Digital Trust

safeguarding tomorrow's security

January 2025

table of contents

acknowledgements

Author

Ying Shaowei
Chief Scientist, NCS

Ying Shaowei coordinates the efforts of NCS' centres of innovation and centres of excellence, including leading one or more of these centres. He builds a global network of technology experts and research institutions which NCS leverages to accelerate client development and delivery work.

Shaowei champions selected innovation programmes or practices by providing executive sponsorship and directing investment funding. He also provides advice to the NCS corporate strategy on new potential market spaces and technology trends to invest and innovate in. Equally important is Shaowei's role in developing the Voice of NCS on emerging technologies and helping to radiate NCS' long-term perspectives on important technology topics that impact businesses.

Contributors

Cyber

Lim Hoon Wei
Principal Director, Cyber Special Ops and R&D

Daniel Ong
Senior Consultant, Cyber Management

Choon Hock Niow
Senior Consultant, Cyber Special Ops and R&D

Farren Tang
Senior Data Scientist, Cyber Special Ops and R&D

Nay Oo
Lead Data Scientist, Cyber Special Ops and R&D

Shantanu Chakrabarty
Senior Research Scientist, Cyber Special Ops and R&D

Ameera Adnan
Consultant, Cyber Special Ops and R&D

NEXT

Dr. Sunil Sivadas
Practice Lead, NEXT Gen Tech

External

John Buselli
Business Development Executive/Offering Manager, IBM Research

Editorial support

Georgia Swanson
Director of Strategy & Growth, NCS NEXT Global Innovation

Mark Addy
Insights Lead, NCS NEXT, Global Innovation

Deirdre Chong
Visual Designer, NEXT Open Innovation

foreword

Maintaining and enhancing Digital Trust has never been more important. The vast majority of organisations, across all sectors, currently rely on security frameworks that are intrinsically based on implicit trust – the idea that all users within a defined system are trustworthy until proven otherwise. Given the complexity of 5G networks, and the very real security issues that quantum computing presents, implicit trust is no longer good enough. There is an immediate need for organisations to begin to implement context-aware security frameworks, based on zero trust, that specifically address the quantum threat.

NCS has invested extensively in human and technological capabilities to develop and implement forward-looking security solutions that the current (and future) digital environment requires. Through our experience conducting research, collaborating with industry peers and government entities, and developing and implementing security solutions, at every layer of the software and hardware stack, we've gained the expertise and understanding of the security required to ensure Digital Trust. We share some of that expertise with you in this report.

digital trust

This document explains the importance of maintaining and expanding Digital Trust, and the questions organisations should ask about zero trust adoption, the role of Artificial Intelligence (AI) and Natural Language Processing (NLP) in enhancing Security Operations Centre (SOC) efficiency, migration to post-quantum security, and 5G security.

Embracing zero trust in cybersecurity: Strategies and challenges for effective implementation: Details the immediate need for zero trust implementation and the technologies required and provides a model and recommendations for a phased approach to implementation.

Managing risks and opportunities for quantum-safe development: Explains the urgency of the quantum computing threat to existing security solutions and details the journey to post-quantum security with respect to risk tolerance and current security posture, strategy, planning, governance, technologies, and organisational capabilities.

A framework for evaluating 5G security solutions based on use case and level of security: Provides a framework for assessing the impact of security features and configurations on 5G network user equipment performance.

Phishing detection: Outlines how NCS has combined Natural Language Processing (NLP) and computer vision to create a system that provides superior detection of phishing attacks.

Engineering cyber resilient OT systems for offshore infrastructure: Discusses the systematic approach required for securing Operational Technology (OT) in critical offshore windfarm substations, focusing on compliance, stakeholder alignment, and best practices for integrating security controls across complex engineering phases, referencing PD CLC/TS 50701 and IEC 62443 standards.

Cryptography as the last line of defence: Highlights cryptography's role as the final layer in a zero trust model, addressing the importance of cryptographic visibility and agility to adapt to evolving threats. Emphasises best practices in cryptographic hygiene to maintain secure and resilient data protection.

The immediacy of the need to migrate to zero trust and post-quantum security is undeniable. We hope that you find the information contained in this report useful and would welcome the opportunity to explain how NCS can partner with you to provide the security required to maintain and expand your organisation's Digital Trust.

introduction

Digital Trust represents the vital intersection of technology and trust in a rapidly transforming digital landscape. It embodies the mission to create ethical, secure, and responsible technology, covering diverse areas such as cybersecurity, responsible Artificial Intelligence (AI), explainable AI, next-generation privacy management, scam detection, post-quantum encryption, trusted execution environments, and federated learning.

The promise of Digital Trust extends to the forefront of technological innovation and is critical to the integration of emerging concepts such as decentralised identity, biometric authentication, privacy-preserving computation, AI transparency, and blockchain-enabled security. It is not just about future-proofing our technology, but also about shaping the evolution of digital society to ensure that the reliability and integrity of technology is deeply ingrained.

Digital Trust also addresses our commitment to the ethical use of technology. It recognises the increasing importance of maintaining privacy, ensuring robust security, and promoting responsible and transparent AI practices in our hyper-connected world. This commitment is mirrored in our roadmap for the development of next-generation solutions that embed trust into their very fabrics, ensuring that the technology we create, and use, is aligned with our fundamental rights and values.

The emphasis we put on Digital Trust is not intended merely to make our technology more reliable, but to foster an inclusive, equitable, and safe digital future – a future that we can all trust and be part of. It is about ensuring that our digital evolution is guided by ethical principles, societal needs, and a commitment to improve life, in all its diversity, for everyone.

At NCS TechCoE, our work on Digital Trust goes beyond addressing the challenges of today and delves into forecasting and shaping the future of ethical, safe, and equitable digital interactions. We are tirelessly working on pioneering projects that promote cybersecurity, explainable and responsible AI, next-generation privacy management, post-quantum encryption, and much more. We're developing strategies to counter fraud, and actively exploring trusted execution environments and federated learning.

Our mission is to weave trust into every technological innovation, so that Digital Trust isn't an afterthought, but a fundamental principle that guides our work. We foresee a future where technology does not merely serve us, but also respects our values, our privacy, and our rights.

We invite everyone to join us on this exciting journey and we are eager to collaborate, share ideas, and continue innovating. The field of Digital Trust is ripe with opportunity for discovery and growth, and we look forward to building this future with you. Let's uphold the banner of Digital Trust together to shape a digital world where trust is the norm, not the exception.

Asking the Right Questions (ARQ) about Digital Trust

Hoon Wei Lim

Asking the Right Questions (ARQ) about Digital Trust

Hoon Wei Lim

Securing digital transformation

Digital Trust is a necessity in a world where digital technologies support and intermediate virtually all economic transactions, social connections, and institutions. It is the expectation of individuals that digital technologies and services, and the organisations providing them, will protect all stakeholder interests and uphold societal expectations and values [WEF22]. The core of Digital Trust is the notion that we need to safeguard:

- Data
- Artificial Intelligence (AI)
- Digital identity, and
- Systems and infrastructure

There are already well-established and mature cybersecurity solutions for securing systems and infrastructure, including firewalls and software for network intrusion detection and prevention, malware analysis and detection, and vulnerability scanning. In this paper, we will focus on what we believe will be crucial to delivering trustworthy digital technologies and services going forward.

In the realm of Digital Trust, three critical security aspects stand out from traditional cybersecurity paradigms. Each aspect addresses specific challenges inherent to the evolving digital landscape:

- **Digital identity management:** In expansive digital domains such as the Metaverse, and within the context of cryptocurrencies in particular, the preservation of digital identity becomes paramount. Protecting individuals and organisations from impersonation and fraud is a multifaceted challenge. Innovative solutions, such as biometric authentication, decentralised identity frameworks, and blockchain technology, are crucial to establishing and safeguarding digital identities. The goal of digital identity management is to create robust systems that can reliably authenticate and verify the digital personas of users to ensure trust and security in virtual spaces.
- **Data privacy:** As our transactions and data processing activities increasingly migrate to the cloud, ensuring the confidentiality of sensitive data, especially Personally Identifiable Information (PII), is imperative. Encryption, secure data transmission protocols, and robust access controls are integral to safeguarding data privacy. Additionally, compliance with data protection regulations, like GDPR, plays a pivotal role in establishing transparent and ethical data practices and fosters trust among users regarding the secure handling of their information in digital environments.
- **AI security:** The rapid advancement of AI introduces a new and unique set of security challenges. Embedding security into AI systems is crucial to preventing malicious or unethical use. Adversarial attacks, biased algorithms, and unintended consequences are potential pitfalls. Implementing secure development practices, robust testing procedures, and ongoing monitoring is essential. Ethical considerations, explainability, and accountability frameworks are also vital in ensuring the responsible deployment of AI technologies. Collaborative efforts across industries and interdisciplinary approaches are necessary to stay ahead of evolving threats in the AI landscape.

To address these aspects of Digital Trust, a holistic and proactive approach is essential. The convergence of technological innovations, regulatory frameworks, and ethical considerations forms the foundation for building resilient, secure, and trustworthy digital ecosystems.

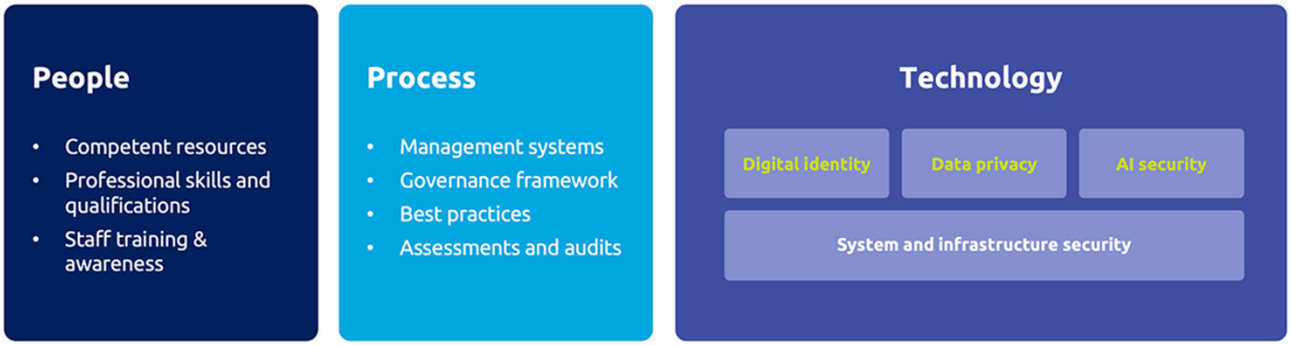


Figure 1: Building blocks of Digital Trust

That said, in building a trustworthy digital economy and society, it is crucial to recognise that technology alone is insufficient. As illustrated in Figure 1, consideration must extend to the people and process aspects when operationalising Digital Trust.

People

- Competent resources: Developing Digital Trust requires a workforce equipped with the necessary professional skillsets and qualifications. Competent resources ensure the effective implementation and management of a variety of emerging technologies that are critical for building and maintaining trust.
- Continuous staff upskilling and training: The dynamic nature of technology requires a workforce that is adaptable and continuously upskilled. Regular training programmes are essential to keep employees abreast of the latest developments, security threats, and best practices, ensuring that they can effectively contribute to Digital Trust initiatives.
- Creating awareness: Organisations must foster awareness of the significance of Digital Trust within their workforces. This includes an understanding of the impact of employee actions on cybersecurity and overall trustworthiness. Employee awareness campaigns contribute to a culture that values and prioritises Digital Trust.

Process

- Management systems and governance frameworks: Establishing proper governance frameworks and management systems is crucial for guiding employees in executing digital transformation initiatives. These frameworks will provide a structured approach to decision-making, risk management, and compliance, ensuring that technology adoption is aligned with the goals of Digital Trust.
- Regular assessments and audits: To identify and rectify potential risks or gaps associated with cybersecurity and Digital Trust, organisations should conduct regular assessments and audits. These evaluations will help in proactively addressing vulnerabilities, enhancing security measures, and maintaining the integrity of digital systems.

In summary, people and process elements are integral components of a strategy to cultivate Digital Trust. By investing in competent resources, fostering continuous upskilling, creating awareness, and implementing robust governance frameworks and assessment procedures, organisations can fortify their digital ecosystems and create trust among users and stakeholders.

In the remainder of this article, we will investigate a set of questions that should be asked by organisations in their digital transformation journeys. The questions and their associated Digital Trust elements are summarised in the table below.

Questions	Digital Trust elements		
	Digital identity and data privacy	AI for security and securing AI	System and infrastructure security
1. Can zero trust be the silver bullet for Digital Trust?	✓		
2. How to wield the double-edged sword of Generative AI?		✓	
3. How can NLP and Generative AI be game changers for Security Operation Centre efficiency?		✓	
4. Is ignoring post-quantum security today, a recipe for disaster tomorrow?	✓		
5. Are we ready for the security requirements of 5G?			✓

Table 1: Mapping from Asking the Right Questions to Digital Trust elements

Q1: Can zero trust be the silver bullet for Digital Trust?

Interest in zero trust security has been largely driven by government mandates, vendor hype, ransomware attacks, and the needs of a hybrid workforce. According to Gartner, over 60% of organisations will embrace zero trust as a starting point for their cybersecurity strategies by 2025 [WDKW22].

Key value of zero trust

Prevailing IT security architectures depend on 'implicit trust', which is granted once certain criteria are met, such as when a user is inside a corporate network. This is a vulnerability that demands remediation to prevent excessive access, as users have relatively unrestricted access to resources once inside the network under implicit trust protocols. The zero trust model dismantles implicit trust, ushering in a paradigm where trust is continuously assessed, explicitly calculated, and dynamically adaptive, contingent on identity and context. This model serves as a guiding principle for security strategies that not only define the architectural landscape but also enhance security posture and fortify cyber resilience. Organisations embracing the zero trust mindset and architecture stand to gain two pivotal technical outcomes:

- **Resilient infrastructure:** Zero trust principles significantly bolster the resiliency of IT infrastructures. A zero trust network, crafted to operate even in the presence of adversaries, excels at containing and managing incidents. This proactive approach diminishes the likelihood of business-impacting events such as ransomware attacks, data compromises, and malware infections. The consequent reduction in risk that zero trust models provide, contributes to the overall robustness and security of the business.
- **Adaptive work environment:** Modern work environments must be adaptable to accommodate the anticipated hybrid nature of work in the future. Zero trust principles seamlessly support remote workers' use of both managed and unmanaged devices, remote data (e.g., IaaS), and remote applications (e.g., SaaS). A secure zero trust implementation enables the realisation of an 'anywhere, any time, on any appropriate device' approach that will be crucial for supporting a dynamic and hybrid workforce.

From zero trust to Digital Trust

A zero trust approach can play a pivotal role in achieving overall Digital Trust by redefining traditional security paradigms, fortifying defences, and instilling confidence in users engaged in digital interactions. As digital transformation accelerates, the conventional approach of assuming trust is no longer tenable, prompting the need for a more sophisticated and proactive security model that emphasises continuous verification, explicit calculation, and adaptive trust based on identity and context. Here are some examples of how zero trust can enable Digital Trust:

- **Digital identity management:** Digital identity is the cornerstone of secure online interactions. Zero trust challenges the conventional notion of trusting users and devices by default. Instead, it advocates continuous authentication and authorisation, ensuring that trust is earned and maintained throughout the digital journey. Zero trust models leverage multifactor authentication, biometrics, and contextual information to establish and validate identities. This meticulous scrutiny reduces the risk of unauthorised access, identity theft, and impersonation. By embracing zero trust principles in digital identity management, organisations enhance their ability to safeguard user identities across various platforms, including the Metaverse and cryptocurrency ecosystems. The continuous assessment of digital identities fosters confidence among users that their online personas are protected, thereby contributing to the establishment of Digital Trust.
- **Data privacy:** Zero trust can be extended to data privacy, which is a critical concern in an era marked by cloud-based transactions and ubiquitous data processing. In a zero trust architecture, the default assumption is that no entity, whether internal or external, should be implicitly trusted. This approach is particularly relevant when transacting and processing sensitive data, including personally identifiable information. Implementing zero trust in data privacy involves encryption, secure data transmission protocols, and robust access controls. By assuming a position of continuous scrutiny, organisations employing zero trust frameworks are better equipped to detect and thwart potential data breaches. This not only enhances the confidentiality of sensitive information but also instils confidence among users that their data is being handled with the utmost care and security.
- **AI security:** As the influence of AI grows, so does the need to secure AI systems from malicious exploitation. Zero trust principles are instrumental in embedding security into AI processes. The rapid evolution of AI technology introduces potential risks including adversarial attacks and unintended consequences. Zero trust in AI security involves integrating security measures into the development lifecycle of AI systems. This includes secure development practices, robust testing, and ongoing monitoring. Moreover, ethical considerations such as transparency, fairness, and accountability are integral to the responsible deployment of AI. By adopting a zero trust approach to AI security, organisations can mitigate the risks associated with the malicious use of AI, thereby reinforcing Digital Trust.

Where are we today?

The implementation of zero trust technologies marks a fundamental shift from traditional network security practices, and while the benefits are manifold in enhancing organisational security posture, the transition to zero trust is far from straightforward. It requires a meticulous rethinking of network design and access strategies, with several challenges that demand attention.

The implementation of a zero trust architecture often brings about considerable operational overhead expenses. This is the case because zero trust mandates the continuous verification of all users and devices trying to access the network, regardless of whether they are inside or outside the organisation's perimeters. For example, an organisation may need to frequently update and monitor access policies to ensure that they accurately reflect the current threat landscape and access needs, a process that can be both time-consuming and labour-intensive.

Furthermore, extending zero trust principles to legacy systems presents a unique set of complications. Older systems were not designed with zero trust in mind, and many lack the necessary interfaces to support modern authentication and authorisation protocols. A typical example can be found in manufacturing firms, where legacy industrial control systems, essential for day-to-day operations, may not support the latest security protocols. Retrofitting these systems to align with zero trust principles can be a resource-intensive task that requires both innovative technical solutions and substantial investment.

Another critical challenge is the scarcity of resources with the requisite skillsets. Zero trust is a relatively new and evolving concept, and there is a limited pool of professionals that has extensive experience in implementing such frameworks. For example, an organisation may struggle to find IT professionals who are adept at configuring the sophisticated access control policies required by a zero trust architecture, or who have the expertise required to manage the sophisticated network segmentation strategies it entails.

In summary, while the zero trust model offers a robust framework for securing modern digital assets, the path to its successful implementation is laden with operational, technical, and human resource hurdles. Addressing these challenges requires a well-structured approach, investment in the right technology, and most importantly, the cultivation of a skilled workforce capable of navigating the complexities of zero trust implementation. It is a complex journey, but one that can lead to a significantly more secure IT environment for organisations willing to make the commitment.

Q2: Taming the machine: How to govern AI for good?

AI security is a key enabler of Digital Trust as AI-supported applications and services are becoming pervasive. AI governance, in turn, sets the foundation, including the overall culture and structure for managing AI risk within an organisation to ensure ethical, lawful, and reliable use of AI in a manner that earns public trust.

Generative AI (GenAI) can be used to create a wide variety of content including text, code, images, and videos. This content can be used with good or malicious intent, so it is important to have safeguards in place to prevent GenAI from being used for malicious purposes.

To address the ethical and societal concerns surrounding AI (including GenAI), it is essential to develop and operationalise effective organisational governance frameworks. These frameworks should be designed to ensure that AI is used in a responsible and ethical manner.

Some of the overarching principles of effective AI governance include:

- **Transparency:** AI systems should be designed in a way that is transparent and accountable. This means that it should be possible to understand how these systems work and to identify the biases that they may contain.
- **Fairness:** AI systems should be designed in a way that is fair and does not discriminate against any particular group of people. This means that AI systems should be trained on datasets that are representative of the population and that they should be used in a way that does not perpetuate existing biases.
- **Accountability:** There should be clear lines of accountability for the development and use of AI systems, and it should be made clear who is responsible for ensuring that these systems are used in a responsible and ethical manner.
- **Safety:** AI systems should be designed in a way that is safe and does not pose a risk to human safety or security. This means that AI systems should be tested for potential vulnerabilities and that they should be equipped with safeguards to prevent misuse.
- **Privacy:** AI systems should respect user privacy and should not collect or use any personal data without a user's consent.

Once we have defined our overarching AI principles, we need to develop a governance framework that sets out how these principles will be put into practice. This framework should include policies and procedures for the development, deployment, monitoring, and evaluation of AI systems.

With the rise of GenAI tools such as ChatGPT, some recommended practices that organisations should adopt to ensure a responsible approach to AI include (using ChatGPT as an example):

- **Approve only a certain set of use cases:** Decide which use cases for ChatGPT are acceptable and which ones are not. For example, organisations might want to allow ChatGPT to be used to generate personalised learning materials for students, but not to create fake news articles or deepfakes.
- **Avoid usage of certain input data:** ChatGPT was trained on a massive dataset of text and code which could have contained personal information, confidential data, or biased content. It is important to avoid using ChatGPT to process any type of data that is sensitive or that could be used to harm or discriminate against individuals or groups.
- **Verify the accuracy of output from ChatGPT:** ChatGPT is a powerful language model, but it is not perfect. It is important to verify the accuracy of any output from ChatGPT before using it. This is especially important for high-stakes applications such as ChatGPT use for medical diagnosis or legal decision-making.
- **Consider legal issues:** When using ChatGPT, it is important to be aware of the relevant laws and regulations. For example, organisations need to ensure that they are not violating any privacy laws when collecting or processing data and that they are not infringing on any copyrights when generating content.

In addition to these recommendations, it is also important to be transparent about how ChatGPT is used. Users need to know what data is being collected, how it is being used, and what they can expect from the output of the model. It is also important to have a process in place for users to report any problems or concerns they have about the use of ChatGPT. By taking these steps, organisations will go a long way in ensuring that ChatGPT is used in a responsible and ethical way.

For further details, the U.S. National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF) serves as a comprehensive resource for organisations of all sizes, to manage AI risks effectively and to promote both trust and the responsible use of AI technology [AI-RMF23]. Figure 2 summarises the core functions of the NIST AI RMF:

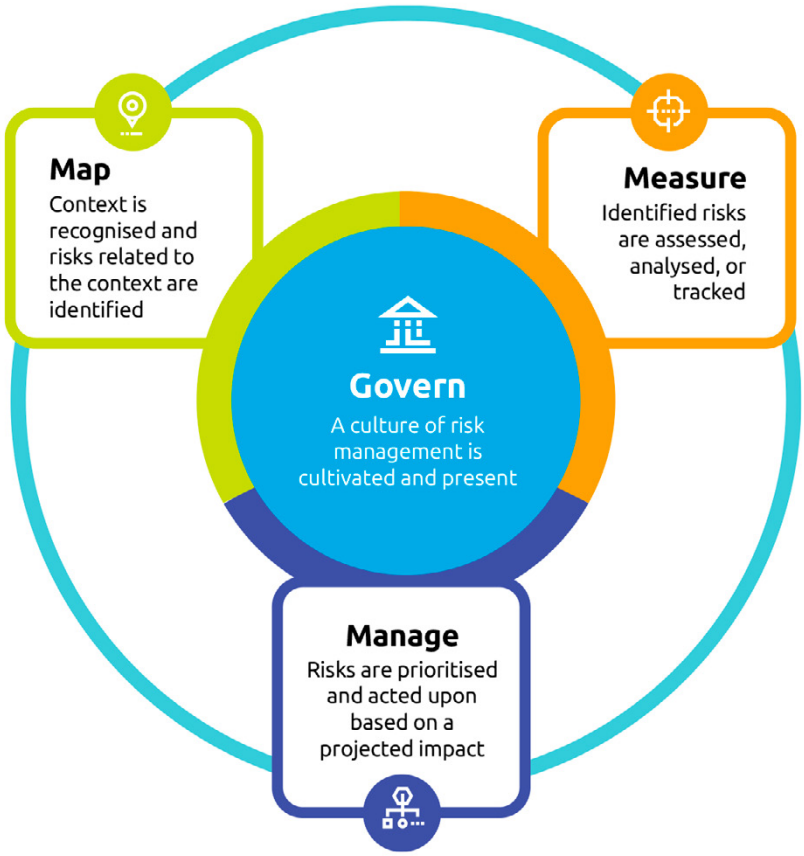


Figure 2: Core functions of the NIST AI Risk Management Framework

Q3: Can NLP and Generative AI be game changers for Security Operation Centre efficiency?

In today's digital landscape, where Digital Trust is at stake and cyber threats are increasingly sophisticated, organisations must prioritise robust security measures to protect their assets, data, and reputations. Security monitoring solutions play a crucial role through the continuous surveillance and analysis of an organisation's security posture to detect, respond to, and mitigate potential threats in real time. A Security Operations Centre (SOC) serves as the 'command centre' for these activities, ensuring that organisations can effectively manage and mitigate cyber risks.

However, the operational challenges that come with running an efficient SOC can be daunting. As an example, the effort required to process and review large volumes of security alerts can lead to 'alert fatigue' among SOC analysts that can potentially result in cybersecurity attacks that aren't detected. The integration of GenAI and NLP holds the potential to be 'game changing' for SOC efficiency.

It is important to understand the current role of NLP in SOC operations, and the differences between NLP and GenAI, before explaining how the combination of the two can improve both SOC efficiency and the security posture of an organisation.

NLP for Security Operations Centre (SOC) use cases

Natural Language Processing (NLP) plays a significant role in enhancing cybersecurity monitoring and threat detection by enabling machines to understand, interpret, and respond to human language. Here are five examples of how NLP can be useful:

- **Log analysis and anomaly detection:** NLP can be used to analyse logs and security events to extract meaningful information from unstructured log data. By understanding natural language patterns in logs, NLP algorithms can identify anomalies or potential security incidents that may go unnoticed through traditional detection methods.
- **Threat intelligence and incident monitoring:** NLP can be applied to process and analyse threat intelligence feeds, security blogs, news articles, and social media to identify emerging threats and vulnerabilities. Security teams can stay informed about the latest cyber threats by using NLP to extract relevant information and perform sentiment analysis.
- **Phishing detection and email security:** NLP can enhance email security by analysing the content of emails and identifying phishing attempts. It can detect suspicious language, unusual patterns, or social engineering techniques, helping to filter out malicious emails and protect users from phishing attacks.
- **Incident response and chatbot security assistants:** NLP-powered chatbots can provide immediate assistance during security incidents. Users can interact with a chatbot in natural language to report incidents, ask security-related questions, or receive guidance on security best practices. Use of NLP chatbots will enhance incident response capabilities and help improve communication between security teams and end-users.
- **User behaviour analytics and insider threat detection:** NLP can be used to analyse user behaviour patterns in communication channels such as email, chat logs, and collaboration platforms. With their ability to understand natural language context, NLP algorithms can detect anomalies in user behaviour that may indicate insider threats, unauthorised access, or compromised accounts.

These examples illustrate how leveraging NLP for cybersecurity monitoring and threat detection enables a more sophisticated and context-aware approach to identifying and responding to security incidents. NLP enhances the capabilities of security systems by processing and understanding human language, thereby improving the overall effectiveness of cybersecurity measures.

While NLP offers valuable capabilities for cybersecurity monitoring, it also comes with certain limitations:

- **Evading linguistic analysis:** Sophisticated attackers can intentionally craft messages to evade linguistic analysis. They may use obfuscation techniques, encryption, or slang to communicate without triggering NLP-based threat detection. This makes it difficult for NLP systems to consistently identify and interpret malicious communications.
- **Limited support for unstructured data:** NLP is more effective for analysing structured data than unstructured data. While it can analyse textual content, much of the relevant cybersecurity information exists in unstructured forms such as log files, network traffic, and system events. Extracting actionable insights from these unstructured sources poses challenges for NLP.
- **Dependency on quality and quantity of training data:** The effectiveness of NLP models depends heavily on the quality and quantity of training data. If the training data is not representative of the diverse language used in cybersecurity contexts, the model may struggle to accurately identify threats. Additionally, biases present in the training data may be perpetuated in the model's outputs.
- **Handling new and evolving threats:** NLP models may struggle to adapt quickly to new and evolving cyber threats. Traditional rule-based systems may be more adept at handling novel attack methods, as NLP models often require retraining with new data to effectively detect emerging threats. The lag in adaptation can pose a significant limitation in fast-paced and dynamic cybersecurity environments.

While NLP provides valuable insights, it should be complemented with other technologies and methodologies to create a comprehensive and resilient cybersecurity strategy.

Generative AI vs NLP

Neither Generative AI (GenAI) nor NLP is inherently superior or inferior to the other, but rather, they serve different purposes and can complement each other across applications. Both are valuable technologies, and their strengths lie in different domains.

GenAI excels at creating new content, whether that be text, images, or other forms of data. It can generate realistic and contextually relevant content based on patterns it has learned during training. It is often used for content creation, creative tasks, text generation, and the simulation of diverse data scenarios. In contrast, NLP focuses on understanding and processing natural language. It deals with tasks such as language understanding, sentiment analysis, text classification, and named entity recognition. It is widely used for applications such as chatbots, language translation, sentiment analysis, and information extraction from textual data.

GenAI, therefore, can be used to complement NLP in multiple aspects. For example:

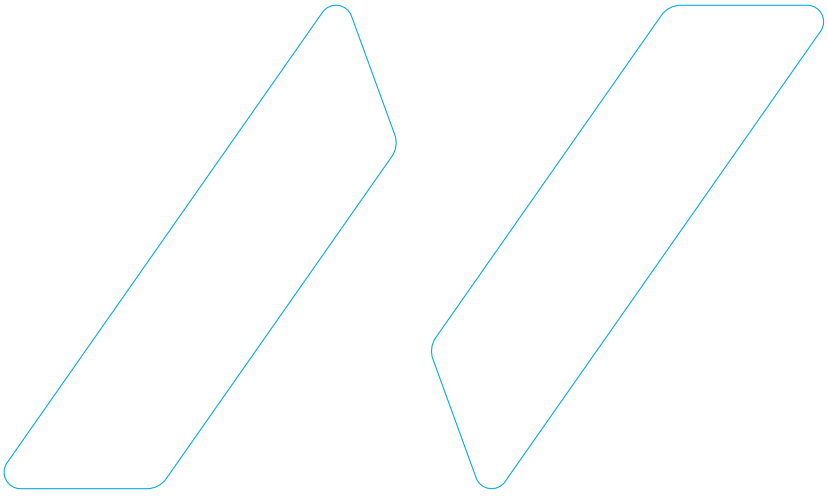
- **Content augmentation:** GenAI can be used to generate diverse and synthetic data, which can be used to augment training datasets for NLP models. This will help improve the robustness and generalisation of NLP systems.
- **Simulating real-world scenarios:** Generative models can simulate realistic scenarios, including cyber threats, which can be valuable for training and testing NLP-based threat detection systems. This can be especially useful when real-world threat data may be limited due to privacy concerns.
- **Enhancing training data quality:** By generating additional data instances, GenAI can be used to overcome limitations in training data quality by generating additional data instances that provide added context and diversity to NLP models.
- **Addressing data privacy concerns:** Generative models can generate synthetic content without relying on real incident data which helps address the privacy concerns associated with using actual threat data for training NLP models.
- **Improving response to new threats:** GenAI can be employed to simulate new and evolving cyber threats, allowing security teams to proactively prepare for, and detect, emerging threats. This complements the reactive nature of NLP-based threat detection.

Enhancement to SOC capabilities

Combining GenAI and NLP can significantly enhance the capabilities of an SOC by providing a more comprehensive and adaptive approach to cybersecurity. This can be summarised as follows:

- **Threat intelligence augmentation:** GenAI can create synthetic threat scenarios to simulate diverse and evolving attack vectors. NLP processes and understands threat intelligence feeds and extracts relevant information about known vulnerabilities, tactics, techniques, and procedures (TTPs). By integrating the synthetic scenarios from GenAI with the understanding of real-world threats NLP brings, SOC teams gain a more enriched and dynamic threat intelligence dataset. This will aid in proactive threat detection and incident response.
- **Automated incident response planning:** GenAI can simulate incident response scenarios and create synthetic incidents for training purposes. NLP can be used to understand and process incident reports and to automate the extraction of relevant information. The SOC can leverage GenAI for realistic incident simulations and use NLP to automatically extract insights from incident reports to streamline incident response planning and execution.
- **Contextual understanding of security events:** NLP analyses logs, alerts, and security event descriptions to understand the context of security incidents. GenAI can generate additional context for security events by simulating potential attack scenarios. The SOC gains a deeper understanding of security events from both NLP linguistic analysis and GenAI contextual enrichment. This will improve the accuracy of threat detection and reduce the number of false positives. These capabilities can also enhance the speed and efficiency of incident and management reporting for the SOC team.
- **Dynamic threat detection and adaptation:** GenAI continuously adapts the scenarios it generates based on evolving threats. NLP processes real-time security information, identifying new threats and vulnerabilities. The SOC benefits from a dynamic and adaptive threat detection system that uses GenAI for scenario simulation and NLP for real-time analysis to improve its readiness for emerging threats.
- **User awareness and training:** GenAI can create synthetic phishing scenarios for user awareness training. NLP can be used to process user feedback and identify common issues related to security awareness. By combining GenAI training scenarios with NLP-driven user feedback analysis, SOC teams can develop user awareness programmes that are more targeted and effective for addressing security vulnerabilities.

By combining the creative content generation capabilities of GenAI with the language understanding features of NLP, a SOC team can create more adaptive, informed, and proactive defence strategies against evolving cyber threats. This collaborative approach can help improve incident response, threat detection, and user awareness and ultimately strengthen the overall cybersecurity posture of the organisation.



Q4: Is ignoring post-quantum security today a recipe for disaster tomorrow?

Quantum computing is a double-edged sword. While it has the potential to solve certain types of complex calculations, including optimisation problems and simulations of quantum systems, more efficiently than classical computational tools, it can also be exploited to break widely used encryption algorithms. Algorithms such as RSA and Elliptic Curve Cryptography (ECC), which form the basis of secure communication on the internet, rely on the difficulty of certain mathematical problems. Quantum algorithms, such as Shor's algorithm, have demonstrated the potential to efficiently solve these problems and pose a threat to the security of encrypted data. These current (and expected future) advances in quantum computing threaten to negate the protection required to maintain Digital Trust. In particular, quantum computing poses significant threats to the three pillars of cybersecurity:

1. Authentication

- **Breaking cryptographic hash functions:** Quantum computers can efficiently crack certain cryptographic hash functions, such as SHA-256, which are used for digital signatures and for verifying the identity of entities (e.g., websites, users). The use of quantum computers could compromise trust and security by allowing malicious actors to forge signatures and impersonate legitimate entities.
- **Man-in-the-middle attacks:** With the ability to break encryption faster, quantum computers could make it easier to intercept and tamper with communication channels and allow attackers to steal authentication credentials or redirect traffic to fake websites.

2. Data integrity

- **Breaking digital signatures:** Digital signatures rely on public-key cryptography and are used to verify that data has not been tampered with. Quantum computers could be used to break these algorithms, allowing attackers to modify data and make it appear unaltered, potentially leading to financial losses, the spread of misinformation, or even physical harm.
- **Manipulating timestamps:** Quantum algorithms could be used to forge timestamps on digital documents, making it difficult to track data provenance and verify the authenticity of records. This could have implications for legal proceedings, financial transactions, and historical records.

3. Data confidentiality

- **Breaking encryption algorithms:** Popular encryption algorithms, such as RSA and ECC, are vulnerable to quantum attacks. Attacks on encryption algorithms could lead to the decryption of sensitive data stored on computers or transmitted over the internet, including financial records, medical information, and personal data.

While quantum computers that pose a credible threat are still years away, the threat of *"Harvest now and decrypt later"* is a real, immediate, security risk that needs to be addressed today [FS-ISAC23]. This is a 'long game' attack where bad actors collect encrypted data, by way of breaches, or undertake passive interception and hoard the encrypted data, waiting for the day when quantum computers can decrypt that information. Therefore, it is imperative to start using quantum-resistant algorithms as soon as possible. Today, a bad actor can record, and store (harvest) encrypted data that is streaming through the internet or cloud, from a specific website, server, email client, or whichever target they deem worthy of attack. With enough resources, that bad actor could capture petabytes of data (or more) from general internet traffic.

The question of when cryptography will be broken by quantum computing is unfortunate, as it implicitly frames the threat to be some time in the future. The threat exists today, but the impact will become apparent in the future. Data that is considered securely protected today is already lost to a future quantum adversary if it has been stolen or harvested. All data—past, present, and future—that is not protected using quantum-safe security is at risk, and the longer we postpone the migration to quantum-safe standards, the more data there will be that is at risk.

Our experience makes it clear that there will not be a one-size-fits-all strategy when it comes to migrating to quantum-safe security. Given the long-term nature of the threat, and the dynamic environment surrounding quantum computing, it is also clear that a cryptographic strategy needs to consider multiple time frames and needs to consider potential step improvements in quantum technology development. To supplement the standards development underway by private industry players, governments need to accelerate their investment in quantum-safe cryptosystems and proactively promote the widespread adoption of the same.

The threat of Cryptographically Relevant Quantum Computers (CRQC) is significant, but the timeline for the materialisation of the threats they will enable is unknown. How can an organisation quantify the risk of Cryptographically Relevant Quantum Computers when they don't yet exist? The immediate best practice suggests creating several scenarios of the risk a quantum threat poses to a specific asset, with some of these scenarios deemed as "more likely" than others.

The argument for starting to address the threat that quantum computers will pose to existing security systems now, is based on the following considerations:

- Cryptographic technologies are integrated into most of the digital products commonly used by organisations to run their daily operations.
- Some of the applications and systems currently used for energy, transportation, finance, and government infrastructure have expected product useful lives of 15 to 30 years, with longer requirements for data protection and privacy.
- The time required to migrate installed cryptographic technologies (e.g., SHA1) to something newer is measured in years.
- The number of cryptographic systems that organisations will need to migrate to use new 'quantum-safe' cryptography will be large.
- Most organisations have no clear view of the cryptographic technologies used in IT operations and this will make it difficult to discover, and then prioritise, the systems to be upgraded to post-quantum cryptography.
- Migrating to quantum-safe security requires a multi-pronged approach that combines proactive action, strategic planning, and continuous adaptation. Table 1 summarises some key considerations.

Stage	Action
Inventory & assessment	• Identify all assets and systems that rely on cryptography, particularly those using vulnerable algorithms like RSA and ECC • Prioritise these systems based on criticality and the sensitivity of the data they hold • Evaluate the potential impact of quantum-resistant algorithms on system performance and compatibility
Pilot & testing	• Conduct pilot projects to test and validate chosen post-quantum cryptography (PQC) solutions in real-world environments • Assess performance impact, compatibility issues, and potential integration challenges • Gather data and feedback to improve future migration strategy
Planning & strategy	• Develop a migration strategy for adopting PQC algorithms • Evaluate and select suitable PQC algorithms based on specific needs and security requirements • Prioritise systems with high-value data and for critical infrastructure • Consider the costs, resources, and training required for each phase of the migration
Deployment & rollout	• Implement PQC solutions in phases, starting with high-risk or critical systems and data • Develop and implement robust key management and lifecycle practices for PQC keys
Awareness & training	• Educate employees about the risks of quantum computing and the need for migration • Train employees on how to use and manage quantum-safe systems securely • Develop a culture of cybersecurity awareness and vigilance
Monitoring & maintenance	• Continuously monitor PQC implementations for vulnerabilities and performance issues • Stay current on the evolving quantum threat landscape and adapt security measures accordingly • Monitor the progress of standardisation efforts by organisations like NIST and ETSI

Table 2: Recommended action plans for starting a quantum-safe journey

Migration to quantum-safe security is a continuous process and will take multiple years. It is important to stay adaptable, embrace new technologies, and adjust strategy as the landscape evolves. By taking proactive steps, and actively engaging with the community, we can ensure that our organisations are prepared for the challenges and opportunities of the quantum era.

Q5: Is the promise of 5G technology overshadowed by its security challenges?

While 5G technology promises transformative benefits like high-speed and low-latency communications, its global adoption has encountered challenges, leading to a slower rollout than initially anticipated. Key factors affecting the pace of rollout include the substantial infrastructure investments required for deployment, regulatory and spectrum allocation delays, and technological hurdles related to ensuring widespread coverage. Economic uncertainties, influenced by global events such as the COVID-19 pandemic, have also impacted investment priorities and consumer readiness, with the initial high cost and limited availability of 5G-enabled devices posing additional barriers. Furthermore, public health concerns, despite lacking scientific backing, have fuelled resistance in some areas. Nevertheless, as these challenges are progressively addressed—through regulatory adjustments, technological advancements, and increasing consumer device availability—5G adoption is expected to accelerate, unlocking its full potential for a wide range of applications and services.

The rollout of 5G technology brings transformative potential for connectivity, speed, and efficiency but also introduces several key security challenges. These challenges stem from the technology's complexity, its extensive use of software, and the broad range of applications and services it aims to support. Key 5G security challenges include:

- **Increased attack surface:** 5G networks utilise a more extensive and complex infrastructure in comparison to their predecessors, including the vast number of connected devices and new technologies such as network slicing and edge computing. This complexity significantly increases the attack surface, offering more opportunities for cyberattacks and making security management more challenging.
- **Supply chain security:** 5G networks rely on a global supply chain that includes many vendors providing hardware, software, and services. Ensuring the security of this supply chain is crucial, as vulnerabilities or malicious insertions at any point can compromise the entire network. The risk is exacerbated by the potential for state-sponsored threats aimed at exploiting supply chain weaknesses for espionage or sabotage purposes.
- **Privacy concerns:** The massive amount of data transmitted over 5G networks, combined with advanced technologies capable of processing this data at unprecedented speeds, raises significant privacy concerns. Protecting user data against unauthorised access, and ensuring compliance with data protection regulations, becomes increasingly complex in a 5G context.
- **End-to-end encryption challenges:** While 5G promises enhanced security features, including improved encryption compared with earlier generations, implementing end-to-end encryption across the entire network and ensuring the confidentiality of data in transit remains a challenge. This is particularly the case for scenarios involving network slicing, where different slices may have varying security requirements and capabilities.
- **Dynamic network configuration and management:** 5G networks enable dynamic network configuration and management to support a wide range of applications with differing performance requirements. This dynamic nature, while being a strength of 5G, complicates the security management of the network. Ensuring consistent security policies and effective incident response across an ever-changing network topology require sophisticated security tools and strategies.

Addressing these challenges is critical for ensuring the security and reliability of 5G networks. It requires a concerted effort from network operators, equipment manufacturers, service providers, and regulatory bodies to develop and implement robust security frameworks that can adapt to the evolving threat landscape associated with 5G technology.

With the ongoing rollout by Mobile Network Operators (MNOs), the Cyber Security Agency of Singapore (CSA) published the 'Guidelines for CII (Critical information Infrastructure) Owners to Enhance Cyber Security for 5G Use Cases' in April 2022. The guidelines outline possible cyber threats to systems connected to 5G services and provides recommendations to mitigate these risks. Here are five key security recommendations from the CSA guidelines:

- **User equipment assurance:** CIIOs must ensure that user equipment connecting to 5G networks achieve high levels of security assurance. This includes maintaining valid security assurance certifications, such as those under CSA's Cybersecurity Labelling Scheme (CLS) and keeping software/firmware updated to mitigate known vulnerabilities. Additionally, equipment nearing the end of its service life should be replaced to prevent network compromises.
- **Data protection:** Protecting data from unauthorised access and corruption is paramount. CIIOs should implement encryption for data in transit across 5G networks. In scenarios where encryption may not be feasible, data integrity verification measures should be applied. Ideally, end-to-end encryption is recommended for all system communications. For data stored on user equipment (UE), secure industry-standard encryption algorithms should be used, with hardware-based root of trust modules (e.g., TPM) deployed to protect critical data.
- **Configuration management:** The configuration of systems connected to 5G networks should be meticulously planned, documented, reviewed, and tested. Implementing technical solutions to document and maintain configurations can facilitate system recovery and prevent misconfigurations. CIIOs should ensure that UE, regardless of location or direct connection to the CII network, complies with the latest cybersecurity policies.
- **Access control:** Access to the CII network should be strictly controlled based on the user's credentials and the security posture of the UE. This encompasses implementing network access control, identity and access management, and interface authentication. Access control policies should be regularly reviewed, and multi-factor authentication is recommended for accessing UE or connecting to the CII network through 5G.

- **Monitoring of devices over the 5G network:** Continuous monitoring of devices is essential for detecting abnormalities and security incidents. CIIOs should monitor both the operational status and physical location of UE to prevent unauthorised relocation. For devices that may not always be connected to the 5G network, such as IoT sensors, system operators should be alerted if the devices fail to connect after a predefined interval or in the event of unauthorised access.

However, 5G is a relatively new technology, and the technical solutions available to system owners—Critical Information Infrastructure Owners (CIIOs) and enterprises—to mitigate the associated cybersecurity risks of deployment, may not be sufficiently tested for effectiveness and performance. Specific details for some of the solutions, such as the encryption schemes to use, have either not been prescribed or are said to be dependent on the 5G use case.

To address the need for testing that details the impact of various cybersecurity solutions on the effectiveness and performance of user equipment within 5G networks, a study on 5G cybersecurity technical solutions was commissioned by CSA. The intent of the study was to provide CSA with information, across a variety of use cases, about how security solutions and measures should be implemented to adequately protect CIIOs' systems without compromising the potential operational benefits of 5G. The findings of the 5G security study are shared in a follow-up article.

Unveiling the strategic advantages of NCS Cyber

NCS, a prominent digital and technology service provider in the APAC region, offers a comprehensive suite of end-to-end services and digital solutions that encompass applications, infrastructure, engineering, and cybersecurity. In the evolving digital landscape, ensuring robust cybersecurity is pivotal to safeguarding organisations at each layer of the technology stack.

- **Applications:** NCS empowers businesses by boosting productivity through cutting-edge business application solutions. We put client needs at the core of the application development process when creating enterprise-grade applications using AI. These applications not only address organisational needs but also cater to market demands to increase business agility for clients.
- **Infrastructure:** A modern, current, infrastructure is crucial to business competitiveness and overall performance. NCS facilitates the transformation of organisational infrastructure to allow businesses to innovate faster and to adopt data-driven business models. NCS builds secure and responsive infrastructure that is tailored to the digital enterprise to ensure competitiveness.
- **NCS NEXT:** The NCS NEXT team develops innovative solutions and experiences that transform and propel communities forward. The NCS team of specialists, located throughout the APAC region, possesses expertise to build and customise first-class enterprise solutions. That expertise extends to cloud innovation with services to ensure secure and compliant migrations, FinOps mastery for client cloud frameworks, and data-driven business evolution and expansion. With innovative products and platforms, NCS provides the tools and emerging technologies to future-proof businesses.
- **Cybersecurity:** The NCS approach to security involves combining global cybersecurity expertise with state-of-the-art technologies to safeguard businesses against evolving cyber threats. NCS helps businesses stay ahead of new threats by providing access to a global team of certified security experts who are skilled in the latest cybersecurity technologies. Personal information security advisors collaborate with clients to design tailored IT security solutions that align with business needs and objectives.

NCS integrates cybersecurity technologies, solutions, and services at each layer of the software and hardware stacks. To ensure protection of critical business applications from potential threats and unauthorised access, NCS addresses vulnerabilities at the application layer by focusing on API and container security. At the infrastructure layer, NCS integrates cutting-edge cybersecurity technologies, such as Database Activity Monitoring (DAM), Data Loss Prevention (DLP), and Network Intrusion Detection System (NIDS). These technologies span edge devices, networks, and cloud platforms and enhance security measures to prevent data breaches, detect unauthorised database access, and identify network intrusions. Recognising the diverse needs of different industries, NCS emphasises the integration and customisation of cybersecurity technologies to address sector-specific challenges through our in-house engineering capabilities. This tailored approach ensures that businesses receive solutions that align with their unique requirements and regulatory environments.

NCS' history of delivering large-scale and complex projects underscores its capability to integrate diverse skill sets across the applications, infrastructure, NEXT, and cybersecurity domains. This holistic approach to cybersecurity, covering multiple layers of the technology stack, positions NCS as a reliable and trusted partner for navigating the challenges of the digital landscape and ensuring comprehensive protection against cybersecurity threats.

References

[WEF22] Earning Digital Trust: Decision-making for Trustworthy Technologies World Economic Forum, Insight Report, November 2022.

[WDKW22] J. Watts, J. D'Hoinne, D. Koeppen, and C. Winckless. Predicts 2023: Zero Trust Moves Past Marketing Hype Into Reality. Gartner, 6 December 2022.

[WML23] J. Watts, N. MacDonald, and T. Lintemuth. 2023 Strategic Roadmap for Zero Trust Security Program Implementation. Gartner, 13 April 2023.

[WPA23] C. Winckless, P. Proctor, and M. Acosta. Outcome-Driven Metrics You Can Use to Evaluate Cloud Security Controls. Gartner, 28 September 2023.

[CSA21] Cloud Security Alliance (CSA). The Continuous Audit Metrics Catalog, 19 October 2021. https://cloudsecurityalliance.org/artifacts/the-continuous-audit-metrics-catalog/.

[Crace19] J. Crace. The Cambridge Analytica scandal changed the world – but it didn't change Facebook. The Guardian, 18 March 2019. https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook.

[Kom23] M. Komnenic. 109 Biggest Data Breaches, Hacks, and Exposures. Termly, 20 December 2023. https://termly.io/resources/articles/biggest-data-breaches/.

[HWW22] N. Henein, B. Willemsen, and B. Woo. Top trends in privacy driving your business through 2024. Gartner, 5 May 2022.

[WW23] B. Woo and B. Willemsen. Hype Cycle for Privacy 2023. Gartner, 24 July 2023.

[WMH22] B. Willemsen, D. Mahdi, and M. Horvath. Three Critical Use Cases for Privacy-enhancing Computation Techniques. Gartner, 10 November 2022.

[AI-RMF23] NIST AI Risk Management Framework (AI RMF 1.0), January 2024. https://doi.org/10.6028/NIST.AI.100-1.

[SWS22] M. Schneider, J. Watts, and P. Shoard. Innovation Insight for Attack Surface Management. Gartner, 24 March 2022.

[DSS22] J. D'Hoinne, P. Shoard, and M. Schneider. Implement a Continuous Threat Exposure Management (CTEM) Program. Gartner, 21 July 2022.

[FS-ISAC23] Future state technical paper. Post-quantum cryptography working group, FS-ISAC, 2023.

embracing zero trust in cybersecurity: Strategies and challenges for effective implementation

Hoon Wei Lim

embracing zero trust in cybersecurity: Strategies and challenges for effective implementation

Hoon Wei Lim

Executive summary

Because of its intrinsic benefits, zero trust is gaining prominence among organisations that seek to fortify their cybersecurity defences. Implementing zero trust enhances an organisation's overall cybersecurity posture by fostering a resilient infrastructure and cultivating an adaptive work environment. At the heart of a zero trust architecture are dynamic policy decisions and enforcement mechanisms that are contingent on the identity of devices or users. This focus, and the adaptability it enables, allows the system to tailor the level of trust based on contextual factors and reduce the vulnerabilities commonly associated with static security measures.

While organisations recognise the advantages of zero trust, there are internal and external challenges that demand attention. Internally, issues such as defining policies at scale, integrating zero trust into legacy and cyber-physical systems, and acquiring organisational implementation and management skills, pose hurdles. Externally, challenges include the ambiguity caused by the unrealistic claims made by vendors in their marketing of zero trust solutions, and the varying levels of maturity of products labelled as 'zero trust'.

This article explains the fundamental principles for zero trust implementation and emphasises the need to address internal and external challenges effectively. It explores the core technologies that are pivotal for enabling zero trust, including access management, analytics for detection and response, security service edge solutions, and macro and micro network segmentation. Furthermore, the article provides insight into the zero trust maturity model defined by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). This model outlines a progressive journey to zero trust implementation across five pillars: identity, devices, networks, applications and workloads, and data. Each stage in the maturity model represents a level of advancement to guide organisations from traditional security approaches to optimal zero trust implementation.

The progress toward zero trust is fuelled by its transformative ability to provide a proactive and adaptive security environment. As organisations navigate the implementation journey, understanding the principles, leveraging core technologies, and aligning with the maturity model can help to maximise the benefits of zero trust and fortify defences against evolving cyber threats.

What is zero trust?

Interest in zero trust security has been largely driven by government mandates, vendor hype, ransomware attacks, and the needs of increasingly hybrid workforces. According to Gartner, more than 60% of organisations will embrace zero trust as a starting place for security by 2025 [WDKW22].

Zero trust is a transformative security model that challenges the traditional notion of implicit trust within IT architectures. It introduces explicit trusts that are continuously evaluated based on identity and contextual risks. It's important to note that zero trust is not a standalone security strategy, but rather, a fundamental component within a broader security approach.

In conventional IT environments, security strategies that rely on implicit trust are the norm, and that reliance on implicit trust leads to potential vulnerabilities arising from excessive access. Zero trust addresses these vulnerabilities by replacing implicit trust with a dynamically assessed and explicitly calculated trust model that hinges on identity and context. Establishing a robust identity foundation is imperative for the effective implementation of zero trust.

Zero trust is not confined to networking alone, as its principles can be extended to multiple facets of enterprise system security. Overall, zero trust represents a paradigm shift, as organisations are forced to continuously reassess and adapt their security postures in the face of evolving threats and changing contexts.

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) defines zero trust architecture (ZTA) as an approach to cybersecurity that is centred around the principle of 'never trust, always verify'. In a zero trust architecture, trust is never assumed for any user, device, or system, even if located within a corporate network. Instead, continuous verification is required of everyone/everything trying to access resources in the network, regardless of its location [RBM20].

Key principles of a zero trust architecture, according to NIST, include:

- **Least privilege access:** Users and systems are granted the minimum level of access or permissions needed to perform their tasks. Access is restricted based on the principle of least privilege.
- **Micro-segmentation:** Networks are divided into smaller segments and access controls are applied to each segment. This limits lateral movement in case of a security breach.
- **Continuous monitoring:** Continuous monitoring of users, devices, and systems is essential. This involves ongoing verification of identity, device health, and other relevant parameters.
- **Risk-based authentication:** Authentication mechanisms are adjusted based on risk assessments. For example, additional authentication steps may be required for high-risk activities or for unknown devices.
- **Policy enforcement:** Strict access policies are enforced across the network. These policies are often dynamic and can adapt to changes in the IT environment or threat landscape.
- **Encryption:** Data is encrypted to protect it from unauthorised access, especially when in transit between users and applications.

A zero trust architecture is designed to address the limitations of traditional perimeter-based security models. It assumes that threats may exist both outside and inside the network and focuses on protecting resources regardless of their locations. This approach aligns with the evolving nature of cybersecurity threats and the need for more robust and adaptive security strategies.

Key benefits of zero trust

Prevailing IT architectures are fraught with implicit trust, a vulnerability that demands elimination to forestall the abuse of unwarranted access. The zero trust model dismantles implicit trust in favour of a model where trust is continuously assessed, explicitly calculated, and dynamically adaptive, contingent on identity and context. This model serves as a guiding principle for security strategies that not only define the architectural landscape but also enhance security posture and fortify cyber resilience. Organisations embracing the zero trust mindset and architecture stand to gain two pivotal technical outcomes:

- **Resilient infrastructure:** Zero trust principles significantly bolster the resiliency of IT infrastructures. A zero trust network, crafted to operate even in the presence of adversaries, excels at containing and managing incidents. This proactive approach diminishes the likelihood of business-impacting events such as ransomware attacks, data compromises, or malware infections. Consequently, this reduction in risk contributes to the overall robustness and security of the business.
- **Adaptive work environment:** In anticipation of a more hybrid nature of future work, organisations must provide work environments that are more agile, flexible, and adaptable. A zero trust security strategy seamlessly supports remote workers, using both managed and unmanaged devices, remote data (e.g., IaaS), and remote applications (e.g., SaaS). A secure zero trust implementation will enable the realisation of an 'anywhere, any time, on any appropriate device' approach that will be crucial for supporting a dynamic and hybrid workforce.

Implementing zero trust

Key considerations

The implementation of zero trust systems within enterprises requires a systematic and strategic approach. The initial step involves identifying specific use cases that will form the basis of an actionable zero trust strategy. For example, initial use cases might focus on reducing exposure to applications and services, mitigating specific threats by restricting the lateral movement of malware, or isolating software supply chains from attack.

Once the use cases are identified, cybersecurity leaders within the organisation need to establish zero trust strategy and requirements. This process involves a comprehensive assessment of the current environment, with a particular focus on existing identity and access management (IAM) technologies and processes. Understanding the strengths and weaknesses of the current IAM framework is crucial for determining how zero trust principles can be effectively integrated.

The notion of zero trust emphasises fine-grained, just-in-time, access control for user-to-application and application-to-application communications. This approach uses dynamic policy decisions and enforcement mechanisms based on the identity of the device and/or user and can adapt the level of trust according to contextual factors (Figure 1).

While a zero trust architecture (ZTA) promises enhanced security, both internal and external complications pose challenges to its effective implementation. Internally, organisations often grapple with the need to define policies at scale and to manage the rapid pace of policy changes. Legacy systems and cyber-physical systems, such as those for Internet of Things (IoT), Operational Technology (OT), and Industrial Control Systems (ICS), present hurdles to extending ZTA approaches. Additionally, the concurrent deployment of new technologies and processes requires skills that are either hard to acquire or difficult to develop within the existing workforce. Externally, complications are exacerbated by vendor marketing strategies that often dilute the meaning of 'zero trust' and create confusion. Products labelled as 'zero trust' also tend to come with higher costs compared to legacy alternatives. Moreover, the maturity and integration levels of products supporting a ZTA vary, and that may impact contextual understanding, management, and reporting.

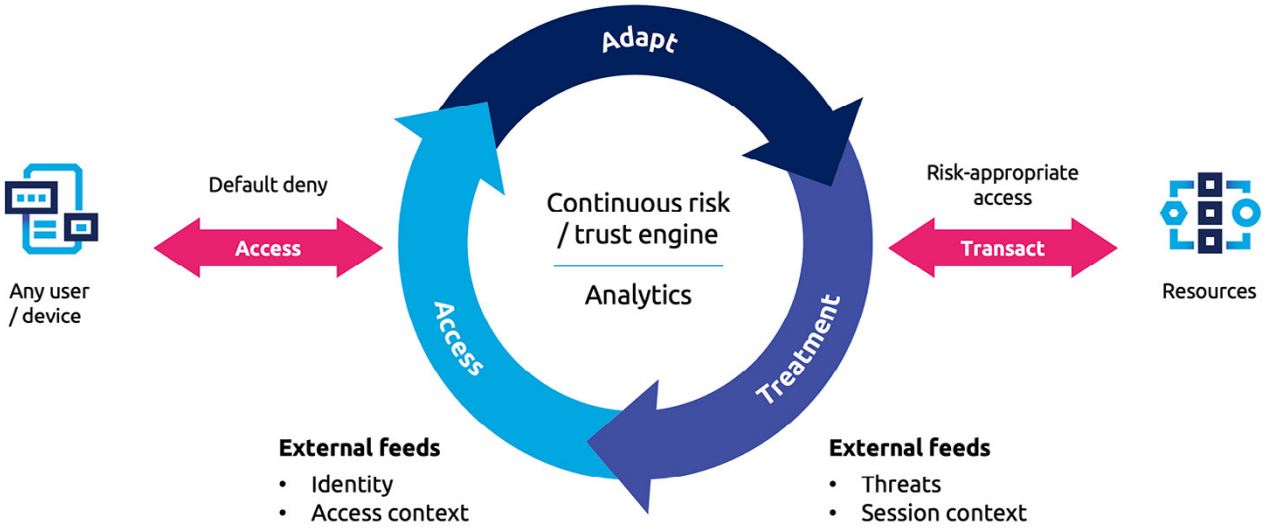


Figure 1: Core functions of the NIST AI Risk Management Framework

Identifying the optimal projects for ZTA implementation is a complex task due to these challenges. It is crucial to recognise that ZTA is not a one-size-fits-all solution available from a single vendor. Instead, a ZTA involves collaboration among multiple technology providers whose products must seamlessly integrate to establish a continuous-identity and context-aware adaptive trust model.

Internal challenges demand a strategic approach to policy definition and adaptation, especially in the face of evolving technologies and legacy systems. Overcoming skills shortages requires comprehensive training programmes and strategic workforce planning. For external challenges, organisations must navigate vendor landscapes carefully and critically evaluate products labelled as 'zero trust' to ensure that they align with security needs and budget considerations.

Roadmap for implementing zero trust technologies

Implementing ZTA requires that cybersecurity leaders prioritise organisational definitions of zero trust and select technology implementations that align with their envisioned future state. Table 1 provides some examples of potential gaps that will need to be addressed to take an organisation from a current state to a desired future state.

Contrary to common misperceptions, transitioning to a ZTA does not necessitate the complete replacement of existing technologies. Many existing tools can support the shift with appropriate configurations. To facilitate this transition, cybersecurity leaders should adhere to the following fundamental principles [WML23]:

- **Context-driven access rights:** User account and/or device context, coupled with the criticality of organisational resources, should dictate access rights. This principle emphasises the importance of understanding the context in which users and devices operate to determine the appropriate level of access to sensitive resources.
- **Continuous runtime assessment:** Access rights enforcement should not be a static process. Continuous runtime assessment of user account and/or device context, along with the resources being accessed, is crucial. This dynamic evaluation ensures that access rights evolve in response to changing contexts, enhancing security by adapting to real-time conditions.
- **Secured network communications:** Regardless of physical location, all network communications between organisational resources must be secured. This principle emphasises the need for robust encryption and security measures for data in transit to mitigate the risk of unauthorised access or interception.

By adhering to these basic principles, organisations can lay the foundation for a ZTA. This approach involves a strategic reassessment and reconfiguration of existing technologies to align with the core tenets of zero trust, and ultimately, to the creation of a security model that prioritises continuous verification and dynamic access controls.

Future state	Current state	Gap
Authenticate before access is granted	Authentication relies on a weak single and/or additional factor	Lack of budget/business case
Granular access segmentation between users, applications, and workloads	Coarse-grained or limited segmentation between users, applications, and workloads	Lack of skills and resources
Logging and monitoring of device and user activity	Reliance on network security perimeter controls to protect resources	Organisational resistance
Continuous risk and trust assessment	Full network connectivity is granted before authentication	Fragmented user and device identity and processes

Table 1: Strategic roadmap for zero trust security programme implementation

It is also important to note that a zero trust strategy must be driven by a business decision that weighs the investment an organisation can/will make versus the benefits that it will accrue from that investment. As organisations improve their capabilities in explaining cybersecurity as a critical business investment, zero trust efforts will be measured against other programme-level security efforts and be viewed as scoped, structured, and proactive as opposed to tactical and reactive.

Core technologies for enabling zero trust

Implementing a ZTA necessitates the integration of diverse technologies from different vendors. According to Gartner, several key technologies form the core of a future-state ZTA:

- **Access Management (AM):** At the foundation of a zero trust approach, AM involves establishing, enforcing, and managing runtime access controls for internal and external identities across multiple applications. Implementing continuous adaptive AM, password-less authentication, and a security posture with Identity Threat Detection and Response (ITDR) is pivotal in evolving AM practices and shaping zero trust roadmaps.
- **Analytics, detection, and response technologies:** In the zero trust evolution of security monitoring and analytics, technologies such as Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), Network Detection and Response (NDR), and Extended Detection and Response (XDR) play crucial roles. These technologies provide security analytics, incident response, and incident response playbook automation, contributing to context-based access controls in a ZTA.
- **Security Service Edge (SSE):** SSE technology secures access to web, cloud services, and private applications irrespective of user or device location. It enhances security and visibility in Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) environment. SSE, often integrated within a Secure Access Service Edge (SASE) framework, includes Zero Trust Network Access (ZTNA) capabilities. It offers advanced analytics and trust-scoring for identity- and context-based logical access boundaries around private applications and SaaS services.
- **Macro and micro network segmentation:** Macro-segmentation refers to traditional grouping based on shared characteristics, such as physical location or business importance, and focuses on controlling north/south traffic within a network. It serves as an in-depth defensive component that complements micro-segmentation. Micro-segmentation involves the creation of granular and dynamic policies with the goal of controlling east/west traffic within a macro-segmentation segment. Implemented at the application layer, it enforces a positive security model and reduces the risks associated with lateral movement.

While these technologies form the core of zero trust, there are additional niche technologies supporting zero trust implementations. A robust ZTA extends beyond core technologies to incorporate a layer-of-defence approach that reduces the attack surface and prevents lateral movement. It is crucial to align these technologies with zero trust principles to create a comprehensive security posture. This layered approach provides a resilient defence against evolving cyber threats and ensures a robust and adaptive security framework.

Journey to maturity

Industry surveys indicate that more than 60% of organisations are either planning or actively implementing a zero trust strategy [OKTA23]. However, Gartner observes that though many clients have a strategy, and are working to implement zero trust technologies, few zero trust implementations can be considered as 'mature'. There are several reasons for the nascent state of many ZTA implementations including a lack of interoperability between vendor products, limited scopes of deployment, and a lack of functionality in commercially available products [LLWT23].

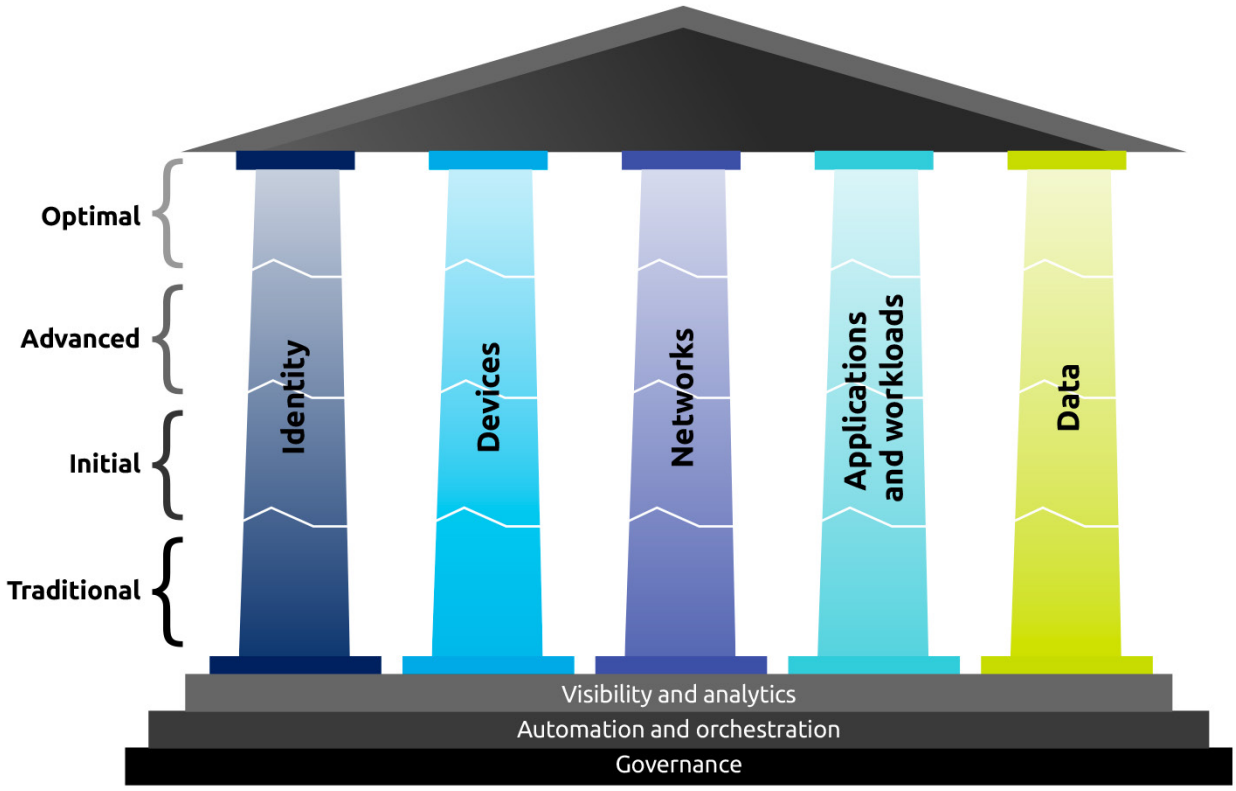


Figure 2: Zero trust maturity evolution as defined by CISA [CISA23]

The journey towards implementing a zero trust architecture (ZTA) involves a gradual process that unfolds over time, reflecting the dynamic nature of cybersecurity challenges. The U.S. Cybersecurity & Infrastructure Security Agency (CISA) has outlined a comprehensive zero trust maturity model that encompasses five pillars: identity, devices, networks, applications and workloads, and data. These pillars are integral to establishing a robust security framework, and each has specific cross-cutting capabilities, including visibility and analytics, automation and orchestration, and governance [CISA23].

As organisations progress through the model, the transition from a traditional approach to an optimal ZTA happens over three distinct stages: Initial, Advanced, and Optimal. This staged approach allows for a systematic evolution that allows organisations to distribute costs over time rather than requiring a substantial upfront investment.

In the traditional stage of the CISA model (Figure 2), organisations rely on manual configurations, static security policies, and siloed enforcement, addressing one pillar at a time. The Initial stage of the CISA ZTA maturity model recommends automation, with attributes being assigned and policies configured dynamically. The adoption of least privilege access at this stage results in responsive changes for post-provisioning and greater visibility increases for internal systems. At the Advanced stage, organisations implement automated controls for lifecycles and configurations across pillars. Centralised visibility and identity control become the norm and policy enforcement integrates seamlessly. Responses are predefined, and changes to least privilege are based on risk and posture assessments, laying the foundation for enterprise-wide awareness.

The Optimal stage is characterised by fully automated lifecycles and assignments, dynamic policies triggered by automated observations, and just-in-time access, and is the zenith of the ZTA journey. Least privilege access becomes dynamic, ensuring assets and dependencies adhere to enterprise-wide thresholds. Cross-pillar interoperability and continuous monitoring contribute to centralised visibility, offering comprehensive situational awareness.

Organisations navigating this maturity model must evaluate each pillar against specific criteria, at each stage, to ensure consistency across the ZTA framework. By aligning pillar maturity with mission needs and the ability to scale across all pillars, organisations can progressively fortify their security postures. This structured approach empowers organisations to adapt to evolving threats and to ultimately achieve an optimal ZTA that provides dynamic, adaptive, and comprehensive security.

Further details of the zero trust maturity model, including key aspects of the pillar-specific functions for each pillar, and across each maturity stage, can be found here [CISA23].

Zero trust adoption requires cross-organisation collaboration and the involvement of senior leadership, IT personnel, data/system owners, and users. Effective implementation relies on collective engagement to meet design objectives and enhance cybersecurity posture. During ZTA planning, decisions should be guided by factors such as risks, mission, cybersecurity requirements, and operational constraints. The general guide must be tailored based on interactions with external partners, stakeholders, and the service providers involved in ZTA to ensure alignment with organisational dynamics and create a comprehensive approach to security.

How NCS can help you with your zero trust journey

As a leading digital and technology service provider, NCS Cyber has a team of highly qualified and experienced cybersecurity professionals with deep domain expertise in zero trust architectures. This expertise ensures clients receive state-of-the-art guidance tailored to their specific needs, enabling a robust security framework built on the principle of 'never trust, always verify'.

Central to our value proposition is a strong specialisation in cryptography through our team of consultants and engineers who are extremely proficient in developing quantum-safe solutions and privacy-enhancing technologies. Our focus on advanced cryptographic measures is fundamental to establishing a secure zero trust environment that protects against both current and emerging cyber threats, particularly those posed by future advancements in quantum computing.

Our competency is bolstered by our partnerships with strategic vendors on a broad spectrum of services ranging from identity and access management to secure network segmentation. These essential components of zero trust architectures ensure strict control and monitoring of access based on verified identities and contextual information, thereby minimising the attack surface, and mitigating potential breaches.

Furthermore, our commitment to continuous support, through consulting and professional services, ensures that the zero trust architecture remains effective and adaptive to new cybersecurity threats and changes within the IT landscape. By offering a comprehensive, flexible, and forward-looking suite of services, NCS empowers clients with readiness for the challenges of the modern digital world through the creation of highly secure and resilient cybersecurity environments.

References

[MMW23] A. McQuaid, N. MacDonald, J. Watts, and R. Kaur. Market Guide for Zero Trust Network Access. Gartner, 14 August 2023.

[RBM20] S. Rose, O. Borchert, S. Mitchell, and S. Connelly. Zero Trust Architecture, NIST Special Publication 800-207, August 2020.

[WML23] J. Watts, N. MacDonald, and T. Lintemuth. 2023 Strategic Roadmap for Zero Trust Security Program Implementation. Gartner, 13 April 2023.

[LLWT23] T. Lintemuth, A. Lerner, J. Watts, and K. Thielemann. Predicts 2024: Zero Trust Journey to Maturity. Gartner, 15 December 2023.

[OKTA23] okta, The State of Zero Trust Security 2023, https://www.okta.com/au/state-of-zero trust/.

[CISA23] Cybersecurity and Infrastructure Security Agency (CISA), Zero Trust Maturity Model, version 2.0, April 2023.

managing risks and opportunities for quantum-safe development

Hoon Wei Lim, John Buselli

managing risks and opportunities for quantum-safe development

Hoon Wei Lim (NCS), John Buselli (IBM)

Executive summary

In today's rapidly evolving digital landscape, the emergence of quantum computing presents both a challenge and an opportunity. Businesses that fail to prepare for quantum-safe security may face significant risks, including data breaches and a loss of competitive advantage. This summary highlights the essential steps and benefits of transitioning to quantum-safe practices to ensure that your business remains secure, competitive, and future-proof.

Our world depends on digital infrastructure and digital communications – all of which inherently rely on cryptography to ensure trust. Cryptographic technologies are used throughout governments and enterprises across a variety of industries, to authenticate sources and protect the confidentiality and integrity of the information that we communicate and store. Cryptographic technologies include a broad range of protocols, schemes, and infrastructures.

Trust is at risk as asymmetric cryptography is likely to be broken when a Cryptographically Relevant Quantum Computer (CRQC) becomes available. This risk extends to symmetric cryptography, which will not be directly impacted, but will require new strategies for mitigation as well. As quantum computing advances, organisations face the need to protect their sensitive data from potential vulnerabilities.

The quantum computing era will unfold over time, but the need for quantum-safe solutions is immediate. The strategic planning, preparation, and remediation effort required to support crypto systems, even pre-quantum computing, can require several years because of the complexity involved. Business, technology, and security leaders face an urgent need to develop quantum-safe strategies and quantum-computing roadmaps now.

The IT landscape has become increasingly complex over the years. This landscape is composed of many components including internally developed digital applications, IT capabilities inherited through acquisitions, third party software products and SaaS, and services consumed from cloud providers. The scope of technology that organisations need to upgrade to become quantum-safe, or remediated to use quantum-safe cryptography, is significant. As a result, it is not unreasonable to anticipate several years of effort for an enterprise to become quantum-safe.

Developing quantum-safe cryptography capabilities is crucial to maintaining data security and integrity for critical applications. This includes developing and applying cryptographic agility approaches to switch between multiple cryptographic primitives without making any major changes to infrastructure to ensure a rapid response to any cryptographic threat.

Cryptographic agility requires more than just an inventory of cryptographic assets and usage. It requires having the relevant information, at the right time, in the right place, with the right governance. A programmatic and iterative quantum-safe programme, developed in collaboration with stakeholders, will provide a structured approach to implementing quantum-safe solutions that adapt to emerging threats and continuously improve overall security.

Planning for quantum-safe

The scope of what needs to be upgraded to be quantum-safe or remediated to use post-quantum cryptography (PQC), is significant. The journey to a quantum-safe future must be well planned and incrementally executed based on business and technical priorities and several other critical considerations. The following provides an overview of critical steps to consider on the journey to a quantum-safe future:

- **Inventory current cryptography usage:** The first step is to ensure a comprehensive understanding of cryptography usage across the organisation. This can be achieved by developing an inventory of both the static and dynamic view of cryptography usage. The scanning of cryptography usage in custom applications used within an organisation provides a static view, and scanning networks for cryptography calls provides a dynamic view of cryptography usage. This comprehensive inventory of cryptography usage is best represented in a standard form such as a Cryptography Bill of Materials (CBOM).

- **Identify and prioritise 'crown jewels':** Having a comprehensive inventory is necessary but not especially useful from a planning perspective. It is critical that the 'crown jewels' (i.e., the most critical data and assets with your organisation) are identified and safeguarded first. This can be achieved by classifying all assets within the organisation, based on both business and technical importance, and weighing the criticality of each asset. The resulting prioritised view of the asset landscape can then be used to develop a transformation plan or roadmap.

- **Develop a transformation roadmap:** It is not possible to transform all applications and systems in one massive initiative. The transformation must be broken into several phases, with each phase building on the collective experiences and capabilities of prior phases. Developing such an incremental transformation roadmap is a particularly important step and must be undertaken with great thought and a depth of understanding of the challenges involved. This is typically a transformation where the implementation team starts small, learns from each iteration, builds reusable components, establishes comprehensive transformation approaches, and executes these diligently over several years. The scope of the transformation must include systems within the control of the organisation, and outside of the organisation. External or third-party entities that integrate with the organisation's systems must also complete their own transformations.

- **Begin transformation to become quantum-safe:** Having developed an actionable transformation roadmap, beginning to execute against that plan is the next step. The transformation journey will typically take several years. Given this expected project duration, it is important that the transformation roadmap be periodically validated with findings from the ongoing transformation, as well as other environmental considerations and changes, and adjusted accordingly. One key aspect of this transformation step is ensuring that 'crypto agility' is part of the transformation. Ensuring that future cryptography-related changes do not require core changes to an application is what is typically referred to as crypto agility. This assurance allows for ease of transition from one post-quantum cryptography algorithm to another in the future, should the need arise. All activities must include enabling crypto agility as part of the transformation.

  Another key aspect of the transformation step is to not assume that the effort is simply one where old cryptography technology is replaced with new post-quantum cryptography. While this is indeed one approach, it is not the most efficient or effective way. Identifying the appropriate remediation approach or pattern for transforming an application or system is important. It is very likely that organisations with a lot of applications can establish and use multiple patterns repeatedly across their IT landscapes.

- **Gain familiarity and expertise in the use of new algorithms:** An activity that must be undertaken right from the start, and executed in parallel with the previously enumerated steps, is to establish a credible level of competency in the judicious application of post-quantum cryptography. The new post-quantum cryptography algorithms are quite complex and are quite different from existing algorithms. Understanding the appropriate use of the algorithms, and their performance profiles and resource consumption characteristics, among other factors, is very important.

  This level of competency can be achieved by establishing a centre of excellence, and by identifying dedicated cryptographic engineers and security architects and providing them with an environment and opportunities to experiment and learn. For learning purposes, establishing a sandbox to test new algorithms in the organisation's environment is very important, as is the execution of targeted pilot projects.

Recent developments in quantum computing

The world is on the cusp of another computer revolution that will be driven by the convergence of powerful technologies, chief among which are high-performance computing, Artificial Intelligence (AI), and quantum computing. Quantum computing is not simply a faster way of doing what today's computers do – it is a fundamentally different approach that promises to solve problems that classical computing can never realistically solve. It holds the promise to help humanity confront important challenges, from solving long-standing questions in science, to overcoming obstacles in improving industrial efficiency. Working in conjunction with classical computers and cloud-based architectures, quantum computers could even be the answer to problems we haven't yet dreamed of. The benefits to society and the economic opportunities are potentially limitless.

In the case of quantum computing, the theme of the past few decades has been the emergence and establishment of this innovative technology. The quantum community has been focused on laying the groundwork: experimenting with quantum hardware, devising use cases, and educating people on how to use quantum computers, while running experiments benchmarking devices. Recently, IBM made quantum computing real.

A June 2023 paper by IBM and UC Berkeley outlines a path toward useful quantum computing. Read here for new insights into how we demonstrated that quantum computers could run circuits beyond the reach of brute-force classical simulations. For the first time, IBM has hardware and software capable of executing quantum circuits with no known a priori answer at a scale of 100 qubits and 3,000 gates. Quantum is now a computational tool, and what makes us most excited is that we can start to advance science in fields beyond quantum computing itself. It is clear that a heterogeneous computing architecture consisting of scalable and parallel circuit execution and advanced classical computation is required. This has culminated in IBM's vision for high-performance systems for the future: quantum-centric supercomputing (IBM Debuts Next-Generation Quantum Processor & IBM Quantum System Two, Extends Roadmap to Advance Era of Quantum Utility).

The quantum threat

The security of most standard algorithms relies on extremely difficult mathematical problems that take years to solve with current computers. Modern public-key encryption protocols are satisfactory for protecting against most of the technological tools at the disposal of today's threat actors. However, that won't last. Quantum computers will be capable of breaking these math-based systems in a matter of seconds. In addition, threat actors are now harvesting large quantities of encrypted data and storing it until they can break the encryption keys using quantum computing. Data that is encrypted today is vulnerable to decryption tomorrow.

"Quantum computers promise transformative powers for businesses and organisations across the globe and through a diverse range of industries. However, they also introduce significant risks to the current digital economy. In the near future, sufficiently powerful and commercially available quantum computers will undermine current cryptographic standards protecting most digital communications and vast amounts of sensitive data."

– Quantum Readiness Toolkit: Building a Quantum-secure Economy, World Economic Forum, 2023[1]

When large-scale quantum computers are built, they will be capable of breaking many of the current public-key cryptography systems. Global funding for quantum computing start-ups increased by 13.5% last year, to $1.1 billion. According to McKinsey, China plans to invest $15.3 billion in the industry, and the European Union has set aside $7.2 billion for investment. Without significant preparation for moving to post-quantum cryptography, quantum computers in the wrong hands could significantly compromise the privacy and security of the digital communications that the world increasingly relies on.

1. https://www3.weforum.org/docs/WEF_Quantum_Readiness_Toolkit_2023.pdf

Why start preparing now?

The question of when cryptography will be broken by quantum computing is unfortunate as it implicitly frames the threat as some time in the future, when in reality, the threat exists today, but the impact will only be felt in the future. Data that is considered securely protected today has already been lost to a future quantum adversary if it has been stolen or harvested. All data, past, present, and future, that is not protected using quantum-safe security, is at risk, and the longer we postpone the migration to quantum-safe standards, the more data there will be that is at risk.

Our experience makes it clear that there will not be a one-size-fits-all strategy when it comes to migrating to quantum-safe security. Given the long-term nature of the threat, and the dynamic environment surrounding quantum computing, it is also clear that a cryptographic strategy needs to consider multiple time frames address potential step improvements in quantum technology development. Governments have a role to play. To supplement the private sector's engagement in standards development, governments need to accelerate investment in, and promote the adoption of, quantum-safe cryptographic solutions that can safeguard data now and long into the future.

The threat of Cryptographically Relevant Quantum Computers (CRQC) is significant, but the timeline for when that threat will be realised is unknown. How can an organisation quantify the risk of CRQCs when they don't yet exist? The immediate best practice suggests creating several scenarios of the risk of a quantum threat to a specific asset, with some of these scenarios deemed as 'more likely' than others.

The argument for starting to address the threat that quantum computers will pose to existing security systems now, is based on the following considerations:

- Cryptographic technologies are integrated into most of the digital products commonly used by organisations to run their daily operations.
- Some of the applications and systems used in the infrastructure within the energy, transportation, finance, and government sectors have product lifetimes of 15 to 30 years, and requirements for data protection and privacy are even longer.
- The time needed to migrate installed cryptographic technologies (e.g., SHA1) to something newer is usually measured in years.
- The cryptographic systems that organisations will need to migrate to new 'quantum-safe' cryptography will be numerous.
- Most organisations have no clear view of the cryptographic technologies used in IT operations and this will make it difficult to discover, and then prioritise, the systems to be upgraded to post-quantum cryptography.

Guiding principles for preparing a quantum-safe journey

The World Economic Forum (WEF) recently published a set of guiding principles that outline the steps that organisations can take to become quantum cyber-ready [WEF23] in preparation for a quantum-secure economy. The guidelines also highlight the importance of a cohesive global and cross-border approach to governing quantum that includes involving business stakeholders and experts from business, governments, regulators, and academic institutions. However, as organisations vary in size, industry, and maturity, there is no single approach or strategy that serves as a one-size-fits-all solution.

We outline five key guiding principles that any organisation should consider as it starts to prepare for the transition to quantum-safe security.

Look beyond the development time frame for quantum computing

In contemplating the potential impact of quantum computing on the digital landscape, it is crucial to adopt a forward-thinking perspective that extends beyond the technology's current developmental stage. Quantum computing holds transformative potential, yet remains an active area of research, with scientists exploring more reliable and scalable methods. Attempting to predict precisely when quantum computers will break existing encryption technology is challenging, so strategic preparation efforts should be decoupled from specific development timelines. Relying solely on projected quantum computing evolution can create a false sense of security. Instead, organisations should focus on building a robust cybersecurity foundation, with quantum-resistant algorithms, irrespective of the uncertain future arrival of quantum computers. This approach involves developing cryptographic strategies that are not time-dependent, embrace post-quantum cryptography (PQC), and continuously enhance security. By building in adaptability and resilience, organisations can proactively secure digital assets in preparation for the full realisation of quantum computing.

Understand where you are now

Preparing for the imminent era of quantum computing requires organisations to proactively strengthen their cybersecurity defences. A foundational step in this process is conducting a thorough cryptography inventory and assessment, and this is especially crucial for entities that safeguard data requiring prolonged protection. The scrutinisation of cryptographic infrastructure allows organisations to identify vulnerabilities and bolster defences against quantum computing threats. This preparatory phase involves the identification of assets and systems that rely on cryptography, and emphasis should be placed on those using vulnerable algorithms such as RSA and ECC. Prioritisation is critical. Organisations should categorise systems based on data criticality to strategically allocate resources. Evaluating the potential impact of transitioning to quantum-resistant algorithms ensures a seamless integration without compromising operational efficiency. This proactive approach positions organisations to navigate the challenges posed by quantum computing effectively.

Establish a governance framework

Establishing quantum-safe security requires a meticulous approach and the active involvement of senior executives in the establishment and enforcement of a robust governance structure. A dedicated governance team should oversee the entire process to ensure alignment with organisational goals. This involves developing a quantum-safe roadmap which is in sync with quantum risk assessments and the organisation's risk appetite.

Moreover, integrating quantum risk into the existing cybersecurity operating model fortifies defences against emerging threats. Designating cryptographic 'champions' within the organisation will help to socialise the potential impact of quantum risk and drive the implementation of quantum security plans. In essence, effective governance will form the foundation for successful quantum security projects by instituting robust structures and mandates that ensure clear direction and accountability throughout the quantum-safe transition.

Hybrid approach

In enhancing cybersecurity against the uncertainties introduced by quantum computing, a prudent and conservative approach is essential. We advocate a strategy embracing a hybrid approach that strategically combines classical and quantum-safe cryptographic algorithms. A nuanced strategy will include the consideration that today's quantum-safe algorithms may encounter future challenges from computing advancements or unforeseen weaknesses, as has often been the case throughout the history of cryptography. By adopting a multi-layered defence mechanism through a hybrid approach and not relying solely on the resilience of a single cryptographic algorithm, organisations can more efficiently fortify their security postures. This approach may involve combining classical and quantum-safe algorithms, or the integration of multiple quantum-safe algorithms that have distinct properties. A forward-looking strategy should emphasise adaptability and robustness and reflect a commitment to proactive security measures that are diverse and redundant.

Continuous capability development

In the pursuit of quantum-safe security, continuous capability development is crucial for organisations seeking a proactive and adaptive transition. This involves conducting small-scale pilots to validate PQC solutions in real-world scenarios to assess performance, compatibility, and integration challenges. These pilots will yield valuable data and feedback that will inform and enhance the overall migration strategy. Simultaneously, employee education should play a leading role in raising awareness about quantum computing risks, and the necessity for migration. Training programmes will empower workforces with knowledge and the skills to securely use and manage quantum-safe systems, while helping to establish a culture of cybersecurity awareness. Continuous monitoring of PQC implementations will ensure the ongoing identification of vulnerabilities and performance issues that will be crucial for staying ahead of the evolving quantum threat landscape. The governance team should remain agile and adapt security measures based on emerging challenges and insights gained through ongoing monitoring. Regular tracking of standardisation efforts by organisations like NIST and ETSI will solidify the organisation's commitment to quantum-safe security and ensure alignment with industry best practices and standards. Through these multifaceted efforts, organisations can fortify their capabilities and readiness to navigate the quantum era with resilience and foresight.

Adopting quantum-safe practices isn't just about security; it's a strategic business move. In this subsection, we translate technical principles into business strategies and detail how being 'quantum-safe' can be a unique selling point and enhance customer trust.

Risk management

Strategy and preparation

Our experience shows that the journey to 'quantum-safe' must be well planned and incrementally executed based on a number of considerations including business and technical priorities. An effective quantum-safe approach combines technology with first-step guidance to prioritise quantum-safe initiatives, and to assess organisational risk, IT strategy, supply-chain dependencies, and ecosystem operations. Core to this approach is the creation of cryptographic inventories as well as corresponding risk and governance plans. Quantum-safe migration is a multi-step process requiring both operations and cryptographic experience. Alignment with broader business transformation efforts is another dimension for effective planning across this multi-year initiative. External factors involving regulatory agencies, standards bodies, and ecosystem partners must also be considered.

IBM Quantum Safe approach

The IBM Quantum Safe approach combines first-step guidance for prioritisation with IBM Quantum Safe technology that is tailored to meet clients' organisational risk, IT strategy, supply-chain dependency, and ecosystem operational objectives. The IBM Quantum Safe offering extends to include capabilities designed to provide a better understanding of applications and network operations. The overall approach supports a quantum-safe change programme through the creation of cryptographic inventories and corresponding risk and governance plans.

There are two main elements:

- **Strategy:** Services designed to enable clients to initiate a quantum-safe transformation programme and prepare to fund and scale the programme across the organisation. The IBM Quantum Safe programme establishes an approach to assess the requirements to transition to quantum-safe cryptography and creates a plan for adoption. The approach includes clear phases and outcomes via agile information collection methods with delivery dependencies and parallel activities.
- **Technology:** Designed to guide clients through initial pilots to demonstrate the ability to accelerate the transition to quantum-safe cryptography, accelerate the remediation of applications within the enterprise, and establish a programme for full-scale deployment.

IBM Quantum Safe technology offers a comprehensive set of capabilities and approaches, combined with deep expertise, to help plan and execute a migration to quantum-safe cryptography. Quantum cyber resilience can be carried out over three phases—Discover, Observe, and Transform—each powered by IBM Quantum Safe technology:

- **IBM Quantum Safe Explorer** can enable organisations to scan source and object code to locate cryptographic assets, dependencies, and vulnerabilities to build a CBOM. This allows teams to view and aggregate potential risks into one central location.
- **IBM Quantum Safe Advisor** enables the creation of a dynamic or operational view of cryptographic inventory to guide remediation and analyses cryptographic posture and compliance to prioritise risks. Quantum Safe Advisor performs an enterprise-wide analysis of your cryptography and builds a comprehensive cryptographic inventory that details the types and locations of your cryptographic instances, the relationships between assets and data flows, and potential vulnerabilities to quantum technology.
- **IBM Quantum Safe Remediator** enables organisations to deploy and test best-practice-based quantum-safe remediation patterns to understand the potential impact on systems and assets as they prepare to deploy quantum-safe solutions. Remediator helps organisations to create an architecture for seamlessly upgrading cryptographic infrastructure to become quantum-safe.

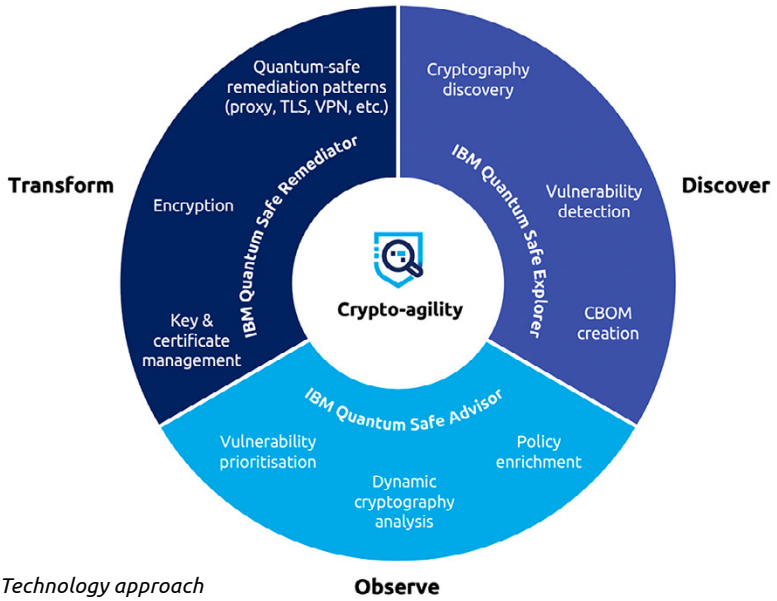


Figure 1. IBM Quantum Safe Technology approach

Cybersecurity and data protection guidelines

There are multiple existing cybersecurity risk management guidelines and frameworks that have been widely adopted by organisations, such as the following:

- **NIST Special Publication 800-37:** Risk Management Framework (RFM) for information systems and organisations: A system life cycle approach for security and privacy [RMF18].
- **NIST Cybersecurity Framework (CSF)** for improving critical infrastructure cybersecurity [CSF18].
- **ISO/IEC 27001:** Information security, cybersecurity and privacy protection – Information security management systems [ISO22a].
- **ISO/IEC 27005:** Information security, cybersecurity and privacy protection – Guidance on managing information security risks [ISO22b].

These standards share a common focus on effective risk management in information security, emphasising a systematic approach to comprehensively identify, assess, and manage risks. They advocate continuous monitoring, assessment, and improvement to address evolving cybersecurity threats, considering technical aspects, governance, processes, and human factors.

In Singapore, the Personal Data Protection Act (PDPA) aims to protect individuals' personal data by establishing guidelines for its collection, use, and disclosure. Organisations must implement reasonable security arrangements to safeguard personal data from unauthorised access, disclosure, alteration, or destruction. Cryptography plays a crucial role in cybersecurity risk management in ensuring data confidentiality, integrity, and authenticity. For example, encryption is used to secure data at rest, in transit, and during processing to mitigate the risk of data breaches and unauthorised disclosures, in alignment with PDPA requirements.

Despite their widespread adoption, current risk management frameworks lack provisions for quantum-safe security and reveal gaps that must be addressed. Consideration of quantum risks should be integrated into existing risk assessment processes. Organisations must focus on evaluating the longevity of the data that supports critical applications. For prolonged data protection, there is a pressing need to introduce additional mitigating controls. Quantum computing threats pose risks to sensitive health and financial data, compromise the confidentiality of communications, challenge the integrity of digital documents, and threaten cryptocurrencies.

The emergence of 'harvest now, decrypt later' tactics underscores the urgency for organisations to fortify their cybersecurity measures against quantum advancements. Proactive adjustments to risk management strategies are crucial to navigate evolving threats and ensure the resilience of information security frameworks in the face of quantum challenges.

Quantum risk assessment

In what follows, we give an overview of two examples of quantum risk assessment frameworks which have been published within the quantum-safe community: Mosca's Quantum Risk Assessment (QRA) [MM23] and Crypto Agility Risk Assessment Framework (CARAF) [Ma21]. Moreover, we highlight the limitations of the frameworks.

Mosca's QRA uses a time-based approach to define risk that is dependent on when migration to a quantum-safe state begins and considers 'harvest now, decrypt later' attacks. The methodology for the framework has been adapted from the six stages for conducting a risk assessment outlined in the NIST Cybersecurity Framework [CSF18].

Mosca's 'x, y, z' quantum risk model focuses on the dimensions of the impact of quantum computing. The 'x' parameter represents the lifetime of assets (the number of years encryption must be secure). The 'y' parameter indicates the time required to migrate to a quantum-safe state (the number of years required to bring current IT infrastructure to a quantum-safe state). The 'z' parameter considers the time until current cyber defences collapse in the face of threat actors with access to quantum technology (the number of years before a large-scale quantum computer is built). Based on these parameters, organisations can assess the urgency and potential consequences of quantum threats as a guide for the development of strategic and timely responses that ensure the security of their cryptographic systems.

CARAF builds on Mosca's QRA by specifically addressing cryptographic agility. Cryptographic agility involves the swift replacement of vulnerable cryptographic primitives, algorithms, and protocols with more secure alternatives. The conventional process of transitioning from one cryptographic solution to another can be time-consuming and can potentially leave organisations exposed to security risks during the transition period.

The CARAF framework can be used to systematically analyse and assess the risks arising from the absence of cryptographic agility. By leveraging CARAF, organisations can thoroughly evaluate their cryptographic systems' agility, identify potential vulnerabilities, and assess the associated risks. This analysis can be used for the development of a mitigation strategy that aligns with the organisation's risk tolerance. Essentially, CARAF provides a structured approach for organisations to navigate the challenges of crypto agility, enabling them to make informed decisions about their cryptographic infrastructure and security postures in the face of evolving threats and technological advancements. Further details on CARAF and Mosca's QRA, and their comparison can be found in [FS-ISAC23a].

Cautionary notes: The methodology used for the Mosca framework often results in assigning a low-risk classification when 'z' representing the time to compromise, ranges from 15 to 20 years. This approach tends to prioritise items with extended security and expected useful life timeframes over high-impact areas that may not require a prolonged security useful life. The emphasis is placed on identifying sensitive or critical data that could be vulnerable to future threats, including scenarios such as a 'store now and decrypt later' attack. The risk determination process categorises assets as either 'at risk' or 'not at risk' without considering nuanced risk levels for effective prioritisation. This means that assets with significant impact, such as the telecommunication control plane, may have lower 'x' or 'y' values but should not be categorised as having low, or no risk, and points to the need for more nuanced risk assessment [GSMA23].

Perspectives on quantum risk management

In 2016, the National Institute of Standards and Technology (NIST) projected that a quantum computer capable of breaking 2000-bit RSA encryption could be built by 2030 for about a billion dollars [Chen16]. However, various research institutes and technology firms have offered different timelines that range from less than 10 to up to 30 years. A reliance on speculative quantum timelines for risk assessment could potentially lead organisations to adopt a passive 'wait-and-see' approach. Organisations run the risk of being caught off guard, or left with insufficient time to take mitigation measures, if there is a breakthrough in the advancement of quantum computing in the near future. This risk increases if there is a new discovery, or design flaws, in the current crypto systems running in existing environments.

Our suggested approach moves away from relying on a specific quantum timeline and instead focuses on strengthening the overall cybersecurity risk management framework. Rather than adopting an entirely new framework, quantum risk management should be integrated into existing cybersecurity practices. The process should be continuous and adaptable based on dynamic threats, emerging vulnerabilities, and evolving regulatory environments. With an eye toward the need for the constant vigilance and adaptability that an ever-changing cybersecurity environment requires, key factors for managing quantum risk within an organisation are outlined below:

Get the basics right

Addressing the quantum threat requires that organisations proactively assess their readiness and understand both known challenges and potential unknown implications. The first step involves cataloguing all instances of cryptography usage which will include encryption keys, algorithms, applications, and their associated business processes. This comprehensive inventory will empower organisations to achieve crypto agility and enable strategic planning and adaptability in the evolving quantum-safe security landscape.

Effective monitoring of potential impacts requires careful consideration and the maintenance of critical elements. At a minimum, these elements should encompass the following aspects [FS-ISAC23a]:

- **Applications:** Organisations should assess both in-house and vendor applications, examining their utilisation of cryptographic algorithms. An inventory of critical and high-availability applications, along with an overview of internal and external application connections, is vital for a thorough understanding of the cryptographic landscape.
- **Third-party vendors:** Evaluate vendor roadmaps to ascertain their support for post-quantum cryptography. Procurement considerations should align with the organisation's commitment to PQC to ensure that vendors comply with evolving security standards.
- **Data:** It is crucial for organisations to determine the duration required for data asset protection. Classifying datasets based on sensitivity and criticality aids in developing a targeted security strategy. Additionally, organisations must assess the risk of a 'harvest now, decrypt later' attack scenario, especially for highly sensitive information.
- **Regulations:** Organisations should be prepared to respond to potential queries from regulators regarding compliance with industry standards and guidelines. Addressing questions promptly and transparently is essential to maintaining regulatory compliance.
- **Location of data:** Data residency introduces a layer of complexity, as different jurisdictions may have varying timelines for adopting post-quantum cryptographic measures. Organisations must align their strategies with regional timelines to ensure a cohesive and effective implementation of security measures. By systematically addressing these considerations, organisations can proactively navigate the challenges posed by the evolving quantum threat landscape.

Start small, start now

According to the World Economic Forum's Global Future Council on Quantum Computing, a staggering 20 billion digital devices are projected to require upgrading or replacement with PQC within the next two decades [WEF20]. Based on the scale of the required transition, it will not be a mere switch-out or patch. PQC will profoundly transform numerous devices and systems including ATMs, TV set-top boxes, smartphones, and many more. Algorithm replacement, a key aspect of transition, is disruptive and often requires years to complete. There is an urgent need for organisations to plan for, and adopt, a posture of crypto agility.

Commencing this transformative journey is not just recommended – it's a strategic imperative. Organisations are advised to adopt a pragmatic and phased approach, with key plans and objectives serving as a foundational framework for the migration process:

- Identify critical business processes: Identify key processes that are heavily reliant on critical data to understand specific areas demanding immediate attention.
- Conduct comprehensive risk assessment: Undertake a thorough risk assessment against critical business processes to evaluate vulnerabilities and potential threats for the creation of a risk register for structured mitigation.
- Establish risk tolerance and crypto agility: Define risk tolerance levels and embrace crypto agility principles, prioritising remediation efforts based on asset value or risk. Understand quantum technology capabilities and challenges, assessing the business impact of quantum computing advancements for informed decision-making in the quantum era.

A phased approach enables gradual adaptation, a focus on higher-value or higher-risk assets, and strategic alignment with the evolving quantum technology landscape.

Continuous learning and monitoring

Following the identification of cryptography uses for key business processes, and an initial risk assessment, organisations must adopt a vigilant and adaptive strategy that addresses expected quantum-resistant security challenges. Continuous development and monitoring are imperative:

- Monitor quantum computing development: Stay informed about ongoing developments, breakthroughs, and potential quantum applications that could impact existing cryptographic systems.
- Understand vulnerabilities in crypto systems: Develop a comprehensive understanding of both known and emerging cryptographic vulnerabilities associated with quantum threats through continuous research and awareness initiatives.
- Adhere to standards and regulatory requirements: Align with the emerging standards and regulatory requirements set by national cybersecurity institutions, such as the three new PQC standards recently announced by NIST [NIST04].
- Evaluate vendor readiness: Assess the readiness of third-party vendors and solution providers in the quantum realm, including technologies based on PQC, quantum key distribution (QKD), and quantum random number enerators (QRNG).
- Enhance crypto agility: Strive to efficiently update cryptographic algorithms, parameters, processes, and technologies to respond adeptly to new protocols, standards, and security threats posed by quantum computing. Consider factors such as data and cryptographic assets, cryptographic keys, and infrastructure limitations.

Furthermore, organisations should consider hybrid solutions that integrate classical and quantum-ready approaches. This strategic approach overlays existing security measures with robust post-quantum cryptography algorithms, providing assurance during the transition to quantum-safe security.

By adopting these ongoing measures, organisations can establish a resilient posture in the face of quantum computing advancements. This continuous development and monitoring strategy will fortify cryptographic systems and enable organisations to navigate the complexities of the evolving quantum landscape with agility and preparedness.

Next steps

Forward-leaning companies and governments are preparing for a quantum computing future and positioning themselves to capture the many benefits of this technology. Yet, more can and should be done, and collaboration is needed. Governments, researchers, academics, and industries will need to work together on policies to accelerate the adoption of new educational curricula, fund research and development, and create new talent pipelines.

Migrating to quantum-safe security requires a multi-pronged approach that combines proactive action, strategic planning, and continuous adaptation. In what follows, we summarise key next steps and considerations:

- **Inventory & assessment:** Start by identifying all assets and systems that rely on cryptography, especially those using vulnerable algorithms such as RSA and ECC. Prioritise assets based on their importance and the sensitivity of the data that they handle. Evaluate how the adoption of quantum-resistant algorithms might impact their performance and compatibility.
- **Pilots & testing:** Engage in pilot projects to test chosen PQC solutions in real-world scenarios. Assess the impact of PQC solutions on performance, check for compatibility issues, and identify potential integration challenges. Gather valuable data and feedback from these pilot projects to refine and enhance the overall migration strategy for the future.
- **Planning & strategy:** Develop a comprehensive migration strategy for adopting PQC algorithms. Evaluate and select PQC algorithms that align with specific security needs and requirements. Prioritise systems holding high-value data and critical infrastructure. Factor in costs, resources, and training considerations for each phase of the migration.
- **Deployment & rollout:** Implement PQC solutions in a phased manner, starting with high-risk or critical systems and data. Establish robust key management and lifecycle practices specifically designed for PQC keys to ensure their secure and effective use.
- **Awareness & training:** Educate employees on the risks associated with quantum computing and emphasise the necessity for migration to quantum-safe systems. Provide training to equip teams with the knowledge and skills required to securely use and manage quantum-safe systems. Foster a culture of cybersecurity awareness and vigilance across the organisation.
- **Monitoring & maintenance:** Continuously monitor implemented PQC solutions for vulnerabilities and performance. Stay informed about the evolving quantum threat landscape and adapt security measures. Keep a close eye on standardisation efforts by organisations such as NIST and ETSI.

The IBM-NCS value proposition

Why an IBM-NCS partnership?

The partnership between IBM and NCS is driven by the shared commitment to ensure quantum-safe security for organisations in Singapore and beyond. IBM, a global leader in quantum computing development, has not only been at the forefront of quantum technology but has also played a crucial role in creating quantum-safe technologies that were showcased in the NIST post-quantum cryptography competition. Three of the four technology finalists in that competition were developed by IBM in collaboration with industry and academic partners.

NCS stands out as a prominent digital and technology service provider in the Asia Pacific region and is particularly known for its role as a trusted system integrator for government agencies in Singapore over the past four decades. With a strong track record in successfully executing large-scale projects, NCS Cyber complements NCS' core capabilities in applications, engineering, and infrastructure with security solutions and services. This collaboration allows NCS to leverage IBM's expertise in quantum-safe security, ensuring that clients receive top-notch consultancy services.

The IBM-NCS partnership offers more than just advanced security solutions. We bring practical benefits to your business, such as ensuring compliance, gaining competitive advantage, and building customer trust in the era of quantum computing.Recognising the profound impact quantum-safe security will have on both legacy systems and new deployments dealing with sensitive data, NCS and IBM aim to prepare clients for a quantum-safe future through our combined knowledge and experience.

Specialised domain knowledge and capabilities

The collaboration between NCS and IBM brings together a wealth of specialised resources, including Ph.D.-trained personnel, qualified consultants, and skilled engineers. These resources each possess in-depth knowledge of the evolving quantum-safe technology landscape. This expertise spans the intricacies of cryptographic algorithms, their applications, and the systems and infrastructure where these algorithms find deployment.

This partnership transcends the conventional supplier-client relationship by offering more than just technology solutions. It extends to delivering comprehensive packages that encompass expert advisory services, processes, and experiences. Clients stand to benefit not only from cutting-edge technological advancements, but also from the collective expertise and proficiency of a team that is well-versed in navigating the complexities of quantum-safe implementations. As a result, the IBM-NCS collaboration ensures a holistic approach to addressing the challenges posed by quantum threats.

Localisation

NCS has a profound understanding of prevalent cybersecurity risk management and data protection frameworks that allows us to intricately navigate the guidelines and best practices stipulated by local authorities. We have a comprehensive knowledge of, and experience with, regulatory standards such as the Personal Data Protection Act (PDPA), IM8, CCoP 2.0, as well as sector-specific guidelines for the banking and healthcare industries. By leveraging this extensive expertise, NCS and IBM are uniquely positioned to align with local requirements in the realm of quantum risk assessment and management. The joint offerings of the partnership are designed to complement existing risk assessment frameworks and ensure a seamless integration that addresses the specific needs and intricacies of the local regulatory landscape. This approach underscores our commitment to delivering quantum-safe solutions that not only meet global standards but also resonate with the nuanced requirements of the communities they serve.

References

[WEF23] Quantum Readiness Toolkit: Building a Quantum-secure Economy. World Economic Forum, Jun 2023.

[Ma21] C. Ma et. al., CARAF: Crypto Agility Risk Assessment Framework, Journal of Cybersecurity, pages 1-11, 2021.

[MM23] M. Mosca and J. Mulholland, A Methodology for Quantum Risk Assessment. Global Risk Institute, 2023.

[Chen16] L. Chen et. al., Report on Post-quantum Cryptography, Vol. 12. US Department of Commerce, National Institute of Standards and Technology, 2016.

[GSMA23] GSMA, Guidelines for Quantum Risk Management for Telco version 1.0, 22 September 2023.

[RMF18] NIST Special Publication 800-37 - Risk Management Framework (RFM) for Information Systems and Organisations A System Life Cycle Approach for Security and Privacy, Revision 2, December 2018.

[CSF18] NIST Cybersecurity Framework (CSF): Framework for Improving Critical Infrastructure Cybersecurity version 1.1, April 2018.

[KM20] NIST Special Publication 800-57 - Recommendation for Key Management: Part 1 - General. Revision 5, May 2020.

[ISO22a] ISO/IEC 27001: Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems, 2022.

[ISO22b] ISO/IEC 27005: Information Security, Cybersecurity and Privacy Protection – Guidance on Managing Information Security Risks, 2022.

[FS-ISAC23a] FS-ISAC: Risk Model Technical Paper, Post-quantum Cryptography (PQC) Working Group, 2023.

[WEF20] WEF: Global Future Council on Quantum Computing, June 2020. https:// www3.weforum.org/docs/WEF_Global_Future_Council_on_Quantum_Computing.pdf.

[NIST24] NIST Releases First 3 Finalised Post-quantum Encryption Standards, August 2024. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

a framework for evaluating 5G security solutions based on use case and level of security

Choon Hock Niow, Hoon Wei Lim

a framework for evaluating 5G security solutions based on use case and level of security

Choon Hock Niow, Hoon Wei Lim

Introduction

5G networks promise to bring significant improvements over 4G including faster data rates, ultra-low latency, and massive device connectivity. They also support new capabilities such as network slicing and edge computing to enable multiple 5G services. These 5G networks are designed with improved security features based on cybersecurity principles such as 'defence-in-depth', 'zero trust architecture', and 'secure by design'. However, the complexity that comes with 5G networks inadvertently increases the attack surface and adds security risks for 5G network operators and users. The key challenge that enterprises face today is how to implement the security required to protect their 5G services against cyber threats without impacting the operational benefits of the 5G network.

To address this challenge, NCS worked with the Cyber Security Agency of Singapore (CSA), a part of the Prime Minister's Office that is managed by the Ministry of Communications and Information, to conduct a comprehensive study on how available cybersecurity solutions could impact the effectiveness and performance of the User Equipment (UE) deployed within 5G networks. As 5G technology is still relatively new, there are no established guidelines to study the performance impact of the cybersecurity solutions on the UE in 5G networks. NCS developed the following evaluation framework to address this need:

- Identify suitable 5G use cases that include a range of 5G applications
- Define the security features by level of security
- Collect and process data for analysis
- Assess the operational impact of different configurations of security features on the UE in the 5G network
- Conduct a gap analysis to identify and address 5G cybersecurity gaps to further advance 5G cybersecurity solutions in the industry

Identification of 5G use cases

The use cases for the NCS study were selected after consultation with stakeholders to identify cases that cover a range of 5G applications and performance metrics. These use cases are as follows:

- Teleoperations over 5G to simulate the robotics and teleoperation industries
- Video streaming and facial recognition over 5G to simulate 5G video analytics operations applied across multiple industries
- Mixed reality over 5G to simulate 5G applications of mixed reality devices in operational environments (i.e., usage in healthcare settings)
- 5G Network slicing to test the availability and reliability of slicing capabilities of the 5G network

The diagram below shows how the use cases were set up in the 5G testbed and Multi-access Edge Computing (MEC) over a 5G network.

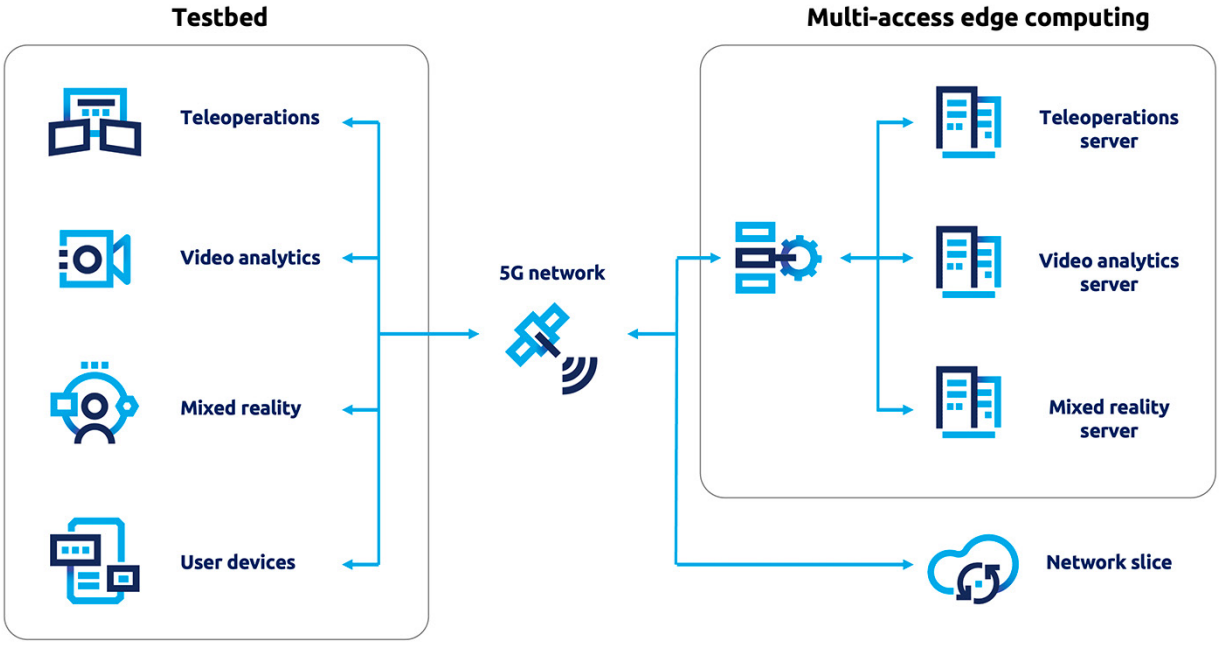


Figure 1: An overview of our 5G testbed setup

The performance metrics selected for the study were throughput, latency, battery consumption, CPU usage, and memory usage. Metric selection was based on the ability to assess impact on operations (i.e., an increase in latency and battery consumption may impact performance of a teleoperations application over 5G).

For testing purposes, all UE deployed in the use cases should ideally be 5G-native to ensure end-to-end secure communication over the 5G network. If the UE deployed cannot be 5G-native (due to device limitations), it should be securely connected, either wired or wirelessly, to 5G Customer Premise Equipment (CPE) or other 5G devices to ensure secure end-to-end connectivity to the 5G network.

Definition of security features

To assess the impact on operations, at each security level, across use cases, the required security features at each level must first be defined so that they can be implemented on the UE. The hypothesis is that the performance impact is related to the number of security features and the security settings used. By way of illustration, a UE should be expected to have high CPU usage if a large number of security features, with high security settings, is used.

As there is no generally agreed framework for defining these security features at different security levels, established5G cybersecurity standards such as those provided by the U.S. National Institute of Standards (NIST) and the European Union Agency for Cybersecurity (ENISA) were used as the basis for selecting the relevant security features and mapping those features across different security levels. For instance, there is no agreement on the security features required for a 'baseline security' level, while a 'low security' level must have the minimum number of security features and lowest security settings (e.g., AES-128) required to secure the UE in the 5G network. A 'high security' level will have all security features enabled and set to the highest security settings (e.g., AES-256) on the UE.

All security features should be available within the identified cybersecurity solution to ensure an end-to-end performance evaluation, however, as a practical matter, there is no cybersecurity solution that can fully cover all security features. For instance, some security features may not be available due to factors such as an unsupported device operating system or a lack of market demand for the security feature. As such, there is a need to identify and address these cybersecurity gaps through a gap analysis.

Data collection and process

The data collected for assessing performance metrics should be automated, to the extent possible, using data logging to minimise human error and workloads. Automation can be achieved through installing agents within the UE or via simple written codes that log data during measurement and retrieve the data after the measurement is completed. Data formats should be standardised to support data processing and analysis. Measurement should be performed as close to the application layer as possible, and live traffic from the application should be used for measurement to ensure the most accurate representation of the user experience during operation.

Multiple runs should be conducted to collect as much data as possible to derive the average, upper limit, and lower limit of the performance metric. The average can be used to determine the typical value of the performance metric, and the upper and lower limits will determine the spread of the performance metric.

Operation assessment

After data is collected and processed for the performance metrics measured in each of the use cases based on different security levels, the results of the performance metrics at low to high security levels can be compared against the baseline security level to determine the percentage change in the performance metrics. For instance, a 50% increase in latency translates to a two-fold increase in response time, and a 50% increase in battery consumption means that the battery-operated device can last only half as long. This will provide a comprehensive and quantitative assessment of the operational impact for each use case.

Gap analysis

After the assessment of impact to operations is completed, a gap analysis should be conducted to compare the available security features used during the study versus the required security features. This will help to identify the gaps in the security features for 5G devices and point to recommendations, such as development of security features, to bridge the gaps. The key findings from the gap analysis performed by NCS in its study are as follows:

- Not all security requirements for 5G devices can be covered by a single security solution. A combination of solutions is required to secure the 5G devices and network. Devices should be carefully selected to ensure that they can support the security features provided by vendors.
- Vendors can develop new security features to address the identified feature gaps in their product roadmaps. However, development will be dependent on several factors such as market trends and user demand for the security features in 5G devices.
- Some security features can be developed in-house through writing software code to build customised applications.
- System integration is required to ensure different security solutions can interoperate within the same 5G devices and network with minimal performance impact or impact to operations.

NCS strategy for 5G security

NCS possesses the necessary skills, resources, and capabilities to address the 5G cybersecurity gaps and further advance 5G cybersecurity solutions in the industry. These include:

- A suite of 5G professional services that is built on the expertise of NCS and its partners in areas such as compliance and risk management
- A team of qualified and certified cyber professionals with unique domain knowledge in IT, OT/ IoT, and 5G security
- Strong research capabilities and close collaboration with the National University of Singapore (NUS) and leading cybersecurity vendors

Conclusion

5G capabilities such as network slicing are still evolving. There is a need to stay current on the latest 5G cybersecurity technical solutions that will protect critical 5G systems and services against emerging threats. At the same time, there is also a need for a balance between meeting cybersecurity needs and ensuring minimal impact to the performance of 5G services.

This evaluation framework provides a systematic approach to validating the most suitable security configurations that will maximise 5G benefits and minimise impact to operations, based on use case. At the same time, it also allows enterprises to identify 5G cybersecurity gaps, so that system integrators, such as NCS, can develop the required security features to meet the enterprise's operational and security requirements.

References

Cybersecurity Agency of Singapore. (2022). Guidelines for CII Owners to Enhance Cyber Security for 5G Use Cases.

phishing detection

Nay Oo, Hoon Wei Lim

phishing detection

Nay Oo, Hoon Wei Lim

Executive summary

Phishing, an increasingly complex cyber threat, affects various communication channels beyond emails, such as texts and social media.

These attacks, aimed at stealing personal data or financial fraud, use sophisticated social engineering, challenging traditional firewall defences. Phishing's global impact, financial damages, and targeted nature necessitate advanced solutions.

This white paper introduces a novel AI-based approach using Natural Language Processing (NLP) and computer vision to counter these evolving cyber threats.

The scope of phishing

Phishing attacks have become a prominent threat globally and consistently rank among the top cybersecurity concerns in numerous reports. They cause significant financial losses annually. The FBI's Internet Crime Complaint Centre reports more than US$1.8 billion was lost in the United States in 2021 due to business email compromise (BEC) scams alone. The frequency and sophistication of phishing attacks has been increasing, with cybercriminals employing more advanced methods to evade detection.

Targeted spear-phishing

Spear-phishing attacks are highly targeted attempts where cybercriminals customise their deceptive messages to specific individuals or organisations. These attacks are more successful because they often use personal information to create a semblance of legitimacy.

Industry-specific vulnerabilities

Certain sectors, notably finance, healthcare, and government, are more vulnerable to phishing attacks due to the sensitive nature of the data they manage.

Phishing detection techniques

Current phishing detection solutions range from simple rule-based heuristics to advanced machine learning and AI-based methods. These solutions include user behaviour monitoring, the sandboxing of suspicious links or attachments, URL analysis using blacklists and reputation databases, and real-time URL scanning. Multiple deep learning models, including computer vision and NLP, can be combined to create a novel, comprehensive, anti-phishing solution.

The growing threat of phishing

Phishing in 2023

Around 4,100 phishing attempts were reported to the Singapore Cyber Emergency Response Team (SingCERT) in 2023, less than half of what was reported in 2022. Notwithstanding the decline, the number of phishing attempts was still about 30% higher than that in 2021.

Evolving phishing strategies

Bad actors are constantly refining their phishing strategies to bypass conventional detection methods. They often use URL shortening services to obscure malicious links and create webpages that are visually indistinguishable from legitimate sites. Advanced phishing schemes also use image-based text to avoid text-based detection and employ homograph attacks to trick users into visiting harmful websites.

Our innovative solution

In response to the sophisticated and evolving nature of phishing attacks, we have developed a state-of-the-art detection system that synergises deep learning models, including computer vision and NLP. Our system has an in-depth understanding of phishing markers and operates on a proactive knowledge base that is continuously updated with the latest information on popular global websites, with a particular focus on Singapore.

In Table 1, we evaluated the features included with Google Safe Browsing, Microsoft Office 365, and other readily available commercial off-the-shelf (COTS) solutions in the market, and compared those to our solution:

No.	Capabilities	Ours	Google Safe Browsing	Office 365	COTS
1	Computer vision	Yes	Yes	No	No
2	Knowledge-based centric	Yes	No	No	No
3	Logo detection	Yes	No	No	No
4	Heuristics	Yes	No	Yes	Yes
5	HTML text NLP	Yes	No	No	Yes
6	URL and domain reputation	No	No	Yes	No
7	Suspicious files	No	No	Yes	Yes
8	Sandboxing	No	No	No	Yes
9	Behaviour-based detection	No	No	No	Yes
10	Blacklist OSINT	No	Yes	Yes	Yes

Table 1: Capabilities comparison table

Brand verification

Our system compares webpages that are suspected of being fraudulent to a list of known, legitimate, brand webpages. This process helps us identify instances where a webpage appears very similar to a legitimate brand's website but uses a different domain. When we detect such a similarity, we flag the webpage as a phishing site that is targeting the brand it resembles.

Advanced phishing detection techniques

Brand verification

Our system meticulously compares suspicious webpages with an extensive list of legitimate brand webpages, identifying deceptive sites that mimic the appearance of authentic brands but operate under different domains.

Employing computer vision

We utilise advanced computer vision algorithms to analyse webpage screenshots and logos. This analysis is instrumental in detecting phishing sites that imitate the visual design of legitimate brands and enhances our ability to identify potential threats accurately.

Natural Language Processing

Complementing our computer vision capabilities, we employ NLP to extract and analyse information from the HTML source code of webpages. This process helps us to identify the indicative linguistic patterns and cues of phishing attempts.

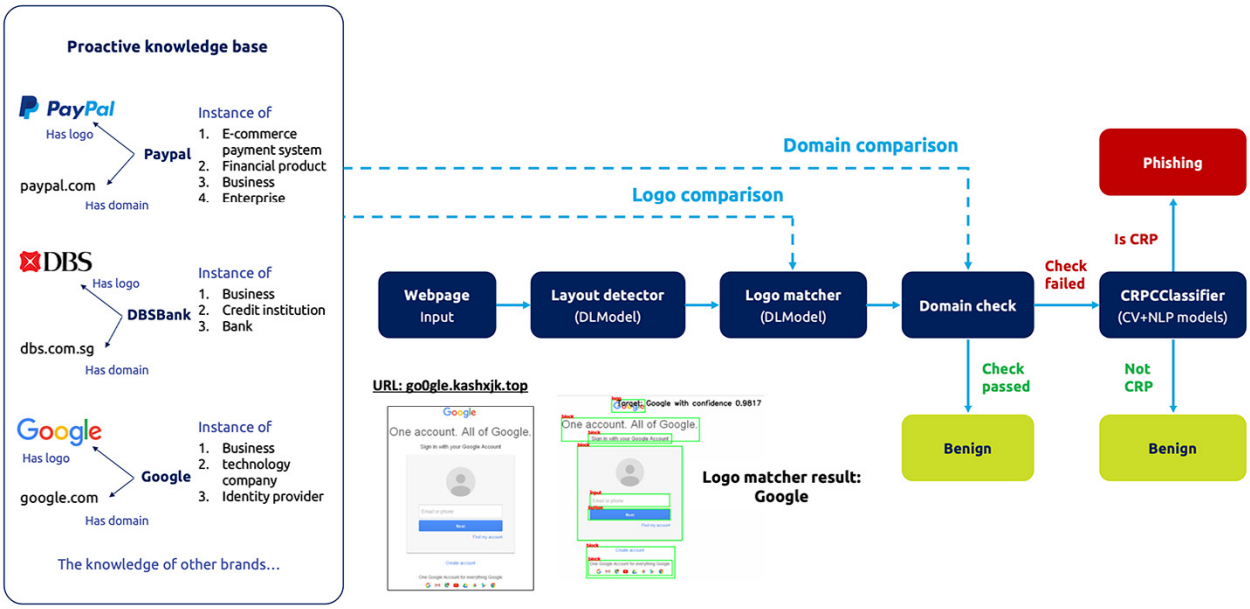


Figure 1: NCS Multi-model Phishing Detection system

As depicted in Figure 1, our detection system incorporates a suite of deep learning models, enabling us to detect sophisticated phishing attempts that elude traditional detection methods. We analyse multiple elements, including webpage layout, logos, and textual content, to ensure a comprehensive approach to phishing detection.

Deep learning for explainable detection

Our multi-model approach includes several critical components:

- Web page layout detector: Analyses webpage layouts for inconsistencies and anomalies that are characteristic of phishing sites
- Logo matcher: Compares logos against known brands to detect counterfeit usage
- Domain checker: Scrutinises domains to identify suspicious or deceptive URLs
- Credential Request Page (CRP) classifier: Identifies pages designed to capture sensitive information

Proactive knowledge base

A key feature of our system is its proactive knowledge base, which serves several essential functions:

- Continuous updates: Houses and continuously updates current information on popular websites globally
- Focus on Singapore and government sites: Specifically tracks Singaporean websites and government portals for enhanced local protection
- Semi-automatic knowledge retrieval: Gathers information from multiple sources, including the Google Image API and Wikidata Extractor to ensure a comprehensive and up-to-date database

Advantage of our solution

Our AI-powered approach offers several advantages over standard phishing detection solutions:

- Enhanced detection accuracy: The combination of computer vision and NLP enables us to detect phishing sites accurately, even when fraudsters employ advanced tactics to mimic legitimate brands. In testing using the OpenPhish and Tranco datasets, our solution received an F1 score of 89%, demonstrating the robustness of our approach. Moreover, our model demonstrated exceptional precision, reaching 97.1%, which indicates a low false positive rate. Additionally, our experiment showed a recall rate of 82.3%, indicating our ability to effectively detect malicious websites. These outcomes highlight the efficacy of our methodology in enhancing cybersecurity measures and identifying phishing threats.
- Adaptability: As phishing techniques continue to evolve, our solution can be updated to recognise new patterns and trends to ensure ongoing protection against emerging threats.
- Reduced false positives: By employing multiple detection techniques, we reduce the likelihood of false positives and minimise disruptions to legitimate web traffic.
- Protection for targeted sectors: The financial services, government, and logistics sectors are frequent targets of phishing attacks, and can benefit greatly from our advanced detection system.

Conclusion

Phishing attacks are a persistent problem for individuals and organisations alike. The tactics employed by malicious actors are constantly evolving, making it difficult to rely on traditional rule-based firewall defences.Our AI-powered phishing detection solution leverages advanced NLP and computer vision techniques to provide a more robust defence against these malicious tactics.

Our solution compares suspicious webpages to a database of legitimate brand sites, analyses visual elements, and extracts information from HTML source code to deliver enhanced detection accuracy, adaptability, and protection for targeted sectors. We believe our approach represents a significant step forward in the ongoing battle against phishing attacks, particularly in a world where cyber threats are constantly changing.

References

Singapore Cyber Landscape. (2023). Cyber Security Agency, 2024. Retrieved from https://www.csa.gov.sg/docs/default-source/publications/2024/singapore-cyber-landscape-2023.pdf.

engineering cyber resilient Operational Technology (OT), Industrial Control Systems (ICS), and critical systems

Teo Harn Chin (Ken)

engineering cyber resilient Operational Technology (OT), Industrial Control Systems (ICS), and critical systems

Teo Harn Chin (Ken)

engineering cyber resilient OT systems

For large complex systems, there are literally millions of ways to fail to meet objectives, even after we have defined the 'right system'. It is crucial to work all the details completely and consistently and ensure that the design and technical activities of all the people and organisations remain coordinated.

– The Art and Science of Systems Engineering, NASA

Introduction

For complex engineering projects, adopting a systematic security engineering process is a vital step in developing Cyber Resilient Systems[1]. Not only is it commonly mandated for compliance reasons, but it is also the key enabler for:

- Integrating all activities related to achieving a well-planned and secure system into meaningful outcomes that meet security objectives
- Prioritising high value security controls
- Making meaningful trade-offs[2]
- Ensuring traceability and clear communication of impact, and
- Disseminating information to other stakeholders and downstream activities

However, in many projects, the project teams struggle, often encountering pitfalls that lead to:

- Inefficient and ineffective use of the time and efforts of stakeholders in security-related workstreams
- Security requirements that do not align with other considerations
- Communication gaps that impact the dissemination of information to stakeholders or downstream activities
- Challenges in conducting assessments and providing well-supported justifications for deviations and requests[3]
- Reworking cycles to remedy these issues

Collectively, this can result in significant costs due to wastage. Many of these pitfalls can be avoided by working with an experienced Operational Technology (OT) Security team that can skilfully lead and help stakeholders navigate the complexities. This paper highlights the six important areas for OT Security teams supporting complex engineering projects to consider, with examples drawn from the real-life delivery of a project that involved fabricating a new substation for an offshore wind farm.

Understand process best practices

We cannot overemphasise the importance of having a systematic process and a clear understanding of its requirements. This involves not only a thorough grasp of cybersecurity activities, but also the crucial integration of these activities and considerations into the overarching systems engineering and project processes.

In the context of critical systems or systems delivery in highly regulated industries, it is typically mandatory to establish a security programme that incorporates lifecycle process best practices. Applicable highly regulated industries include Aviation, Maritime, Land Transport & Rail, Healthcare, Power & Utilities, Oil & Gas, and Critical Information Infrastructure.

Various publications discuss compliance requirements or provide guidance on security programmes and best practices[4]. While general concepts and best practices are usually consistent across these publications, the level of detail on specific subtopics may differ. In our experience, PD CLC/TS 50701, the cybersecurity standard for rail applications, provides the clearest guidance on executing a robust security programme. Although it is intended for rail systems, it is aligned with ISA/IEC 62443, making it relevant and applicable across various industries. The process described in PD CLC/TS 50701 is also largely consistent with the process our team applies for our consultancy projects.

The PD CLC/TS 50701 standard provides detailed elaboration on the cybersecurity activities and the integration of cybersecurity with other project activities and deliverables across the 13 lifecycle phases (0-12), aligned with EN50126 Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). Table 1 shows details extracted from PD CLC/TS 50701 as a subset of these lifecycle phases for illustration[5] purposes. We recommend reading the relevant chapters of the original publication for complete details. Appendix B: 'Example Process Flowchart for Security and Safety Co-engineering' further illustrates the process for security and safety co-engineering.

Phases (Referenced EN 50126-1)		Synchronisation points and deliverables	Cybersecurity activities
0			
1	Concept	<u>SuC (system under consideration) Identification:</u> A) Operational environment incl. existing security-related controls and a high-level zone model A) Applicable security standards A) Purpose and scope B) Project cybersecurity management plan (incl. cybersecurity context, goals and lifecycle activities)	• Review of the level of security achieved up to now • Analysis of the project's security implications and context (incl. generic threats) • Alignment with railway operator/asset owner and stakeholders' security goals • Consideration of security lifecycle aspects (patch management, monitoring, etc.) • Plan cybersecurity-related activities
2	System definition and operational context	<u>System definition</u> <u>Operational context and criticality:</u> A) Essential functions B) Initial risk analysis results B) Zones and Conduits	• Review of the initial system architecture and of the logical and physical network plans • *Initial Risk Assessment for the SuC • *Partitioning of the SuC into zones and conduits • *Documentation of components interfaces and characteristics for each zone and conduits ** This activity and the corresponding synchronisation point may also be conducted in phase 3*
3-4			
5	Architecture and apportionment of system requirements	<u>CRC breakdown:</u> A) System cybersecurity requirements specifications incl. security-related application conditions B) Subsystem cybersecurity requirements specification incl. security-related application conditions, technical and organisational compensating countermeasures	• DRA update, incl. assessment of the SL-C for components and definition of compensating countermeasures incl. security-related application conditions • Assigning the technical security requirements to components • Assigning responsibilities for the organisational and physical requirements for the railway operator/maintainer or asset owner • Establish third party management for security aspects, incl. supplier security capabilities and support contracts
6-12			

Key

A) Information to be provided by all stakeholders contributing to the development, delivery, operation, maintenance and disposal of the SuC (e.g., System Engineering, Safety, RAM, V&V, etc.) to the cybersecurity team

B) Information to be provided by the cybersecurity team to the other stakeholders

<u>Underlined text</u> indicates synchronisation points

Table 1: Redacted contents on security-related activities within a railway application lifecycle (Reference: PD CLC/TS 50701:2023)

Determine the high-level compliance requirements and applicable publications

At the beginning of an advanced system engineering project, the OT Security team may face confusion about how to approach the project. Team members may be aware of some compliance standards, such as IEC 62443, ISO 21434, CLC/TS 50701, or DO-326, and specific functional requirements like central logging, continuous monitoring, and equipment patching. Additionally, the project may require various documentation deliverables, such as an OT Security management plan, vendor management plan, account management policy, and vulnerability management procedure.

However, the initial list of standards provided may not cover the full scope of necessary compliance. For instance, Singapore regulations mandate that Critical Information Infrastructure (CII) systems comply with CCOP, healthcare systems handling patient data may be subject to HIPAA, and airborne systems requiring airworthiness certification may need to adhere to standards like DO-178. Therefore, relying solely on the standards guidance provided by project stakeholders may result in incomplete adherence to the complete regulatory and standards requirements.

Meeting functional requirements such as central logging impacts the entire system development lifecycle. This necessitates prioritising devices with logging capabilities and built-in log exportation features, which must be validated throughout the development process. To ensure that these activities are properly executed, adopting a suitable framework such as the approach described in NIST SP 800-160 is essential. Additionally, other guidelines and publications may be needed to develop specific documentation deliverables such as an account management policy.

The OT Security team should proactively conduct its own research and assessments to determine the full suite of applicable regulations, standards, and publications. Early discussions with project stakeholders are crucial to ensure that all requirements are identified and understood. Documenting this information in relevant management plans, such as the OT Security management plan and vendor management plan, is essential for effective information flow and alignment throughout the project.

Understand the context for systems and stakeholders

Understanding the contexts—for stakeholders, systems, and roles—is crucial for successful planning and project execution in an advanced systems engineering project. This comprehensive understanding lays the foundation for effective planning and ensures that all aspects of the project are well-coordinated and aligned with the goals.

The system context, including early indicators from risk assessments, is vital for planning and assessing the system's criticality. Before conducting detailed risk assessments, initial judgments can be made based on the system's intended function, asset composition, interactions with other systems, communication interfaces, and the data traversing these interfaces. These early insights help in shaping the security strategy and expected efforts for the system.

In such projects, the OT Security team will likely interface with multiple stakeholders, including regulators, asset owners, and system operators. For systems in highly regulated domains, or requiring external certifications, stakeholders may also include regulators or external compliance/certification bodies. Security and the Information Security Management System (ISMS) considerations impact most stakeholders. Planning and strategy activities that lead to deliverables like plans and procedures require an understanding of these stakeholders' contexts to define their roles and responsibilities within the ISMS framework effectively.

As the subject matter experts, the OT Security team is expected to provide advice to other stakeholders on project efforts, activities, and various scenarios. Its expertise is crucial for guiding stakeholders through the planning process, helping them understand the projected efforts and activities affecting their work streams, and advising on the next steps for different scenarios, such as seeking deviations or waivers and determining endorsements. A deep understanding of the context is essential for performing this advisory role professionally.

Understand the expected information available, shortlist the applicable non-cybersecurity technical deliverables for tracking, and determine the information gaps

Security-related activities and deliverables cannot be accomplished without close participation and input from technical subject experts and project sub-teams. Security practitioners must be able to play an active role to lead the process, as they cannot rely on non-security-trained stakeholders to know or anticipate the required information or to document it in a format directly relevant to security activities. Effective and meaningful discussions and clarifications are often necessary to bridge this gap.

Security practitioners should leverage non-security resources to gain the initial context needed to lead meaningful discussions, assessments, and surveys. In our experience, the master document list (or master document register) of the project is an excellent starting point. It provides insights into the information that will be documented throughout the project lifecycle, and when this information will become available.

Wiring construction diagrams or electrical connection diagrams are valuable references for understanding the expected network and communication interfaces between components. We have used information from these documents to create system network diagrams and data flow diagrams for threat modelling. Additionally, documents on functional safety assessments and failure analysis are useful for understanding the functional criticality of system components and the corresponding impact of failures. These documents provide meaningful knowledge that is essential for performing cybersecurity risk assessments.

Implement adequate security controls

Implementing security controls involves the act of balancing the adequacy of protection for the system against the cost of implementing those security controls. A risk-based approach towards implementation will allow adequate security controls while also ensuring the distribution of budget across the system based on needs and necessity.

In our experience, IEC 62443-3-3 is a great reference that provides a comprehensive list of security controls to be considered, and a breakdown of controls based on the severity level of the system components. When planning the security controls to implement, planners can reference the publication as a good starting point, even for projects that do not mandate IEC 62443 compliance.

In summary

Engineering cyber resilient OT systems requires meticulous planning, a thorough understanding of the system and stakeholder contexts, and effective collaboration among various teams. The OT Security team plays a pivotal role in guiding stakeholders and ensuring that security requirements are well-integrated into a project's broader objectives. They undertake six main tasks: understanding compliance requirements, engaging stakeholders, conducting risk assessments, implementing security controls, ensuring continuous monitoring, and facilitating patch management. By leveraging non-security resources and integrating early risk assessment indicators, the team can develop a comprehensive security strategy that aligns with a project's goals and lifecycle. This proactive and context-driven approach enhances the security posture, facilitates efficient resource use, and ensures that security considerations are seamlessly incorporated into the system development process.

Appendix A: Detailed Extracts from PD CLC/TS 50701:2023 on Cybersecurity Process and Synchronisation

Phases (Referenced EN 50126-1)		Synchronisation points and deliverables	Cybersecurity activities
0	Prerequisites		• Railway operator's security programme is established • Manufacturer's and integrator's secure development process is established • Legal and regulatory framework is identified
1	Concept	<u>SuC identification:</u> → Operational environment incl. existing security-related controls and high-level zone model → Applicable security standards → Purpose and scope ← Project cybersecurity management plan (incl. cybersecurity context, goals and lifecycle activities)	• Review of the level of security achieved up to now • Analysis of the project's security implication and context (incl. generic threats) • Alignment with railway operator/asset owner and stakeholder's security goals • Consideration of security lifecycle aspects (patch management, monitoring, etc.) • Plan cybersecurity-related activities
2	System definition and operational context	<u>System definition:</u> → System boundaries → Initial system architecture, incl. list of functions, interfaces and generic systems → Logical and physical network plans ← Initial system architecture review, logical and physical network plans review Operational context and criticality: → Essential functions ← Initial risk analysis results ← Zones and conduits	• Review of the initial system architecture and of the logical and physical network plans • *Initial Risk Assessment for the SuC • *Partitioning of the SuC into zones and conduits • *Documentation of components interfaces and characteristics for each zone and conduits * *This activity and the corresponding synchronisation point may also be conducted in phase 3*
3	Risk analysis and evaluation	<u>DRA:</u> → Functional requirements (linked to essential functions) ← Initial threat log ← Potential updates (zones and conduits, network plans)	• Detailed Risk Assessment (DRA) • Derive technical (e.g., SL-T), physical and organisational countermeasures or assumptions for zones and conduits • Consider business continuity aspects (incl. incidence response and recovery) for the SuC
4	Specification of system requirements	<u>CRC release:</u> ← System cybersecurity requirements specifications incl. security-related application conditions	• SuC-specific refinement of normative requirements • Definition of organisational and physical requirements • Definition of security-related application conditions
5	Architecture and apportionment of system requirements	<u>CRC breakdown:</u> → System cybersecurity requirements specifications incl. security-related application conditions ← Subsystem cybersecurity requirements specification incl. security-related application conditions, technical and organisational compensating countermeasures	• DRA update, incl. assessment of the SL-C for components and definition of compensating countermeasures incl. security-related application conditions • Assigning the technical security requirements to components • Assigning responsibilities for the organisational and physical requirements for the railway operator/maintainer or asset owner • Establish third party management for security aspects, incl. supplier security capabilities and support contracts

6	Design and implementation	No synchronisation	• Follow product lifecycle (EN IEC 62443-4-1 and 4-2 or other adequate cybersecurity standards) • Consider and prevent potential conflicts between component cybersecurity functionality and functional architecture
7	Manufacture or procurement	No synchronisation	• Follow product lifecycle (EN IEC 62443-4-1 and 4-2 or other adequate cybersecurity standards) • Consider and prevent potential conflicts between component cybersecurity functionality and functional architecture
8	Integration	<u>Subsystem and component integration:</u> ← Cybersecurity acceptance of security components used by the SuC → Integration test documentation including SuC environment information ← Cybersecurity verification results of the integrated SuC	• Review of logical and physical network plans, list of systems and installed applications after implementation • Security verification of security components • Security testing of the integrated system under consideration (e.g., penetration testing and vulnerability scanning) • Check and ensure removal of unnecessary software, hardware and services • Update of threat risk assessment based on the results of phases 6 'Design & Implementation" to 8 "Integration'
9	System Validation	<u>Subsystem and component integration:</u> ← Cybersecurity case incl. security-related application conditions ← Security guidelines	• Verification of security guidelines • Validation of configuration and security functionality • Applicability verification of organisational requirements and security-related application conditions
10	System acceptance	<u>Cybersecurity acceptance:</u> ← Cybersecurity case updated incl. security-related application conditions ← Security guidelines updated	• Completion by the system integrator of the cybersecurity case and security-related guidelines • Security handover between system integrator and railway operator • Review of business continuity aspects (incl. incidence response and recovery) for the SuC
11	Operation, maintenance and performance monitoring	<u>Cybersecurity case updates:</u> ← Continuous updates of the cybersecurity case based on vulnerabilities, incidents and changes incl. security patches	• Maintenance of the logical and physical network plan and the list of the IT systems and installed applications • Perform security and vulnerability monitoring and risk-based incidence response including risk analysis updates • Perform patch and/or configuration management • Perform data backup and auditing procedures to enable data recovery • Maintenance of restrictive access authorisations • If applicable, prepare and perform security (compliance) audits
12	Decommissioning	<u>Disposal of confidential material:</u> ← Disposal report	• Disposal of components taking security criteria into account

Key

→ *Information to be provided by all stakeholders contributing to the development, delivery, operation, maintenance and disposal of the SuC (e.g., System Engineering, Safety, RAM, V&V, etc.) to the cybersecurity team*

← *Information to be provided by the cybersecurity team to the other stakeholders*

<u>Underlined text</u> indicates synchronisation points

Table 2: Security-related activities within a railway application lifecycle (Source: PD CLC/TS 50701:2023)

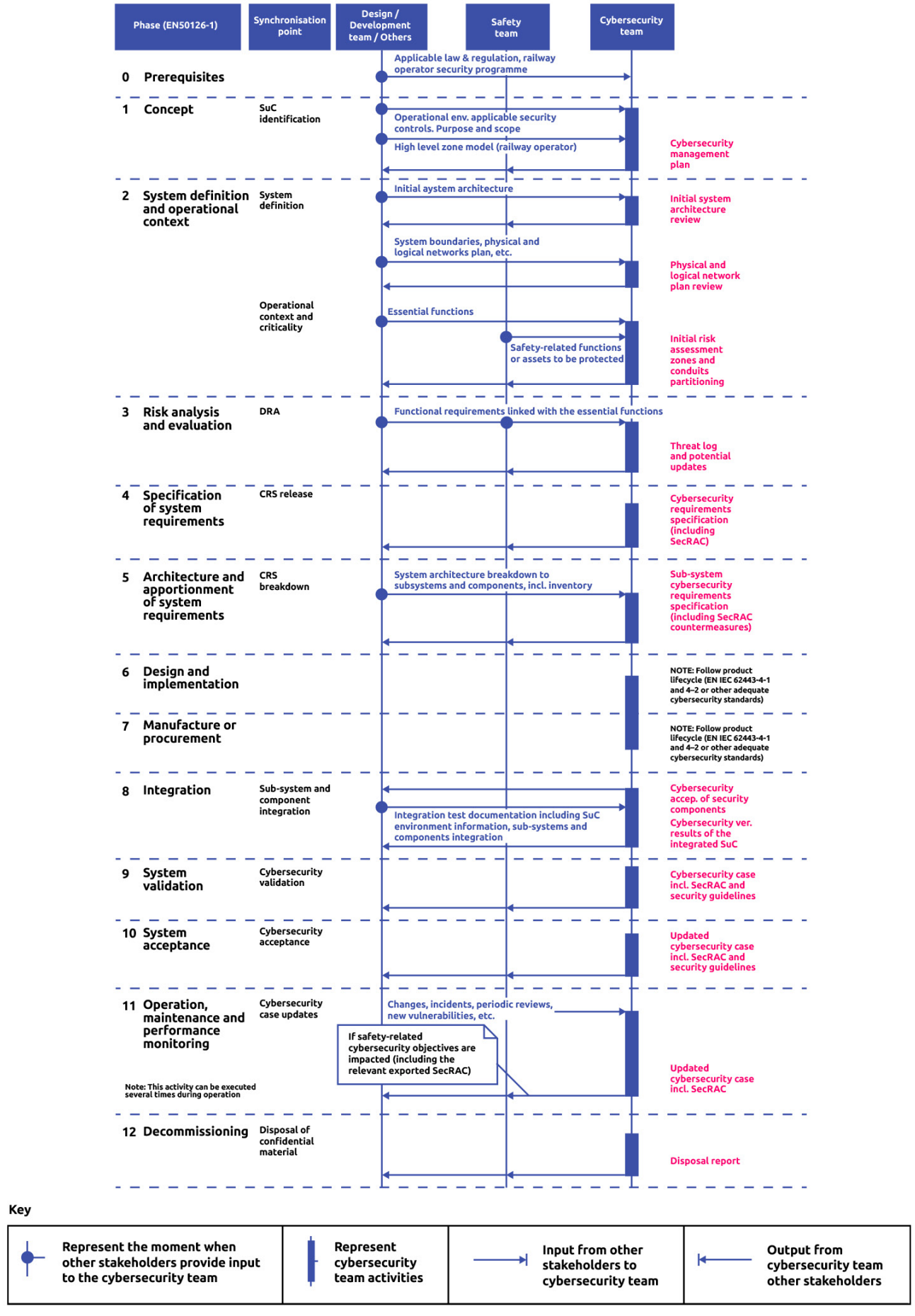


Figure 1: Synchronisation between cybersecurity team and other stakeholders (Source: PD CLC/TS 50701:2023)

Appendix B: Example Process Flowchart for Security and Safety Co-engineering

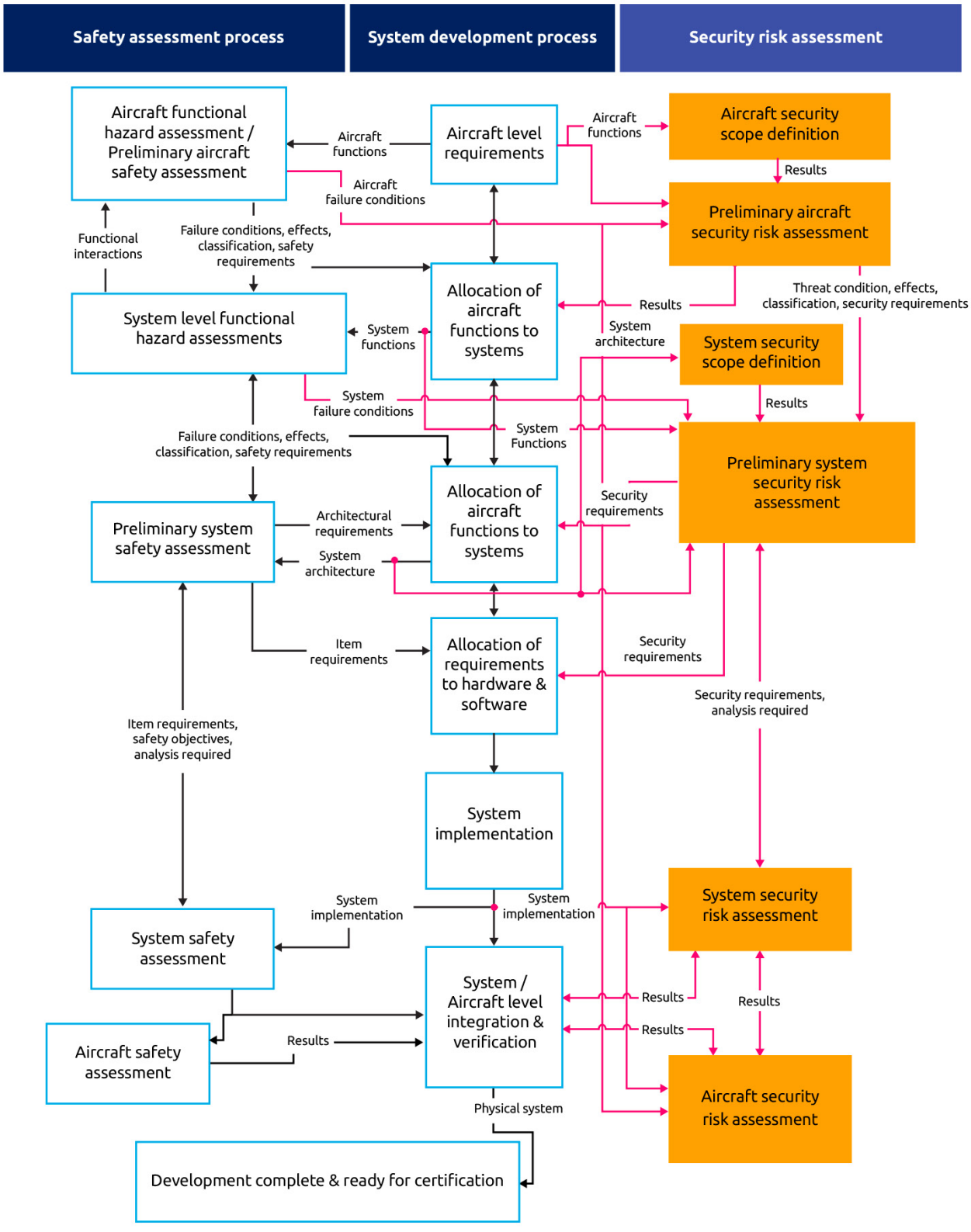


Figure 2: Airworthiness security process as part of Aircraft Certification Process (Source: Recommendations for Security and Safety Co-engineering, Information Technology for European Advancement)

fortifying the last line of cyber defence through cryptography

Choon Hock Niow, Hoon Wei Lim

fortifying the last line of cyber defence through cryptography

Choon Hock Niow, Hoon Wei Lim

Executive summary

Cryptography is foundational and ubiquitous in data security, yet its importance and complexity are often undervalued. As computing technology becomes increasingly powerful and sophisticated, strong cryptography is more crucial than ever. It can serve as the last line of defence in a zero trust model that relies on multi-layer security to protect an organisation's most valuable assets. However, implementing cryptography correctly is challenging and requires specialised expertise. This article explores the complexities of cryptography and provides insights on managing the cybersecurity risks associated with its use and management. We emphasise the importance of cryptographic visibility—maintaining an up-to-date inventory of all cryptographic assets—and cryptographic agility – the ability to quickly adapt to new threats by updating or replacing algorithms. These practices are essential components of good cyber hygiene that will ensure robust and adaptable cryptographic security. By focusing on these areas, organisations can better protect their data and maintain the integrity of their systems in an ever-evolving threat landscape.

Cryptography translates to trust

Cryptography is the practice of securing information by transforming it into an unreadable format that is only decipherable by those who possess a secret key. In the digital world, cryptography is a cornerstone of trust. It acts as the backbone of secure communication and data protection, enabling trust in online interactions, and safeguarding valuable information. More than 96% of current web traffic is protected through cryptography (Figure 1).

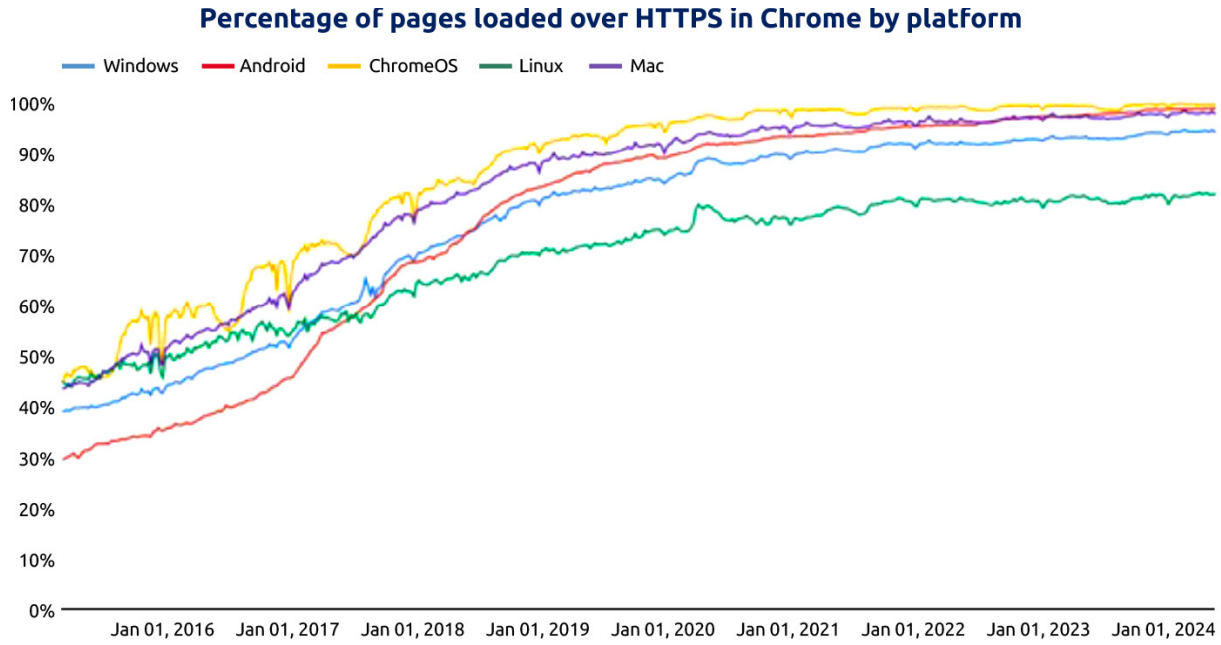


Figure 1: Google transparency report indicated that more than 96% of today's web traffic is encrypted.

Cryptography is essential to cybersecurity in multiple ways. It ensures confidentiality and protects sensitive data from unauthorised access and enables the detection of tampering or alteration of data for integrity verification. It also serves as an authentication mechanism, through the use of digital certificates, for identity verification of users and systems. Furthermore, cryptographic controls are often required for regulatory compliance, with many regulations mandating the implementation of specific cryptographic measures to safeguard data. By fulfilling these roles, cryptography provides a robust foundation for securing information and maintaining trust in digital communications and transactions.

Emerging trend: zero trust and last line of defence

For defence-in-depth, or multi-layer security, cryptography serves as the last line of defence. If a network or system is compromised, strong cryptography is crucial for preventing access to critical assets. It provides resilience against data breaches, ensuring that even if all other security measures fail, the encrypted data remains protected. Cryptography is fundamental to the zero trust model, supporting authentication, enforcing access control policies, and securing data both at rest and in transit. The encryption of sensitive information ensures that unauthorised parties cannot access or decipher the data, and that confidentiality and integrity can be maintained, even in a compromised environment.

Kevin Kenan, in his book *Cryptography in the Database: The Last Line of Defence* [Ken05] emphasises the critical role of cryptography in safeguarding databases and positions it as the final layer of defence against potential breaches. As the 'crown jewels' of any organisation, databases require an additional layer of protection—strong cryptography—as the ultimate shield for scrambling data into unintelligible ciphertext that becomes useless if accessed by unauthorised parties.

Intricacies of cryptography

Effectively implementing cryptography is challenging for a number of reasons:

- **Algorithmic complexity:** Cryptographic algorithms are based on complex mathematical concepts such as prime numbers, finite fields, and elliptic curves that require specialised knowledge to understand and apply correctly. A subtle design flaw can significantly weaken an algorithm. For example, a flaw might compromise the required level of randomness or unintentionally reveal partial information about the secret key used for encryption.
- **Implementation challenges:** Turning theoretical cryptographic algorithms into practical applications introduces complexity. Issues can arise from programming errors, side-channel information leaks, and the use of insecure random number generators. These implementation flaws can undermine the security of the cryptographic system, making it vulnerable to attacks.
- **Key management:** Effective key management is critical for cryptographic security but is notoriously difficult. Setting up and maintaining a Public Key Infrastructure (PKI) is complex, particularly establishing a reliable root of trust rather than using self-signed certificates. Additionally, some organisations fail to update or renew cryptographic keys in their critical systems, further compromising security.
- **Human factors:** Humans are often the weakest link in cryptographic security. We are prone to errors and may overlook or simplify complex aspects of cryptography. Mistakes in key management, configuration errors, and the improper handling of cryptographic materials are common issues, introduced by humans, that can lead to vulnerabilities.

Given these challenges, getting cryptography right is a not-trivial matter, and managing cryptographic risks is critical.

Cryptographic risks

The improper use and management of cryptography can lead to increased risks of compromising data security or cybersecurity incidents. Such cryptographic risks can emerge from several sources:

- Legacy applications often use weak cryptographic methods that are challenging to upgrade. These outdated systems can create vulnerabilities that are difficult to address without extensive modifications.
- Vendors bound by existing support contracts may struggle to promptly implement new cryptographic algorithms in response to common vulnerabilities and exposures (CVE) reports. This lag in updating can leave systems exposed to known vulnerabilities for extended periods.
- New discoveries and breakthroughs in cryptographic research can render existing algorithms insecure. As researchers uncover weaknesses, or develop more advanced cryptographic techniques, previously secure methods may become vulnerable.

An evolving landscape requires constant vigilance and adaptation to maintain robust cryptographic defence. Ongoing updates and revisions to cryptographic practices and systems are essential as the dynamic nature of cryptography means that what is considered secure today may not be secure tomorrow.

Lessons learned from past decades

Let us take the Transport Layer Protocol (TLS) protocol, today's most widely used cryptographic protocol, as an example. Figure 2 summarises the evolution of the TLS protocol.

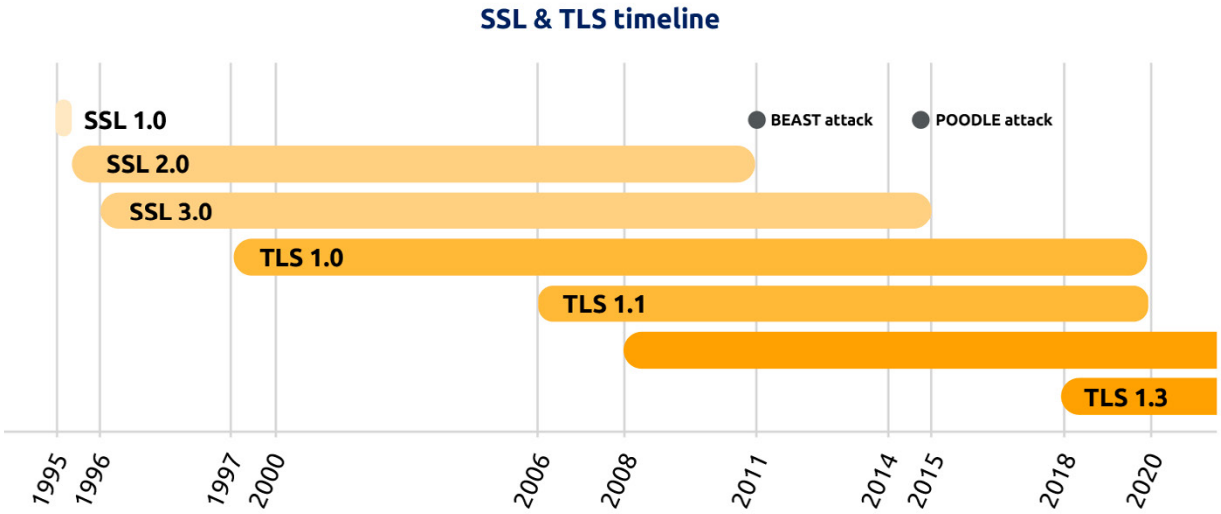


Figure 2: Evolution of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, which have been the foundation of securing web traffic.

When TLS was first introduced, then called Secure Sockets Layer (SSL), it had numerous design flaws and vulnerabilities. SSL 2.0, for example, lacked message integrity protection and relied on weak cryptographic algorithms like RC4 and SSL 3.0, and was susceptible to the POODLE attack, which exploited a fallback mechanism to downgrade secure connections to vulnerable sessions.

To address these issues, stronger cryptographic algorithms were incorporated into TLS 1.2, released in 2008. This version was widely adopted and remained a standard for a considerable period. The most recent version, TLS 1.3, brought significant improvements that focus on both performance and security. TLS 1.3 simplified the handshake process and eliminated outdated cryptographic algorithms, representing a major overhaul.

Some key lessons from the development of TLS over the past two decades include:

- **Continuous evolution:** Security protocols like TLS must continuously evolve to counteract emerging threats and vulnerabilities. The progression from SSL to TLS 1.3 demonstrates the necessity of ongoing updates and enhancements to maintain robust security.
- **Backward compatibility risks:** Supporting outdated protocols and algorithms for compatibility purposes can introduce significant vulnerabilities. It is crucial to phase out weak cryptographic algorithms to protect against potential exploits. The transition away from SSL to newer versions of TLS highlights the importance of updating cryptographic standards.
- **Implementation matters:** Even the most secure protocols can be compromised by poor implementations. A prime example of this is the 'Heartbleed' vulnerability in the OpenSSL software library, which exposed significant weaknesses despite the underlying protocol's strength. This underscores the importance of meticulous implementation and regular audits to ensure security.
- **Balancing performance and security:** Achieving the best security and performance simultaneously is challenging. TLS 1.3 demonstrates the importance of achieving a balance between these two aspects. The latest version of TLS not only enhances security but also optimises performance by streamlining the handshake process and removing obsolete algorithms.

Recommended cyber hygiene

Cryptography is foundational and ubiquitous in data security, yet its importance and complexity are often undervalued. As computing technology becomes increasingly powerful and sophisticated, strong cryptography is more crucial than ever. It can serve as the last line of defence in a zero trust model that relies on multi-layer security to protect an organisation's most valuable assets. However, implementing cryptography correctly is challenging and requires specialised expertise. This article explores the complexities of cryptography and provides insights on managing the cybersecurity risks associated with its use and management. We emphasise the importance of cryptographic visibility—maintaining an up-to-date inventory of all cryptographic assets—and cryptographic agility – the ability to quickly adapt to new threats by updating or replacing algorithms. These practices are essential components of good cyber hygiene that will ensure robust and adaptable cryptographic security. By focusing on these areas, organisations can better protect their data and maintain the integrity of their systems in an ever-evolving threat landscape.

Cryptographic risks

Having good visibility of what cryptography systems are in place and where and how cryptography is used within an organisation is essential for effective cryptographic risk management. This visibility allows for a comprehensive inventory of cryptographic tools and protocols and ensures that no critical assets are overlooked. It helps organisations to prioritise risks based on the sensitivity and importance of the data and allows for efficient resource allocation to the most critical areas.

As illustrated in Figure 3, cryptography plays a crucial role in telco customer-facing use cases by ensuring secure communication and protecting personal data. TLS encrypts online interactions between customers and telco servers, safeguarding sensitive information such as login credentials and personal data. Telco-provided VPNs enhance security by encrypting all internet traffic from a customer's device, especially over public Wi-Fi networks. Furthermore, encryption protects customers from the data stored in telco databases and ensures that it remains inaccessible without decryption keys. End-to-end encryption for SMS and voice services ensures that only intended recipients can access the content of messages and calls.

Internally within a telecom operator, cryptography secures the communication links and operational data within its networks. Encryption protects links between base stations and core network gateways, preventing unauthorised access to data such as call metadata and user locations. Encrypted channels safeguard sensitive operational data, such as configuration updates sent to base stations, from interception and manipulation. In the SIM provisioning process, cryptographic keys embedded during manufacturing authenticate and encrypt communications to prevent cloning and fraud. Encrypted data exchanges during SIM distribution secure provisioning information from interception or alteration. Overall, cryptography ensures secure communication, data protection, and operational integrity in the provision of telco services.

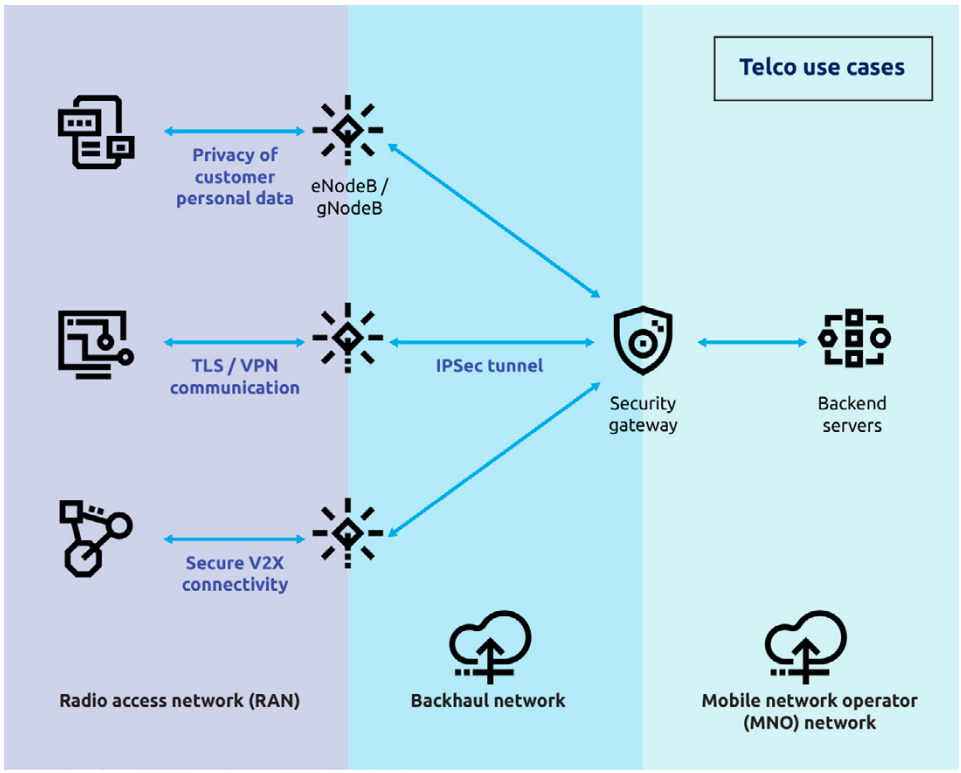


Figure 3: Evolution of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, which have been the foundation of securing web traffic.

A number of tools, both code-based and network-based, can be used to build a comprehensive cryptographic inventory, which is essential for effective risk assessment. This inventory should encompass information associated with all cryptographic assets deployed within or owned by the organisation. These assets may be related to in-house or third-party applications, and internal or external network services. Furthermore, the inventory should specify the lifetime of data that needs to be protected, and the implication to business goals if the data is compromised. By thoroughly cataloguing these elements, organisations can better identify vulnerabilities, prioritise mitigation efforts, and ensure that robust security measures are in place to protect sensitive information and maintain operational integrity.

Cryptographic agility

Once we have good cryptographic visibility, it is crucial to implement processes and mechanisms that can be used to swiftly respond to new cryptographic threats, while minimising the impact on interoperability with existing systems. This will ensure that as new vulnerabilities or advancements in cryptographic techniques arise, the organisation can adapt quickly without compromising security or disrupting operations. Establishing such responsive processes will involve regular monitoring, updating cryptographic protocols, and maintaining flexibility in systems design to integrate new algorithms seamlessly. This proactive approach will help in maintaining a robust security posture against emerging threats.

Cryptographic agility is a key concept in this adaptive approach. Cybersecurity products designed with cryptographic agility can access multiple cryptographic algorithms, allowing system owners to configure the product to use the most suitable algorithms for their specific needs. When existing configuration options are no longer sufficient, these systems have built-in processes to introduce new configuration options that ensure continuous protection. This means that as older algorithms become obsolete or new, more secure, algorithms are developed, the system can be updated with minimal disruption. By incorporating cryptographic agility, organisations can stay ahead of threats and be confident that their security measures evolve in line with technological advancements and emerging vulnerabilities.

Figure 4 shows how a crypto-agile TLS protocol can be configured to adapt swiftly to new threats. Suppose an application within an organisation relies on TLS 1.3, which supports cryptographic algorithms X and Y. If a vulnerability is discovered in algorithm X, rendering TLS 1.3 insecure, the system owner can quickly check the cryptographic inventory to see if the affected algorithm is in use. If it is, there should be a process to promptly disable algorithm X. Consequently, when a new request for a secure connection is made, the system will reject the vulnerable algorithm and instead opt for the secure alternative, algorithm Y. This will ensure continued security without significant disruption to daily operations.

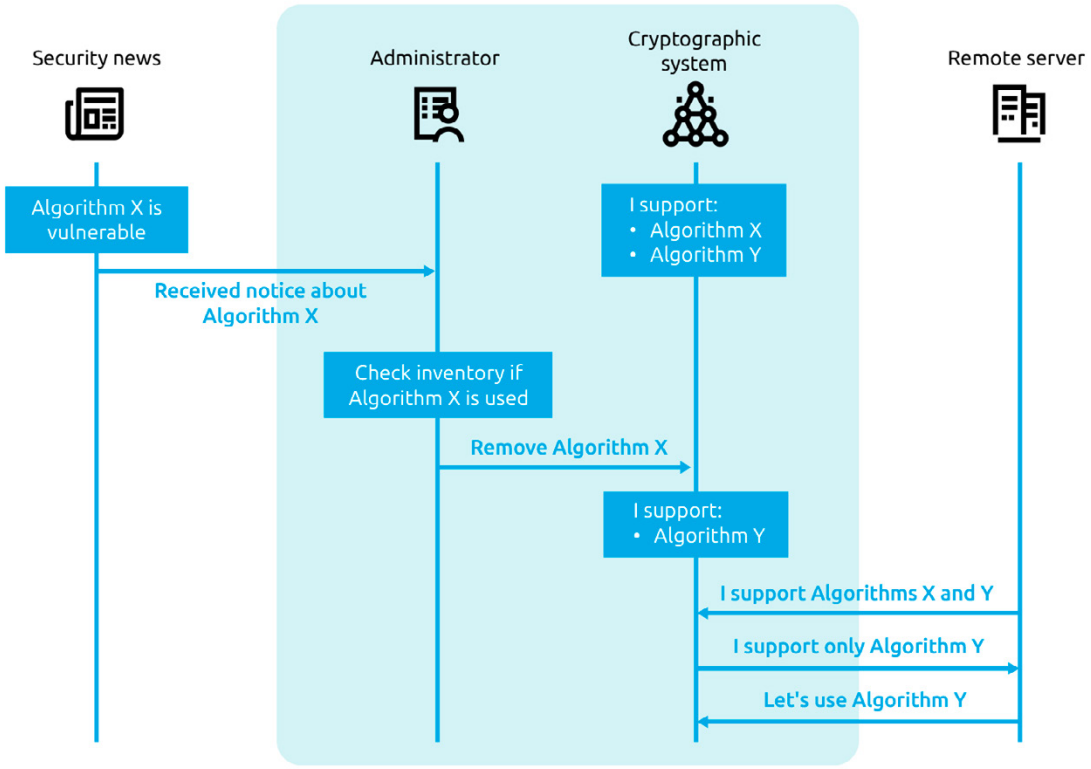


Figure 4: In the event there is a new cryptographic threat or vulnerability, update cryptography without impact to the overall system. (Source: Guidance on becoming cryptographically agile - ITSAP.40.018, May 2022.)

In summary, crypto agility is a crucial DevSecOps activity that involves several key components. First, it requires maintaining an up-to-date inventory of all cryptographic algorithms currently in use to ensure a clear understanding of the organisation's cryptographic landscape. Second, it involves writing and enforcing crypto replacement policies that define procedures for updating or replacing algorithms when vulnerabilities are discovered or when new, more secure, options become available. Third, a requirement for testing and validating these implementations is essential to ensure that changes do not introduce new vulnerabilities or disrupt existing systems. Finally, continuous monitoring of changes to applications, networks, and data is necessary to detect and respond to potential threats promptly. By integrating these activities, organisations can ensure a robust and adaptable cryptographic security environment that is capable of responding swiftly to emerging threats to fortify their last line of defence.

References

[Ken05] K. Kenan. Cryptography in the Database: The Last Line of Defence. Addison Wesley, 2005.

[CSF24] The NIST Cybersecurity Framework (CSF) 2.0, Feb 2024. https://doi.org/10.6028/NIST.CSWP.29