Department for Science, Innovation & Technology

5G Testbeds and Trials

Security Insights

Contents

1. Executive Summary

1.1. Introduction

The Department for Digital, Science, Innovation and Technology (DSIT)[1] 5G Testbeds and Trials (5GTT) programme[2] was created to stimulate the development of new innovative 5G technologies through practical use cases.

The aim was to accelerate 5G adoption in the UK by supporting projects that could maximise the benefits of 5G and create new opportunities for suppliers and users of the technology, while gaining insight into the cyber security challenges presented by such deployments.

This white paper articulates some of the high-level cyber security insights identified, by NCC Group for DSIT, in a review of a cross section of the 5GTT projects in the programme. It also aims to identify good security approaches that future projects should consider when planning similar deployments of 5G technology.

1.2. Key Themes

The projects within the 5GTT programme covered a wide range of 5G use cases, in areas such as healthcare, manufacturing and transportation, which involved innovative and varying technologies. New insight was gained on the associated cyber risks in such 5G deployments.

The projects particularly brought into focus concepts that future projects should consider:

- **Security best practice** – the projects had a wide variety of stakeholders with differing levels of cyber security skills and levels of risk tolerance, plus employed a variety of new technologies aligned to innovative use cases. However, despite such variations, the projects demonstrated that, when deploying 5G technologies to enable new services, most associated cyber risks can be addressed using well-established fundamental cyber security best practices.
- **Risk methodology and assessments** – when deploying new technology in a new environment, identifying an appropriate cyber risk methodology might be viewed as difficult. However, the 5GTT projects affirmed that it is critical to define this process at the outset, so risks can be clearly understood by all, and appropriate security measures can be prioritised and built in. Even with the mix of new technologies, existing, well developed risk assessment methodologies and tools can readily be used to identify risks and prioritise their mitigation.
- **Ecosystem risks** - the increase of cyber risk to organisations, from businesses that they work with or procure from (often referred to as “third parties”), is a clear and growing issue globally. All the 5GTT projects involved multiple organisations working together as project delivery partners, users, and suppliers, and the cyber resilience of such ecosystems is key to delivering a resilient project. Given that any one of those in the ecosystem might be vulnerable to a cyber incident, robust assurance of the security of all parties involved is essential to achieving and maintaining that resilience.
- **Guidance on security** - there is a wide range of effective cyber security insight available on deploying public and private 5G networks. However, the programme did reveal opportunities to develop further specific guidance for private networks, especially in relation to aspects such as private and public network interfaces and handovers.

[1] Formerly Department for Digital, Culture, Media and Sport (DCMS)

[2] https://www.gov.uk/guidance/5g-testbeds-and-trials-programme#about-the-programme

- **Privacy requirements** - the issue of data confidentiality, integrity and availability is a key factor in the deployment of the 5G networks especially those collecting data, including sensitive personal information, from environments where it was not previously gathered or retained. Mapping how and where such data is created, transmitted, stored, and analysed is an essential consideration in the development and implementation of a new system to ensure it is appropriately protected and in compliance with relevant privacy and data protection regulations.
- **Physical security** - the 5GTT projects demonstrated the need to consider the physical security risks in private 5G networks, especially for critical assets such as 5G core services and particularly where sensors or other equipment deployed in public locations such as transport or street furniture.
- **Technology vulnerabilities** – 5G focused projects may still include older technologies such as 4G components in the case of Non-Standalone (NSA) deployments. Therefore, it is essential to consider legacy system vulnerabilities alongside new technologies. In addition, commercial off-the-shelf Internet of Things (IoT) devices enabling new services and efficiencies, may have security vulnerabilities or a lack of appropriate security controls, that when deployed at scale can become a significant on-going risk to manage.

1.3. 5G Test Beds and Trials in scope of this white paper

A full list of the 5GTT projects in scope of this white paper is set out in Annex A of this white paper.

1.4. Summary

The 5GTT programme projects provided significant insight, not only into the realities of using 5G technologies to support innovative new use cases and increased efficiencies in existing environments, but also how security needs to be an inherent part of any such deployments. Examples of areas of insight gained include: using Logical Key Hierarchy to manage high volumes of user authentication to 5G services; approaches to providing assurance of a wide range of organisations in ecosystems required to deliver new 5G use cases; new methodologies to assess security risks to better define required levels of security; and leveraging Machine Learning for deep analysis of service information to forecast potential attacks and so enable improved mitigations to be put in place.

Even where new innovative solutions were being implemented in public or private networks, or when using connected devices such as IoT, the 5GTT projects showed that applying fundamental and well-established cyber security best practices, such as secure by design, validation through security testing, effective audit and supply chain assurance, most security issues can be addressed.

The projects proved that for any new 5G solution, a consistently applied risk-based approach from the start, which adapts with the evolution of the technology and environment, is the best approach to ensure that the most appropriate cyber security posture can be designed, developed, implemented, and maintained throughout the life of any 5G programme.

2. UK Cyber Security & Telecommunications Security Background

2.1. UK cyber security

Centrally funded multi-sector cyber security initiatives have helped grow the cyber security capability and capacity across the UK, by enabling partnering between government, industry, academia, and other communities. Such initiatives have included:

- The formation of the **UK Cyber Security Council**[3] - to drive forward the cyber security profession.
- Funding **CyberASAP**[4] - to help cyber security start-ups.
- Supporting **start-up and accelerator hubs** like Plexal[5], CylonLab[6] and CyNam[7] - to provide additional advice, capability, culture, and community to grow small start-ups into fully fledged companies.
- Creating **Cyber Security Clusters**[8] - to support the development and improving reach and insight into local and regional cyber security sector ecosystems.
- Developing the **National Security Technology and Innovation Exchange** (NSTIX[9]) - to enable the delivery of innovative national security outcomes through a coordinated and systematic approach to research and capability development.

With this growth in capability has also come increased opportunity for UK security companies to offer services and products in the UK and abroad. The European Union (EU) and United States (US) are important markets for UK businesses specialising in cyber security; while there is increasing activity in Australia, Singapore, India, and the United Arab Emirates (UAE). In recent years, the attractive UK market has also resulted in increased inward investment from international cyber security companies, who have set up a presence in the UK, providing additional local employment opportunities.

2.2. UK telecommunications security

With the greater societal dependence on safe and efficient communications systems, and as the lead government department for the security and resilience of the telecommunications networks, DSIT invested heavily to develop the telecommunications sector. This included the 5GTT programme, to improve 5G network coverage, stimulate new services and spearhead work to secure next generation networks and provide the foundations for the UK's economy.

DSIT also developed legislation such as the Telecommunications (Security) Act 2021 (TSA) allowing the UK government to create new security regulations and issue a code of practice for the telecommunications sector. As a result of the TSA, on the 1st of October 2022 the Electronic Communications (Security Measures) Regulations 2022 came into force and on 5th December 2022 the new Telecommunications Security Code of Practice (TSCoP) was published[10]. Both are intended to address risks to the UK's public networks and services by driving forward improved application of security best practice by the telecommunication operators.

The sector's suppliers, such as equipment vendors and managed service providers, are also seeing increasing expectations of security flow down via contracts from the operators subject to the TSA. This is proving to be a commercial incentive to improve security alongside the increasing potential business impacts from malicious activities such as ransomware.

There has also been a great deal of work done on security standards for the next generation of telecommunications networks (e.g., at the 3GPP organisation[11]). The UK government agencies, companies and industry experts continue to play a key role in providing input to these standards.

[3] https://www.ukcybersecuritycouncil.org.uk/

[4] https://ktn-uk.org/programme/cyberasap/

[5] https://www.plexal.com/

[6] https://cylonlab.com/

[7] https://cynam.org/

[8] https://cyberexchange.uk.net/clusters/

[9] https://www.gov.uk/government/organisations/national-security-technology-and-innovation-exchange

[10] https://www.gov.uk/government/publications/electronic-communications-security-measures-regulations-and-draft-telecommunications-security-code-of-practice

[11] https://www.3gpp.org/

3. Security Insight

3.1. Security best practice

The 5GTT programme projects covered a wide range of use cases, including manufacturing, transport, and healthcare, as well as different technologies and innovative system architectures. This meant new insight was being gained on the associated cyber risks in the evolving 5G technology stack while the projects were being developed and deployed.

With such diverse environments and systems, the projects used security best practice approaches, such as penetration testing and network scanning, to identify vulnerabilities. There was also consideration of the wide range of potential cyber threat actors with their differing motivations, through the security strategy work that was undertaken at the outset of each project, as part of guidance issued by DSIT. This threat information was then maintained on an on-going basis by some of the projects.

Within the project teams there was a wide variance of cyber security skills and capabilities to address issues. These ranged from those with practical understanding of the use cases being deployed, but with no cyber security background, to those with extensive cyber security expertise. Such a diverse base did present some challenges in ensuring appropriate security was in place, but it also enhanced the understanding of the practical issues in deploying security from a user perspective, and provided an environment in which those involved could increase their cyber security awareness.

The projects proved that where innovative use cases and evolving technologies, such as 5G and IoT, are being deployed it is essential to include in their development the Secure by Design[12] approaches, whilst ensuring that the latest security and resilience standards, developed by organisations such as the mobile standards body 3GPP, are adhered to. Examples of Secure by Design implemented by some of the projects included zoning of network architectures and ensuring appropriate security controls to segment them. This approach makes it harder for threat actors to traverse the networks during an attack, slowing them down and providing greater opportunity for attack detection and a response.

Failing to adopt Secure by Design approaches did result in some projects being potentially more susceptible to exploitation by malicious actors. Also, it made it harder to then implement appropriate security later in an efficient and timely manner.

It became clear that, no matter how innovative the use case or the technology being deployed, the application of established fundamental cyber security best practices and standards can be used by any similar project to address most potential cyber risks, whether they relate to people, process, or technology. Understanding which risks need to be prioritised for mitigation, or identifying those that might be specific to the nature of a 5G environment, were noted by the projects as being best defined through on-going risk assessments that can adapt to any change in technology or process.

3.2. Risk methodology and assessments

Given the increasing levels of safety and security compliance expected by regulators, customers and business partners, organisations need to ensure that risks are kept at the lowest reasonable level and plans are in place to limit the damage of any compromises that occur. Based on the variety of use cases across the 5GTT projects, which involved private and public sector organisations each with their own threat profile and regulatory landscape, projects rightly looked at applying the most appropriate risk assessment method to their environment.

[12] https://www.ncsc.gov.uk/collection/cyber-security-design-principles

Identifying an appropriate methodology to understand the cyber security posture of a project with varying stakeholder types is difficult; but the projects proved it is critical to define this at the start so risks can be clearly understood, and security can be built in from the outset. Those projects that did not do this acknowledged that they were not able to fully understand the security risks they were exposed to and having that insight would have changed how they deployed their projects to deal with some of the security issues they subsequently faced. For those that did define risks at the start, it allowed a baseline security posture to be assessed and monitored throughout the lifecycle of a project, to ensure that risks were understood and addressed if they moved outside acceptable levels.

It is essential for any project to monitor and assess the risk throughout the project and maintain a good understanding of an acceptable level of risk, as the business pressure to deliver can lead to a level of risk tolerance that is too high, degrading required security work. Such business pressure is even greater where new types of deployments are being developed in a constrained period, as was the case for the 5GTT projects. Where having an increased risk tolerance is accepted, for example a test or trial deployment, having a risk framework against which to make such a decision, and to document how a full deployment would have appropriate security, is essential for successfully taking any trial to commercial deployment.

Some of the 5GTT projects proved able to adapt their project to ensure implementation, despite the deployment of technology in new use cases that presented sometimes unexpected challenges especially as 5G was an evolving technology and the impact of the COVID-19 pandemic at the time. Such impacts on the projects varied from supply chain constraints that meant alternative equipment needed to be used, to a lack of guidance on how to securely configure systems for a new type of use case. Such impacts reinforced the need for any risk assessment methodology to be adaptable to changes and easily updatable to ensure an understanding of cyber security risk profile is maintained as a project evolves.

As a result of these new environments, some of the projects developed innovative approaches to assess the associated risks, an example of this is the cyber security scorecard created by Weaver Labs as part of the Smart Junctions 5G project, which is summarised in Annex B of this white paper. Whilst organisations may develop a risk methodology and assessment approach specifically tailored for their needs, in almost all scenarios the 5GTT projects proved that existing well-developed approaches and supporting assessment tools could readily be used. This could include, for example, the National Cyber Security Centre (NCSC) Cyber Assessment Framework[13] (CAF). As the NCSC CAF is outcome-based, rather than specific to use cases and technologies, it is already widely used in the UK across multiple sectors and critical national infrastructure including telecommunications.

3.3. Ecosystem risks

All the 5GTT projects involved multiple organisations working together as project delivery partners, users, and suppliers. In such environments, the cyber resilience of each of the parties in the ecosystem is key to achieving an overall resilient project implementation.

This is against a backdrop that cyber risk for organisations from those that they might partner with or procure from (referred to here as 'third parties') is a clear and growing issue globally, as seen in several high profile and high impact supply chain cyber security compromises such as that of SolarWinds[14]. As a result, this is an area that has attracted increasing scrutiny and regulatory activity from governments, regulators, and insurers.

Third-party risks can manifest in several ways. For example: direct access and compromise by a third-party employee; disruption through exploitation of a vulnerability introduced by third-party software or hardware;

[13] https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework

[14] https://www.ncsc.gov.uk/news/ncsc-statement-on-solarwinds-compromise

and disruption due to the inability of the third party to provide services because of impact on their own systems.

As the delivery of any similar project might be affected by the disruption of one of the partners or suppliers, part of the governance required must include an understanding of the cyber assurance of each of the involved organisations. In the 5GTT programme this was undertaken in a variety of ways, for example requiring evidence of existing cyber security assurance reviews or providing funds for parties to undertake and share a cyber security assessment in line with the project's approach to risk. Similar projects should note these approaches and consider existing tools in the marketplace to support such activity:

- Work-flow - automation of assurance process work to support completion and decision making.
- Third-party security exchanges - allowing organisations to access libraries of pre-completed security assessments.
- Ratings - supplying a security score from an independent third party to inform decisions.
- Monitoring – services that monitor third parties and provide alerts to subscribers for any security event of note related to those third parties.

One of the striking features of the 5GTT projects was the high level of collaboration required between a wide range of stakeholders, from local councils and healthcare organisations to multinational companies. Having such a diverse range of stakeholders did mean that in some cases establishing and agreeing risk tolerance to define appropriate security was a challenge. So, implementing an agreed risk methodology would help all parties understand the risks and align on appropriate security to enable delivery of resilient services, especially where this involves deployments of new use cases and technology.

The 5GTT programme also demonstrated that sharing security learnings between projects brings benefits for all partners by allowing them to benefit from insight that contributes to security improvements being understood and deployed. An example of this is the MANY 5GTT project set out in Annex C of this white paper. A culture of sharing security insights is to be encouraged, especially where innovative approaches and technologies are being developed and implemented.

3.4. Guidance on security

There is a wide range of cyber security insight available on deploying public and private 5G networks, for example the NCSC "Connected Places: Cyber Security Principles"[15]. There is also clear guidance within the TSCoP that both public and private network operators can use even if the services are not in scope of the TSA.

Telecommunications, including private networks such as those deployed in the 5GTT programme, increasingly rely on cloud-based services to enable rapid development and deployment. Whilst cloud-based platform services can be highly secure and improve speed of delivery, if incorrectly configured they also present an opportunity for leakage of data and credentials that can be exploited for malicious activity. It is essential that available guidance, including the NCSC Cloud security guidance [16] on the secure use of cloud-based platform services, is part of the risk management of future projects.

The 5GTT programme also revealed opportunities to develop further specific guidance for private networks especially in relation to aspects such as private and public network interfaces and handovers. Such gaps in guidance are under review and the insight from the 5GTT will support activity in this area.

[15] https://www.ncsc.gov.uk/collection/connected-places-security-principles

[16] https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

3.5. Privacy requirements

Across the 5GTT programme there was good awareness within the teams of the challenges of safe and secure data handling, whether that be the potential for personally identifiable information (PII) to be collected or for sensitive information such as patient data, to be transmitted and stored in the projects' systems.

In the ever more connected world, the issue of data confidentiality, integrity and availability is a key factor in the deployment of any system. Mapping how and where data is to be transmitted and stored is an essential consideration in the development and implementation of any new system and a Data Privacy Impact Assessment (DPIA) should be considered as part of the security design process.

To address the challenges, the projects demonstrated that a clear understanding of potential privacy mitigations, such as removal or minimisation of data where possible (e.g., masking PII or faces in video feeds), encrypting data and retaining it for the minimal amount of time to meet processing or regulatory requirements, was needed. Guidance on this is available, such as the NCSC "GDPR security outcomes"[17] and the Information Commissioner's Office (ICO) "Data protection by design and default"[18] which will help future projects remain compliant with the legislation.

In future, projects must also ensure that as they develop and change during production, they do not drift away from the accepted protocols surrounding the privacy of the data subjects without completing a new DPIA.

3.6. Physical security

When some 5GTT projects experienced damage to publicly accessible equipment, this emphasised the need to consider the physical security risks in private 5G networks, particularly where a use case involves sensors or other equipment deployed in public locations such as transport or street furniture.

More generally, private networks may have 5G network core servers that are more exposed than those typically used by mobile network operators (MNOs) who are familiar with deploying stringent physical security to protect network core assets. Any such exposure of such a critical part of the network could potentially lead to exfiltration of data and interference or complete disruption of services.

There is the real potential for higher risks to a project, due to inadequate physical security, than might be anticipated in the development phase. Therefore, projects should thoroughly assess the physical security risks to ensure that these are properly addressed during the design phase. Guidance, such as that from the National Protective Security Authority (NPSA) on Physical Security[19] , will enable projects to build in physical security from the outset. This will help reduce the potential for equipment interference or damage that might lead to malicious access to the wider network.

3.7. Technology vulnerabilities

The technology underpinning 5G is designed to offer increased data security compared to previous mobile technologies. But, as with most existing public and private networks, the majority of the 5GTT projects were non-standalone (NSA) 5G networks and so were reliant on some 4G systems. In such 4G/5G hybrid environments the 4G security vulnerabilities can have an impact on the 5G network operation. Therefore, it is essential that future hybrid projects have the capability to understand any 4G or other legacy system vulnerabilities in addition to those of the 5G related functions which may be the focus.

[17] https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes

[18] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

[19] https://www.npsa.gov.uk/physical-security

Off-the-shelf Internet of Things (IoT) devices as used by several 5GTT projects, which, whilst enabling new services and efficiencies, can harbour increased security vulnerabilities such as weak and/or default usernames and passwords, complex or unclear mechanisms for applying security updates. There is also the potential for supply chain uncertainty due to use of various modules and components being developed to differing security standards. These issues can present threats to a network[20].

There is also the potential for data transmitted from the IoT devices to central systems to be unencrypted in transit. To address this, encryption should be used, but where that is deployed using key based encryption such as Transport Layer Security (TLS) it can introduce security issues if keys are not rotated due to the overhead of key management. Future projects could consider a cloud key management service (KMS[21]), or a similar on-premises solution dependent on their specific environment.

In addition, where IoT devices are used in larger and more complex deployments with IoT gateways, the gateways themselves can be critical points that malicious attackers will look to exploit. Therefore, the IoT gateways and the IoT devices require proper assurance testing before deployment, and ongoing security monitoring.

4. Summary

The 5GTT programme projects provided significant insight, not only on the realities of using 5G technologies to support innovative new use cases and increased efficiencies in existing environments, but also how security needs to be a fundamental part of any such deployments. Without appropriate risk management governance and resources in place to assess the risk and define approaches to deal with them, new risks and vulnerabilities can be introduced along with a lack of understanding of how to deal with them. Therefore, those looking to implement 5G connected environments such as those covered in this white paper should ensure that, from the outset, they have a security lead who can coordinate the selection of an appropriate risk methodology and security standards that need to be adopted. Once in place, they can drive the subsequent security implementation, whilst keeping all relevant stakeholders informed in a manner appropriate to their understanding of cyber security, so that informed decisions can be made.

Whilst increased data security is part of 5G mobile network technology specifications, 5G cyber security is about more than just 5G technology: it includes technology, people, and processes. The 5GTT projects showed how diverse the project ecosystem can be and demonstrated the need to have a risk methodology in place so that all stakeholders can understand the appropriate security needed. And whilst there is always a drive to get a project service up-and-running quickly, there is a real need for the project to not accept too high a security risk tolerance. Rather, it is advisable for any project to include the level of security in its initial stages that will be needed for full-service deployment, as this will provide key insight and support any future commercialisation of the project. Adding security retrospectively to meet increasing regulatory compliance and client requirements will always be less efficient, more costly, and potentially make the project not viable.

Most importantly, the 5GTT projects proved that even where new innovative solutions are being implemented, by applying fundamental and well-established cyber security best practices such as secure by design, validation through security testing, effective audit, and third-party assurance, most security issues can be addressed. Applying these concepts using a consistently applied risk-based approach that can adapt with the evolution of the environment, will help in ensuring that the most appropriate cyber security posture can be designed, developed, implemented, and maintained.

[20] https://www.ncsc.gov.uk/report/organisational-use-of-enterprise-connected-devices

[21] https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/choosing-and-configuring-a-kms-for-secure-key-management-in-the-cloud

Finally, in driving through initiatives such as the 5GTT programme DSIT has supported UK organisations in gaining new insight that can be used to improve security guidance for the telecommunications and wider sectors, and support those undertaking similar 5G initiatives using private or public networks to do so more securely.

Annex A - 5G Test Beds and Trials in scope of this white paper

Project Name	Main Area of Project Focus
5G CAL (Connected Automated Logistics)	Logistics: Connected Heavy Good Vehicles
5G Connected Forest	Tourism: AR visitor experiences
5G Edge-XR	Augmented Reality (AR) / Virtual Reality (VR): Business and leisure AR/VR solutions
5GFoF (5G Factory of the Future)	Manufacturing: Utilising 5G to allow secure/resilient connectivity factories
5G Festival	Media: Virtual festival using live music artist collaboration and audience engagement
5G Logistics	Logistics: Enhancing cargo monitoring and transit in a port
5G New Thinking	Fixed Wireless Access / Agriculture: Rural community and agricultural connectivity
5G Ports - Port of Felixstowe	Transport: Port crane connectivity
5G VISTA	Sport: Enhancing sports fans viewing experience of football
5G Wales Unlocked	Tourism / Transport / Education / Agriculture: Leveraging 5G and IoT for improved farming, public transport, visitor attractions and education in Wales
5G-AMC2 (Accelerate Maximise Create for Construction)	Construction: Improving the productivity of building sites through enhanced connectivity of systems and equipment
5GEM UK (5G Enabled Manufacture UK)	Manufacturing: Connected manufacturing machines and AR for workers
5G-ENCODE (ENabling COnnectivity for Digital Engineering)	Engineering: Enhanced asset tracking and AR/VR for engagement/training
Green Planet AR	Tourism: New visitor experience using edge compute and 5G connectivity
Liverpool 5G Create	Healthcare: Connected applications to enhance health and social care
MANY (Mobile Access North Yorkshire)	Tourism / Civil Engineering/Healthcare: Monitoring of structures and the environment, remote connectivity for healthcare and interactive AR for tourists
MONeH (Multi Operator Neutral Host)	Rural Connectivity: Providing internet coverage in rural communities
Smart Junctions 5G	Transport: Optimising traffic flow on roads
West Mercia Rural 5G	Healthcare: Rural healthcare connected applications to enhance patient care
WM5G (West Midlands 5G) Transport	Transport: Part of W5GM focused on improving transport related efficiencies, customer experience and environmental impact

Annex B - Case Study - Smart Junctions 5G Project

One of the main learnings for the Smart Junctions 5G project team was around the challenge to develop strategies for certain security standards so that investment and resources could be applied as efficiently as possible.

To overcome this, one of the partners in the project team, Weaver Labs, created an organisational risk assessment/analysis tool to address the gap between existing policies and provide a means for any organisation to adopt a security posture relevant to their business scope. This cybersecurity ranking tool or scorecard was created to:

- identify the cybersecurity posture for any organisation in the supply chain.
- capture an action plan that aligned with the nature of the business and the software product.
- calculate a score that is representative the organisation’s current risk profile.

The tool was designed to measure the risks and impacts of an organisation’s current and controlled postures with regards to business processes including:

- the organisation's technical posture and procedures.
- management and operations protocols.

The scorecard uses inputs of the existing security posture, analyses the existing risks, and gives an organisation an understanding of their risk exposure and their threat landscapes. This way gaps are more easily identified, and an action plan can be put in place. As an output of the analysis, the scorecard provides:

- a comprehensive risk gap analysis.
- an overview of the current security profile.
- the target security profile and the existing gaps to get there.
- an action plan, with the policies and references to execute it.

This is done through a process of policy aggregation and mapping, for example doing a mapping of UK NCSC Zero-Trust to the NIST.SP.800-53 security controls. The risk analysis is done to identify the threat landscape, plus both controlled and uncontrolled risks. The objective is to identify the impacts of both risk types, apply risk scores and risk mitigation strategies. It also designed to provide a means to set and monitor the risk goals and measure the risk progress. To create the target profile, the tool provides a simple way of selecting policies and associating it to the risks, plus gives the ability to set priorities to the policies and tasks in the action plan.

As an output, the organisation can see a comprehensive analysis of their baseline security risks and threats, and a score associated with it. This score is a means of grading an organisations’ risks and informing their security policy selection.

Annex C - Case Study - MANY Project

MANY (Mobile Access North Yorkshire) consisted of a diverse set of nine use cases with different requirements.

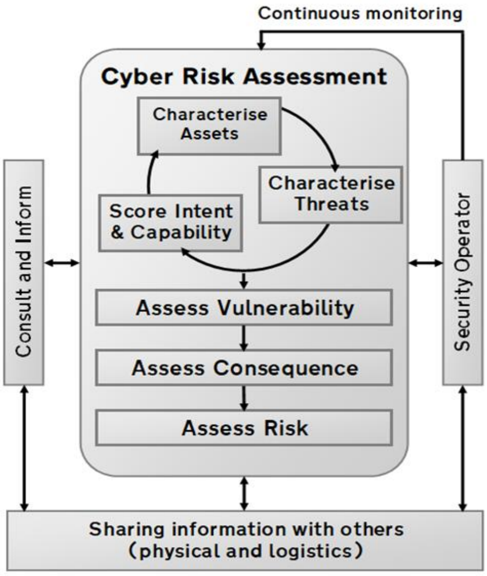
The security work provided an opportunity to enable new business and functionalities, plus communication between project members who did not normally communicate with one another.

Cyber Risk Assessment

As part of the approach to identifying and addressing security risks associated with the project use cases, the Cyber Risk Assessment process (shown in the diagram to the right) was used to elicit use case requirements by facilitating knowledge-exchange and leveraging expertise in the project.

The Cyber Risk Assessment process yielded several security activities including:

- for one of the project use cases risk to data was identified as an area of concern. As a result, a data protection impact assessment (DPIA) was undertaken. One of the outcomes of the DPIA, and actively engaging project members, was the operational team became more confident in having conversations around data protection.
- a risk of under-trained staff emerged and so an integrated training plan was also deployed.



Security-by-design

The security approach applied by the project involved moving from a technology-centric to one based on holistic security-by-design. This was achieved by leveraging stakeholder engagement and prioritising security advocacy project wide.

One of the results of putting security work on the agenda as a design consideration led to NYCC involving penetration testers as part of their use case within MANY, and wider working practice.

Lessons Learnt

At the MANY project final conference in June 2022 a security workshop was held under the title: “How can we make security relevant; the importance, the challenges and opportunities”. The reflections from this session highlighted the changing nature of security work, and a need for flexibility on approach and appropriate scoping. For example, one of the use cases had been so early an innovation that physical security had been the prime consideration. As the technology develops for that use case, data (identity/location) protection will be an increasing a concern, as will the associated network security and access control.

In summary, the MANY project is an example of the need for engaging partners across a project for effective and ongoing security work, and the consortia were advocates for this. To reinforce this, they considered that teams should draw security requirements into their observation and reporting processes and consider metrics that they can use to demonstrate security, or its value within the use case. To achieve this a cyber security toolkit was created for the project, this enabled conversations about security to take place as early as possible.

NCC Group
XYZ Building
2 Hardman Boulevard
Spinningfields
Manchester, M3 3AQ

www.nccgroup.com

Making the world safer and more secure