress. Leadership must actively embrace change, with initiatives like the Charter of Trust serving as prime examples of how collaboration can drive meaningful advancements. To address these challenges, inter-corporate collaboration across borders is vital, as it lays the groundwork for global regulatory alignment and more unified approaches to cybersecurity.

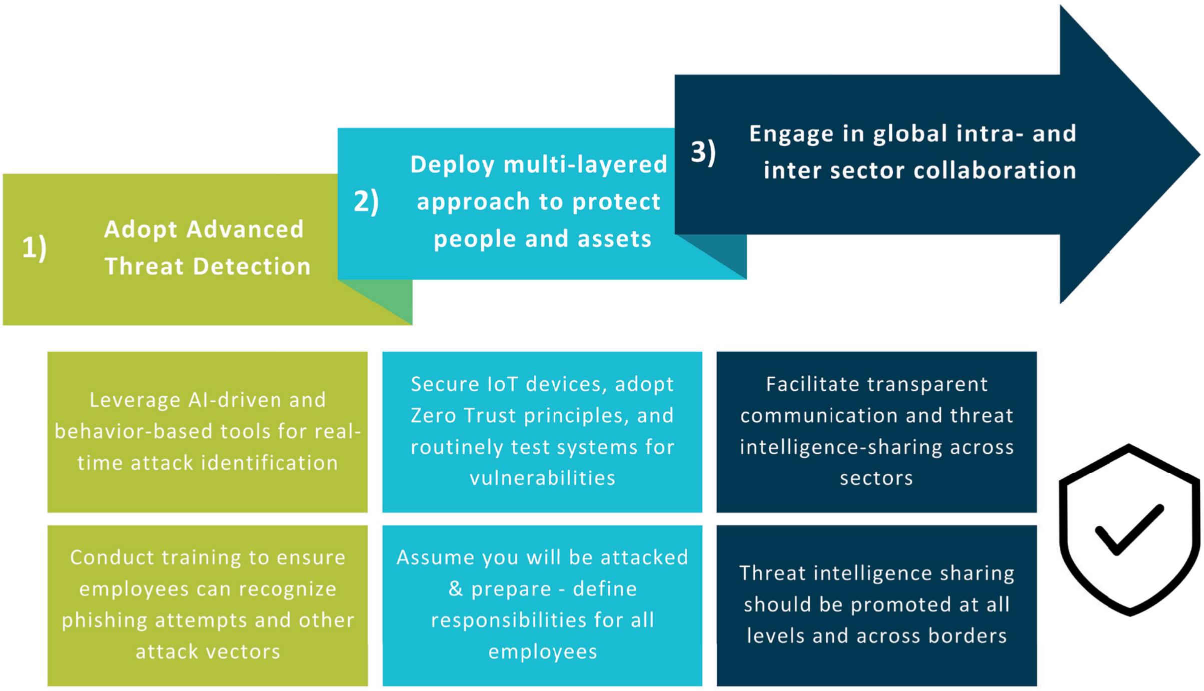
5. Unifying Cybersecruity Policies and Establishing Common Standards

Looking ahead, a collaborative and global approach to cybersecurity is essential. Natalia Oropeza, Siemens Global Chief Cybersecurity Officer, stresses the need for unified efforts, saying, "hacking and cybersecurity do not know borders, so it is not wise to focus only on national policies; instead, work towards international standards and agreements." Initiatives should prioritize professionalization of cybersecurity practices by defining clear processes and procedures, which should be ideally equivalent or aligned across geographies and industries. To be truly effective, the current fragmented ecosystem of cybersecurity initiatives must consolidate. She observes that "now is the moment for consolidating different cybersecurity initiatives to be more efficient."

A unified front will not only simplify collaboration but also amplify the impact of cybersecurity strategies worldwide. Beyond organizational hurdles, substantive challenges also impede effective information sharing. "The lack of standardized metrics for attacks leads to disparate and difficult-to-compare results. Establishing a common measurement and interpretation framework would enable comparability and trend analysis", says Bosch CCSO Christoph Peylo. By fostering policy harmonization and aligning with international regulations and agreements, companies help to establish global norms for cybersecurity and conflict prevention, fostering a secure and predictable operating environment.

The CISO experience shows that robust threat detection mechanisms are key. Effective monitoring combines advanced AI-driven tools for real-time analysis with skilled teams to interpret and respond to threats. This proactive approach ensures timely and actionable responses to hybrid threats. Governments and organizations can adopt these models by investing in tools that provide system-wide visibility and training personnel to make informed decisions based on intelligence.

The multi-layered cybersecurity strategies of multinational organizations also highlight the value of defense in depth. Techniques such as network segmentation, endpoint protection, encryption, and regular audits help reduce vulnerabilities and mitigate potential breaches. These practices demonstrate the importance of adopting multi-layered defenses to address the diverse nature of hybrid threats, which encompass cyber, physical, and informational dimensions. Governments and critical infrastructure operators can enhance their resilience by implementing similar strategies.



1) Adopt Advanced Threat Detection

2) Deploy multi-layered approach to protect people and assets

3) Engage in global intra- and inter sector collaboration

Leverage AI-driven and behavior-based tools for real-time attack identification

Conduct training to ensure employees can recognize phishing attempts and other attack vectors

Secure IoT devices, adopt Zero Trust principles, and routinely test systems for vulnerabilities

Assume you will be attacked & prepare - define responsibilities for all employees

Facilitate transparent communication and threat intelligence-sharing across sectors

Threat intelligence sharing should be promoted at all levels and across borders

The three steps of cybersecurity strategies against hybrid threats for multinational organizations

5

FINAL REMARKS

The rise of hybrid threats underscores the necessity for a proactive, collaborative approach to cybersecurity. Multinational corporations are well positioned to lead such efforts, given their role as both targets and defenders. Kyle Oetken, Director Cyber Defenses at AES states, “we see threats as a persistent reminder to continuously enhance cybersecurity capabilities, innovate in threat detection, and collaborate with other organizations for collective defense and response”. Collaborative frameworks, such as those advocated by the Charter of Trust, provide a foundation for unified action, addressing threats that transcend national and sectoral boundaries.

The experiences of the Charter of Trust partners offer valuable lessons for addressing the complexities of hybrid threats. These organizations operate in dynamic, high-stakes environments where the stakes of disruption and their ability to adapt and thrive in such conditions provide a blueprint for peers in the industry to improve preparedness.

Infineon CISO &CSO Raphael Otto concludes that “we and all the other companies in the sector should prioritize measures to safeguard our supply chains, the implementation of a threat-informed approach to cyber security, and fostering a cyber security culture where best practices are consistently implemented and employees show ownership for security within their own area of responsibility and work life as those are crucial in in maintaining a strong defence against cyber threats.”

Initiatives like the Charter of Trust exemplify the power of collective action in strengthening the global cybersecurity ecosystem. By embracing these lessons – blending technology, strategy, collaboration, and adaptability – stakeholders can build stronger defenses against the growing complexity of hybrid threats and ensure a secure future.

Endnotes

[1] Wall, D. S. (2024). Cybercrime: The transformation of crime in the information age. John Wiley & Sons.

[2] Müller, J. (2024). New Hackonomy—The Alternative Platform Economy. In Turning Point (pp. 193-226). Springer, Wiesbaden

[3] https://www.statista.com/chart/31805/countries-responsible-for-the-largest-share-of-cyber-incidents/

[4] ENISA Threat Landscape Report 2024 - https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[5] IBM Cost of a Data Breach Report 2024: https://www.ibm.com/reports/data-breach

Publication information
Charter of Trust

Agora Strategy Group AG
Residenzstraße 7
80333 Munich

Kekst CNC – Communications &
Network Consulting AG
Leopoldstr. 10
80802 Munich

Contact
www.charteroftrust.com
contact@charteroftrust.info

Text and Editing Agora Strategy Group AG | Kekst CNC | Charter of Trust
Concept and Design Agora Strategy Group AG | Kekst CNC
Editorial Office Verena Kasirye, Anne Blickhan, Leandro Neff, Mathis Böhm, Lina Blumenröder
Print Zimmermann GmbH Druck & Verlag

NOTES

NOTES

WWW.CHARTEROFTRUST.COM

CONTACT@CHARTEROFTRUST.INFO

CHARTER OF TRUST