Northern Gas Networks

A11 - NGN RIIO-2

IT and Cyber Security Plan

together we are the network

Table of Contents

Introduction

Northern Gas Networks (NGN) is an Operator of Essential Services (OES) within the UK. As an OES, we play a vital role in society by ensuring the distribution of gas in the North East, Northern Cumbria and much of Yorkshire, where the reliability and security of these services are essential to everyday activities. As we have seen from numerous cyber security incidents, the network and information systems that uphold these services can be an attractive target for malicious actors, with the magnitude, frequency and impact of cyber-attacks increasing.

NGN recognises that information is a critical asset and how networks and information systems are managed, controlled and protected has a significant impact on the delivery of services to our customers. A growing worldwide cyber threat, which has exponentially increased in recent years, compounds the need for further investments and strategic planning to minimise the risk to our assets and increase NGN's resiliency to all threats. Information assets must be protected from unauthorised use, disclosure, modification, damage and loss and additionally, they must be available when needed, particularly during emergencies and times of crisis.

The evolution of NGN's history and therefore computing environment is inherently difficult to manage and secure. A number of domains, infrastructures and applications supported by different 3rd party partners have led to a disparate management and security model. In addition, NGN has inherited, rather than developed and enforced cyber governance to reduce the risks associated with its SIAM (Service Integration and Management) environments. Much of the hardware and software originally developed to facilitate this interconnected environment has prioritised efficiency, cost and the convenience of the user, but has not always had security designed in from the start. Malicious actors, hostile states, criminal or terrorist organisations and individuals, can exploit the gap between convenience and security. Narrowing that gap is an NGN priority.

This strategy is the first company-wide cyber security strategic plan and is intended to shape NGN's policy, whilst offering a coherent and compelling vision to share across the business. It sets priorities for how NGN can efficiently and effectively address the management, control and protection of its network and information systems. In addition, this document outlines the strategic outcomes that all future initiatives are based on and identifies the components necessary to iteratively improve the security posture of the company.

In this strategy, 'cyber security' refers to the protection of information and information processing facilities from adverse confidentiality, integrity and availability affects. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.

Strategic Context

The scale of technological change throughout GD1 has evolved significantly. The trends and opportunities described then have since accelerated. New technologies and applications have come to the fore and we have seen a greater uptake and demand for internet-based solutions to deliver business benefits. These developments have brought or will bring significant advantages to NGN as we continue to strive to be the safest, most efficient and customer centric gas distribution network and in fact, business in the UK. But as our reliance on networks and information systems grows, so do the opportunities to compromise our systems and data.

Malicious cyber activity knows no boundaries. We face increasingly growing threats from a number of avenues at home and abroad with a shift in the geopolitical landscape. The next section sets out the nature of these threats to Northern Gas Networks.

Threats

NGN face a growing number of cyber threats to its network and information systems across both the Information technology and operational technology landscapes. Threats, which if came to fruition, could have serious consequences on NGN's reputation, legal and regulatory standing, financial position and human safety. These threats come from a number of sources:

- State actors who have offensive cyber capabilities.
- Cyber criminals who are broadening their efforts and expanding their strategic operations to achieve higher value pay-outs.
- Terrorists, and their sympathisers, are conducting low-level attacks and aspire to carry out more significant acts.
- Hacktivist groups, who are selecting their targets in response to perceived grievances, introducing a vigilante quality to many of their acts.
- Script kiddies, who are looking to obtain valuable data and profit from its sale
- Insider threats, malicious insiders who are trusted employees and have access to critical information systems, can indeed pose the greatest threat. Or of equal concern, those employees who are accidently causing cyber harm through inadvertently leaking data, infecting machines through infected USB's or ignoring security procedures.

The below table sets out risks posed by these threats and the impacts that each may have on NGN:

Risk								Impact			
Negligible		Low		Medium		High	Extreme	Reputation	Financial	Legal / Regulatory	Health & Safety
Breach of customer data											
Breach of employee data											
Breach of operational control systems and networks											
Breach of corporate and telecommunications networks											
Sabotage or disruption to business operations											
Unavailability / Loss of sensitive data											
Loss or modification of strategic or financial data, or intellectual property											
Breach of government regulations											

Consequently, this would lead to the following:

Reputation

- Loss of customer confidence
- Loss of partners and service providers

Financial

- Remediation costs following a cyber attack
- Fraud
- Loss of contracts
- Operational disruption

Legal / Regulatory

- Fines from regulators (GDPR – 4% of turnover or £20m, NIS - £17m)
- Enforceable undertakings
- Loss of license to operate

Health and Safety

- Injuries, loss of limbs or life to employees, customers or the general public

Vulnerabilities

Business Change

NGN is undergoing transformations across its business operations, looking to leverage technology and information more effectively to achieve its business outcomes and strategic goals. Change is fraught with opportunity and risk and none more so than during transformation programmes. Transformation is about change, agility, speed, connectivity, real-time economy, customer expectations, disruption and all those things. Security in the eyes of many stands in the way of all this. It's about rules and regulations, protection, defence (even if, in reality, cybersecurity becomes pro-active and offensive), training, awareness, and a layer that some believe to slow down the digital transformation initiatives. This often results in corners being cut, security activities being missed out and risks being taken in order to maintain velocity of these programmes. Cyber security risk management within NGN it is fair to say, is at a low level of maturity and is still seen as a bolt on as opposed to being baked into information system lifecycle activities and often late in the day during projects and initiatives. Only by creating a security aware culture and the investment of time and resources in cyber security capabilities, will we see maturity levels starting to increase in these activities.

Expanding interconnected world

Until more recently, most people saw cyber security defence through the mechanisms of protecting the endpoints (desktops, laptops, etc) and infrastructure and this is where NGN has traditionally invested in cyber security. Since then the internet has become deeply ingrained into our business operations, something we are largely oblivious to, and information is fast becoming the new oil, where its value both to businesses and adversaries continues to increase. The borders of our technology estate is no longer at the perimeter of our network as cloud services have created opportunities for efficiency. The rapid implementation of connectivity and integratory techniques between cloud and traditional on premise is opening up the possibility of devices and information, which were never vulnerable to such interference in the past with potentially disastrous consequences. Therefore, we are no longer just vulnerable to cyber harms caused by the lack of cyber security on our own devices but by threats to the interconnected systems and supply chain that are fundamental to our business operations and ways of working.

Legacy Technology

NGN relies on legacy information and operational technology to operate parts of its estate and the task of updating or replacing it would be expensive and difficult to do so. Some of this technology, especially in the operational space, will have been in place for tens of years, and at the point of implementation, Cyber Security wouldn't have been a consideration. The older the technology, the less chance there is that it is up to dealing with the sophisticated threats, externally and internally as they often rely on older unpatched versions. The threats now facing these legacy technologies leaves NGN vulnerable to cyber-attack.

Cyber Hygiene

Cyber hygiene relates to the practices and precautions users take with the aim of keeping information and information processing facilities safe, and secure from theft and outside attacks. These practices are often part of a routine to ensure the safety of identity and other details that could be stolen or corrupted. Much like physical hygiene, cyber hygiene is regularly conducted to ward off natural deterioration and common threats. NGN hasn't necessarily neglected this practice but there are definitive gaps in its hygiene processes. Cyber-attacks are not necessarily sophisticated or inevitable and are often the result of exploited, but easily rectifiable and, often, preventable vulnerabilities. In most cases, it continues to be the vulnerability of the victim, rather than the ingenuity of the attacker, that is the deciding factor in the success of a cyber-attack. NGN decide on where and how to invest in cyber security based on a cost-benefit assessment, but we are ultimately liable for the security of our network and information systems. Only by balancing the risk to our critical systems and sensitive data from cyber-attacks, with appropriate investment in people, technology and governance, will we reduce our exposure to potential cyber harm.

Conclusions

The future of the NGN's security and prosperity rests on our digital foundations. The challenge NGN face is to build an interconnected digital platform(s) that allows us to achieve our business outcomes and strategic goals, that is both resilient to cyber threats and equipped with the knowledge and capabilities required to maximise opportunities and minimise risks.

NGN has developed policies, giving direction and has established security controls and mechanisms that have enhanced our defences and mitigated some of the threat we face in cyberspace, but there is plenty of work to be done if we are to stay ahead of the constantly evolving threat.

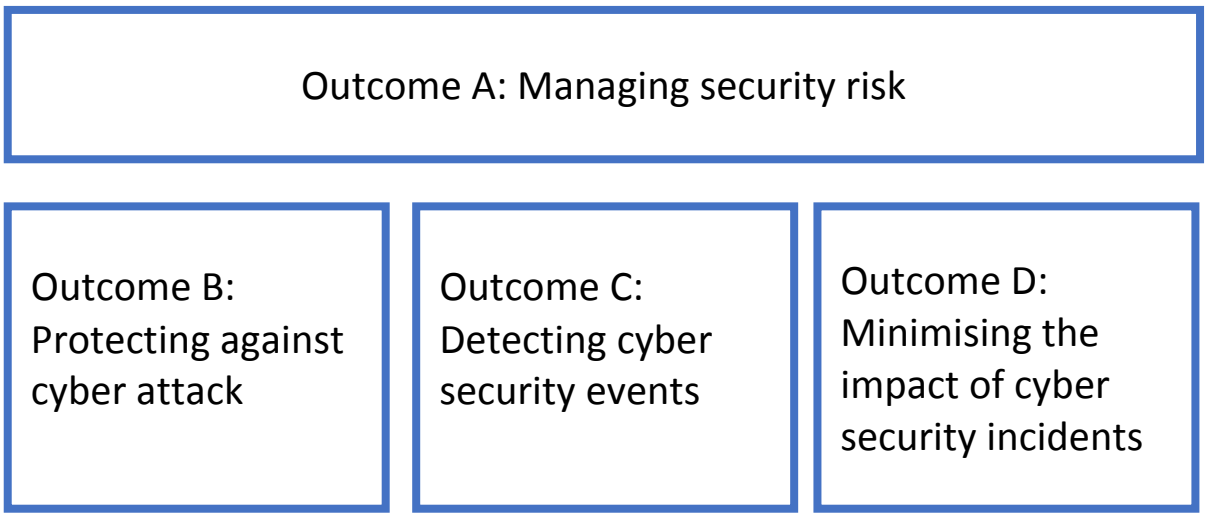
Strategic Response

To mitigate the multiple threats and safeguard our interests in cyberspace, we need a strategic approach that underpins NGN actions in the digital domain over the next five years and beyond. We have dependencies on the Internet; however, it is inherently insecure and there will always be attempts to exploit weaknesses to launch cyber-attacks. This threat cannot be eliminated completely, but the risk can be greatly reduced to a level that allows NGN to continue to prosper, and benefit from the huge opportunities that digital technology brings. Our current approach needs to achieve the scale and pace of change required to stay ahead of the fast-moving threat. We need to be more pro-active, rather than reactive, and this section sets out our vision and strategic approach of how we can go about achieving that goal.

Vision

Our vision is to ensure that resilient security is integrated as seamlessly as possible and built into everyday operations, enabling a safe and secure environment that nurtures innovation and protects against an ever-changing threat landscape.

To realise this vision, we will work to achieve the following outcomes, aligned to the Cyber Assessment Framework:



Principles

In working towards these objectives, NGN will apply the following principles:

- our actions and policies will be driven by the need to both protect our employees, customers, and business
- we will apply a risk-based strategy, ensuring our critical assets are identified and prioritised;
- we will deliver proportionate security mechanisms;
- we will act in accordance with the law;
- we will work collaboratively with government, regulators and industry to contribute to the security of our services and the UK;
- we will preserve and protect our employees and customers privacy.

Strategic Plan

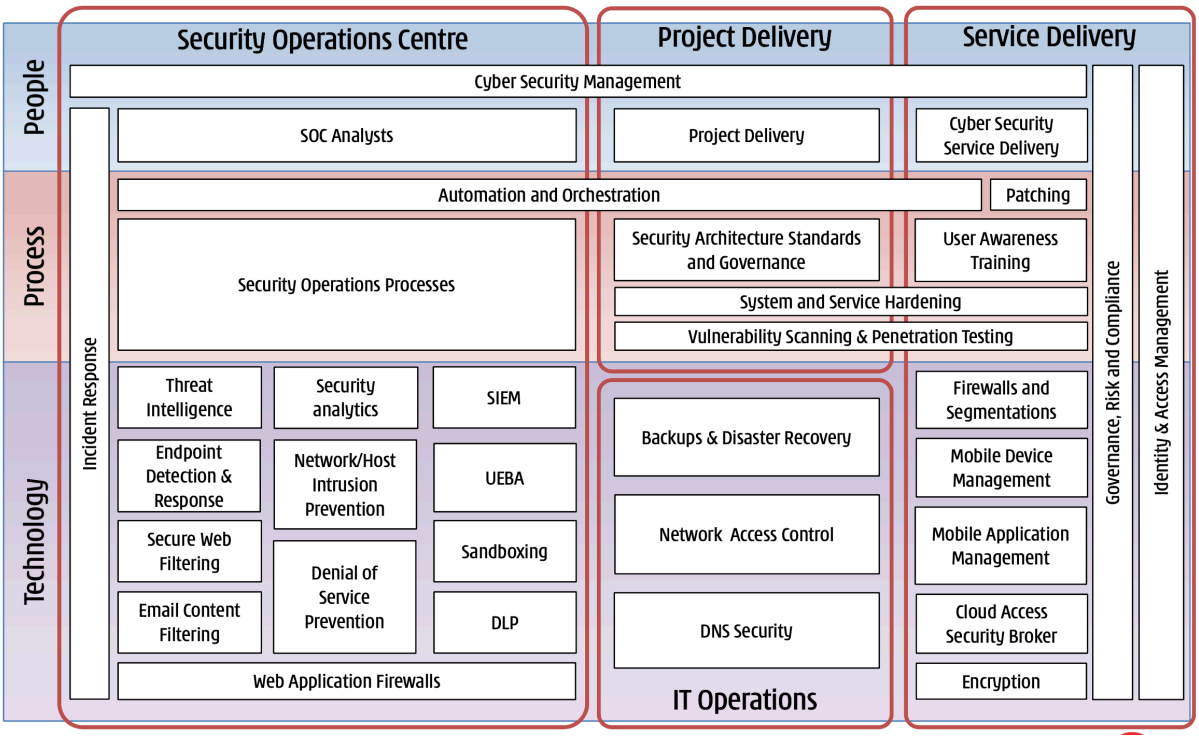
Our goals for NGN's cyber security over the next few years are rightly ambitious. To achieve them, we must align and coordinate resources within our teams and departments, across multiple offices and locations. Activity to deliver our vision will advance the four primary outcomes of the strategy:

to ensure we are **PROTECTING** our network and information systems, **DETECTING** adversaries through advanced capabilities and **MINIMISING** any potential impact, all of which are underpinned by effectively **MANAGING SECURITY RISK**.

A number of key strategic themes will be delivered in GD2, aligned to the four outcomes and our Target State. Individual projects and initiatives will then align to these key themes.

Target State

In order to mature as an organisation so that our cyber security practices are no longer a bolt-on and we have holistic protective mechanisms in place, a number of people, process and technology capabilities need to be introduced. This is illustrated in the diagram below, applying to both Information Technology and Operational Technology environments in principle and where appropriate.



This implementation programme sets out the key themes that will mature our cyber practices from our current state towards the target state and to enable our Vision.

Key Themes

Assured Governance, Risk and Compliance

Key Outcomes

- have an embedded security management system in place across NGN
- have effective organisational security management led at board level and articulated clearly in corresponding policies.
- establish roles and responsibilities for the security of networks and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.
- have senior-level accountability for the security of networks and information systems and delegated decision-making authority appropriately and effectively. Risks to network and information systems related to the delivery of our services are considered in the context of our other organisational risks.
- have effective internal processes for managing risks to the security of network and information systems related to the delivery of our services and communicating associated activities.
- have demonstrable confidence in the effectiveness of the security of the technology, people, and processes relevant to our services.
- ensure compliance with legislation

Identity and Access Management

Key Outcomes

- robustly verify, authenticate and authorise access to the networks and information systems supporting our services.
- assure good management and maintenance of identity and access control for our networks and information systems supporting our services.
- extra mechanisms are in place to secure accounts such as MFA, routine validation and review and further emphasis is placed upon privileged users

Proactive Security Operations

Key Outcomes

- ensure data sources used to monitor allow for timely identification of security events, which might affect the delivery of our services.
- ensure logging data is held securely and read access is granted only to accounts with business need. Data will not be able to be modified or deleted except when no longer required to be retained.
- act upon logged data, to identify those security incidents that require some form of response and evidence this.
- monitor staff skills, tools and roles, including any that are out sourced, reflecting governance and reporting requirements, expected threats and the complexities of the

network or system data they need to use. Monitoring staff have knowledge of our services that are critical to our services.
- define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify.
- use an informed understanding of more sophisticated attack methods and of normal system behaviour to monitor proactively for malicious activity.
- automation and orchestration are used throughout and used to remediate

Response and Recovery

Key Outcomes

- have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of our services and covers a range of incident scenarios.
- have the capability to enact our incident response plan, even in the most extreme of circumstances, including effective limitation of impact on our services. During an incident, we will have access to timely information on which to base our response decisions.
- ensure our organisation carries out exercises to test response plans, using past incidents that affected our (and other) organisations, and scenarios that draw on threat intelligence and our risk assessments.
- we identify the root causes of incidents we experience, wherever possible.
- our organisation uses lessons learned from incidents to improve our security measures.

Data, Mobile and Cloud Security

Key Outcomes

- have adequately and proportionately protected stored and the transit of data important to the delivery of our services.
- securely configure information systems that support the delivery of our services.
- we leverage third party assurance in our risk assessments of cloud services
- we are able to enforce our security, compliance and governance policies on all our cloud applications
- know and have trust in the devices that are used to access our networks, information systems and data that support our services.
- we know where our data is

Threat and Vulnerability Management

Key Outcomes

- proactively gain intelligence regarding threats to the network and information systems that support the delivery of our services.
- proactively manage the network and information systems that support the delivery of our services to enable and maintain security.
- manage known vulnerabilities in our network and information systems to prevent disruption of our services.

Security Conscious and Aware Employees

Key Outcomes

- develop and pursue a positive cyber security culture.
- encourage staff to spot and report all suspicious Cyber Security events
- initiating regular and engaging user awareness training programmes
- continually improvement our techniques to deliver positive outcomes
- testing user awareness through simulated phishing campaigns
- rewarding staff for positive Cyber Security behaviour

Conclusion

The rapid evolution of the cyber landscape will constantly throw up new challenges as technology evolves and our adversaries act to exploit it. However, this strategy aims to provide a range of policies, tools and capabilities that will ensure we can respond quickly and flexibly to each new challenge as it arises. Should we fail to act effectively, the threat will continue to outpace our ability to protect ourselves against it and we should continually expect a proliferation of threat capability at all levels.

The Cyber Security Office will maintain a leadership role, collaborating with other departments and teams, the industry, government, and other stakeholders, across all of its cybersecurity strategic areas to ensure that cybersecurity risks are effectively managed, information systems and networks are protected, vulnerabilities are mitigated, cyber threats are reduced and countered, incidents are responded to in a timely way, and the cyber ecosystem is more secure and resilient.

If we can ensure security is designed and built in, by default, into our technologies, into our business and our ways of working, we would have less cause to worry about cyber security.
Meeting the outcomes outlined in this strategy goes a long way to achieving that goal and achievement requires a unified, long-term approach across the business. Aligning business wide network and information systems protection with traditional risk management, information sharing, and incident response efforts will enhance Cyber Security efforts moving forward and provide Northern Gas Networks with a secure cyberspace for its future business endeavours.