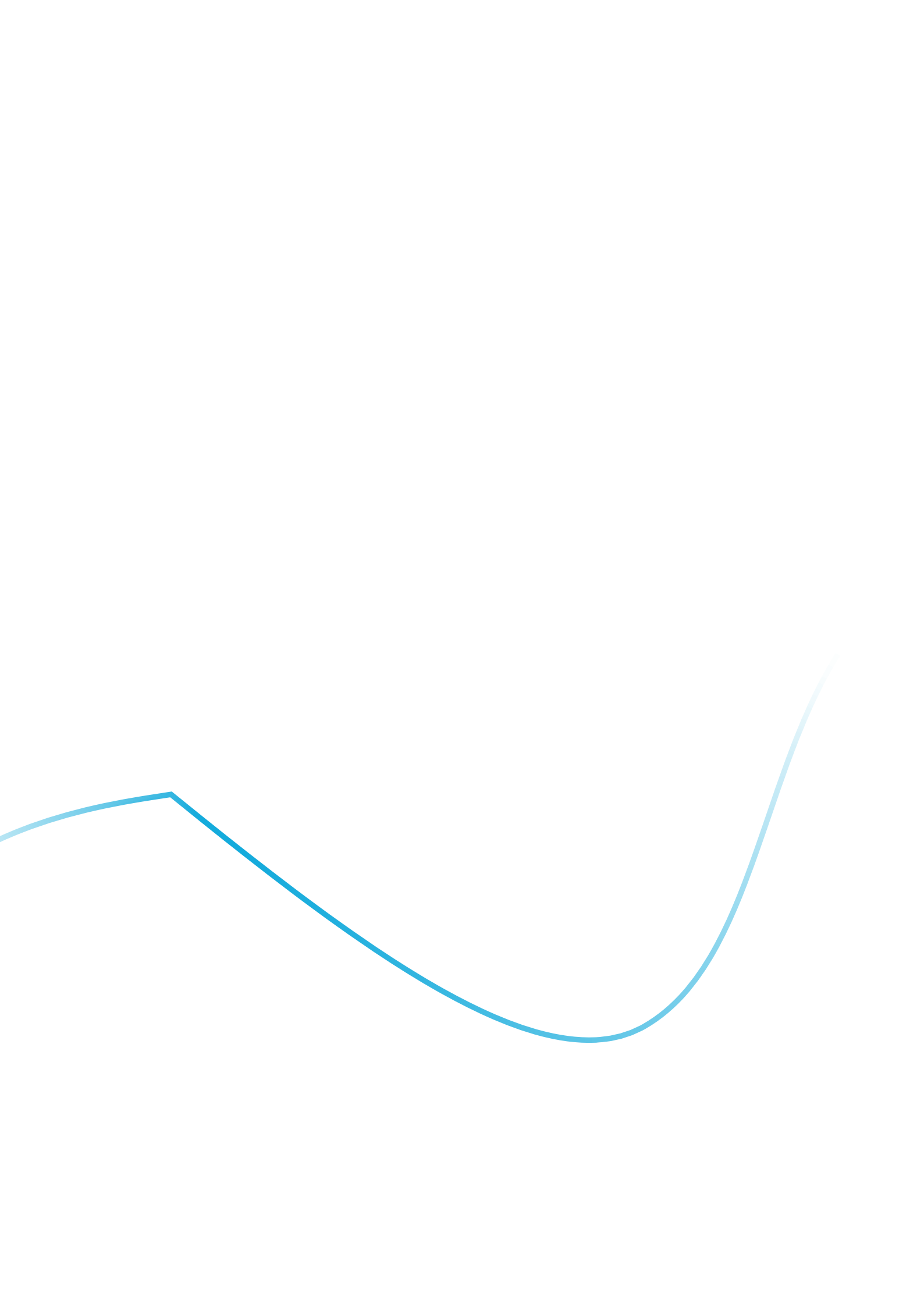


STAYING SECURE IN A CONNECTED WORLD

Trends in Cybersecurity 2024





STAYING SECURE IN A CONNECTED WORLD

Trends in Cybersecurity 2024

MANAGEMENT SUMMARY: STAYING SECURE IN A DIGITAL WORLD

Thank you for reading this brand-new edition of Trends in Cybersecurity. The theme of this year's edition is; staying secure in a digital world. In a world that is increasingly connected, upholding the security of all of us is more important than ever. Not surprisingly, Compliant Security Operations is a recurring topic in this trends report; it has a crucial role in safeguarding security in a digital world.

Over the last few years, organizations have faced various challenges. A few examples:

- Forced remote working;
- Threats caused by cyber criminals and state actors;
- Disruptions in the supply chain;
- An increasingly complex compliance landscape.
- Safeguarding and demonstrating compliance calls for a flexible security organization that is able to uphold all the necessary measures and checks.

My name is Hans Marcus. I am the author of this management summary, together with Ruud Koning, IT Manager at the Foundation for Preparation of the PALLAS Reactor (Stichting Voorbereiding PALLAS Reactor) and responsible for all IT-related subjects – including all aspects of cybersecurity.

The Foundation for Preparation of the PALLAS Reactor (PALLAS) is designing and building a new nuclear reactor in the Netherlands, the first one to be built in this country in decades. This reactor is specially designed for the production of medical isotopes that are crucial for nuclear medicine, and the diagnosis and treatment of diseases such as cancer.

Besides the reactor, the future PALLAS organization will also operate a Nuclear Health Center. There, medication will be produced, created with the nuclear isotopes from the reactor. Almost everyone knows someone who has had to deal with cancer, and who has had the diagnosis or treatment with the nuclear medicine. PALLAS estimates that it will be able to produce 30 to 40% of the global demand for medical isotopes, an enormous contribution to health care.

However, realizing a project such as PALLAS brings along several complex challenges. PALLAS needs to comply with many sets of rules and regulations, such as the Dutch Nuclear Energy Act (KEW, Nederlandse Kernenergie Wet), NIS2 and GxP. Complying with these rules and guidelines requires a well-organized security operation. Ruud Koning is committed to answering all the questions that revolve around Compliant Security Operations; not only for the Foundation itself, but also for the future PALLAS organization.

Ruud: "The organization of PALLAS has grown enormously in recent years. Designing the nuclear reactor and the supporting systems and processes is a big job. The operational IT organization of the Foundation may seem small, only 3 or 4 people, but the whole group of people who are involved in IT and cybersecurity for the new reactor is a lot bigger. And there are people designing the reactor and the supporting systems. In the cybersecurity group, more than 10 people are working on the design of the technical systems, the security management system, and the overall cybersecurity architecture. Together, these people support hundreds of engineers and architects who are working on the physical systems, physical buildings, operating systems, and the future organization of the PALLAS installation."

A solid security operations model should go hand in hand with compliance. The article Cyber resilience and security baselines: Do baselines such as BIO lead to cyber resilience? investigates whether a baseline such as BIO (Baseline for governmental information security) is sufficient to safeguard cyber resilience. The article describes how a solid security operations model and compliance can go together. According to the authors, a consistent operational model not only safeguards compliance, but it also makes compliance demonstrable.

Ruud: "We do not only design the reactor and its systems. We also design the future organization and the business model we want. Combined with the shared executive board with the operator of the current High Flux Reactor, this results in several interesting challenges around the repositioning of people and operations – not only for future operations, but also during the building period and the commissioning of the installation. The security operations model is highly relevant, and an important aspect of all we are doing."

PALLAS is not the reality yet. Both the reactor and the organization are still in the design and build phase. However, there are a lot of third parties involved in the project – organizations that are responsible for aspects of the design of the reactor and its supporting systems.

Ruud: *"The design of the reactor and its organization is really all about people: How do you get everybody lined up behind the common goal? We adhere to the systems engineering method and its engineering flows and, for instance, PDRs: Preliminary Design Reviews. This entails constantly checking whether everybody is still aligned and making progress towards that common goal. We devote a lot of attention to logic and the applications that will steer the operating and security systems in the right direction. All this work is done by different companies and involves large groups of people."*

Risk management regarding third parties is an important aspect of this work, and the commitment of the right stakeholders is essential. The article 'Third Party Risk Management (TPRM)' provides an answer to a crucial issue: How can organizations organize their risk management more effectively, and how can the Board prioritize TPRM? The article stresses the importance of third-party risk management, and the involvement of the right stakeholders. It provides insights into the improvement of risk management within organizations, and ways in which the Board can prioritize TPRM.

In many organizations, SAP takes care of ERP functionality. Securing all the aspects of the SAP platform – infrastructural and otherwise – can be a big challenge. In the article 'Secure SAP in Blueprint: best practices and strategies for protecting your business', the authors demonstrate how security should be a by-design feature of the SAP platform, to comply with rules and regulations. The article focuses on answering the main issue: 'how to design a blueprint for the security of the SAP application layer?' As such, it stresses the importance of an all-encompassing approach, to safeguard optimal protection.

The PALLAS reactor is a large, complicated machinery that needs to be able to operate securely. The products made by this machinery should be distributed to the patients in time, in the right amounts and to exact specifications. PALLAS aims to become a digital enterprise, with a digital heart: a true 'Intelligent Industry.'

Ruud: *"The DES, or Digital Enterprise Strategy, is the design for the future PALLAS organization. The DES aims to deliver a digital organization that optimizes the production process and provides optimal security for that process against outside influences. In this DES, our primary process and the demands for security and compliance meet - by design and foundation, ensuring that the business process is not only highly effective and efficient, but demonstrably compliant and safe, too. The DES informs the architecture and the configuration of the PALLAS application landscape; both for the business and the operation. It's a true digital blueprint!"*

The field of OT security is specialized in the security of Cyber-Physical systems – systems where production process and information meet.

Ruud: *"PALLAS contains a great deal of systems that govern and monitor physical processes. We're looking at a total of about 250 systems, across nuclear and conventional control systems, transport systems, laboratories, radiation monitoring, energy systems, climate control. But also physical security, communication with internal and external parties and, of course, business systems that are used by administration, planning and analysis. All these systems directly or indirectly influence the primary process: the production of nuclear medicines. All these systems must be protected, while considering the physical process as well. That's why we regard security as a by-design feature, that's integrated in the design process from the start."*

Once everything is designed and built, someone should be made responsible for maintaining security. Many organizations choose to hire a Managed Security Service Provider (MSSP). In the article "How to choose the perfect security service provider for your organization," we discuss the search for the right provider for your organization. Technical requirements may be easy to determine, but how about the overall service experience?

Discover the complex world of security and stay ahead of the curve in a fast-changing digital environment! This new edition of Trends in Cybersecurity

reveals the challenging reality of the design, implementation and management of a security organization that meets the strictest demands. Staying secure in a digital world is essential; we are proud to invite you to join us on this journey toward a secure future.

We hope you will enjoy this second edition of Trends in Cybersecurity, and that it provides you with insight into the challenges and opportunities for a secure future in a digital world.

About the authors:

Hans Marcus
OT Security Expert



Ruud Koning
CISO bij PALLAS



CONTENT

Section	Title	Author	Page
	Management summary: staying secure in a digital world	Hans Marcus Ruud Koning (PALLAS)	02
	The evolution of cybersecurity at NS: future proofing the security of Netherlands' biggest provider of public transport	Serge Dujardin Dimitri van Zantvliet (NS)	06

ORGANIZATIONAL ASPECTS OF SAFETY





Unleashing the power of the cloud: ensuring security and compliance	Yagmur Bozcuk Rahul Mishra	10
Cyber resilience and security baselines	Renato Kuiper Jule Hintzbergen	16
The indispensable role of the board in 'third party risk management'	Britt Huveneers Christiaan Koopman Manisha Ramsaran	23
Why business continuity is crucial in times of social unrest	Manouck Schotvanger Rachel Splinters	29
The perfect match: how to choose the perfect security service provider for your organization	Arjen van der Post Dick Bruines Sebastiaan de Vries	35
Navigating nis2: organizational challenges and solutions	Florianne Kortmann Sasha Brouwer	39

SECURITY IN EMERGING (OR EXPANDING) AREAS OF TECHNOLOGY



Data in the metaverse: who is the owner?	Alfredo Acuña Salswach Selma Mujcic	46
The value of test beds in a quantum safe migration journey	Julian van Velzen Gireesh Kumar	51
Privacy and ethics in the ai revolution: how to build a strong organization	Jorrit Tromp Selma Mujcic	56

Section	Title	Author	Page
DETECTION AND RESPONSE			
	Empower ot soc security: eliminate threats with custom intelligence and cloud infrastructure	Sourabh Suman	62
	Threat hunting and cybersecurity maturity: are you trying to run before you can walk?	Saskia Kuschke	66
TECHNOLOGY-FOCUSED SECURITY ASPECTS			
	Secure sap in blueprint: best practices and strategies for protecting your business	Ali Cifci Ankit Arya	71
	Better security, without compromising performance	Sebastiaan de Vries Laura Adelaar Dennis van de Water Jeroen van Hulst	74
	Publications		79

**THE EVOLUTION OF
CYBERSECURITY AT NS:
FUTURE PROOFING THE
SECURITY OF
NETHERLANDS'
BIGGEST PROVIDER OF
PUBLIC TRANSPORT**



Dutch Railways (Nederlandse Spoorwegen, NS) has been operating trains in the Netherlands for 184 years. Since then, a plethora of security areas have been developed to cope with the changing security landscape and to integrate emerging insights. Cybersecurity is the tenth security area for NS – and the company is in the midst of its development. In this article, we discuss the present and future of the cyber function at NS.

Attack surface

So, why has cybersecurity become a focus area for NS? There are several factors in play. Firstly, the attack surface is bigger than ever. Nowadays, everything's stored in the cloud, which brings its own particular vulnerabilities. Plus, NS's services increasingly revolve around mobile devices. NS's portfolio of travel products itself is constantly expanding – travel products that increasingly include travel options outside of the Netherlands. In total, approximately 520 Application Programming Interfaces (APIs) have been built. Together, they process 12 billion calls every year. As such, the potential attack surface is huge.

Compliance

Secondly, NS must comply with Dutch and international rules and regulations. In December 2021, NS was designated Operator of Essential Services. As a result, the public transport provider is subject to the European Network and Information Systems legislation (NIS). This also has consequences for cybersecurity; in one of the articles in this report, we take a closer look at this aspect. In another article, we discuss NIS2, the most recent version of this legislation. As you'll learn, compliance with NIS in all its guises is one of the pillars of a secure digital future.

OT Security

Thirdly, while the attack surface has grown, the threat landscape has intensified severely, too. It's a development that has only been exacerbated by the outbreak of the war in Ukraine and all its subsequent developments. And it turns out that Operational Technology (OT) is vulnerable to cyber-attacks as well. As an example, malware and wiper ware have been developed by bad actors that target the Ukrainian railway. Luckily, such malware hasn't been encountered in the Netherlands – and indeed NS has acted upon this threat and taken measures – but we must remain vigilant. Further on in this report, we analyze the vulnerabilities of OT, and the need for constant vigilance in the Netherlands.

Cyber strategy

Under the direction of the director of cybersecurity Dimitri van Zantvliet, NS has established its first long-term cyber strategy. This cyber strategy reflects the crucial role in society of NS. Dutch Railways are under scrutiny; traveler numbers must be regained; green mobility must be facilitated – and NS should give shape to its role of enabler of economic and civil activity. The level of trust in NS in part depends on the level of cybersecurity the company can realize.

All in all, it's not a surprise that cyber is a board room priority to NS. To give shape to that priority, the cyber function was recently separated from the IT function. As director cybersecurity, Dimitri regularly has his own seat at the table, and his department has its own directorate.

Building blocks

NS's cyber strategy is based on several building blocks. Firstly, the strategy prescribes a radical shift-left when it comes to cyber; cyber and privacy

nowadays are by-design features of any functional and non-functional design. For NS, this is not only a matter of security; adding the necessary cyber layers after the fact is far more labor, cost and resource intensive. To facilitate this process, the department provides centralized, standardized cyber services to developers such as threat modelling, secret scanning, and PEN testing. That's the second building block. For developers, this makes it easy to incorporate such services into the pipeline. By regarding cyber as a by-design feature, NS is better positioned to identify and prevent cyber threats. For more information about such detection efforts, don't forget to read the article about threat hunting, included in this report.

The implementation of zero trust is the third building block. At the time of writing, NS predominantly uses perimeter-based security. In the coming years, this will shift towards identity-based security. It's a totally new philosophy, based on zero trust, which will come to fruition between 2026 and 2030. The fourth building block focuses on the aspect of culture: NS is determined to establish a cybersafe culture throughout its organization.

The human factor

Due to the growing complexity and size of the threat surface, combined with the intensifying threat situation, the need for expert personnel is growing. OT security, cloud security, identity security: these are all specific disciplines, with their own complexity, requiring specialized skills and expertise. For this, NS needs specialists – and in the light of the global scarcity of talent, fulfilling this need is a big challenge. To cope with this, NS increasingly trains its own specialists, at its own cybersecurity academy.

This includes 'horizontal career mobility'; as an example, NS recently hired a machinist who wanted to become a hacker and work in cybersecurity. Such people are not only trained at NS itself, but they also bring in their own unique experiences and insights from the perspective of the train's cockpit; such OT insights can be very valuable in increasing cybersecurity. In the article on security service providers, included in this report, we take a deep dive into the role of external parties and their specialists, and how they can contribute to the upskilling of your workforce.

At the same time, NS is aware that it's fighting an uneven battle - a battle it cannot win. What NS can do is adopt an infinite game mindset, embrace continuous learning, and focus on the matters it can influence. Cybersecurity will always, up to a certain level, remain a reactive activity; knowing this, fast detection and quick response are key. Should things go seriously wrong, NS has playbooks in place to mitigate the results as much as possible. In this report, we devote an article to an essential part of cybersecurity: Business Continuity Management.

The cyber threat for legacy platforms

Large organizations such as NS often – in part – run on old legacy platforms; offline platforms that are end-of-life and that are no longer updated. Still, such platforms have a function within complex organizations such as NS, with all its (local) assets, real estate, and infrastructures. And even though legacy is often air gapped and unconnected, it isn't completely invulnerable, and it's not beyond the realms of possibility for legacy platforms to become infected and become a source of infection for the rest of the organization. Such installations, then, should not be forgotten in cyber strategies. If they're needed, they should be able to run unimpeded – unthreatened, and unthreatening.

AI

At the other end of the spectrum is Artificial Intelligence (AI). At NS, too, Generative AI has worthwhile use cases. Chatbots could be interesting tools in travel information or contract information, they could be trained with operation manuals for trains – there are lots of possibilities. Already, NS is deploying AI to rationalize train wagon logistics, for instance at hubs or at servicing stations. NS operates thousands of wagons; AI, then, offers many opportunities for better efficiency. At the same time, NS refrains from storing AI-related data at an external party. For more insights in the interrelations between AI, privacy, and security, we recommend the article on AI that you'll find in this report.

The fact that even a traditional nuts 'n' bolts company such as NS considers cybersecurity to be a main priority, is indicative of the unprecedented rate of developments in the security field. This is true both for the evolving threat landscape, and for our ability to withstand these threats and anticipate them.

We hope you'll enjoy reading this edition of Trends in Cybersecurity.



Serge Dujardin

Vice President - Global Head Cyber GTM, Capgemini Nederland B.V.



Dimitri van Zantvliet

Director cybersecurity / CISO, NS

01

Trends in
Cybersecurity
2024

ORGANIZATIONAL ASPECTS OF SAFETY





UNLEASHING THE POWER OF THE CLOUD: ENSURING SECURITY AND COMPLIANCE

How can organizations harness the full potential of cloud while ensuring security and compliance?

Highlights

- Cloud boosts scalability, innovation, and efficiency.
 - Cloud computing presents challenges despite its benefits.
 - In a shared responsibility model, it can be complex to address the individual roles.
 - Organizations need to take astute measures to mitigate potential risks.
 - GRC tools support security and compliance but may have limitations.
-

Cloud computing overview

The digital age has revolutionized the business landscape. Cloud technology continues to play a pivotal role, offering significant opportunities for businesses to scale, innovate, and improve efficiency.

However, cloud computing brings numerous challenges to organizations regarding cybersecurity, regulatory compliance, and data privacy. This article explores these challenges and provides insights on effectively addressing the challenges.

One of the key benefits of cloud computing is cost efficiency, as it eliminates the need for expensive servers and infrastructure. Dropbox's hybrid cloud model is an excellent example of how organizations can reduce costs while maintaining data security. Cloud services also offer scalability and flexibility, enabling organizations to adjust their IT resources based on demand. Netflix's¹ utilization of Amazon Web Services showcases the ability to handle fluctuating user demands effectively. Cloud technology facilitates mobility and collaboration efficiency, enabling remote work and real-time collaboration. Google Workspace² exemplifies the transformative power of cloud-based collaboration tools in enhancing productivity and efficiency. Cloud providers offer robust security features for data storage, ensuring data safety. Capital One's³ use of AWS demonstrates how organizations can rely on cloud providers' security measures to protect sensitive information. Additionally, cloud platforms provide reliable and cost-effective disaster recovery solutions. Airbnb's⁴ AWS data backup is a prime example of leveraging the cloud for effective disaster recovery. Cloud computing also contributes to environmental friendliness by reducing energy consumption and carbon footprint, as observed in Microsoft's Azure platform.

Leading cloud service providers cater to diverse business needs across various industries. Amazon Web Services (AWS) commands 32% of the global

market share in 2022⁵, making it the largest cloud platform. It is favored by businesses of all sizes, including prominent companies like Netflix and Airbnb. AWS's extensive offerings and expertise in AI, ML, analytics, and IoT services make it a popular choice for businesses seeking advanced technological capabilities. Microsoft Azure closely follows with a 23% market share⁶, and is particularly dominant in Europe. It finds popularity among Microsoft software users, offering seamless integration and compatibility with Microsoft products. This makes Azure a preferred choice in sectors such as finance, manufacturing, and retail.

Google Cloud Platform (GCP) is a rapidly growing provider with a 10% market share, excelling in machine learning, big data, and analytics. Twitter and PayPal have chosen GCP for its expertise in these areas. When selecting a cloud provider, businesses consider their unique requirements, preferred technologies, specialized services, and reputation for reliability and performance. Security and compliance are crucial aspects of cloud-based systems. Cloud security safeguards data, applications, and infrastructure through features like firewalls, intrusion detection, IAM (Identity and Access Management), and encryption. Compliance ensures adherence to rules and regulations, with non-compliance resulting in fines and reputational damage. For instance, a renowned medical care company faced millions of fines for violating HIPAA regulations. Cloud service providers assist organizations in meeting compliance requirements through specialized tools and dedicated security teams.

In conclusion, the move to the cloud offers substantial benefits for businesses but also presents challenges in terms of security and compliance. By understanding these challenges, leveraging the capabilities of leading cloud service providers, and prioritizing security and compliance, organizations can harness the full potential of the cloud while safeguarding their data and reputation.

ORGANIZATIONAL ASPECTS OF SAFETY

Navigating the Shared Responsibility Model

Cloud providers play a crucial role in ensuring cloud security and compliance. This is paramount as they handle a large amount of sensitive data and operate in a variety of regulatory environments. The shared responsibility model in cloud security and compliance is a fundamental principle that divides security responsibilities between the cloud service provider and the customer.

To put it concisely, the security "of" the cloud (infrastructure, physical and visual platform security) is the responsibility of the cloud provider, while the customer bears the responsibility for security "in" the cloud (data, applications, and access controls). While this statement may seem to clearly indicate the role division between customers and cloud providers, in practice it brings about numerous questions and challenges in terms of security and compliance.

Role distributions not only vary based on the models of cloud solutions

utilized by the customer but also shift the burden of role allocation between the customer and the cloud provider. As visualized by the National Cyber Security Centre (NCSC), considering the operation of an application in an IaaS (Infrastructure as a Service) development model (figure 1), it is possible to say that the responsibility scale tilts towards the customer in terms of being secure and compliant.

Cloud providers routinely attain and maintain certifications for various global and regional regulations, like GDPR, HIPAA, and GxP, proving they comply with these regulations. However, achieving compliance is also a shared responsibility. Providers are responsible for the compliancy of their infrastructure and for providing tools and services that help customers meet their compliancy needs. Customers, on the other hand, are responsible for ensuring that their data and usage of cloud services comply with relevant laws and regulations.

Although the cloud providers take care of many aspects of security,

customers are ultimately responsible for the security of their own operations, including their use of the cloud services. Providers also offer Governance, Risk and Compliance (GRC) tools that assist customers in managing their own security and compliance requirements. Despite the need for cloud customers to ensure the security and compliance of their critical applications, including those with financial processes through GRC tools, these tools may have limitations. Apart from the lack of clarity in roles and responsibilities between customers and providers, limitations may exist such as incomplete automation, insufficient updating of regulations and compliance landscapes and limited integration the existing architecture of the customer.

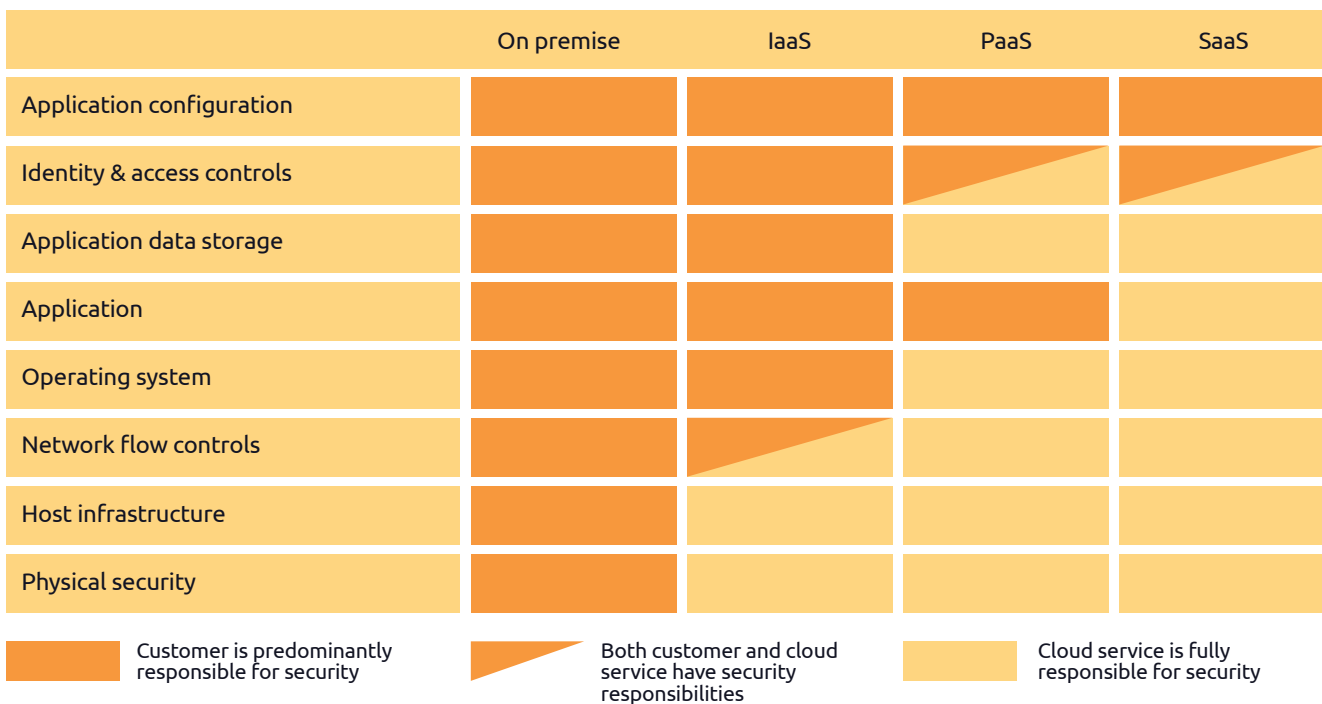


Figure 1: NCSC's Shared Responsibility Model between Providers and Customers⁷

The Cloud Conundrum: addressing the risks and challenges faced by organizations

Organizations face numerous challenges in maintaining cloud security and compliance. This can create complex situations regarding data privacy and protection, adhering to multiple regulations, ensuring visibility and control, effective identity, and access management (IAM), understanding the shared responsibility model, and mitigating insider threats. Clear delineation of roles and clear processes ensures that everyone understands their responsibilities and actively contributes to maintaining security and compliance in the cloud environment.

In addition to role clarity, organizations should utilize robust security tools to proactively identify and address vulnerabilities. These tools help in monitoring and managing security incidents, detecting unauthorized access attempts, and responding promptly to potential threats. Comprehensive staff training programs are crucial for educating employees on best practices in cloud security. This ensures that they possess the knowledge and skills necessary to uphold a secure and compliant cloud environment, working alongside effective tools.

By fostering transparent and timely communication, organizations can address challenges proactively and make informed decisions. To overcome those challenges and ensure a successful cloud migration, organizations should implement a holistic approach that considers people, processes, and technology. Robust encryption and access controls should be implemented to safeguard data during its transfer and storage in the cloud. Clear responsibilities and contracts should be defined to ensure that all parties involved understand their roles and obligations throughout the migration process. This includes outlining the responsibilities of the organization, cloud service provider, and any third-party vendors or partners. By clearly defining these responsibilities, organizations can

avoid misunderstandings and gaps in security and compliance coverage. By implementing strategies such as robust encryption and access controls, conducting thorough risk assessments, complying with industry regulations, establishing clear responsibilities and contracts, and fostering effective communication and collaboration, organizations can overcome these challenges and achieve a successful cloud migration.

Safeguarding your organization: key steps to stay secure and compliant

The rapid adoption of cloud computing has transformed the way organizations operate, offering scalability, flexibility, and cost savings. However, with this shift comes the need to prioritize security and compliance in the cloud environment.

First and foremost, regulatory decision-makers, experienced professionals, and auditors strongly advise cloud customers to understand their roles and responsibilities within the shared responsibility model. It is recommended to follow best practices, update policies and procedures, and operate their control mechanisms in line with effectively designed procedures. Regularly updating these documents to align with evolving threats, technological advancements, and regulatory requirements ensures that the cloud customer's security measures are up to date and effective in mitigating potential vulnerabilities.

Conducting regular and comprehensive assessments to identify potential risks is also emphasized. By understanding the risks, cloud customers can develop targeted strategies and allocate resources effectively to mitigate these risks. Establishing a well-defined incident response plan is valuable for effective security incident management. Regularly reviewing logs, performing continuous security audits, and utilizing advanced threat detection mechanisms helps to identify vulnerabilities and potential breaches.

Staying up-to-date with relevant regulations and industry standards

is essential for compliance with regulations and standards. Engaging with experienced professionals can provide valuable insights, identify blind spots, and ensure organizations are following industry best practices. In this context, regular training is essential to keep individuals updated and focused on the security and compliance practices. It is advised that cloud customers provide support to employees' professional development, such as facilitating knowledge sharing by keeping up with the best practices through classes, hubs, or platforms. This empowers employees to stay current in the ever-changing landscape of cloud security.

By adhering to these recommendations, cloud customers can significantly enhance their security posture and reduce the likelihood of significant deficiencies in security breaches or compliance violations. Comprehensive GRC tools help cloud customers maintain these basics. These tools can provide centralized management, facilitate risk identification and assessment, support compliance management, streamline policy and control management, aid in incident response and management, enable auditing and reporting, and facilitate continuous monitoring and assessment. By leveraging these tools, organizations can enhance their cloud security posture, maintain regulatory compliance, and effectively mitigate potential risks. However, organizations need to be aware of the capacities and limitations of these tools to ensure full security and compliance.

ORGANIZATIONAL ASPECTS OF SAFETY



In conclusion, security and compliance are vital aspects of cloud computing. The shared responsibility model outlines the roles of cloud service providers and customers, but challenges arise in understanding and implementing it effectively. Cloud customers encounter a range of difficulties when it comes to maintaining cloud security and compliance, creating a complex situation to navigate. To stay secure and compliant, organizations are advised to conduct risk assessments, implement strong access environments in line with the best practices, stay updated on regulations, and provide support to their teams to achieve a secure and compliant implementation of cloud services. GRC tools offer centralized visibility and automation, streamlining governance processes. However, they have limitations and should always be supplemented with human expertise and proactive security measures. By prioritizing security and compliance in the cloud and taking appropriate steps, cloud customers can mitigate risks, protect data, and leverage the benefits of cloud computing while ensuring regulatory adherence.

About the authors:

Yagmur Bozcuk



Yagmur is working as a Senior Consultant in the field of cybersecurity. She has a strong background in IT and Business Processes Audit of multiple sectors and various audit methodologies and frameworks, as well as in IT & cybersecurity and Compliance.

Mail: yagmur.bozcuk@capgemini.com

LinkedIn: <https://www.linkedin.com/in/yagmurbozcuk/>

Rahul Mishra



Rahul is a highly experienced Managing Consultant with a decade of expertise in leading consulting positions focused on cybersecurity Audit, Risk, and Compliance Management. He possesses a strong track record of designing and implementing business-driven security models, establishing Security Operations Centers (SOC), and Computer Emergency Response Teams (CERT) to meet audit standards across diverse industries, including banking, telecom, government, and pharmaceuticals. Rahul holds certifications as an ISO 27001 Lead Auditor, Qualys Vulnerability Assessment Expert, and various other cybersecurity product certifications.

Mail: rahul.f.mishra@capgemini.com

LinkedIn: <https://www.linkedin.com/in/rahul-mishra-64990052/>

Sources:

1. <https://www.lucidchart.com/blog/hybrid-cloud-benefits>
2. <https://website.xebia.com/eu/digital-transformation/cloud/cloud-first-workplace/google-workspace?hsLang=en-us>
3. <https://dl.acm.org/doi/fullHtml/10.1145/3546068>
4. <https://www.linkedin.com/pulse/why-airbnb-using-aws-cloud-services-what-benefits-provides-saxena>
5. <https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/>
6. <https://www.edx.org/school/googlecloud>
7. <https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/cloud-security-shared-responsibility-model>

CYBER RESILIENCE AND SECURITY BASELINES

Do baselines such as BIO ensure cyber resilience?

The BIO (governmental Baseline Information Security) aims to improve the level of information security of the government and its services to a certain minimum level. BIO is based on the ISO 27002 management guidelines, supplemented with government-specific detail measures and a number of measures adopted from the VIR-BI (Guideline Information Security Civil Service), level Dep. V (departmental confidential). Baselines are mostly compliance-based; this does not guarantee factual resilience.

Cyber resilience encompasses preparing for cyberattacks, while staying operational during such attacks. The National Institute of Standards and Technology (NIST) provides the following definition:

CYBER RESILIENCE = The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

Cybersecurity Resilience should be expressed as the amount of disruption your organization can avoid in its regular operations when a cybersecurity event occurs. Cybersecurity resilience is reinforced by protective security controls and reactive security controls¹.

In this definition, cyber resilience focuses on the following aspects:

- **Anticipate:** Anticipate upon what's coming your way. This translates into a threat assessment that indicates which actors are targeting the organization, which systems or information these actors are targeting and how relevant the actual threat is. Being aware of your vulnerabilities, and being able to mitigate them, starts with the implementation of basic processes and basic measures.
- **Withstand:** The ability of the organization to prevent and adequately withstand attacks. This aspect mostly focuses on preventive measures such as firewalls, breach detection, anti-virus, access management and encryption of vital information.
- **Recover from:** This focuses on the ability to recover and resume normal services, in case of a severe disruption. This aspect focuses on the security incident response, business continuity, disaster recovery and the management of the crisis that has ensued.
- **Adapt to adverse conditions:** This focuses on the measures taken to deal with attacks and compromised systems, such as the ability to detect attacks and identify system breaches.

Highlights

- There's a clear, unequivocal definition for cyber resilience.
 - Adhering to BIO alone is not enough to attain cyber resilience.
 - A Security Operating Model (SOM) can contribute to the structuring of an organization's security capabilities.
 - There are clearly defined security capabilities that as yet have not been incorporated in the BIO.
 - Cyber resilience could be improved if the approach is threat-based instead of compliance-based.
-



The question is whether the BIO alone provides enough context to adequately give shape of these security considerations. True, BIO incorporates all the management measures, but is this enough to safeguard the business goals of the organization? The ability to structure security capabilities is crucial; SOM (Security Operating Model) makes this possible, by describing the required security capabilities and governance. As such, it complements BIO; BIO describes security goals and measures but does not describe the security capabilities themselves.

The SOM framework helps you to structure and organize the security measures and processes of organization. It's a structured approach towards the design, implementation, and management of an organization's security function.



Security Operating Model (SOM) safeguards cohesion

Cohesion is a by-design feature of the SOM. The approach of SOM is two-pronged: 1. securing existing (legacy) systems and 2. (innovative) security and securing new information systems. The SOM has four domains, as displayed in figure 1.

- Strategy and governance
- Secure and transform
- Dynamic defense
- Innovation and security



Figure 1: Standard Security Operating Model (SOM).

Strategy and governance

This domain encompasses governing security capabilities such as:

- **Risk management and compliance management**, for risk management (risk identification, risk analysis, risk monitoring and reports) and the demonstrable adherence to compliance demands.
- **Enterprise security architecture** for the integrated design and implementation of all security capabilities.
- **Security awareness**, of all coworkers in the organization, so that they know what to do when under threat of a cyberattack.
- **Policies, standards, and guidelines** that address the guiding principles for security, translating them into policies for specific security areas (such as Incident and Vulnerability Management and Identity and Access Management (IAM). Standards and guidelines for implementation provide support.

Secure and transform

- These security capabilities are required to secure existing information systems and/or professional assets such as IAM, Vulnerability management, Antivirus, Cryptography or Network security.

Dynamic defense

- These security capabilities are used to detect (attempted) attacks (breach detection), monitoring such attempts (security monitoring, threat modelling) and to provide at-scale incident response, crisis management and business continuity management in case of security incidents.
- These capabilities support both the secure & transform and the innovation & security SOM capabilities.

Innovation and security

- These security capabilities provide quick support for new services, for instance cryptography to encrypt

data throughout the organization, federative IAM for improved collaboration throughout the value chain, or cloud security to safely embed new services in a cloud environment.

- Apart from these capabilities, DevSecOps is another important capability to safeguard security in Agile development processes.

Figure 2 shows an example of how an organization’s SOM could be structured.

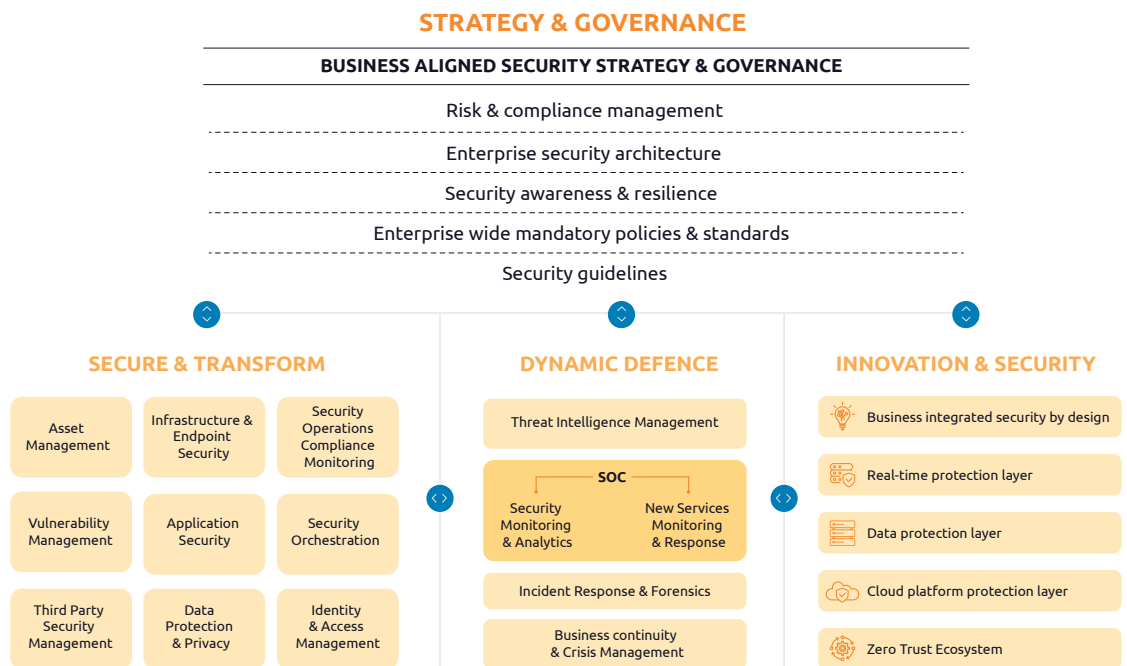


Figure 2: Example of SOM

A SOM for Cyber Resilience

Table 1 lists the required security capabilities for cyber resilience, based on the NIST definition.

Cyber resilience requires an integrated approach towards the development and implementation of security capabilities. This approach is a security program managed through Enterprise Security Architecture (ESA). This ESA safeguards insight into, overview of and integration between all security capabilities.

Presented as a SOM, this would look as figure 3.

ASPECT	SECURITY CAPABILITY
Anticipate	<ul style="list-style-type: none"> Threat modelling and threat assessment. Risk management. Security standards. Training and drills. Classification of information. Security policy, planning and procedures for threat management, Security incident management, IAM, Network security, Security Monitoring, Business continuity, Encryption, System scanning and operation procedures.
Withstand	<ul style="list-style-type: none"> Network security. Breach detection and breach prevention. Antivirus. Encryption. Vulnerability management and patch management. Safe development of hardware and software.
Recover from	<ul style="list-style-type: none"> Security incident management, crisis management. Business continuity and disaster recovery. Change management (known to manage changes in a secure way). Backup and restore.
Adapt to adverse conditions	<ul style="list-style-type: none"> Security monitoring. Threat hunting.
Overview and insights	<ul style="list-style-type: none"> Enterprise Security Architecture (ESA). Internal reporting and compliance. Asset & configuration management (know what you have).

Table 1: Cyber resilience security capabilities.

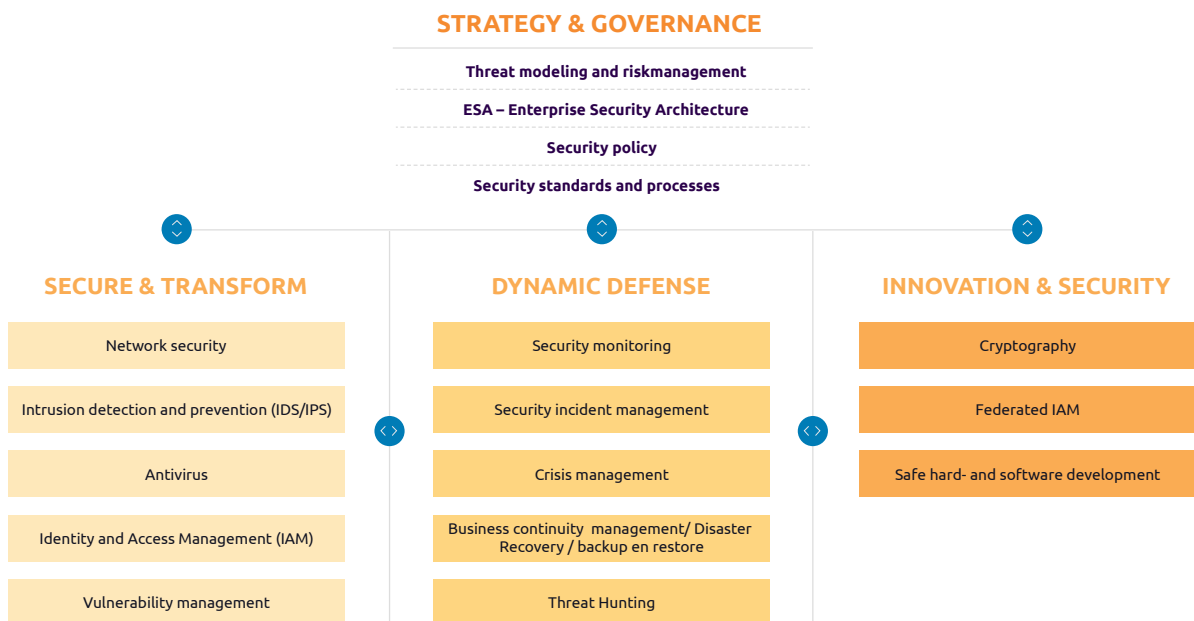


Figure 3: Cyber resilience security capabilities

The SOM and the BIO

The BIO describes security goals and measures; it does not describe security capabilities. Based on the BIO, we can derive a SOM as depicted in figure 4. The numbering of the building blocks corresponds with the chapter structure of the BIO.

This BIO-based SOM is very similar to the Cyber Resilience SOM. However, a number of required security capabilities are missing:

- **Threat modelling:** required to produce a threat assessment. The threat assessment contains an overview of the types of actors (state actors, organized crime, hacktivism, script kiddies, insiders, researchers), preferably identified with the actual names of the actor groups. On top of that, the assessment contains the information systems (IT) and operational assets (OT) they're targeting, their motivation, means and drive. Based on this information, the threat assessment can be used to monitor the Tactics, Techniques and Procedures (TTP) of these actors.

- **Enterprise Security architecture (ESA):** for the required insight, overview, and coherence. The ESA describes the coherence of the security capabilities and the way they are inter-related. Plus, it provides a roadmap for the implementation of the security capabilities. As such, ESA is an instrument for the management of change
- **Threat Hunting (TH):** pro-active searching for compromised areas in IT and OT environment. Threat hunting is based on hypothesized infections of information systems or operational assets, caused by specific threat actor groups; in other words, TH assumes that they are 'already inside'. Based on these hypotheses, the threat hunters investigate potentially compromised areas.

The BIO requires monitoring, but true cyber resilience requires more security monitoring in order to adequately monitor cyber actors and their behaviors (TTP – Tactics, Techniques, Procedures). These actors and their TTP scan be derived from the actual risk assessment. BIO compliance alone is not enough to attain cyber resilience. To become cyber resilient, you should adopt the security capabilities described in the Cyber Resilience SOM.

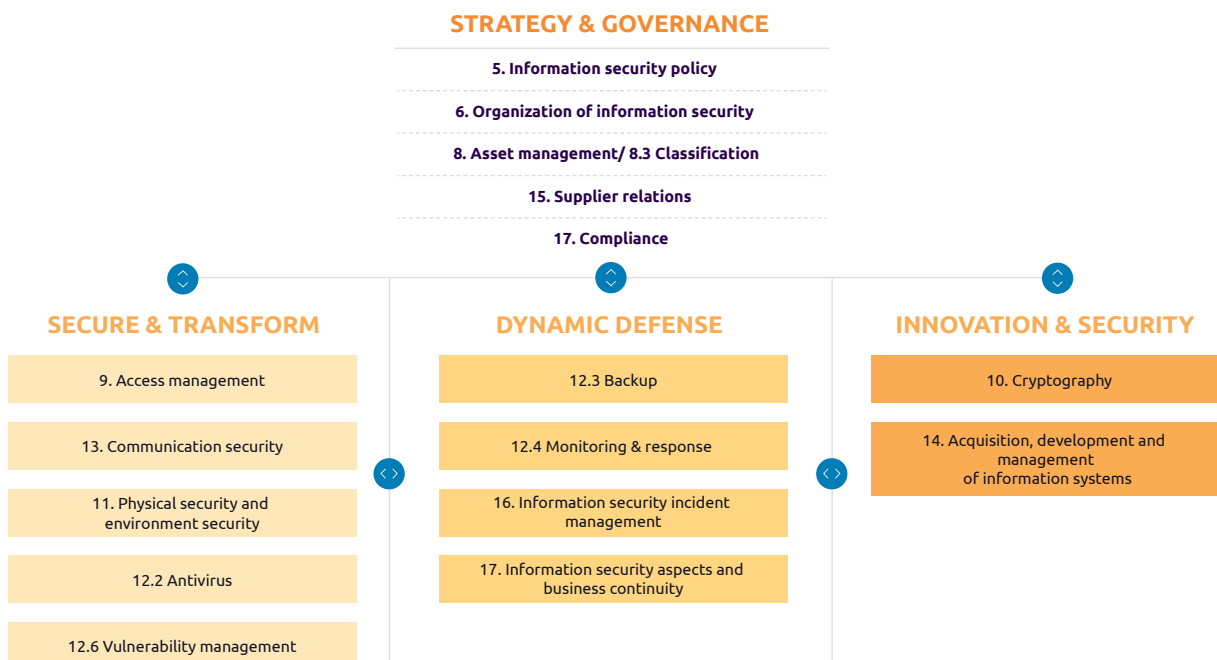


Figure 4: BIO-based SOM

ORGANIZATIONAL ASPECTS OF SAFETY

Our recommendation: You should give priority to the drawing up of the threat assessment and the design of a security architecture. This will allow you to adopt a security capability-based approach towards cyber resilience. Plus, you should assume you've already been compromised, and adopt Threat Hunting to confirm this.

Sources:

1. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf>

About the author:

Renato Kuiper



Renato Kuiper has more than 25 years of experience in security architecture, cloud security, risk management and IAM. Renato was a guest tutor at the executive master Cyber Security at the CSA (Cyber Security Academy). He is a board member of the CSA (Cloud Security Alliance Netherlands) and regularly speaks and publishes about topics in the Security field.

LinkedIn: <https://www.linkedin.com/in/renato-kuiper-3246733/>

Jule Hintzbergen



Jule is an expert in cybersecurity, focusing on strategy, governance, and implementation. Working as a trainer at Capgemini Academy allows him to share his knowledge. Jule is passionate about identity and border management.

Mail: jule.hintzbergen@capgemini.com

LinkedIn: <https://www.linkedin.com/in/jule-hintzbergen-17b486/>



THE INDISPENSABLE ROLE OF THE BOARD IN THIRD PARTY RISK MANAGEMENT

How can organizations more effectively organize their risk management, and make sure that the board of the organization gives priority to Third Party Risk Management (TPRM)?

ORGANIZATIONAL ASPECTS
OF SAFETY



Organizations are increasingly taking steps to improve their cyber resilience. But how to make sure that you don't lose sight of the risks? A very large part of cyber risks can be attributed to third parties that organizations rely on. For instance, the Dutch Data Protection Authority (National Privacy Authority) saw an increase of 88% in 2021 in data leaks, of which the majority originated at third parties, especially IT suppliers¹. Organizations increasingly outsource many of their supporting services. As a result, data regarding customers and personnel are increasingly handled by third parties. Take, for instance, the recent data leak at software supplier Nebu – a supplier that provides its services to many different organizations. This data leak impacted at least 2 million people, underlining the importance of securing the whole digital chain². Next to personal data, third parties also process internal information that can be regarded as critical to the organization. Moreover, third parties often have access to systems that govern collaborative schemes.

It's not surprising, then, that managing the risks involved with usage of third parties - Third Party Risk Management (TPRM) - is an important trend within the cybersecurity domain, and a significant factor in the overall level of risk resilience of an organization. Due to the relative novelty of the concept, many organizations as yet aren't aware of it. The success of any TPRM program depends on the board's acknowledgement of the importance of TPRM. This article discusses pathways towards the successful implementation of a TPRM program. It also addresses the role of the board, being the organizational body that's responsible for the day-to-day governance of the organization and its strategic and tactical direction.

Defining the roles and responsibilities

Clearly determined and communicated roles and responsibilities are part and parcel of any successful TPRM program.

Without clearly defined ownership, the TPRM program will remain ad-hoc, directionless and insufficiently embedded in existing business processes. An organization's board has an important part to play in this: to assign the ownership of TPRM and to communicate its importance to key stakeholders.

Through clearly defined roles and responsibilities, everyone involved with the TPRM program can be made responsible for their actions. As a result, risks can be adequately identified, assessed, and managed.

Once the most important stakeholders have been identified – such as the security and privacy department, senior management, procurement, and other process owners – it is important to define and communicate their responsibilities with regard to TPRM.

As said, an important characteristic of any successful TPRM program is the board's involvement in determining the roles and responsibilities. The board endorses the TPRM and its importance to the organization and is better positioned to monitor the execution of the program. It's the executives' task and responsibility to stay informed about the risks to be mitigated by TPRM, which could impair the continuity of the organization. Based on this information, it is possible to make the right decisions, in order to prevent major incidents such as data leaks or ransomware.

Highlights

- Involve the board in establishing roles and responsibilities.
 - Provide the board with insight into the risk landscape.
 - Inform the board of new insights.
 - As board members, make sure you're asking the right questions.
 - Create cyber awareness at board level.
-

Understanding the risk landscape

Insight into the risk landscape is essential for any organization. As executive officer, you will be held personally responsible when critical cybersecurity or privacy risks are ignored. Risks involving third parties are a major factor in the risk profile of every organization. For instance, many third parties have access to organization and privacy sensitive information and exchange such information with other organizations. It's of vital importance – and a prerequisite for any successful TPRM program - to always keep tabs on data that is managed by third parties. This insight will help you to effectively manage and mitigate risks, preventing them from adversely influencing the organization's activities or reputation. Gaining – and retaining – insight into the data that are managed by third parties is, in most cases, a joint effort of business stakeholders and the IT, privacy, security and risk departments.

Understanding the risk landscape starts with the identification of the third parties, and assessing the negative impact they might have on cybersecurity and privacy. This should be part of the due diligence that should be done before the execution of any agreement between an organization and a third party. On top of that, this due diligence should be repeated regularly with existing relations; the risk landscape evolves, and so must the third party.

In case of third parties that have a significant impact on privacy and cybersecurity, a risk analysis needs to be conducted in agreement with the primary stakeholders. Based on the risks encountered, a risk mitigation plan can be drawn up that focuses on gaining the best results with the smallest effort.

Understanding the risk landscape is one thing, but staying informed about new developments is yet another challenge.

Staying updated about new insights

The risk landscape evolves constantly. Every day, new risks emerge in the shape of zero-day vulnerabilities, viruses, and ransomware. It's the board's responsibility to always have a high-level understanding of the most important developments in the risk landscape. This allows them to ask pertinent questions to security and privacy experts who are tasked with drawing up defenses against these risks.

Recent research by Adaptive Shield points out that, in organizations with 10,000 SaaS-users (Microsoft 365 and Google Workspace), whole ecosystems of third-party apps have emerged; apps that have connected to the SaaS (Software as a Service) solutions. On average, the amount of additional connected apps in such organizations runs to 4,371³. All these connected apps have some kind of authorization regarding corporate data, and in some cases these apps are even authorized to delete all the data from the apps they're connected to. In many cases, these risks are unknown, or not completely in scope.

Moreover, third parties such as suppliers or value chain partners may, in time, change their services. Due to this, the risks such services pose may also change. By periodically mapping these risks, organizations are better positioned to manage them.

TPRM is a continuous process; the context it operates in changes constantly and, as a result, so do the risks. Using an automated platform that continuously scans the attack surface of third parties, combined with structural auditing, holds the key towards successful monitoring of risks incurred by third parties.

Asking the right questions

Many organizations are in the early stages of their TPRM programs⁴. As part of an organization-wide dialogue about TPRM, the board should request the management team to shed light on the different elements of the organization's

TPRM program – and which elements might still be missing. By asking – among others – the following questions, board members may gain insight into the status and the potential challenges of the TPRM program currently underway within the organization:

- Have roles and responsibilities been effectively defined in the organization's TPRM program?
- Does the organization also include fourth, fifth and sixth parties in the TPRM program?
- Which information related to third party-incurred risks is provided to the board by the program's management?
- At which levels and with what frequency and relevance is the information presented?
- Are internal auditors and risk management involved in the assessment of the TPRM program? And if so, in what way?
- What tools does the organization use to measure and manage TPRM, and are they effective? What does the escalation ladder look like, in case of risks incurred by third parties? And how effective are mitigation measures?
- What investments should the organization consider to improve the TPRM program and integrate it throughout the organization?

Creating awareness

Combined, all the aspects described above increase boardroom-level knowledge about TPRM. But to really understand the importance of their ongoing support for TPRM program, the board members should be made aware of privacy and security in a broader sense.

To grow this awareness, board members should be given insight into the specific risks for the organization incurred by critical third parties, and the impact such risks can have on the organization. These aspects are usually included in general awareness efforts regarding data protection. The focus on TPRM risks could easily be added to existing activities.

Additionally, storytelling can be a useful tool in helping the board understand the TPRM challenges in a broader context. Board members read the news, talk with peers and are usually aware of large-scale cybersecurity incidents involving third parties. For example, incidents in the supply chain domain are often talked about. It may be useful to be familiar with stories about these incidents, and especially to compare these stories with the situation within the own organization. At a boardroom level, recognition is an important factor: how could incidents potentially take place at your organization – or why couldn't they?

Finally, some organizations involve their board members in internal awareness training. A potent example is the involvement of the board in incident response training, together with critical suppliers. By simulating a cyber incident such as a ransomware virus outbreak, together with critical suppliers and the board, awareness can be created about the impact of an incident on the

organization. Based on simulations like these, the organization can check whether the necessary measures are in place to safeguard business continuity.

Can organizations more effectively organize their risk management by adopting TPRM? This depends on several factors. It all starts with established ownership of TPRM. Through ownership the organization can chart a clear trajectory and effectively embed the program in existing business processes. The board of the organization has a crucial role in establishing the responsibilities of the stakeholders within the organization.

On top of that, it is crucial for the board to gain insight into the organization's risk landscape. Based on this insight, mitigation measures can be drawn up to avoid or minimize the risks. As such, it is important to regard TPRM as a continuous process. Risks evolve constantly. For this reason, it may be a good idea to consider an automated platform that lessens the pressure on the organization.

By actively asking questions about the organization's TPRM program, board members gain insight into the status and the possible challenges faced by their organization's TPRM program. These questions should address the roles and responsibilities, the scope of the TPRM program, reporting, involved actors, tooling that could be used and questions about further investments that could improve the program.

Sources:

1. <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-datalekken>
2. <https://nos.nl/artikel/2469510-datalek-nederlandse-bedrijven-steeds-groter-zeker-2-miljoen-klanten-getroffen>
3. <https://www.adaptive-shield.com/saas-to-saas-3rd-party-app-risk-report-2023>
4. <https://www.gartner.com/en/newsroom/press-releases/2023-02-21-gartner-survey-shows-third-party-risk-management-misses-are-hurting-organizations>

ORGANIZATIONAL ASPECTS OF SAFETY

About the authors:

Britt Huveneers



Britt helps public and private organizations to secure compliance with safety regulations. Her expertise predominantly lies in the field of (sensitive) data, the use of new technologies and data ethics.

LinkedIn: <https://www.linkedin.com/in/britt-huveneers-b8b186114/>

Christiaan Koopman



As Managing Consultant at Capgemini, Christiaan provides advice about the way cybersecurity can be safeguarded within existing and new business processes. His expertise lies in the implementation of cybersecurity strategies, IT risk management and governance and compliance in the context of regulatory standards such as ISO 27001, BIO & ISAE 3402.

Mail: christiaan.koopman@capgemini.com

LinkedIn: <https://www.linkedin.com/in/christiaan-koopman/>

Manisha Ramsaran



Manisha's expertise lies in the implementation of privacy by design principles, providing advice about privacy risks in the context of new processes and technologies and raising awareness about data protection.

LinkedIn: <https://www.linkedin.com/in/manisha-ramsaran-91aa1b140/>



**WHY BUSINESS
CONTINUITY IS CRUCIAL
IN TIMES OF
SOCIAL UNREST**

How can business continuity management help us deal with effects of social unrest?

Highlights

- Organizations often focus on reacting to crises or solving incidents, causing them to lose sight of the importance of business continuity.
 - Organizations often regard crisis management, incident response and business continuity as disconnected activity areas, even though these three domains need to be regarded as a whole in order to promote resilience.
 - Disruptive events in society can have a disruptive impact on business continuity. This is often overlooked in business strategy.
 - The migration of organizational infrastructures to the cloud is essential.
 - By regularly testing business continuity strategies, organizations can identify weak points.
-



Since COVID-19, countries are more frequently faced with social unrest. This unrest is often driven by protests about economic hardship, climate concerns, police violence and so on. Such issues cause unrest within society, disrupting the normal course of things. The actions against pension reforms in France, for instance, resulted in road or railway blockages; actions at refineries caused gasoline shortages. For each country, it is instrumental to react effectively to such actions to make sure that 'business as usual' can resume as quickly as possible. The same principle applies to the digital world. In this article, we consider the connection between social unrest and business continuity. As such, we offer insights to organizations that can help them improve their resilience. Political and social unrest can bring about risks and threats to organizations, such as hacking of a country's or city's critical systems. This also means that a society's cyber resilience is an important factor to keep in mind in safeguarding business continuity.

What is business continuity?

To exemplify the importance of business continuity during periods of social unrest, we must first clearly define what exactly we mean by business continuity. Even though there are different definitions within the security domain, we adhere to the following definition: business continuity is the ability of an organization to protect essential functions during a disaster and continue them afterwards. It provides risk management processes and procedures that aim to avoid disruptions in critical services, or deal with them, allowing the organization to resume normal services as quickly and smoothly as possible.

BENEFITS OF CERTIFICATION

Certification helps to increase an organization's resilience, with over a quarter citing it helps to reduce insurance costs

The benefits of certification to organizations

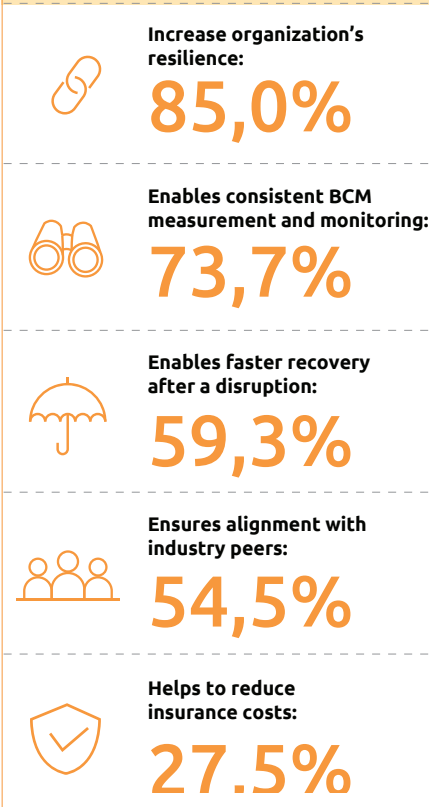


Figure 1: Benefits of certification²

Lack of focus

During demonstrations and protests, society is predominantly focused on its reaction to the unrest. This often overshadows 'business as usual'. As a society, we are trained to react immediately to problems and to devote all our attention and assets in solving those problems. As such, normal life is pushed to the background in times of crisis. In businesses, too, it's all about the organization's ability to react to crises or to solve issues; resilience is defined in terms of the organization's ability to apply the crisis management cycle (response, recovery, mitigation, preparedness). And even though organizations plan for different scenarios, the fact that business as usual is paramount in itself is insufficiently acknowledged – both after a crisis and during a crisis. Still, attention to business as usual is crucial to safeguard business continuity and the organization's health. Certain ISO (International Organization for Standardization) best practices and standards express business continuity. These standards are often overlooked or regarded as being beyond the scope of the business continuity management or crisis management department of an organization. Business continuity activities are essential, because they allow the organization to at least keep on running in 'safe mode' during a crisis, and to quickly react to interruptions. An effective approach towards business continuity saves money and time and helps to protect the reputation of the organization. Prolonged business interruptions, on the other hand, can lead to financial or reputational damage.

Domains and the ways they overlap

In our field, we often encounter organizations that have divided their resilience department into separate elements: incident response, crisis management, business continuity, et cetera. Each element has its own reporting scheme. The elements often fall under the same department, but the way they interact is not always clear.

ORGANIZATIONAL ASPECTS OF SAFETY

By improving this organizational structure, collaboration would be strengthened – and effective collaboration always benefits resilience. In organizations with disconnected disciplines, it can be very hard to effectively deal with actual crises, because incidents are approached from several different perspectives. In case of technical incidents, business continuity often gets very little attention – or none – when dealing with the issue at hand. Awareness of the impact of the issue on the organization is often lacking, and it only becomes clear later what management should do to mitigate or solve the issue. This lack of integration and collaboration often leads to a delayed response by the organization, which in turn causes reputational damage. Better integration between crisis management, business continuity management and incident response can improve the organization’s ability to react to a disruptive event, by decreasing the risk of delays, conflicting priorities, and miscommunication.

Societal instability results in poor business continuity

Recent societal events such as natural disasters, terrorist attacks and pandemics have resulted in greater attention for business continuity. Even though the focus was already shifting during the Covid-19 pandemic, different studies since then have pointed out that geopolitical changes and conflicts between nations have caused organizations to regard such disruptive events through the lens of business continuity. When geopolitical changes occur, organizations focus on the strategic consequences such as changing alliances and dependencies, the impact of foreign aid and economic sanctions, and the commercial repercussions against countries and companies. Hostilities between nations may occur in the shape of war, other armed conflicts, state terrorism, attempts to influence election results and fomenting civil unrest.

Impact on the future of organizations

All such matters may severely impact organizations and their continued existence. For instance, companies could decide to suspend their activities in certain countries, due to civil unrest. Continuing operations may, for instance, no longer be viable because of supply chain issues. The magnitude of such issues may be such that the impacted part of the total operation becomes too large. It’s important to tackle such issues by focusing on the aspects that relate to business continuity. Such aspects should then be integrated into the business continuity plans of the organization. An example of a support tool for organizations is threat intelligence analysis.

THE ISO 223XX SERIES – SOCIETAL SECURITY

DESIGNATION	WHAT IT ADDRESSES
ISO 22300:2012	Societal Security-- Vocabulary
ISO 22301:2012	Business Continuity Management Systems -- Requirements
ISO 22311:2012	Video Surveillance
ISO 22313:2012	Business Continuity Management Systems - Guidance
ISO 22315:2014	Mass Evacuation - Guidelines
ISO 22320:2011	Emergency Management – Requirements for Incident Response
ISO 22322:2015	Emergency Management – Guidelines for Public Warning
ISO 22324:2015	Emergency Management – Guidelines for Color-Coded Alert
ISO 22351:2015	Emergency Management – Message Structure for Interoperability
ISO 22397:2014	Guidelines for Establishing Partnering Arrangements
ISO 22398:2013	Guidelines for Exercises
ISO 22399:2007	Guidelines for Incident Preparedness and Operational Continuity Management

Figure 2: ISO norms regarding business continuity and societal unrest³

Cloud can improve business continuity

An attack on IT-systems that are relevant to society can have a big impact. In 2021, the Irish health care system was hit by ransomware. This severely impacted the continuity of the country's health care system. Patient data was no longer available for health care workers and patients, appointments were cancelled, and re-installing all the servers and applications took four and a half months. Access to critical data, processes and systems is of vital importance for the continuity of health care. Using the cloud for such matters may be helpful; data is stored and accessed online, making it less vulnerable to attacks. This can positively impact business continuity.

Advantages of cloud use

A well considered implementation of cloud-based software within an organization can enhance business continuity with easily accessible back-ups and high-on unlimited scalability. Many organizations still heavily depend on internal networks and data centers, and inefficient or obsolete technology. Because of this, even a local power outage or internet outage may cause unplanned downtime. By using cloud solutions, organizations can significantly reduce downtime. Critical processes and applications will continue to run, without having to fall back on physical alternatives. The cloud offers unlimited, subscription-based opportunities for data storage. As such, business continuity is more easily attainable, because any user can use any internet-enabled device to access the data. The rise of remote working during the Covid-19 pandemic is a recent example of how effective the cloud can be. Thanks to cloud solutions, co-workers of organizations were able to continue their normal activities from home; activities that would normally be performed from the office. Thus, business continuity was protected.

Effective disaster recovery is another advantage of the cloud. Back-ups are continuously and automatically uploaded to the cloud, allowing

organizations to protect critical data from disasters and/or attacks. The cloud can lessen the impact of cyberattacks such as Denial-of-Service (DoS) attacks. A DoS attack aims to overwhelm IT systems and prevent them from handling normal workloads. Cloud services can be scaled to meet certain workload demands; as a result, the impact of DoS attacks is lessened. In other words: business continuity is protected. By making use of multi cloud strategies – the storing of back-ups at several different cloud suppliers – organizations can avoid becoming dependent on one single back-up.

Practicing and training enhances the effectiveness of business continuity strategies

The success of business continuity strategies depends on co-workers' ability to effectively develop, document and – especially – execute them. This implies that co-workers should be well-trained and educated. A workforce that's trained to implement business continuity strategies allows the organization to react effectively to events that would otherwise impact that continuity. Co-workers should also be familiar with communication tools, and make sure to constantly stay aware of new information about possible business continuity issues – information that could for instance be offered by technical personnel. Senior managers involved in the company's response activities should be aware of their responsibilities during an incident and be familiar with the available tools. This will help the organization to validate response strategies and shorten the response time. An example of a drill could be a tabletop exercise that simulates an incident in real time.

Business continuity is crucial during social unrest

During the protests in France, officials focused predominantly on the chaos that was created by certain developments. During periods of social unrest, organizations should be aware that not only the unrest itself should be addressed, but that business as usual also warrants attention. This article has

described business continuity to be an important topic for any organization. Thus, organizations should make sure to have clear strategies and guidelines in place, or to assess existing strategies and guidelines for their attention towards the integration between elements such as crisis management and incident response. By focusing on innovative strategies such as the use of cloud solutions, in combination with practicing and training for incidents that may impact business continuity, organizations can enhance the effectiveness of their business continuity strategy during periods of social unrest.

Social unrest or cyberattacks can't always be avoided. But organizations that invest in effective business continuity management can make sure that business continuity is safeguarded in the face of such events.

ORGANIZATIONAL ASPECTS OF SAFETY

About the authors:

Manouck Schotvanger



Manouck is a cybersecurity consultant at Capgemini Nederland. She specializes in crisis and security management within the cybersecurity domain. Her focus lies with business continuity and crisis management in the public and private sectors.

LinkedIn: <https://www.linkedin.com/in/manouck-schotvanger/>

Rachel Splinters



Rachel is a cybersecurity consultant. She specializes in security management within the cyber domain and focuses on the development of cyber crisis training courses for the public and private sectors.

Mail: rachel.splinters@capgemini.com

LinkedIn: <https://www.linkedin.com/in/rachel-splinters-6825b7137/>

Sources:

1. <https://drive.drii.org/2022/12/08/8th-trends-report/>
2. <https://www.globenewswire.com/news-release/2023/06/14/2688019/0/en/ACT-Achieves-HITRUST-Certification-for-Healthcare-Services.html>
3. <https://www.techtarget.com/searchdisasterrecovery/definition/business-continuity>
4. <https://drive.drii.org/2022/12/08/8th-trends-report/>
5. <https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf>



THE PERFECT MATCH: HOW TO CHOOSE THE PERFECT SECURITY SERVICE PROVIDER FOR YOUR ORGANIZATION

It's easy to define technical requirements. But what do you expect from the service experience?

Highlights

- Every good Managed Security Service Provider (MSSP) focuses on the 'service experience'.
 - When we look at the service experience, we define three categories: people, process, and business.
 - Regarding the processes between you and the MSSP, it's important to choose the right type of governance.
 - The three most common types of governance are: a delivery organization, a directing organization, and a demand organization.
 - The specialists your organization needs are always readily available at the MSSP.
-

Tender processes tend to focus on functional requirements. Unfortunately, the resulting services often fail to meet expectations. Luckily, this is a well-known problem, and the solution is already available.

At the end of the day, we can't ignore the importance of functional requirements. Service providers in most cases are able to fulfill those requirements. If they can't, this usually becomes clear at an early stage. That's why, in this article, we will ignore the functional requirements and concentrate on the non-functional requirements. In other words: the service experience.

The service experience comes in many different guises. First and foremost, it should meet your requirements: corporate culture, level of (in-)formality, interpretation of the contract (i.e. to the letter, or the intent), etc. A service experience that succeeds in establishing an effective and pleasant collaboration between your co-workers and the Managed Security Service Provider (MSSP), will result in the most effective security service.

We can divide the notion of service experience into three primary categories:

1. People
2. Process
3. Business

Security is a people's business

When talking about employment, we can't ignore two factors: the new way of working, and the shortage of technical specialists. There is a worldwide demand for 3.5 million cyber specialists, and standards are shifting towards more flexibility for employees. As a result, the labor market is enormously competitive.

Due to this competitiveness, your organization probably experiences the same skill shortages as the average MSSP. This can be a problem if both organizations are looking for the same profiles. Should the profiles both organizations are looking for

be complementary, this can be an advantage. The MSSP will attract different candidates than your organization.

Broadly speaking, the culture of your organization is defined through the following values:

- **Globalization:** do you have a global or a local organization?
- **Performance:** what is your organization's definition of success, and how does your organization treat success?
- **Demography:** what is the average age and cultural background of your personnel?
- **Hierarchy:** how does your organization deal with hierarchies?

When your values align with those of your MSSP, it becomes easier to establish a productive business relationship. Consequently, this leads to a more efficient operation between the customer and the supplier.

Globalization is the odd one out. Some people don't care about working in an international environment; for others, it's a must. Your MSSP can play an interesting role in this regard. If your MSSP values globalization differently, it may be able to source specialists that would be unreachable to you otherwise.

In the end, the interactions between people are too complex to discuss exhaustively within the bounds of one single article. We can be sure, however, that the personnel selected by the MSSP to perform certain services should have a good relationship with the personnel that benefit from this service. If the chemistry between people isn't there, neither processes nor technique will be able to help you.

Processes define the service, but you make the decisions

Different services have different processes. Washing a car, for instance, is not the same as cloud migration. But when we consider the processes between you and your MSSP, it is especially important to consider

governance. The type of governance you choose, decides the level of influence you have at an operational, tactical, or strategic level.

We identify three primary types of governance: a delivery organization, a directing organization, and a demand organization (figure 1).

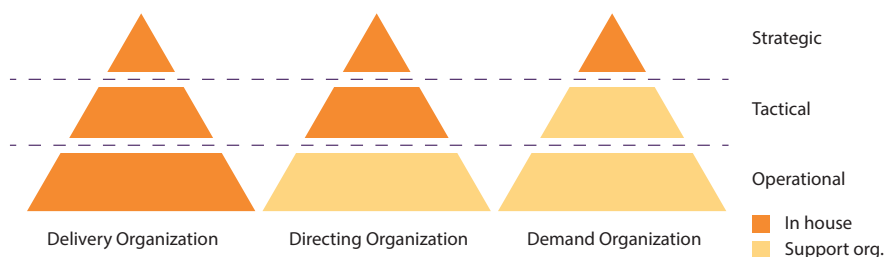


Figure 1: Governance types

In case of a delivery organization, the operational, tactical, and strategic matters are all governed by your own organization. You can outsource operational, tactical, and strategic aspects in the case of a delivery organization, but ultimately, you, so to speak, ‘call the shots.’

When you outsource the operational activities but remain in charge of the tactical and strategic matters, you have what we call a ‘directing organization’. In this situation, the MSSP is involved in the execution of tasks, but everything the MSSP does is done by your request. A service desk is a classic example: no ticket, no service.

Is the MSSP also allowed to make tactical decisions in support of your organization? In that case, you have a ‘demand organization’; you decide on the strategy, but it’s up to the MSSP to give shape to it. A workplace management service is a good example. You indicate that you want a secure workplace for your personnel; your MSSP decides to apply a combination of configuration hardening and antivirus to meet your request.

Of course, you can use different types of governance, for different types of services. In the end, the choice is yours – based on your in-depth knowledge of your organization. Do you have the in-house expertise to make tactical or operational decisions?

Business enablement through security services

To conclude, let’s take a look at the subject of your organization: the business. Just as IT supports the business, security should also be regarded as an enabler. Examples are rules and regulations, but also the context of your company and your ambitions for growth.

Rules and regulations are clearly linked to the MSSP and are matters that you should comply with. An MSSP can assist you in this; many parties will already have experience with this, simply because these rules and regulations also apply to other organizations.

However, when we look at the context of your company and its ambition for growth, a unique outlook emerges. No two organizations are ever the same. It’s important, then, to find an MSSP that understands you and that acts in your best interests.

Your ambition for growth is a good example. MSSPs often offer ‘optional’ services. You are only charged for such services if you actually make use of them. This may provide flexibility and transparency, but it can turn out to be disadvantageous if you plan to make extensive use of such services. Take, for instance, personnel screening: an MSSP could charge a fixed fee per screening. However, if you have the ambition to significantly expand your workforce in the coming years, such a scheme may prove expensive. In such cases, it could be better to opt for a structure that flexibly adapts to your growth.

This brings us to the context of your company. Your organization has a primary reason for being, and it isn’t securing your IT; the latter, in itself, does not make for a viable business. However, if your MSSP has a firm grasp of what your reason for being is, it can provide better support. Let’s take another look at the example of a growing workforce and the screening service: does your primary task benefit from having a large workforce, or does your company have a seasonal demand for personnel?

ORGANIZATIONAL ASPECTS OF SAFETY

In the last case, the MSSP should understand that your company deals with activity peaks, and that every task should always be fulfilled – especially in peak season.

Three important considerations

In order to select the best MSSP for your organization, you need to consider a number of things. But first, you need to clearly define what exactly your own wishes are. Do you require a tactical, a strategic or an operational focus from your MSSP? Whichever you choose, each focus will have to be considered in the light of the three main factors: People, Process and Business (Figure 2).

At the end of the day, all options may be valuable. It is our advice, therefore, to consider the following questions:

- What is my vision on collaboration between my people?
- How do I want to interact with my MSSP?
- How do I want to direct my MSSP?

About the authors:

Arjen van der Post



Arjen is a senior delivery manager with extensive experience in transitions and transformations, and supplying new services to a wide range of customers within Capgemini's infrastructure and cybersecurity unit.

Mail: arjen.vander.post@capgemini.com

LinkedIn: <https://www.linkedin.com/in/arjen-van-der-post-75627714/>

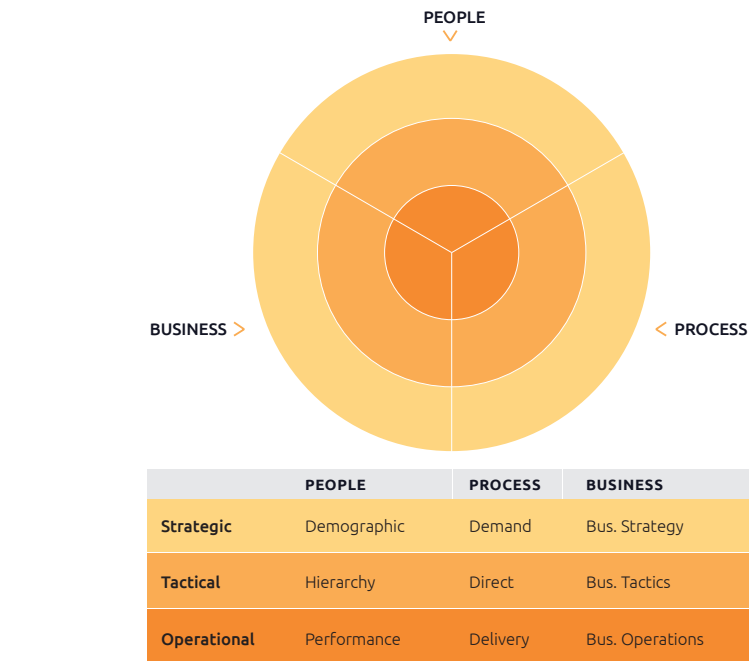


Figure 2: MSSP selection considerations

Sources:

1. <https://fortune.com/education/articles/the-3-cybersecurity-hiring-trends-experts-predict-for-2023/>
2. <https://www.dbxuk.com/statistics/cyber-security-risks-wfh>

Dick Bruines



Dick has more than twenty years of experience in service management. In delivering IT and security services to his customers, he always strikes a balance between contractual agreements and what customers really need. Dick has worked in both small teams and large teams, and always focuses on the customer's success, through successful partnerships.

Mail: dick.bruines@capgemini.com

LinkedIn: <https://www.linkedin.com/in/dick-bruines-a1619a2/>

Sebastian de Vries



Sebastian de Vries is an experienced security expert. Next to his technical expertise, he is always fully up to speed with the latest compliance standards. His aim is to help customers transform security from a necessity into an advantage.

LinkedIn: <https://www.linkedin.com/in/gsdevries/>



NAVIGATING NIS2: ORGANIZATIONAL CHALLENGES AND SOLUTIONS

What are the top three NIS2 implementation challenges for organizations?

ORGANIZATIONAL ASPECTS OF SAFETY

On 16 January 2023, the Network and Information Security Directive 2 (NIS2 Directive) entered into force, replacing its 2016 predecessor NIS1. NIS2 requires essential and important entities to take steps to adequately manage cybersecurity risks and incidents. NIS2 should contribute to greater European harmonization and a higher level of cybersecurity in organizations. Member States are obliged to incorporate this directive in their national laws and regulations and Member States must comply with NIS2 from 18 October 2024 onwards.

With an increasing amount of cybersecurity attacks across the world and fast-growing reliance on (digital) infrastructure, NIS2 appears to replace NIS1 at the right time. NIS2 brings some welcome changes as it incorporates stricter, more explicit requirements for cybersecurity that provide opportunities for security enablement and risk reduction in organizations.

Highlights

- NIS2 impacts a larger part of the economy and society.
- NIS2 incorporates stricter and more explicit requirements for cybersecurity.
- NIS2 increases requirements for supervision and non-compliance.
- Top three NIS2 implementation challenges are (1) scoping (2) SCRM and (3) Duty of Notification in relation to Security Incident Management.
- Every challenge presented by NIS2 creates opportunities for enhancing security and reducing risks in vital and critical industries and organizations.

Nevertheless, complying with NIS2 also entails costs and will inevitably confront organizations with implementation challenges.

NIS2 and the change for the cybersecurity landscape

As introduced earlier, NIS2 came into effect this year, bringing significant changes compared to its predecessor, NIS1. So, how does NIS2 change the cybersecurity landscape and what exactly does this mean for organizations? Below, the key changes will be discussed.

1. Extended scope

Under NIS2, active identification of entities in scope is no longer performed by sector specific national competent authorities (e.g., Dutch National Bank). Instead, all enterprises that are medium or large sized and operate in the (sub)sectors and types of services as portrayed below will fall in the scope of NIS2. NIS2 will also apply to some entities regardless of size if provided certain conditions are met². As such, NIS2 includes all the sectors under NIS1 but supplements these with new sectors. As a result, NIS2 clearly covers a larger part of the economy and society than its predecessor NIS1, as illustrated below in figure 1:

NIS2 also removes the distinction between Operator of Essential Service (OES) and Digital Service Provider (DSP) and introduces 'essential' and 'important' entities which are differentiated based on the criticality of the associated sector³.

Finally, NIS2 will not only apply to important or essential entities established in the Member States but will also apply to important or essential entities that offer services to the respective Member State.⁴ As such, the NIS2 Directive will be a Directive with an extraterritorial impact like the General Data Protection Regulation (GDPR).

2. Explicit and stricter cybersecurity requirements

NIS1 stated that OES and DSP had to take appropriate and proportionate technical and organizational security measures to manage the risks posed to the security of network and information systems used in their operations. It also noted that OES must take appropriate measures to prevent and minimize the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, aimed to ensuring the continuity of those services. Finally, NIS1 stated that OES must notify the competent authority or Computer Security Incident Response



Figure 1: Differences in scope between NIS1 and NIS2

Team (CSIRT), without undue delay, of incidents with a significant impact on continuity of essential services. These notifications must include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident⁵.

NIS2 makes these requirements more explicit. First, NIS2 includes a list of security requirements that all entities must implement to manage security risks to their networks and information systems, to prevent incidents and mitigate their effects on consumers of their services (see figure 2).

Second, NIS2 explicitly requires entities to manage and mitigate supply chain risks by conducting due diligence on cybersecurity. This means that organizations that originally may not fall within the scope of NIS2 must be cybersecure⁶ as well. This is a logical next step as supply chain attacks increased by 742% over the last three years⁷.

Third, NIS2 upgrades the existing reporting obligations under NIS1, as any significant incident or major cyber threat that could lead to a significant incident must now be reported to the national CSIRT or relevant supervisory authority within 24 hours. Additionally, an incident notification must be sent within 72 hours and a final report must be submitted no later than one month after the incident.⁸ NIS2 also introduces a duty of notification to recipients of the service affected by the significant incident, thereby mirroring existing obligations under the GDPR.⁹

3. Supervision and consequences for non-compliance

NIS1 did not contain clear-cut supervisory and enforcement mechanisms. This is in sharp contrast with NIS2 which allows supervisory authorities to conduct inspections or request evidence and temporarily banning CEO's (Chief Executive Officer) from performing their duties (provided a court order is obtained) in case of non-performance¹⁰. It also introduces a mechanism for non-compliance that enables supervisory authorities to impose fines of up to EUR 10 million or 2% total global annual turnover¹¹.

Finally, NIS2 introduces governance and accountability obligations that require management boards to approve risk measures and oversee its implementation¹².

4. Upgrade CSIRT tasks and competences

Besides the above-mentioned changes, NIS2 also significantly upgrades tasks and competences of member state CSIRTs. Besides the standard monitoring and analyzing duty, CSIRT is now responsible for aiding entities during incidents, providing coordinated vulnerabilities disclosure, collecting, and analyzing forensic data and providing risk and incident analyses. For entities this provides the right to utilize the assistance and threat intelligence information of the national CSIRT¹³.

Unravelling NIS2 implementation challenges

The previous section discussed the key changes of NIS2 that compared to NIS1 should provide opportunities for security enablement and risk reduction in organizations. Below, we consider the key implementation challenges that organizations face, based on our experience in assisting clients with NIS implementation.


Challenge 1: Determining the scope of NIS2 for your organization

Determining the scope of NIS2 within an organization has proven to be a challenging and time-consuming task as it requires extensive business, IT, and security knowledge from experts. Yet, it is the most crucial step towards becoming NIS2 compliant as the scoping determines what services, assets, and business processes must comply with NIS2. Based on our experience assisting customers with scoping for NIS2, we identify the following key challenges:

Striking an effective balance between required business resilience and cost efficiency.

Security in business resilience (i.e., quickly adapting to disruptions) and cost efficiency (i.e. being able to deliver projects and services at the lowest possible price without compromising quality) are often at odds with each other. Yet, both are vital for an organization's longevity. Striking a dynamic balance is important but the weight often falls more on cost efficiency than resilience. NIS2 forces organizations to reconsider this balance, as organizations are obliged by law to increase their digital resilience. During

SECURITY REQUIREMENTS IN NIS2

	Policies on risk analysis and information system security		Beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen
	Incident handling		Basic cyber hygiene practices and cybersecurity training
	Business continuity		Policies and procedures regarding the use of cryptography and encryption
	Supply chain security		Human resources security, access control policies and asset management
	Security in NIS acquisition development and maintenance		The use of multi-factor authentication or continuous authentication solutions

For more information see Article 21 of the NIS2 Directive

Figure 2: Security requirements in NIS2

ORGANIZATIONAL ASPECTS OF SAFETY

scoping, a newly defined balance must be struck that is in line with NIS2. Stakeholders such as IT, security, and business may have different conflicting interests, and different opinions on how far to take this.

Determining scope selection criteria.

Not all business services and underlying business processes and assets required to deliver a business service may be important or essential for NIS2. The challenge that organizations often face is the lack of NIS2 knowledge and expertise to determine what business services and underlying processes and assets are essential or important under NIS2. Therefore, organizations find it difficult to translate the meaning of NIS2 into clear-cut selection criteria that may assist the organization in determining the way forward. Yet, such clear-cut selection criteria are crucial to adequately balance business resilience with cost efficiency in order to determine the way forward.

Limited insight into assets and processes.

Insight into assets and processes often is limited because organizations may lack complete asset management and business process documentation. It could also be the case that organizations have not documented business processes. Such insights must be created, but organizations may find that knowledge and expertise about assets and processes is scattered across business, IT, OT, and cybersecurity stakeholders. Even if the right NIS2 expertise is present and scope selection criteria are successfully determined, without a clear-cut view on assets, processes and the right stakeholders, scoping will become incredibly difficult.

Challenge 2: NIS2 Supply chain risk management

NIS2 requires organizations to implement robust Supply Chain Risk Management (SCRM) assessments and management processes to ensure the security of their critical infrastructure. This means that technical and non-technical risks associated with the distributed and interconnected nature of IT/OT product and service supply chains must be identified,

assessed, and managed. The goal is to ensure that organizations have a comprehensive understanding of the risks posed by their supply chain and to take appropriate action to mitigate those risks. However, setting up and implementing effective SCRM processes can be challenging, particularly for organizations that rely on many suppliers. Based on our experience assisting customers in SCRM for NIS2, we identify the following key challenges:

Identification of stakeholders and dependencies on stakeholders

A clear view of the supply chain is essential to effective SCRM. However, creating this overview can be difficult because the information may not be readily available and/or may be fragmented throughout the organization. Moreover, NIS2 not only requires the identification of key external stakeholders, but also of the dependencies on these stakeholders from the perspective of NIS2. To do so it must be determined whether the use of the external service or asset may impact confidentiality, integrity and availability and thereby affect business continuity. Setting criteria and determining this can be challenging as it requires a structured approach and cooperation from stakeholders and dependencies.

Integrating SCRM in existing procurement and contract management processes

Several aspects must be considered when integrating supply chain risk management (SCRM). For organizations that already have procurement and contract management processes in place, it is important to assess if cybersecurity elements are included. If cybersecurity elements are included, it must be verified whether the whole supply chain is explicitly covered in contracts. If this is not the case, contractual terms may need to be strengthened or changed, to be compliant with NIS2. Another option is that organizations may have covered NIS2 cybersecurity elements in procurement processes, but the implementation itself is lacking. Gaining insight into the status of SCRM is important. While challenging, this is crucial for maintaining your SCRM and safeguarding NIS2 compliance.

Monitoring compliance and meeting requirements

NIS2 or SCRM assessments are distributed to check current levels of security, compliance, and risk of suppliers. However, not all suppliers may be willing to cooperate without contractual agreements, as they might view the monitoring practices as intrusive or burdensome. Another complicated aspect is risk acceptance, meaning that an organization must decide which risks they are willing to take when future or existing suppliers, who are crucial for business, do not meet requirements.

Challenge 3: Security Incident Management & Reporting obligations

NIS2 upgrades existing reporting obligations and makes explicit what is required of organizations. Meeting these requirements results in the following implementation challenges:

Setting up and integrating NIS2 in security incident management process

To be able to meet the duty of notification of NIS2, security incident management must be in order.

Setting up such a process may be challenging as it requires clear-cut governance and ideally, implementation of centralized log management with security analytics to aggregate, correlate and analyze activity across the IT/OT environment. Not every company may have the budget, expertise or

even maturity to do so, thereby placing organizations at risk of failing to meet the strict Security Incident Management and Reporting Obligations. Besides, with maturity of each organization being different, it is hard to pinpoint exactly when detection capabilities are sufficient to meet NIS2 reporting obligations. Another complicating factor may be that an organization has outsourced its security incident management function. This means that NIS2 reporting obligations may not be incorporated in SLAs, which, in turn, would require contractual renegotiations.

Defining 'significant incident' and 'suspicious activity'

A significant incident or major cyberthreat leading to a significant

incident must be reported to the national CSIRT but interpreting whether suspicious activity is an incident or may lead to significant incident and thereby requiring notification may prove difficult and is different for each organization. It may also take longer than the designated timeframes to conclude this. Without clear agreement on what is considered a significant incident within the organization and with strict timelines to adhere to, an organization may face the risk of significantly overburdening the security incident management team out of fear of non-compliance.



ORGANIZATIONAL ASPECTS OF SAFETY

Over de auteurs:

Florianne Kortmann



During the writing of this report, Florianne Kortmann was a senior cybersecurity consultant with expertise in IT strategy, governance (supply chain), risk management, and compliance. She had experience in NIS 2.0 and ISO27001 consulting and implementation projects and was involved in business development related to NIS 2.0. Florianne welcomed challenges as opportunities to enhance security to a higher level.

LinkedIn: <https://www.linkedin.com/in/florianne-kortmann/>

Sasha Brouwer



Sasha is a cybersecurity consultant with a focus on strategy, risk, and compliance. She is experienced in NIS 2.0 business development, third-party risk management and ISO27001 implementations in both private and public sector.


Mail: sasha.brouwer@capgemini.com

LinkedIn: <https://www.linkedin.com/in/sashabrouwer/>

Sources:

1. [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2021\)689333](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333)
2. <https://eur-lex.europa.eu/eli/dir/2022/2555> (Article 2 NIS2 Directive)
3. https://doi.org/10.1007/978-981-19-6414-5_18
4. <https://eur-lex.europa.eu/eli/dir/2022/2555> (Article 26 NIS2 Directive)
5. <https://eur-lex.europa.eu/eli/dir/2016/1148/oj> (Article 14 NIS1 Directive)
6. <https://eur-lex.europa.eu/eli/dir/2022/2555> (Article 21 NIS2 Directive)
7. <https://securityboulevard.com/2023/05/how-software-supply-chain-vulnerabilities-lead-to-attacks>
8. <https://eur-lex.europa.eu/eli/dir/2022/2555> (Article 23 NIS2 Directive)
9. <https://www.stibbe.com/publications-and-insights/the-revised-network-and-information-security-directive-enhancing-eu>
10. <https://eur-lex.europa.eu/eli/dir/2022/2555> (Article 32 NIS2 Directive)
11. <https://eur-lex.europa.eu/eli/dir/2022/2555> (Article 34 NIS2 Directive)
12. <https://eur-lex.europa.eu/eli/dir/2022/2555> (Article 20 NIS2 Directive)
13. <https://eur-lex.europa.eu/eli/dir/2022/2555> (Article 10,11,12 NIS2 Directive)
14. <https://eur-lex.europa.eu/eli/dir/2022/2555> (Article 23 NIS2 Directive)

SECURITY IN EMERGING (OR EXPANDING) AREAS OF TECHNOLOGY

A woman is shown from the chest up, wearing a black VR headset. She is looking forward with a neutral expression. The background is a dark, futuristic environment with blue and yellow lighting. There are grid-like patterns and glowing elements in the background. A thin blue line curves across the top left of the image. A small yellow horizontal bar is located below the main title.

02

Trends in
Cybersecurity
2024



DATA IN THE METAVERSE: WHO IS THE OWNER?

How can we establish a secure framework for managing personal data ownership in the metaverse; one that empowers users and ensures that they are in control of their identities and data?

Highlights

- The new ways of interacting in the online metaverse will require new, different types of data inputs that can fall under privacy regulations.
- Current data privacy frameworks might become obsolete if they are not analyzed and developed properly for Web 3.0.
- Companies can act accordingly by proactively thinking about their Web 3.0 privacy policies.
- Persistent, live, synchronous, and interoperable experiences in the metaverse will generate an unprecedented amount of data in continuous traffic.
- Data pseudonymization will become the priority in Web 3.0.
- Decentralized identities will be accepted as the new global identifiers on Web 3.0 due to their distributed ledger architecture, which grants more security and ownership of users' data.
- Decentralized identities simplify the process of identity validation in interactions in the metaverse, thus providing a better user experience.

When Gary Kovacs introduced Collusion, a privacy solution for Firefox, he stated that "Privacy is not an option, and it should not be the price we accept for just getting on the internet"¹. Although from 2012, this quote still rings true today, as billions of internet users trade private information while browsing, highlighting the persistent challenge of trading private information.

However, with increasing awareness of this "trade" within Web 3.0, people are keen to restrict access to their data, especially in the metaverse, where having an identity is crucial for participating in interactions. The metaverse is a world full of possibilities, but it also presents challenges in terms of data protection. This article delves into the issue of data ownership in the metaverse and presents a potential solution that can empower users by granting them control over their data.

The upcoming challenges of the new digital world

During the past 32 years, the number of online interactions grew progressive. This has allowed the internet to move from just reading (Web 1.0) to reading and writing (Web 2.0) and finally to what is known today as the semantic web (Web 3.0), which not only allows for the decentralization of the information, but also grants ownership to content creators. This new generation explores the vast potential of the online world and discovers modern capabilities like the blockchain and the metaverse. Such technologies could revolutionize the way we use the internet, transforming it into an entirely new experience.

Considering that the metaverse is a novel concept that enables people to engage with the world and each other in unprecedented ways, there is an opportunity to enhance these interactions through innovative technologies. This could involve incorporating users' full senses into Web 3.0, resulting in new types of data being imported, stored, processed, and transmitted. As the new online environment encourages decentralization and individual ownership of information, coupled with the increasing processing of sensitive

data, it's inevitable that concerns regarding data privacy will surface.

It is crucial to address this subject. First, we need to acknowledge that the rules governing privacy and data protection were created for use with actual filing cabinets and were later amended for use with the current internet. To effectively prepare the legal framework for a Web 3.0 environment and meet the new issues that emerge, we will need to take this into account, e.g. by implementing privacy by design.

However, because regulations, standards and policies often lag on the technological developments, we should also consider how we can approach adapting the upcoming policies to the metaverse. We could start with considering it as an actual alternate digital real-time existence that offers a persistent, live, synchronous, and interoperable experience with an unprecedented amount of data in continuous traffic. To address these challenges, it is essential to first assess the current state of privacy and determine how best to ensure data ownership in the metaverse moving forward.

Privacy and security considerations when thinking of data ownership in the metaverse

The metaverse facilitates connections between users and their digital avatars, which may contain unique identifiers. It is evident that existing privacy and data protection laws, such as the General Data Protection Regulation (GDPR), already apply to this context. However, due to the global reach of the metaverse, it cannot be confined to a few data privacy regimes, as multiple privacy laws may apply to the same data and individual.

SECURITY IN EMERGING (OR EXPANDING) AREAS OF TECHNOLOGY

Due to the unique characteristics of the metaverse, it may be necessary to revise the existing procedures under these privacy regimes. An example can illustrate this. Suppose a person in the metaverse interacts with another user by talking to them (speech patterns) or making physical movements (via their avatar). This data can then be collected and analyzed by third parties for commercial purposes, such as customizing advertising or improving product development based on users' behavioral data.

In addition, the metaverse presents new categories of personal data for processing. This may include biometric data like facial recognition and data on physical movements and interactions with others. Therefore, appropriate data protection and privacy laws are necessary to protect this data. Thus, we can already predict that security may prove to become a major concern in the metaverse, particularly when transmitting personal data from one metaverse to another (interoperability), or when allowing third parties inside the Web 3.0 to use such information for business purposes.

Although there is currently no stringent legislation regarding privacy and data security in the metaverse, companies that aim to distinguish themselves on a unique reputational level should consider integrating these measures into their operations early on. This builds trust with their users, especially when coupled with providing more ownership of the data to their users themselves. Measures may include reviewing and updating internal privacy policies, in accordance with global privacy regulations. Implementing effective data protection measures that consider future developments may also be advisable, particularly in relation to self-preferencing of content by metaverse platforms.

Are there solutions already on the radar?

With many challenges already at the front door, it is necessary to define how we can adapt existing legal and technical solutions to ensure that the data ownership resides within the users, empowering them to be rulers over their information and the types of interactions that information can be included in.

If it appears that the data is likely to be used by different companies for different purposes such as business continuity analysis, there are options that can make both ends meet. A first option is pseudonymization, in which the users retain control over their privacy and their information, and where companies retain the ability to elaborate such processing without having to know the full dataset of the users. A second option is the use of decentralized identities, working as a private data wallet for end users. In data pseudonymization, personal identifiers are replaced with placeholders for such values. This allows users to confirm information, such as whether they are of legal age, or whether they have a university degree, without having to provide their birth date or the university where they studied. This principle can be applied not only to basic concepts like this, but also to larger and more complex datasets like neuroimages, biometric information and legal information of the users. This could provide a baseline for role-based access models in the different metaverses in the future (for example, accessing specific governmental metaverses based on passports or ID pseudonymized data).

However, data pseudonymization is only one essential element in the equation of a user's identity dataset in a Web 3.0 context. We still need to answer a crucial question: where is this identity dataset stored or concealed? Self-sovereign identities, also known as decentralized identities, have the potential to become not only a trend, but a common practice in the metaverse in the coming years.

The Self-Sovereign Identity (SSI) as a cornerstone

Decentralized identities can be traced back to 1991, when the internet started and discussions arose about using a single identifier to surf the web. Early approaches of Decentralized Identities appeared on "Establishing Identity without Certification Authority" (1996), a publication by Carl Ellison, where he analyzed an approach on how the identities were created and proposed ideas on how these identities could carry on in the web without the need of trusted certificates. These ideas became reality in the 21st century, with the introduction of blockchain and decentralization and the rise of crypto markets.

The decentralized identities that contain pseudonymized information can increase the security of the data storage and prevent data breaches or loss of information, since the information held by the identity is not stored in a silo or kept by a unique trusted issuer.

Instead of that, the data is stowed on a “distributed ledger” or “blockchain” as it’s more commonly known, that this can be accessed by both the issuer (the one that confirms that the data is correct) and the verifier (who needs to claim the authenticity of the data). The distributed ledger capability of the decentralized identity also allows for not only one but multiple issuers over the same identity. This allows the user to have confirmed information from entities like their government, university, insurance company, email provider or any other inside the same identity set. As a further advantage, this reduces the number of interactions between any verifier and the many issuers that can be involved in a validation process, thus reducing the network traffic to servers that just focus on storing this data.

Approaching metaverse identities as self-sovereign ones not only makes the environment more secure, but also

guarantees that the user experience will be more seamless. Thus, it grants users a better interaction experience in their preferred landscape, with more robust safety and control of their information.

Gary Kovacs’ quote holds even greater significance in the context of the metaverse. In this new digital realm, users will inevitably generate vast amounts of personal data as they interact with one another and with the environment. It is critical to ensure that this information stays private and secure to build a trustworthy and safe metaverse in which users have control over their data. To achieve this, pseudonymization and self-sovereign identities are vital solutions. When implemented correctly, these solutions can serve as a differentiating point for businesses adopting metaverses to demonstrate their trustworthiness and privacy concerns.



SECURITY IN EMERGING (OR EXPANDING) AREAS OF TECHNOLOGY

About the authors:

Alfredo Acuña Salswach



Alfredo Acuña is a skilled professional who combines his engineering background with a thoughtful approach to his work. He excels as a natural team player and his experience in Identity and Access Management has made him the point of reference on his team on the topic. With a master's in Chemical Engineering, the cybersecurity complex and dynamic fields of studies have become part of his passion, and the Web 3.0 and Metaverse stands in his top 3.

Mail: alfredo.acuna-salswach@capgemini.com

LinkedIn: <https://www.linkedin.com/in/alfredo-acuna-salswach/>

Selma Mujcic



Selma is an experienced privacy consultant who combines her knowledge of innovative technologies with a strategic approach to privacy and cybersecurity to help businesses achieve sustainable and secure growth. Selma's expertise and insight make her unique in her field and enable her to assist companies in navigating this ever-changing digital world.

Mail: selma.mujcic@capgemini.com

LinkedIn: <https://www.linkedin.com/in/selmamujcic/>

Sources:

1. <https://www.wired.com/2012/02/ted-mozilla-collusion/>



THE VALUE OF TEST BEDS IN A QUANTUM SAFE MIGRATION JOURNEY

How can testbeds support efficient systems design and implementation experiments in the battle against the quantum threat?

Highlights

- Quantum computers threaten existing encryption systems. To deal with the threat, test beds and innovative solutions are necessary.
- Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) are promising tools in the battle against the quantum threat.
- Migrating to quantum-secure cryptography represents a step into the unknown. It needs careful preparation, and a strategy to deal with the complexities involved and with the lack of available experience and expertise.
- Test beds can support experiments with algorithms and protocols, and as a result promote more efficient implementation.
- Test beds can support the improvement of system design and implementation and help to overcome experience gaps. As such, test beds are crucial elements of a successful, quantum-secure migration in an OT environment.

The age of the quantum computer is almost upon us. Such computers can solve problems that are beyond the grasp of traditional computers. An undesired side effect of these developments is the danger quantum computers represent to the security of current encryption systems. Quantum computers can breach traditional asymmetrical cryptographic algorithms; the type we currently use to protect our sensitive information. Such algorithms offer the security we need, based on the complexity of mathematical problems such as the factoring of prime factors; solving such problems is almost impossible for traditional computers. As an example, a standard, current computer would take almost 300 trillion years to crack an RSA-2048-bit encryption key. A quantum computer with sufficient capacity could do the factoring in a matter of hours.¹ This represents a threat to the security of our systems. How can test beds and innovative solutions help us to tackle this threat, and surmount the challenges we face?

We identify two solutions to this quantum conundrum:

1. Post-Quantum Cryptography (PQC). PQCs are cryptographic algorithms that belong to the 'traditional' domain. They should be able to resist attacks from both traditional and quantum computers. We expect that PQCs will be able to interact with existing, traditional systems.
2. Quantum Key Distribution (QKD). QKD, on the other hand, is based on the principles of quantum mechanics and is regarded as the safest encryption method currently available in the quantum domain.

Several leading security institutes in France², Germany³, the UK⁴ and the United States⁵, recommend PQC as solution of choice against the quantum threat. Their conclusions are based on the system requirements, the lack of industrial standards and the current level of maturity of QKD technology. Because of these recommendations, this article will focus on PQC.

Challenges surrounding the introduction of quantum-secure cryptography

To stay protected against threats from quantum computers, organizations should upgrade their systems from existing, vulnerable cryptography to PQC. The upgrade process involved is regarded as an enormous, very costly, and hugely complex assignment that can take many years, depending on the scope of the organization. Any transition program with such an impact, touching upon almost every critical element of an organization, should only be attempted through thorough preparation. As an important aspect of these preparations, you should investigate new cryptography algorithms and experiment with them, to safeguard an efficient, cost-effective execution of the quantum secure transition. During the preparation process, you should make sure to tackle a number of challenges first; if you succeed in doing so, your quantum secure journey can begin.

1. No drop-in replacements

PQC algorithms differ from traditional encryption algorithms. These algorithms are based upon several different mathematical approaches and require more computing power. PQC deploys different key lengths for public and private keys, which results in a new design for coding systems. Existing cryptography can't simply be replaced by new, quantum secure cryptography.

2. Several kinds of PQC algorithms with different characteristics

Different kinds of PQC algorithms are selected and standardized. It's essential to choose the right combination of algorithms and protocols, that suits your specific applications and your demands for effective functionality and optimal performance.

The National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce standardizes quantum secure algorithms for key encryption and the use of digital signatures. For each category, NIST is expected to select and standardize several algorithms. This is and has been a long selection process, consisting of several rounds. In July 2022, NIST announced the selection of the first group of PQC algorithms. This first group contains one key encapsulation method, the CRYSTALS-Kyber⁶ algorithm for general encryption, and three algorithms for digital signing: CRYSTALS-Dilithium⁷, FALCON⁸ and SPHINCS+⁹. In the fourth round of the evaluation process, a further four algorithms for key determination mechanisms will be evaluated. These selected algorithms will, in all probability, become standards in 2024.

3. Lack of experience and expertise

PQC-algorithms are relatively new. Yet, they haven't been applied at scale in real world applications. Because of this, experience and expertise with the implementation and use of such algorithms is lacking. Due to this lack of experience, it can be difficult to make well-informed design decisions that meet the demands of security and performance for both the algorithms and the applications they're attached to.

4. Increased complexity, caused by hybrid approaches

Because PQC algorithms are new and unproven, experts are worried about the robustness of their security¹⁰. That's why they recommend hybrid approaches; combinations between traditional and PQC algorithms. This hybrid approach adds to the complexity of implementations of protocols and applications.

Quantum Safe Test beds – a possible solution

To deal with these challenges, every organization should gather expertise and knowledge about PQC algorithms and related protocols, and about the related requirements regarding computing power, bandwidth and memory. But organizations should also have an idea of the overall impact of PQC implementations on the functionality and performance of applications. Without such insights, quantum secure migrations can run into serious trouble; applications may have to be refactored, application performance may be substandard, functional problems may occur, et cetera. More importantly, such troubles may be exacerbated in OT-environments with their embedded systems with limited resources and real-time performance demands.

Using test beds to test and evaluate PQC algorithms and security protocols may present a solution to such issues. Test beds are special environments, designed for the testing and evaluation of the performance and functionality of quantum secure cryptographic and protocols, for functionality and performance in a specific applicative context. These test beds may consist solely of software, or of a combination of software and hardware with the required interfaces for input and output, combined with other components that are necessary to simulate real life conditions.

Test beds allow researchers to experiment with PQC algorithms, in isolation or in hybrid settings, for specific use cases and application scenarios, and in simulated conditions that represent real life conditions. In this way, you can gain insight into the specific benefits and weaknesses of quantum secure algorithms and related protocols. This is important, because certain combinations of algorithms may be better suited to specific applications than others. The test beds are useful when conducting experiments in a laboratory setting on functionality, performance and security demands for individual applications and

system scenarios that may apply to the organization in question.

When using quantum test beds to perform evaluations, you should adhere to the following recommendations:

- Identify the applications that require protection against quantum computers and determine the application scenarios or workflows that should be tested.
- Determine application-specific security requirements that offer protection against traditional and quantum threats.
- Record and analyze the details of the resources of existing systems, e.g., computing power, memory, network bandwidth, etc. You need this information to configure the test bed for the selected applications and related use case scenarios.
- Determine and configure limitations and network conditions such as latency, transmission errors, the size of transmission units.
- Gather and evaluate implementations of quantum secure algorithms (PQC) and protocols and transfer them to the test bed platform.
- Implement application PoCs or use existing application software and configure algorithms and protocols to meet the requirements of the application scenarios.
- Prepare test scenarios to execute and verify implementations, including the possible limitations or restrictions caused by the application of algorithms and protocols to specific applications. It is preferable to re-use existing test plans and test instances of applications. This evaluation should be conducted for individual quantum secure algorithms, but also for hybrid settings.
- Record the results and compare them with the performance of existing applications. Use this information to prepare for a potential road map and planning.



The use of test beds: three advantages

Even though there are no drop-in post-quantum cryptography replacements available for old cryptography, test beds can assist in system design, implementation improvement (software or hardware), and efficient integration in existing systems, thanks to a better understanding of the functioning of the new algorithms. Using test beds, we could experiment with several different post-quantum algorithms with different security levels and key lengths. As such, we can evaluate and compare performance, and choose the most efficient configurations for specific applications. Test beds may not exactly lessen the complexity of the implementation of hybrid approaches, but they can help you to improve planning and to better manage migration processes. Finally, by allowing you to experiment, test beds help you to develop an intuition around required security levels and the performance of post quantum algorithms. This compensates for the lack of prior experience and expertise.

Use of test bed insights in OT environments

Before we migrate OT landscapes with IoT and other embedded systems, we can use test beds to benchmark the performance and the required resources of these landscapes in scenarios using either traditional or

Sources:

1. <https://quantum-journal.org/papers/q-2021-04-15-433/>
2. <https://www.ssi.gouv.fr/en/publication/should-quantum-key-distribution-be-used-for-secure-communications/>
3. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=4#:~:text=QKD%20promises%20theoretical%20security%20based,post-quantum%20cryp-%20tography.
4. <https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies>
5. <https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/>
6. <https://pq-crystals.org/kyber/index.shtml>
7. <https://pq-crystals.org/dilithium/index.shtml>
8. <https://falcon-sign.info/>
9. <https://sphincs.org/>
10. <https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/>

post-quantum algorithms. Based on these benchmarks, you can make more informed decisions about whether to just upgrade the software or hardware, or to replace the hardware with new hardware that's better suited to deal with the requirements of post quantum algorithms. Migrating quantum secure algorithms without first benchmarking the resources available in OT systems, may result in serious performance issues, a heightened need for refactoring and, in some cases, full loss of functionality. This, in turn, will lead to delays, cost overruns, business losses and a prolonged period of risk exposure.

Conclusion

Organizations embarking on their quantum secure journey should evaluate all the quantum secure algorithms and protocols that could potentially be suitable to specific application scenarios. Such evaluations should take place in a controlled environment. Test beds offer an ideal opportunity to perform such evaluations of quantum secure migrations. Based on the results of the evaluations, organizations can select and document algorithms and protocols and the relevant configurations, for use in real life implementations. This will help organizations to confidently complete their quantum secure journey.

About the authors:

Julian van Velzen



Julian leads Capgemini's Quantum Lab, a global network of experts, partners, and facilities for quantum technology in Sensing, Communication, and Computing. He collaborates with clients to research and build solutions for complex business and societal challenges, leveraging the advantages of quantum technology. Julian is a physicist with a background in condensed matter, studied at the University of Amsterdam, and represents the Netherlands in the European Quantum Consortium (QuIC). He is a member of Capgemini's CTIO community, the Forbes Technology Council, and a co-founder of the Quantum Gateway Foundation.

Mail: julian.van.velzen@capgemini.com

LinkedIn: <https://www.linkedin.com/in/julian-van-velzen/>

Gireesh Kumar Neelakantaiah

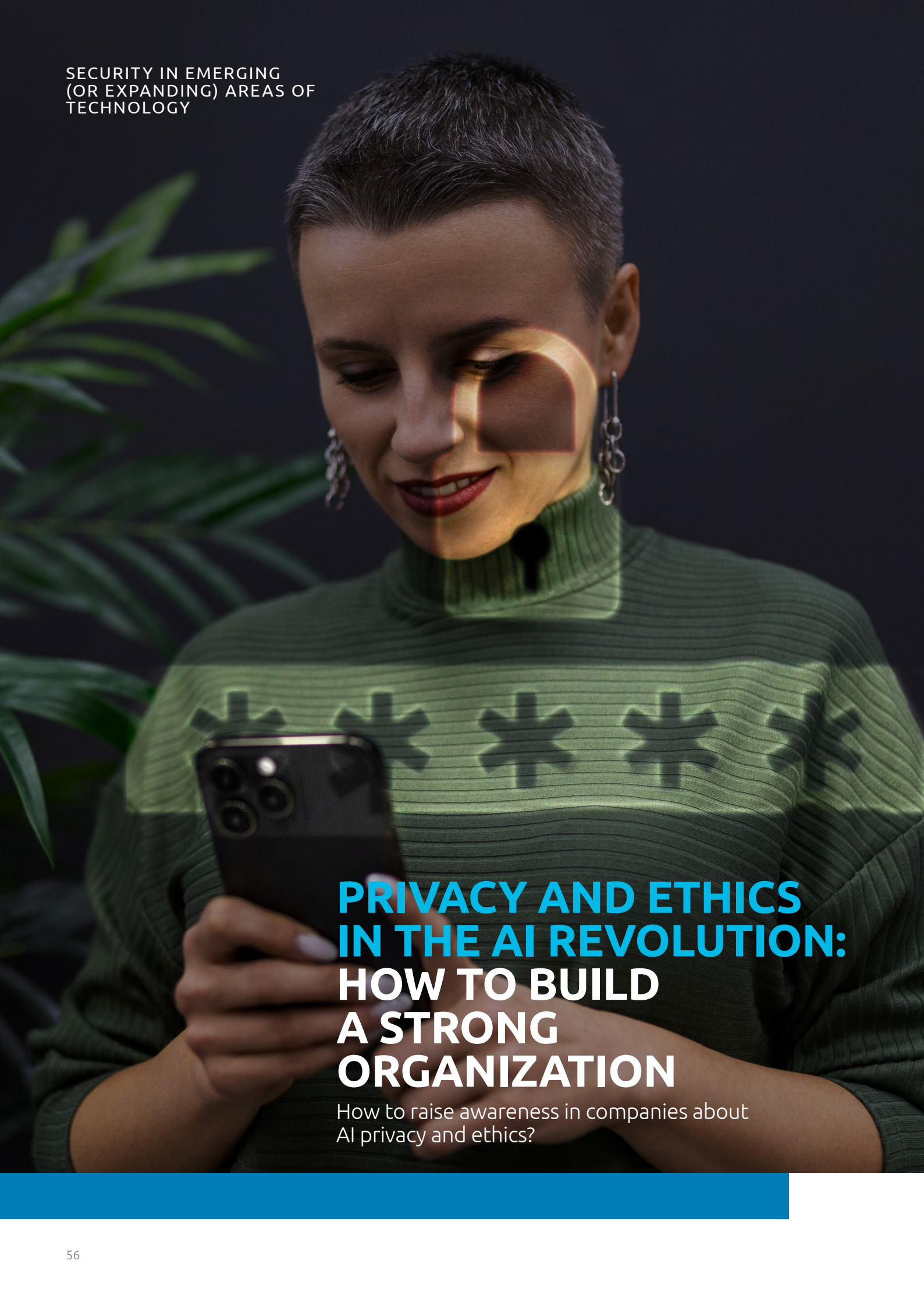


Gireesh is responsible for the strategy and the market introduction of the Quantum Lab and solutions for Quantum Secure Cryptography. He is an experienced professional in product management, strategic planning, innovation of business and commercial models, ecosystem management and IP license management. His personal interests lie in the fields of quantum computing, data science, AI/ML/deep learning, digital production, industrial IoT and cloud computing.

Mail: gireeshkumar.n@capgemini.com

LinkedIn: <https://www.linkedin.com/in/gireesh-kumar-n-5b5a5b1/>

SECURITY IN EMERGING
(OR EXPANDING) AREAS OF
TECHNOLOGY



**PRIVACY AND ETHICS
IN THE AI REVOLUTION:
HOW TO BUILD
A STRONG
ORGANIZATION**

How to raise awareness in companies about
AI privacy and ethics?

Highlights

- AI learns from data and fulfills tasks that require human intelligence.
 - There's a risk of copyright infringement when AI uses material that's protected by copyright and when that material is still recognizable in the AI's output.
 - Users and developers of AI may be confronted with various liabilities.
 - Unethical results can lead to legal liabilities, or negative consequences with customers or stakeholders.
 - Companies can distinguish themselves by taking steps right now.
 - The future of privacy in AI for companies will be lastingly influenced by new technologies such as The Internet of Things (IoT).
-

What is (generative) AI?

AI stands for Artificial Intelligence. It allows machines and devices to independently solve problems, without human interference. Generative AI is an aspect of AI that uses machine-learning data sets to create completely new output. In other words: AI allows an algorithm to create things like a human being would – a far more different application than AI's traditional uses in analytics.¹

The creation of an AI system consists of several different steps, such as data gathering, prepping the data for use, training the AI model and implementing the model. Generally, AI is about creating machines that learn from specially selected data sets and can perform tasks that would normally require typically human intelligence.

Today, generative AI is used in many different applications. The wildly popular chatbots are a good example. OpenAI's ChatGPT is one of these chatbots that make use of generative AI. ChatGPT uses a large language model to generate human-like answers, based on the user's input². Companies can use ChatGPT to automate customer service, create virtual assistants and more³. Another example of generative AI is CarMax Inc, which uses another version of the technology used by OpenAI to summarize thousands of customer reviews and help customers decide which car to buy⁴. Additionally, Generative AI can also make notes during virtual meetings⁵.

All in all, generative AI is a handy tool that can be deployed by companies in many ways. However, the use of generative AI may result in severe external and internal risks for companies. Employees of a company may use generative AI systems in their work and use sensitive information while doing so. As a result, companies risk losing control over this data, and it remains unclear how generative AI uses such data. A recent example is the leak at Samsung, where co-workers of

Samsung caused a leak of classified corporate information when they used ChatGPT in their work.⁶ Externally, bad actors could use AI to create harmful or misleading content that may cause reputational damage for the company. ChatGPT, for instance, claimed that an Australian mayor had been in jail for bribery. This allegation was false, and the mayor didn't have a criminal record, but the damage was done.⁷

Legal and ethical aspects of generative AI

The use of AI has various of legal and ethical dimensions. It's not easy to pinpoint what kind of legislation applies to AI; it all depends on the type of AI involved, its intended use, and the jurisdiction of the parties involved. The European Union is ahead of the pack with the AI Act, which is expected to be enacted by the end of 2023. Moreover, there are many AI-specific regulations and related areas of law that differ wildly from each other, such as intellectual property and data protection/privacy.

Intellectual property law has an important role in the development of AI. In training AI models, developers need to consider various legal aspects to do with intellectual property. First, they must carefully verify the required permissions, and if necessary, have to obtain licenses for material that is protected by copyright, or completely eliminate such material from the dataset. Developers also must make sure they don't infringe on copyrights, for instance when the AI copies material that's protected by copyright and publishes such material in its output. Even companies themselves need to be careful with the use open-source software (OSS) in their commercial software products, because some OSS licenses may only be used if the original author has given their permission, or if the original author is explicitly credited by the software product. Other open-source licenses demand that products that are derived from it are also made available as open source, or solely for non-profit ends.

SECURITY IN EMERGING (OR EXPANDING) AREAS OF TECHNOLOGY



Secondly, liability is an important consideration in AI development or use. In some cases, generative AI may harm third parties, such as when AI generates inaccurate diagnoses in health care, or inaccurate investment advice in financial services. This raises the question: who is responsible when things go wrong? The developers of the AI, or the companies that use the output? Users and developers of AI may be faced with different types of liability, including claims for negligence and product liability. Organizations that use AI must be aware of the liabilities that may ensue from current legal frameworks. In drawing up contractual provisions, companies should devote attention towards the careful allocation and mitigation of such risks.

Thirdly, data privacy is also an important consideration. AI systems are trained with large amounts of data. Such data can contain personal data. That's why you should carefully monitor whether personal data aren't being used and processed, for instance by co-workers. Simply asking someone to check a text for grammatical errors could lead to a data leak, if the text involved contains customer data.

Finally, there's an issue of ethics and discrimination in the use of AI. Ethical objections can arise from prejudice in AI models, or from AI-incurred effects on users or on society. Ethical issues may also arise from data that are used or generated by AI. Unethical results may lead to negative consequences for customers or stakeholders, as well as liabilities for the company. AI can reflect existing prejudices or stereotypes in society and amplify them. Training data can reflect patterns of systemic discrimination. The algorithm itself may even be prejudicial if it's trained on data that's inherently prejudicial as well. In using AI, companies should keep such considerations in mind.

How to safeguard privacy and ethics in generative AI?

To safeguard privacy and ethics in AI, organizations should take the following measures:

1. **Quality control:** Check the output to make sure that data aren't prejudicial, and that the data are relevant, reliable and accurate. Subject matter experts can quickly and effectively assess whether output is correct and relevant. This is important, because some models are very adept in generating convincing output that turns out to be false. Standard procedures should be implemented to check all output for accuracy, relevance, and reliability.
2. **Contractual checks:** Prior to AI use, discuss with customers whether certain personal data should be shared or not – even within authorized AI models. It is often unclear how AI models will use data, even if the AI model's privacy statement indicates that all data will be deleted.
3. **Adjust privacy policy:** It's clear that using generative AI may incur privacy risks. To mitigate these risks, an adjustment in the privacy policy may be of use. Customers could, for instance, be notified of the types of AI that may be in use, and the reasons and ends for the application of these AIs. Customers could also be informed about the ways they will be asked for their permission for the application of AI, and whether they have opt-in or opt-out options.
4. **Accountability and oversight:** Make sure that proper accountability and oversight is in place, by allocating responsible persons or teams who are tasked with managing the AI systems and protecting privacy and ethics. Make sure that accountability, and liability hierarchies are clearly defined and allocated.

Microsoft has already implemented a number of initiatives to promote privacy and ethics in AI. The company has established the AI and Ethics in Engineering and Research (AETHER) Committee; this committee monitors the ethical practices of AI within the company. On top of this, Microsoft has introduced AI principles that stress honesty, transparency, privacy and accountability in the development and implementation of AI technologies.

The AETHER committee works as an advisory organ to the senior board and the Office of Responsible AI. It formulates recommendations with regards to policies, processes, and best practices. The committee has six work groups that focus on the development of specific guidelines, based on their specialized expertise.

OpenAI, the company behind ChatGPT, is working to safeguard ethical and responsible AI. The company has introduced guidelines to ensure that the use of AI aligns with current standards and has taken measures to prevent potential abuses. As an example, OpenAI limits data storage duration to 30 days, is working to anonymize user data it has gathered, and is taking steps to prevent gathered data from being used for goals that may harm the privacy of users.

These companies are aware of the ethical and privacy-sensitive aspects of AI and are taking steps to enhance the privacy of their AI systems⁸.

The future of privacy in AI for companies will probably be influenced by new developments such as the Internet of Things (IoT), virtual assistants and autonomous vehicles. These developments have the potential to transform the ways we interact with technology and with each other, but they also entail new challenges regarding privacy. The Internet of Things, for instance, takes the shape of networks of connected devices, such as smart offices and mobile devices, which can gather and share data. IoT devices often gather large amounts of data that have to do with personal aspects such as our location, our habits, and our

preferences. This data can be used to draw up detailed profiles of individuals. This may even lead to profiling and automated decision making. In other words: generative AI is only the beginning.

Generative AI can undoubtedly be a game changer in effectiveness and productivity. However, as discussed above, it does bring about a wide range of potential privacy infringements and ethical objections. Such negative consequences will potentially only be exacerbated when AI is combined with new technologies such as IoT. Organizations that are already working to protect privacy and ethics in the ways they integrate AI into their business, can positively distinguish themselves by staying ahead of the competition, and instilling trust in their users.

SECURITY IN EMERGING (OR EXPANDING) AREAS OF TECHNOLOGY

About the authors:

Jorrit Tromp



Jorrit is a privacy consultant with a robust background in law. He is passionate about privacy and strongly believes in the importance of protecting personal data in the digital era. He likes to devote his analytical skills contributing to the solving of complex privacy issues.

LinkedIn: <https://www.linkedin.com/in/jorrit-tromp-402627aa/>

Selma Mujcic



Selma is an experienced privacy advisor. She combines her knowledge about innovative technologies with a strategic approach of privacy and cybersecurity, to help companies realize sustainable, secure growth. Thanks to her expertise and insight, Selma is unique in her field, and able to help companies navigate the many challenges of an ever-changing digital world.

Mail: selma.mujcic@capgemini.com

LinkedIn: <https://www.linkedin.com/in/selmamujcic/>

Sources:

1. <https://targettrend.com/nl/generative-ai/>
2. <https://www.entrepreneur.com/science-technology/how-chatgpt-and-generative-ai-can-transform-your-business/445066>
3. <https://www.entrepreneur.com/science-technology/how-chatgpt-and-generative-ai-can-transform-your-business/445066>
4. <https://nl.marketscreener.com/beursnieuws/laatste/Wat-is-Generative-AI-de-technologie-achter-OpenAI-s-ChatGPT--43272490/>
5. <https://nl.marketscreener.com/beursnieuws/laatste/Wat-is-Generative-AI-de-technologie-achter-OpenAI-s-ChatGPT--43272490/>
6. Samsung ChatGPT leak: Samsung workers accidentally leak trade secrets to the AI chatbot | Mashable
7. ChatGPT: Mayor starts legal bid over false bribery claim - BBC News
8. <https://help.openai.com/en/articles/7730893-data-controls-faq>



DETECTION AND RESPONSE



EMPOWER OT SOC SECURITY: ELIMINATE THREATS WITH CUSTOM INTELLIGENCE AND CLOUD INFRASTRUCTURE

How can organizations protect their OT installations from today's and tomorrow's cyber threats?

Recent cyberattacks on operational technology systems globally have emphasized the vital need for safeguarding OT environments. These environments, responsible for overseeing physical systems and processes, feature unique architectures, protocols, and security demands distinct from traditional IT settings. Unfortunately, OT environments are often neglected or insufficiently protected, making them attractive to cybercriminals. By establishing an OT SOC and leveraging a cloud-based SIEM (Security Information and Event Management) solution, you can substantially enhance OT security.

Continuous monitoring, threat detection, and incident response capabilities offered by an OT SOC and cloud SIEM are vital for safeguarding OT assets against cyber threats. Join us as we explore these essential tools and strategies to fortify OT security.

Synergy between people, process, and technology

In industries where OT systems are critical, such as the energy sector, robust cybersecurity measures are essential. That's where an OT SOC comes in. The Core components of an SOC are:

- **People:** Domain experts of SCADA, DCS, automation, process control engineers, multi skilled

- **Technology:** Log collection, visibility of assets, detection of threats, workflows
- **Process:** Consensus based on teams' agreement, fully tested, adaptable and evolving

The OT SOC protects Level 0, 1, 2, 3 of the industrial system architecture. These levels are from the Purdue reference model or contextual model from IEC 62443 for industrial system architectures.

In the technology part there are multiple technologies like EDR, CMDB, firewall management, ticketing, vulnerability management, SIEM, and OT monitoring. SIEM plays a vital role in correlation of logs from all technical controls deployed on site.

Cloud-based SIEMs like Microsoft Sentinel, Splunk, QRadar solutions offer advantages in scalability, cost-effectiveness, and security features. Custom threat intelligence provides tailored capabilities for threat detection and response.

Highlights

- An OT SOC (Security Operations Centre) is a critical component of a comprehensive cybersecurity strategy for organizations that rely on operational technology (OT) systems.
 - Cloud-based SIEM solutions offer advantages compared to on-premises solutions, including greater scalability, accessibility, cost-effectiveness, flexibility, and enhanced security features.
 - OT SOC outsourcing to MSSP (Managed Security Service Provider) reduces the burden on the organization for team creation and infrastructure management.
 - Custom threat intelligence benefits an OT SOC: tailored detection and response, improved accuracy and visibility, faster response times, and improved risk management.
 - The combination of cloud based SIEM solutions and custom threat intelligence can provide a more comprehensive and effective approach.
-

Exploring approaches to enhance OT security with SOC management and deployment

There are several SOC management and deployment approaches:

- Integrating OT capabilities into IT SOC;
- Deploying dedicated OT SOC;
- Outsourcing OT SOC to MSSP;
- Hybrid approach by mixing the above-mentioned.

As cyber threats become increasingly sophisticated and frequent, organizations are under constant pressure to secure their operational technology systems. Attackers with specialized knowledge can exploit weaknesses and disrupt operations, causing financial losses and endangering public safety. Additionally, valuable data and intellectual property stored in OT systems make them attractive for theft or industrial espionage. To address this challenge, specialized security operations centers have been developed to monitor, detect, and respond to cybersecurity threats like ransomware attacks, supply chain, insider attacks and physical sabotage to OT systems.

The tools deployed in OT SOC are evolved from IT but customized for specific industrial communication protocols and threat types for OT industry. In terms of technology and skills, the following is required for OT specific SOC:

- Analyzing and interpreting industrial protocols.
- Understanding OT language and acronyms.
- Managing endpoint diversity, including Windows, Linux, PLC, and proprietary OS/firmware.
- Addressing OT and industry-specific threat landscapes.



Imagine you're a security manager for an oil and gas company that is expanding production units in different locations. To ensure cybersecurity, for achieving higher security level and monitor alerts round the clock, you need to build an OT SOC at each site, which is costly and time-consuming. A cloud based SIEM solution in OT SOC eliminates the need for additional hardware, offers remote access, is cost-effective, flexible, and secure. It's the perfect choice for organizations looking to expand while keeping cybersecurity risks at bay.

Leveraging cloud deployment for enhanced SIEM capabilities

SIEM, when deployed on the cloud, comes with several advantages, such as:

- **Scalability:** Easily scale up or down to meet changing demands, without the need for additional hardware or infrastructure.
- **Accessibility:** Is accessible from anywhere, allowing security teams to work remotely and collaborate with other teams and stakeholders around the world.
- **Cost-effectiveness:** Offers cost benefits compared to on-premises solutions, as they eliminate the need for hardware, maintenance, and upgrades. This can free up resources for other critical cybersecurity investments.

DETECTION AND RESPONSE

- **Flexibility:** Offers greater flexibility in terms of deployment options, allowing organizations to choose the solution that best meets their specific needs and requirements.
- **Enhanced security:** Provides enhanced security features and capabilities, including robust authentication and access controls, encryption, and continuous monitoring.
- **Integration:** Extended integration capabilities with on-premises security monitoring solutions like Nozomi, Dragos and Tenable, reduces overhead for application-level monitoring on site.

An on-premises SIEM necessitates an organization to recruit and retain a team of security professionals responsible for overseeing the security infrastructure. This approach can be costly and time-intensive. In contrast, opting for a cloud-based SIEM outsourced to an MSSP doesn't require any on-site resource mobilization. It allows

organizations to tap into a dedicated team of security experts who handle infrastructure management, resulting in resource savings and a reduced in-house cybersecurity management workload.

Cloud providers adhere to certifications and compliance standards, making it easier for organizations to meet regulatory requirements. Additionally, by storing data in a specific geographical region, organizations can ensure compliance with local data privacy laws and regulations. This reduces latency and improves performance for users accessing the data. Furthermore, storing data in multiple locations within the same geographical region can improve resilience and reduce the risk of data loss or downtime.

High-level, the SOC will look like as shown in figure 1. MSSP's can access Sentinel from any location while the data will stay in the same geographic location.

Maximizing operational efficiency with custom threat intelligence in cloud-based OT SIEM

Adding custom threat intelligence to the cloud deployment of OT SIEM can greatly enhance its operational efficiency. Custom threat intelligence is specific to an organization's unique threat landscape and can provide several advantages, as it is compiled by experts who observe the activity of adversaries in particular industries and geographical regions. The threat intelligence could include information on the tactics, techniques, and procedures (TTPs) used by the attackers, such as the type of phishing email used, the lure used to entice the recipient to click on a link or download an attachment, and the malware used to infect the victim's computer. With this information, security teams can proactively monitor for and detect similar attacks and take appropriate actions to prevent or mitigate them.

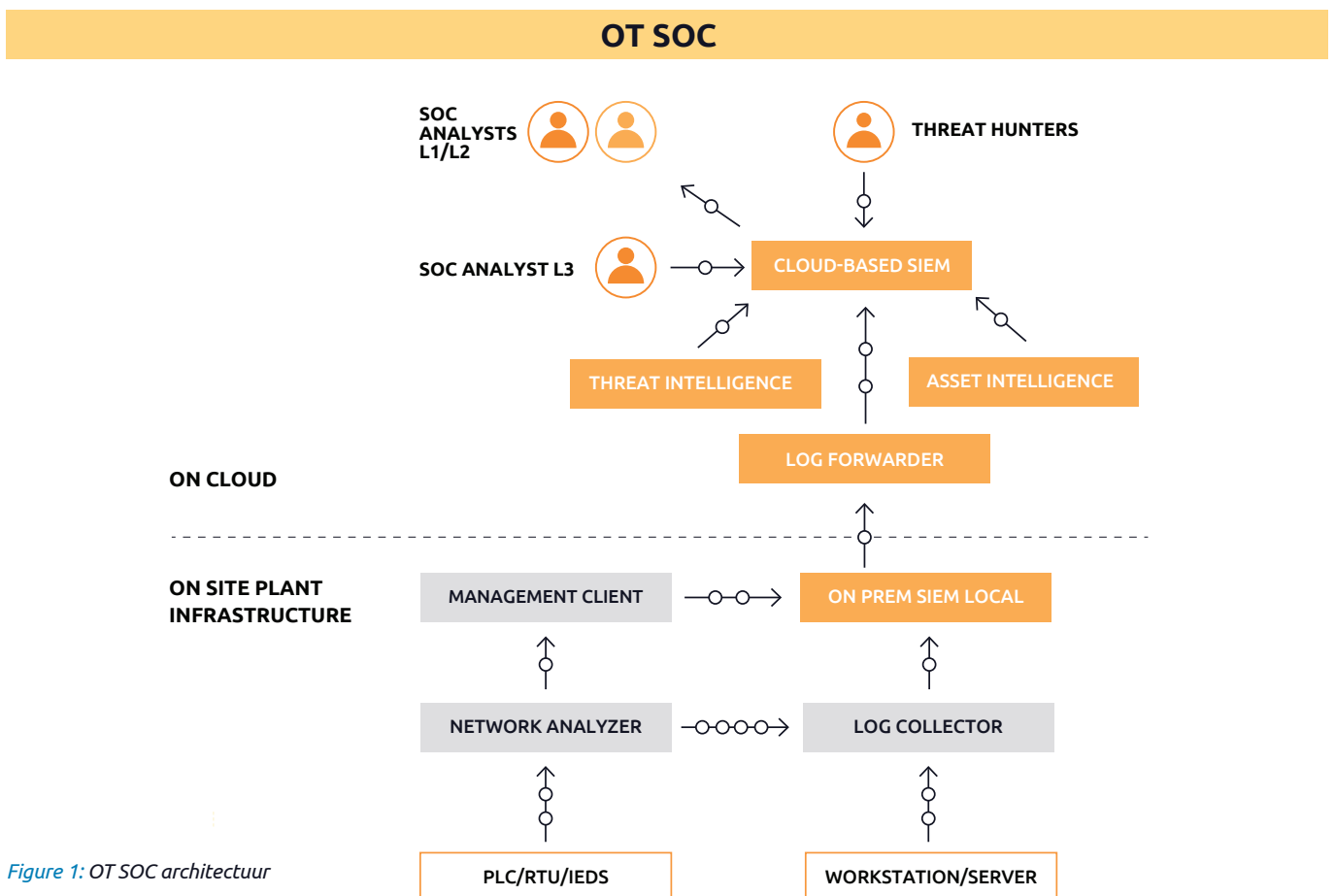


Figure 1: OT SOC architectuur

Some more aspects of OT SOC in an overall perspective are as follows:

- Firstly, it can be tailored to OT environments that have unique threats and vulnerabilities, resulting in more targeted and effective threat detection and response capabilities. Additionally, it improves accuracy in threat detection because it can be customized to the specific types of threats and attack vectors.
- Secondly, by integrating maximum assets into SIEM, it enhances visibility into an organization's OT environment, allowing security teams to identify potential threats and vulnerabilities more effectively.
- Thirdly, it helps security teams respond more quickly to potential threats by providing real-time alerts and automated responses based on customized rules and policies.
- Finally, custom threat intelligence contributes to a more comprehensive view of an organization's risk posture, allowing security teams to prioritize resources and implement risk management strategies specifically tailored to the organization's unique needs and challenges.

With these advantages provided by OT SOC, Cloud SIEM and threat intelligence organizations can better protect their OT environment from potential threats and vulnerabilities. For example, a manufacturing company could use custom threat intelligence to monitor its machinery for potential attacks and quickly respond to any detected threats to prevent production downtime.

The benefits of having an SIEM in the cloud and leveraging custom threat intelligence cannot be overstated. Cloud-based OT SIEM solutions provide greater scalability, accessibility, cost-effectiveness, flexibility, and enhanced security features, while custom threat intelligence helps refine tailored threat detection and response capabilities that are specifically designed to address the unique challenges of OT environments.

By combining these two approaches,

organizations can better protect their critical infrastructure and assets from the evolving threat landscape and more effectively manage their cybersecurity risks. As such, organizations that prioritize the deployment of cloud based SIEM solutions and custom threat intelligence can build a stronger, more resilient security posture that is well-equipped to address the growing cybersecurity challenges of today and tomorrow.

Our suggestion is to explore cloud-based solutions for OT SIEM and connect with custom threat intelligence providers who specialize in securing industrial control systems. This research can help bolster your organization's cybersecurity for industrial control systems. Don't hesitate to get in touch with them to gain a better understanding of their solutions and how they can safeguard your critical infrastructure.

About the author:

Sourabh Suman



Sourabh, a Managing Consultant at Capgemini in the Netherlands, offers expert guidance to clients in the Oil & Gas, Energy, and Manufacturing sectors. Specializing in implementing security standards like 62443 and NIST, he focuses on secure architecture design. Sourabh, a certified GICSP expert, authored "Unblocking Your Potential in ICS Cybersecurity" and serves as an Udemy instructor for ICS cybersecurity. Leveraging his extensive expertise, he assists organizations in identifying and mitigating security risks to ensure robust protection against cyber threats.

Mail: sourabh.suman@capgemini.com

LinkedIn: <https://www.linkedin.com/in/sourabhsuman0/>

Sources: <https://www.techtarget.com/searchsecurity/news/252504484/Gartner-Weaponized-operational-tech-poses-grave-danger>



**THREAT HUNTING
AND CYBERSECURITY
MATURITY: ARE YOU
TRYING TO RUN BEFORE
YOU CAN WALK?**

Highlights

- Threat hunting is about applying a focused and iterative approach to apply your own understanding of the network you're defending to catch attackers proactively.
 - Your organizational maturity and willingness to invest in the basics have a direct impact on the effectiveness of your threat-hunting program.
 - When having discussions about cybersecurity maturity and where to invest first, considering your position as a target of opportunity or as a target of choice is a useful talking point.
 - Matt Swann's hierarchy of needs is an excellent visualization to understand which cybersecurity basic building blocks support one another.
 - Threat hunting is a worthwhile investment in any stage of the cybersecurity journey, with its effectiveness going up as maturity increases.
-

Within the fast-paced world of cybersecurity, we often encounter instances of "that word does not mean what you think it means." In the never-ending battle for defenders to remain current against our adversaries, we develop new methodologies and technologies that reach the general public's ear through a haze of buzzwords and excitement. Considering this, let's spend some time on demystifying the concept of threat hunting – what is it, how does it fit into your cybersecurity posture, and – most importantly – how does it keep your organization safe from advanced threats?

What is Threat Hunting Really?

The SANS whitepaper, *The Who, What, Where, When, Why and How of Effective Threat Hunting* by Robert M. Lee¹ [1] puts it best: threat hunting is "a focused and iterative approach to searching out, identifying and understanding adversaries' internal to the defender's networks." Threat hunting is not triaging alerts on your security tool or throwing an Indicators of Compromise (IOC) feed into your endpoint response and detection platform to see what sticks. It is a proactive, scoped, hypothesis-led investigation that aims to catch and stop the adversary in its tracks before it can execute its objective – be it data exfiltration, ransomware, or any number of violations that will ruin the day of your Data Privacy Officers. In particular, the SANS definition highlights the two most important elements integral to successful threat hunting: understanding yourself and understanding your adversary. To understand the organization that you defend, you must first comprehend your infrastructure and your visibility within it; to understand your adversary, you must comprehend capability, intent, and opportunity (elements that can be drawn from cyber threat intelligence). Then, the threat hunter draws these elements together in a proactive technical investigation supported by the appropriate technology to find signs of smoke before the fire breaks out and burns down your organization's ability to do business. The threat hunter does

not care about commodity malware and a bit of cryptocurrency mining; we care about Advanced Persistent Threats (APTs), organized cybercrime gangs – the adversaries who continue to get past your automated security tooling.

This is the dream, certainly – stopping the threat actor in its tracks and finally providing tangible proof that your request for a larger cybersecurity budget was justified. But is your organization mature enough to implement a threat hunting function? From the SANS 2022 *Threat Hunting Survey*² (an enlightening read on the challenges and successes faced by organizations when it comes to implementing threat hunting programs), the top barriers for successful threat hunting include a lack of skilled personnel, budget and technology constraints, and a lack of defined processes. Also notable was a lack of threat intelligence and a lack of management support when it comes to setting up threat hunting efforts. These challenges tend to be symptoms of the organization's view on cybersecurity, and its relative security – are you willing to invest in the people and technology to do this highly specialized work? Have you committed to ensuring that you have the very basics in place (vision, strategy, governance, budget, perhaps a functioning SOC?) before you give your potential threat hunters the technological equivalent of a sharp stick and duct tape and tell them to "go hunt"? Threat hunting is useful in any stage of the organization's cyber resilience maturity; however, the hunting team's output can be significantly more effective based on your investment in the basics (such as a good asset inventory solution) all the way to the shinier, top-of-the-line security tooling out there. The less time your threat hunting team has to spend compensating for the lack of visibility for things that should already be in place or being tied up in muddied or unclear processes and communication lines, the more time they can spend on catching bad guys.

Threat Hunting and the Matter of Maturity

Of course, these ‘maturity’-related questions are not so easily answered without considering the nuance. In truth, a threat hunting program is not a trivial investment, in any sense of the word. While the cost of a potential high-severity incident is likely to outweigh the cost of safeguarding your operations, it is also about balancing the cost proportional to the problem. One way to start the conversation for the urgency in developing a threat hunting program is related to whether your organization is a *target of choice*, as opposed to a *target of opportunity*.

Being a *target of choice* relates to the intent of the threat actor; in other words, what does the threat actor view as your organization’s crown jewels, and what do they want to do with those crown jewels? Steal, disrupt, or damage? For example, organizations associated with government and critical infrastructure, or organizations specialized in highly proprietary medical, technology, and manufacturing (and more) areas may all be targets of choice for nation state actors. The threat actor invests time, effort, and resources crafting a campaign especially for you, targeting every weakness it can harness, be it your third-party suppliers, your employees’ poor credential and password management hygiene, or a poorly patched system. Against the threat of APTs such as these, a mature, well-organized, and **proactive** cybersecurity function with all the bells and whistles (of which a critical component is a robust cyber threat intelligence (CTI) program) is about the only counter that stands a chance. Being a *target of opportunity* leaves you open to attacks that are not necessarily tailored to your exposed weaknesses – rather, you will likely be targeted as part of a campaign crafted to affect as many common attack vectors as possible, across a select number of targets that may be susceptible. This may seem like a better position to be in than being a target of choice, but your ability to make this judgment is also reliant on a well-functioning CTI

program – except it is likely harder to justify the budget for that as well in this case. Strong cybersecurity hygiene is a good countermeasure for being a target of choice in any case, but this depends on your organization’s maturity as well. Ultimately, the pain of an incident feels the same, no matter your category.

Cybersecurity and a Hierarchy of Needs

In keeping with the creed of *know thy enemy, but also thyself*, the next consideration is a realistic view of what foundational cybersecurity building blocks you already have in place. Matt Swann devised an excellent depiction of the hierarchy needed for an organization to defend its assets (figure 1)³.

Starting from the bottom, each building block is a prerequisite for answering the question posed above it. Notice that “Hunt” sits quite high up in this pyramid. It makes sense: hunting becomes a much harder prospect to do thoroughly and completely when you cannot even provide a network architecture topology or an inventory list of existing software within the environment. Similarly, telemetry and data sources are needed for the hunt to start at all. There is a scope for each of these

building blocks – for example, while an Endpoint Detection & Response (EDR) platform covering your systems would certainly be an excellent coverage boost and large-scale data source for threat hunting purposes, having basic sources available (such as network data, logging, and the ability to query endpoint data via a custom set of PowerShell scripts) also satisfies the basic requirement. Sadly, as with most models that make things seem deceptively simple, reality is anything but. What makes threat hunting an interesting proposition, even at lower maturity levels, is that it can become an effective tool for finding the most critical holes (and likely attack paths) first. A frequent byproduct (that may eventually become an essential source) of threat hunting is identifying misconfigurations, hygiene issues, and visibility gaps: there is no better way to get a good picture of the current situation than getting your hands dirty in the guts of your IT environment. In turn, this can be used as input into a more realistically prioritized cybersecurity roadmap that effectively utilizes what you already have and identifies the critical gaps that need to be tackled first - provided, of course, that we are dealing with management with the appetite and willingness to listen to the bearers of bad news.

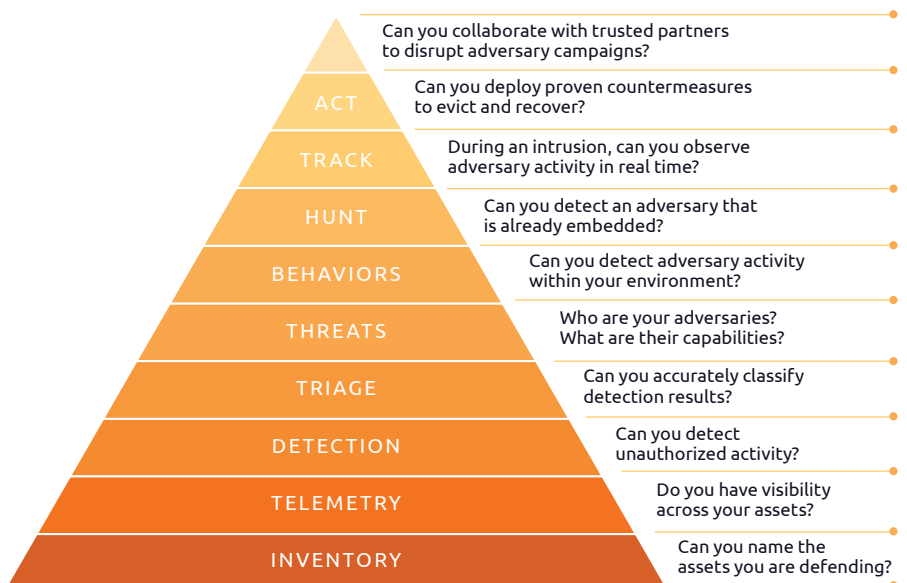


Figure 1: The incident response hierarchy of needs

Finally, an interesting (but perhaps less obvious) measure of how capable your organization is of tapping into the benefits of threat hunting is the organization's view on how to utilize CTI. The attentive reader may have surmised by now, as hinted at previously, that threat hunting's effectiveness is directly linked to how well CTI is utilized in the organization: after all, one cannot boil the ocean, and we must start the hunt somewhere. Good CTI – which should include an understanding of the types of threat actors that may be interested in your organization, as well as a thorough understanding of their tactics, techniques, and procedures (TTPs) – gives the hunter a realistic starting point by analyzing and understanding your organization's threat landscape, and thus a translation is made to target high impact, high severity potential indicators of attack first. How your organization views the necessity of CTI, in addition to how equipped it is in using it to its full effect, can give an indication of the level of understanding of what holistic cyber defense measures should look like. Arguably, the reverse is also true – an organization that has a mature threat hunting program should have CTI incorporated as a core process (as also hinted at in the SANS 2022 Threat Hunting Survey), which in turn implies a mature outlook. Maturity is not only

enshrined in the processes, tooling, and capability within the organization but also in the buy-in and willingness of the management team to recognize and address threats. An organization that understands the proactive approach is more likely to be open to utilizing both threat hunting and CTI in an integrated fashion, rather than seeing them as two separate checkbox exercises.

So Where Do We Stand?

In conclusion – threat hunting is a proactive means to find complex, embedded threat actors in your environment as early as possible in the attack lifecycle. While threat hunting can be a worthwhile addition no matter your cybersecurity maturity level, the effectiveness of the team is directly correlated to whether you have a realistic view of your position in the threat landscape, whether you have an honest view of your own internal strengths and weaknesses, and the willingness of decision-makers to recognize the necessity of robust cyber defense, along with an appetite to invest based on the aforementioned factors. Ultimately, it is only a matter of time until you have to deal with an intrusion in your network: the choice is yours whether you want to be proactive or reactive in your response. Either way: happy hunting!

About the writer:

Saskia Kuschke



Saskia Kuschke is an experienced, GIAC-certified digital forensics and incident response investigator.

LinkedIn: <https://www.linkedin.com/in/saskia-kuschke-9b3a22b3>

References:

1. <https://www.sans.org/white-papers/who-what-where-when-why-how-effective-threat-hunting/>.
2. <https://www.sans.org/white-papers/sans-2022-threat-hunting-survey/>.
3. <https://github.com/swannman/ircapabilities/>.

04

Trends in
Cybersecurity
2024

TECHNOLOGY-FOCUSED SECURITY ASPECTS

A man with brown hair and glasses is looking down at a laptop screen. He is wearing a grey sweater. In the foreground, there is a white document. The background is a blurred office setting with a window. A blue curved line graphic is overlaid on the bottom right of the image.

SECURE SAP IN BLUEPRINT: BEST PRACTICES AND STRATEGIES FOR PROTECTING YOUR BUSINESS

How to define a security baseline for your System Applications and Products (SAP) hybrid landscapes?

Highlights

- Most cyberattacks take place within the application itself. We should take the security of our application layer seriously without relying only on the outer layers.
- A significant risk in the application layer is the absence of important SAP security patches.
- Start fixing the core using default tools and minimal effort.
- We can also integrate SIEM, SAP ASE, and SAP Solution Manager into customer landscapes to encrypt and monitor SAP data.
- Customize the defense strategy and VM plan according to industry compliance standards.

In today's rapidly evolving threat landscape, securing your SAP system by simply defending the (outer) network layer is no longer enough. With cyberattacks becoming more sophisticated and targeted, organizations must adopt a multi-layered approach to SAP security. While defensive firewalls and intrusion detection systems are important, they are not enough to protect against the more advanced and persistent threats that can bypass these defenses.

With an SAP security blueprint based on these baselines, you will have a solid foundation to support organizational change and help eliminate the risk of losing market share or reputation. This SAP security blueprint will cover your SAP landscape, whether running on-premises, in the cloud or a mix of both in a Hybrid Landscape. When using a mix of landscapes, it's necessary to combine various frameworks and approaches to ensure nothing important is overlooked.

SAP application security

SAP systems are critical to the operations of many organizations, making them a prime target for cyber attackers. To protect against these threats, it's important to have a comprehensive approach to SAP application security. Let's explore the why, how, and what.

SAP systems store vast amounts of sensitive data, including financial and customer information. A breach of this data can have serious consequences, including financial loss, reputational damage, and legal liabilities.

Cyberattacks are becoming more sophisticated, and attackers are using a variety of techniques to gain access to SAP systems, including exploiting vulnerabilities in the application itself, social engineering, and phishing attacks. Therefore, it's important to have a robust SAP application security strategy.

SAP application security refers to the measures and practices that are put in place to ensure the confidentiality, integrity, and availability of SAP systems and data. This includes controlling user access, monitoring user activity, protecting against external threats, and complying with regulatory requirements. To protect sensitive business data and prevent unauthorized access, modification, or destruction of data within an organization's SAP systems, application security is critical. A good starting point is to check and implement the SAP security baseline. The SAP security baseline is a set of security configurations and best practices recommended by SAP. It covers a range of areas, including authentication, authorization, encryption, logging, and monitoring. Implementing the SAP security baseline can help to ensure that your SAP system is configured securely and that you are following industry best practices.

The implementation of SAP security baselines can assist in reducing the risk of a data breach or other security incidents. However, it's important to remember that the SAP security baseline is just a starting point. To fully secure your SAP system, you will need to go beyond the baseline and implement additional security controls based on other frameworks like ISO 27001 and 27002. There are several ways to integrate ISO controls into SAP.

One common approach is to map the ISO controls to SAP security controls. This involves identifying the SAP security controls that correspond to each ISO control and ensuring that they are implemented correctly in your SAP system. For example, the ISO control related to access control could be mapped to the SAP user access control functionality.

- The starting point for organizations to create an SAP security blueprint is to take the SAP security baseline and Secure Operations Map as a guideline. Check the different layers which are named in the SAP's security baseline and SOM and create a checklist for the SAP Application Layer, database, OS, interfaces (network), governance etc.
- Make use of existing ISO controls and translate them into checks that apply to the SAP landscape.
- Do this for on premise SAP solutions and for cloud apps like Ariba, SAC, etc. At least a proper authorization concept should be there and monitoring of audit logs (connection with SIEM in some cases) should be performed.
- We can use SAP tools like Security Recommendation Tool for missing SAP Security Notes, EWA (Early Watch Alerts) for monitoring the version of SAP (kernel), database and for missing security configurations, Solution Manager for having insight in landscape and monitoring, and SAP Read Access Logging for monitoring sensitive information.
- Another step is to create internal control and metrics which help you to track your progress. It also allows creating tools to increase the effectiveness and efficiency for implementing SAP business processes.

Fixing the core, low hanging fruit, without extensive tools and low effort

Have you faced challenges when attempting to address complex SAP security issues? Do you think it's better to address these issues first or to focus on the issues that can be fixed quickly?

SAP security is a critical component of any organization's overall security posture. The SAP system is a complex, multifaceted platform with many interdependent components, and securing it requires a multifaceted approach. However, the best first approach is to start with fixing the core and low-hanging fruit.

Fixing the core means identifying and addressing fundamental security flaws in the system. This includes things like securing the database, hardening the operating system, and ensuring that network access is properly controlled. These measures may seem basic, but they are essential to providing a solid foundation for more advanced security measures.

Low-hanging fruit refers to easy-to-fix vulnerabilities that can have a big impact on overall security. These vulnerabilities may include things like default users and weak passwords, unpatched software, and security parameters. By addressing these vulnerabilities first, organizations can make significant progress in improving their overall security posture without investing significant time or resources.

- Make use of SAP default tools like RSUSR003 and SUIM to check quickly on default SAP accounts and users with high authorizations like SAP_ALL profile and/or critical transactions like SE16.
- The SAP SIEM integration can come into the picture, which is part of cyber defense and cyber threat detection. It collects data from various applications, client and/or server OS, information from malware defense, suspicious port-scans, and event-data from business-critical systems.

- Tools like SAP ASE with its authentication & access control mechanisms ensure that only properly identified and authorized users can access data. Data encryption further protects sensitive data against theft and security breaches.
- The System Monitoring application in SAP Solution Manager provides an overview of the status of technical systems, including their associated instances, databases and hosts.
- Passwords for the authentication of users are subject to certain rules. These rules are defined in the SAP password policy. Identity Authentication provides you with two predefined password policies, in addition to which you can create and configure up to three custom password policies.

Using tools from trusted partners for Assessments/Scans

Do you also think you could use some help to manage SAP security by automation? In that case you could consider checking one of the existing SAP security vulnerability and management tools in the market. Fortunately, nowadays there are various tools from SAP security companies that will make it easier to manage SAP security.

There are tools and technologies from trusted partners to identify potential vulnerabilities and assess your systems' overall security posture. With these tools, you can develop a customized defense strategy to protect your valuable data from cyber threats. Employing technologically advanced tools for vulnerability assessment and management activities in SAP will comprehensively address the latest vulnerabilities in line with recent trends. Some of the tools offer real-time monitoring and alerting capabilities to quickly identify any suspicious activity and take immediate action to mitigate risks.

The approach to creating an SAP security blueprint is also suitable for comparing SAP security management tools. Check if your preferable tool covers the SAP security baseline elements and the ISO controls. Find out if it's possible and easy to connect the tool with your existing SIEM solution and if it meets your IT strategy. Some tools are only running from the cloud while some others are available both on-premises and cloud.

To conclude, securing SAP within a Blueprint necessitates the implementation of a comprehensive security plan that encompasses all aspects of the system. It is essential to regularly review and update the security plan to ensure that it remains effective against the evolving threat landscape.

About the authors:

Ali Cifci



Ali Cifci is an SAP Basis & Security consultant with more than 15 years of experience. He has worked on various migration and implementation projects of SAP solutions. Based on data and privacy protection regulations, he assesses SAP systems and advises organizations on potential risks and mitigations to manage them.

Mail: ali.cifci@capgemini.com

LinkedIn: <https://www.linkedin.com/in/cifci/>

Ankit Arya



Ankit is SAP Security and GRC consultant with 10 years of experience in various Leading Consulting roles, especially in Audit, Risk and Compliance Management. Ankit designed and implemented comprehensive business-driven security models for various SAP ERP products, in compliance with audit requirements.

Mail: ankit.arya@capgemini.com

LinkedIn: <https://www.linkedin.com/in/ankitarya1103/>



**BETTER SECURITY,
WITHOUT
COMPROMISING
PERFORMANCE**

Security apps are very useful, but how do you predict their impact on the performance of your systems?

Highlights

- Performance testing should be a part of any security product selection process.
 - System impact encompasses impact on CPU, RAM, storage, and configuration.
 - It is not feasible to test all scenarios. System testing may be the solution you need.
 - Strategies are available to ensure Performance Optimization or Resource Utilization.
 - Some security applications will not stand the test.
-

There is a wide range of security solutions available in the market. These solutions have all many and different advantages. Sadly, these advantages do not come for free. There is always a price with advantages and disadvantages – and the price cannot always be expressed in Euros.

When considering implementing a security application, functionality and limited financial costs are the main drivers. And of course, these considerations are important, but they do not cover everything. The introduction of a new security application impacts the computer system as a whole.

This is even more true in the case of security software. Consider, for example, a virus scanner that uses the main processor (CPU) to scan the system; by taking up all the CPU's capacity, there's nothing left to perform other tasks. In other words: you need to balance security needs with usability requirements.

Three system characteristics you should consider

In every effective IT system, three elements need to exist in harmony: the aforementioned CPU, the memory (RAM) and the storage (disk space). Together, these elements are known as IT system resources.

However, there is a fourth element that's often overlooked – until certain problems arise. This fourth element is the configuration. When several different applications use the same system resources, interactions will take place between the actions of the applications. As an example, you might consider an application that utilizes the IT system's own logging. Application A may require another log level than application B.

Effective or efficient handling of system resources.

Experienced IT system administrators need to know about each security application's peak load. And this is the moment where things get complicated. A security application is not always performing the same actions or using the same system resources. A virus scanner that is not doing anything uses fewer resources than a virus scanner that is actively removing viruses.

To uncover such important information, there are two predominant strategies: Peak Performance Optimization (PPO) and Peak Resource Utilization (PRU). In PPO, the goal is to realize a system that runs as effectively as possible; security applications should always be able to perform their primary task with minimal resource issues. In PRU, however, the goal is to realize a system that runs as efficiently as possible; security applications should always use as many system resources as possible in performing their primary task.

Of course, reality is more nuanced than this, but in the end both strategies focus on the same question: 'how many resources does that security application use?'

Whichever strategy you choose, you should always proceed with care. Of course, when adopting a PPO strategy, you could decide to just add more system resources, but you should not do so without a proper analysis.

Seven tests to predict impact

Measuring is knowing – but measuring can be hard. The three main system resources will fluctuate when the security application is in use. Moreover, these resources are impacted by configuration differences in the system. All in all, the number of variables that impact each other is significant.

Instead of measuring every scenario and putting the resulting data in a table, we prefer to use system testing methods. In system testing, the system is tested as a whole, instead of per system component as is usually the case in unit testing.

TECHNOLOGY - FOCUSED SECURITY ASPECTS

The developer of the application will probably have performed these tests in generic scenarios. However, this does not guarantee that the results will be the same on every system; differences in configuration can have a big impact.

Table 1 provides an overview of what you may expect from the developer, and of the tests you could consider performing yourself.

Every good test has sharply defined acceptance criteria

Determining whether the results of a test are good or bad should always be done on the basis of sharply defined acceptance criteria. Such criteria should

be established prior to the test and be aligned with the chosen strategy; either PPO or PRU.

Acceptation criteria are often documented as 'what to test' – the test scenario – in combination with the expected results of the test. As such, it is crucial to describe the expectations as thoroughly as possible. Once we have defined these cases, we can start thinking about the test data we'll need to measure the results.

As this is getting abstract, let's take a look at an example. In the tables below, we're performing a performance test. To be precise, we're testing CPU use during virus scanning, on a laptop.

At this point, the next steps are clear. We are taking a laptop, installing the application and analyzing the results. Next, we complete the table with test results and evaluation.

SOFTWARE TEST TYPE	DESCRIPTION	PERFORMED BY DEVELOPER	FOR YOUR CONSIDERATION
Functionality Testing	Confirmation that the security application functions correctly		
Recoverability Testing	Confirmation that the security application can deal with faulty input without breaking down		
Interoperability Testing	Confirmation that the security application can work together with other applications		
Performance Testing	Confirmation that the security application, in specific scenarios, stays within the bandwidth of the system resources		
Regression Testing	Confirmation that the security application and all its related sub systems function correctly		
Usability Testing	Confirmation that users and/or systems are able to use the security application as it is intended to be used		
Migration Testing	Confirmation that the security application can be migrated to a new system or infrastructure without trouble		

Table 1

Test Case ID	Test Naam	What to Test	Expected Results	Test Data	Actual Results	Pass/Fail
001	CPU use during virus scan	Total CPU consumption of virus scanner while performing a virus scan on a laptop	20% CPU Consumption by virus scanner	CPU Consumption of all processes on the laptop		

Table 2

Test Case ID	Test Naam	What to Test	Expected Results	Test Data	Actual Results	Pass/Fail
001	CPU use during virus scan	Total CPU consumption of virus scanner while performing a virus scan on a laptop	20% CPU Consumption by virus scanner	CPU Consumption of all processes on the laptop	15% CPU Consumption by virus scanner	Pass, 15% is lower than the expected 20%

Table 3

The most realistic acceptance criteria are the best acceptance criteria

Of course, we can draw up thousands of test cases to cover every possible aspect, but in reality, we see there is only a handful of test cases that are always relevant. These test cases focus on the primary system characteristics:

- Is the CPU up to the task?
- Do we have enough RAM?
- Do we have enough disk space?

Of course, every commercial product will include this information. You can interpret 'minimum system requirements' as the average resource consumption. Possibly, the product will list the 'recommended system requirements'; this considers load peaks. If this is the case, you only need to take into account any areas in your

environment that may deviate from the norm, i.e. applications or systems developed in-house and unavailable to the public.

Finally, you need to take the configurations into account. Here, too, the developer will supply specifications that are similar to those used in their own testing. The most common configuration requirements have to do with virus scanners and firewalls around the application.

Sometimes, the answer is simply: 'no'.

We often see that testing is only discussed after the security application has been selected. And of course, it is not realistic to request a full test of all possible applications. What is possible, however, is to formulate a definition of success prior to selection. You should define beforehand what you expect with regard to useability or

interoperability testing of the security application. On top of that, a smoke test in a testing environment may also be very valuable.

Sometimes a security application just does not work within an existing environment. So, sometimes, you just have to say 'no' and look for another security application. But if you do so, make sure you have an effective testing plan on stand-by.

TECHNOLOGY - FOCUSED SECURITY ASPECTS

About the authors

Sebastiaan de Vries



Sebastiaan de Vries is an experienced security expert. Next to his technical expertise, he is always fully up to speed with the latest compliance standards. His aim is to help customers transform security from a necessity into an advantage.

LinkedIn: <https://www.linkedin.com/in/gpdevries/>

Laura Adelaar



Laura is a cybersecurity consultant with an affinity for AI security options. Thanks to her background in communication and expertise in data centers, Laura brings a broad perspective to the table.

Mail: laura.adelaar@capgemini.com

LinkedIn: <https://nl.linkedin.com/in/laura-adelaar-38728758/>

Dennis van de Water



Dennis is a versatile Cybersecurity Consultant at Capgemini who has in-depth knowledge of both EDR solutions and cyber crisis management. He has extensive experience with setting up and designing cybersecurity solutions with a focus on EDR tooling, consulting on EDR tooling and cyber crisis management and developing cyber crisis simulations.

Mail: dennis.vande.water@capgemini.com

LinkedIn: <https://www.linkedin.com/in/dennis-van-de-water/>

Jeroen van Hulst



Jeroen is a highly technical cybersecurity specialist who brings together IT and strategy. With his background in both IT and OT R&D, he has managed a broad range of projects from developing vulnerability management solutions for governmental organizations to building enterprise cloud environments for the delivery of security services to multiple clients around the world.

Mail: jeroen.van.hulst@capgemini.com

LinkedIn: <https://www.linkedin.com/in/jeroen-van-hulst-aa863b97/>

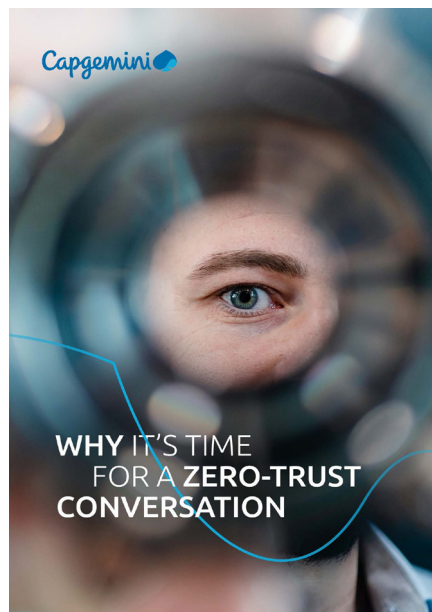
Publications:

In addition to the Trends in Cybersecurity report, we also publish other reports, studies, and whitepapers that may be relevant to you. Below, you will find a concise overview. The complete list can be found at <https://www.capgemini.com/>.



Trends in Cybersecurity 2022 – Secure an accelerated digital transformation.

Cybersecurity is a necessity within every company, providing a secure foundation for transformation and supporting all operations. How do you ensure overview and control of your cyber risk program? How quickly can you return to your daily activities when cybercrime impacts your organization? And does your organization have a scalable approach when it comes to IT security?



Why we need to talk about Zero Trust

Zero trust is here to stay. Zero trust concepts are even starting to find their way into new regulations. So, it's clearly much more than just a passing trend.

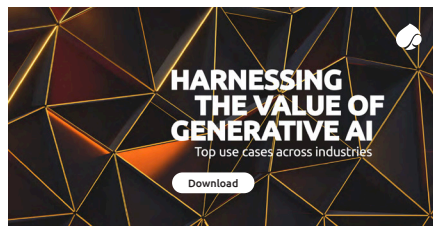
The name 'zero trust security' says it all: when it comes to cybersecurity, you can't trust anything or anyone. Every user is treated with suspicion, until proven otherwise. This may not sound friendly, but this approach ensures that people can securely (co)work, wherever and whenever they want. By adopting zero trust, organizations shift their primary focus to securing information across all platforms. That's why it's time to talk about zero trust, high time.



Transformation Essentials

Digital transformation is essential for a company to survive and differentiate itself from the competition. But how do you do it? What are the 'Transformation Essentials' required for success?

Get inspired by reading, listening, and watching practical examples of organizations in transition in the areas of technology, company culture, and processes. Each with their own challenges, at their own pace, but with the same goal: control of tomorrow.



Generative AI in Organizations

70% of executives believe that generative AI broadens the scope for knowledge workers in their company. Almost all executives (96%) acknowledge that generative AI is a significant topic for their organization. This is revealed in the latest report from the Capgemini Research Institute, 'Harnessing the value of generative AI: Top use cases across industries,' which explores the transformative power of generative AI for innovation within enterprises.

Colophon:

This report was prepared in collaboration with contributions from Bart van Riel, Martijn Gardenier, Natasja Pieterman, Anton Enkelaar, Marieke van de Putte, Hans Marcus, Serge Dujardin, Folkert Visser, Werner Branje, Mohit Sikka, Giselle van Wissen, Storm Poot, and Thomas de Klerk.

Advice, design, and production were provided by Johanna Achterberg and Arindam Dey from the Marketing & Communication team of Capgemini Netherlands B.V.

A large, decorative blue line that starts as a light blue curve on the left, rises to a peak, dips slightly, and then rises again towards the right.

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 360,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2022 global revenues of €22 billion.

GET THE FUTURE YOU WANT | www.capgemini.nl

Capgemini Nederland B.V.
Postbus 2575 - 3500 GN Utrecht
Tel. + 31 30 203 05 00
www.capgemini.nl