Engineering Justification Paper

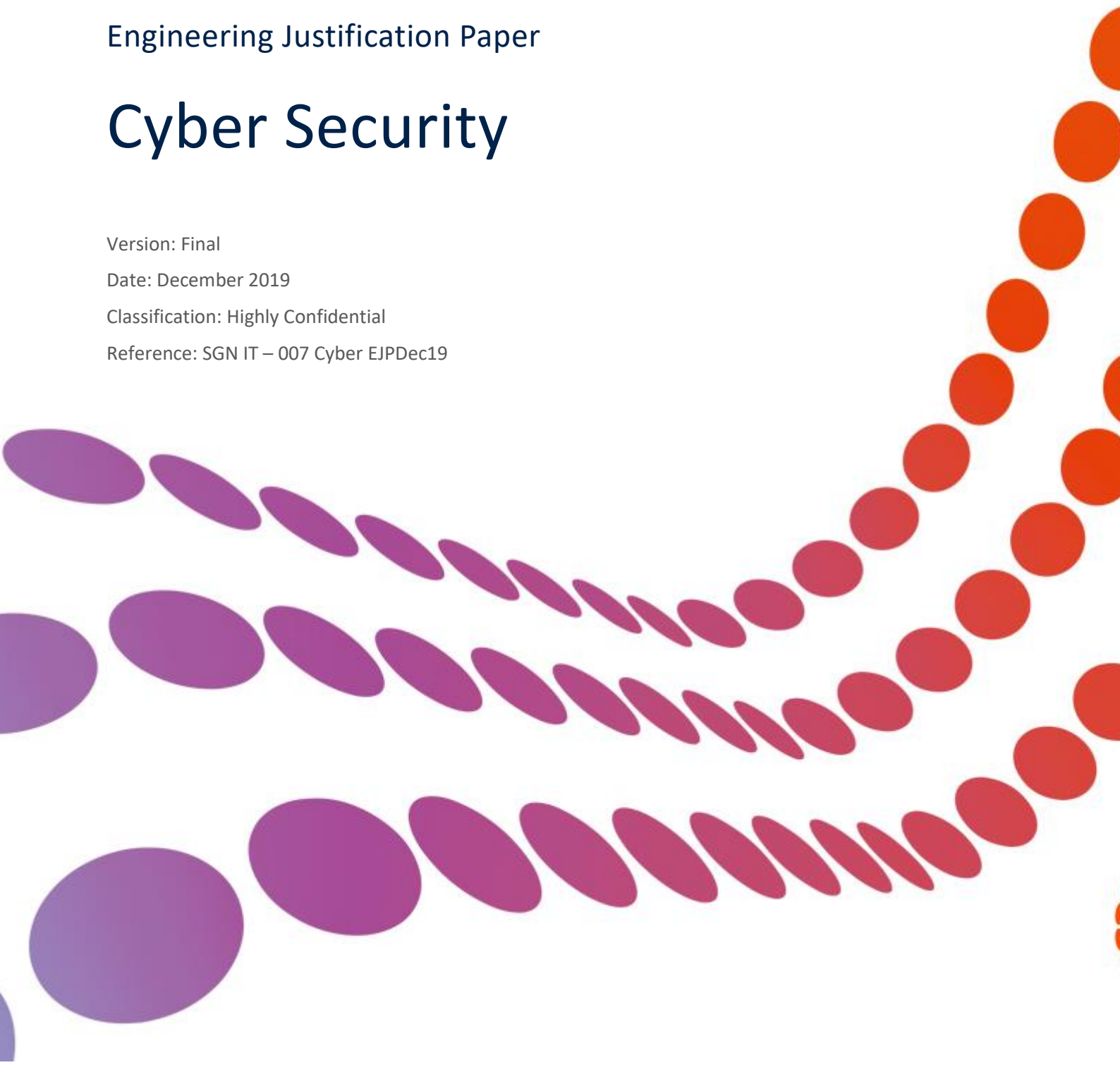
Cyber Security

Version: Final

Date: December 2019

Classification: Highly Confidential

Reference: SGN IT – 007 Cyber EJPDec19



1 Table of Contents

2 Introduction

This paper provides architectural justification to support SGN's proposal to spend £22.318 million (over five years starting in April 2021) on Cyber Security to secure SGN's Operational & Non-Operational Technology Infrastructure.

This paper focuses solely on the investment required to maintaining the current level of operation, keeping our technology infrastructure safe from ever increasing and emerging cyber threats.

Our ability to maintain the safety of our technology infrastructure from Cyber threats underpin SGN's ability to run and maintain a safe and reliable network as required to meet the needs of its customers throughout the GD2 period. A failure in the systems could present significant risk to SGN and its customers leading to loss of life or licence.

The cyber investments cover both what is considered Operational Technology and IT Business Systems Technology as identified in the OFGEM Cyber Guidelines Consultation. It is important to note that due to the global trend of adopting Cloud based technologies and Security

This paper needs to be reviewed in conjunction with EJP – Control Room (*SGN IT - 005 ContRm EJPDec19*), EJP – RTU Refresh (*SGN E&I - 001 Tele - EJP Dec19*), SGN IT - 018 Telem EJPDec19).

2.1 General Background

UK Government and OFGEM as well as numerous stakeholders and advisors recognise the threat to CNI and UK Utilities in general and the need for a substantial increase in Cyber Security. In addition to this, OFGEM have requested additional reporting and assurance on the EU NIS-Directive which exists to significantly improve Cyber Security capability as well as fine companies who are found to breach this directive. The NIS Directive has been implemented at the same time as the new General Data Protection Regulations (GDPR), which require holders of personal data to provide security assurances around that data, and to report on any incidents that might affect them with the same levels of fines associated with breaches (up to 4% of revenue and/or up to 20m Euros).

In line with the UK National Cyber Security Strategy, OFGEM's request to undertake a Cyber Assessment Framework (CAF) and UK Government and OFGEM who are seeking a significant improvement and far reaching assessment of Gas Distribution Networks' Cyber Security as part of the NIS Directive, we have identified an appropriate investment plan based on risks to SGN, our customers and UK Plc which will keep pace with the new and emerging threats in Cyber Security from Nation States and Businesses alike.

We have worked closely with BEIS, NCSC and OFGEM to ensure that our target investment areas are aligned to industry risk. We have also sought advice and input from security and technology advisors (including Commercial Confidentiality). We continue to seek feedback on risk and investment areas through the E3CC utilities industry collaboration group. Sharing and learning about best practice within Utilities on Cyber Security. We have linked our investment plans to the NIST Cyber Security Framework and BEIS's Cyber Assessment Framework. and is aligned to OFGEM's plan to measure and track Cyber risk for each company on an ongoing basis.

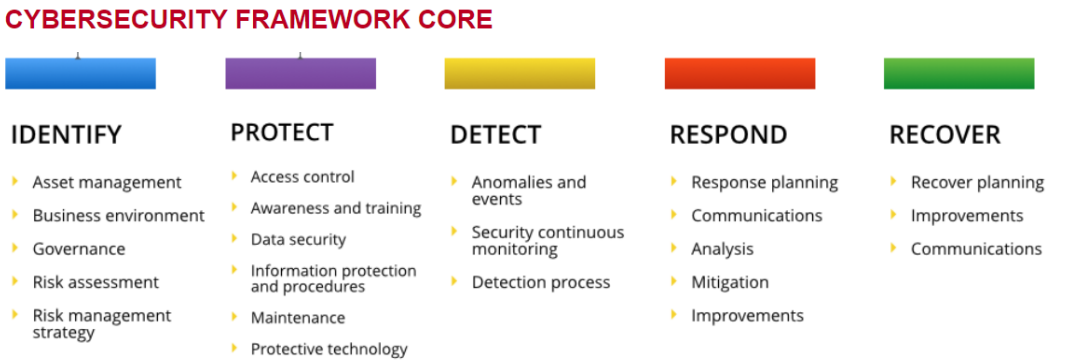
As a regulated company we have guaranteed standards of performance that we adhere to. Investing in the right levels of technology allows us to meet and track these standards over all our outputs. We are also measured and required to produce additional reporting to OFGEM on our adherence to the EU NIS-Directive. The UK Government identifies 'cyber' as one of six Tier 1 threats to national security. This note focuses on the cyber threat to the UK's critical national infrastructure, describes measures to improve cyber security and challenges in how to implement them. Our Cyber Security investment plan has identified the essential investments needed in the areas to ensure we continue to protect our infrastructure from nation state levels of capability and is based on the best information available at this time to ensure we can continue to provide the best service to our customers, maintain the security of supply and protect our assets and people.

2.2 Site Specific Background

The investments called out in this paper underpin all areas of SGN and are not site specific.

3 Equipment Summary

The scope of investment in Cyber Security has been aligned to the National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF) and is intended to meet both EU Network & Information Systems (NIS) Directive requirements and wider Critical National Infrastructure (CNI) needs. The picture below summarises the scope of the framework.



To give a sense of scale, our IT estate runs, maintains and supports:

- Security
- Security
- Security
- Security
- Security

In addition to the above, we also must manage Security
This covers:

- Security
- Security
- Security
- Security
- Security
- Security
- Security
- Security
- Security

This paper recommends investment that underpins our ability to ensure our critical application estate remains adequately secured from cyber threats.

4 Problem Statement

Investment in Cyber Security is critical to address SGN's response to the increased threat to CNI & UK utilities highlighted by UK government & National Cyber Security Centre and the need to mitigate an ever-increasing risk to the availability of our services, the resilience of our network management, availability of our safety critical gas escape response service and our ability to operate safely and respond to and protect our customer's needs.

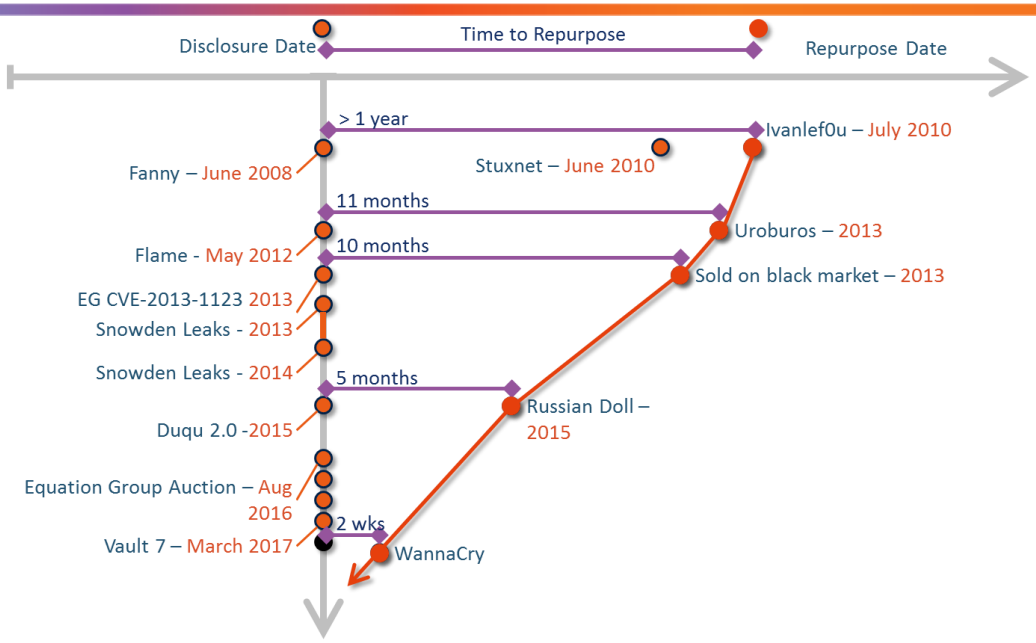
If this investment is not provided, Security

The success of our investment will be apparent by our ability to continue to keep our infrastructure safe, continue to respond to emerging cyber threats as well as continue to operate our network safely. As well as the above risks, there is the additional risk of loss of information which could lead to fines from the Information Commissionaire's office under the General Data Protection Regulation Act.

4.1 Narrative Real-Life Example of Problem

The threat response time all companies now face when aiming to deal with cyber threats has moved from circa 12 months in 2012/13 i.e. the beginning of GD1, to less than a fortnight as was the case with the WannaCry attack experienced in 2017. This compression of time to respond to malware and cyber-attacks means that companies risk a higher level of exposure and disruption to operations if they are unable to detect, protect and respond to these attacks in a matter of hours and days rather than months. This means that those companies who are at high risk, such as CNI organisations like SGN, need to have a significantly improved Cyber security capability.

The diagram below illustrates this compression of the time to response by citing real examples of attacks and malware that occurred;



SGN has received several, very material and real cyber risk warnings. Commercial Confidentiality :

- Commercial Confidentiality
- Commercial Confidentiality
- Commercial Confidentiality
- Commercial Confidentiality
- Commercial Confidentiality
- Commercial Confidentiality
- Commercial Confidentiality

In addition, the following Alerts have been received recently from external agencies:

Alert (TA18-276B)

Advanced Persistent Threat Activity Exploiting Managed Service Providers

The National Cybersecurity and Communications Integration Center (NCCIC) is aware of ongoing APT actor activity attempting to infiltrate the networks of global managed service providers (MSPs). Since May 2016, APT actors have used various tactics, techniques, and procedures (TTPs) for the purposes of cyber espionage and intellectual property theft. APT actors have targeted victims in several U.S. critical infrastructure sectors, including Information Technology (IT), Energy, Healthcare and Public Health, Communications, and Critical Manufacturing.

This Technical Alert (TA) provides information and guidance to assist MSP customer network and system administrators with the detection of malicious activity on their networks and systems and the mitigation of associated risks. This TA includes an overview of TTPs used by APT actors in MSP network environments, recommended mitigation techniques, and information on reporting incidents.

https://www.us-cert.gov/ncas/alerts/TA18-276B

Advisory: Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices
This advisory provides information on the worldwide cyber exploitation of network infrastructure devices (e.g. routers, switches, firewalls, Network-based Intrusion Detection System (NIDS) devices) by Russian state-sponsored cyber actors.

https://www.ncsc.gov.uk/alerts/russian-state-sponsored-cyber-actors-targeting-network-infrastructure-devices

Indicators of Compromise for Malware used by APT28

Advanced Persistent Threat group, APT28 (also known as Fancy Bear, Pawn Storm, the Sednit Gang and Sofacy), is a highly skilled threat actor, best known for its disruptive cyber activity against the US Democratic National Committee (DNC).

According to publicly available information, APT28 has previously used tools including X-Tunnel, X-Agent and CompuTrace to penetrate target networks. These tools can be used to hook into system drivers and access local passwords and the LDAP server. Reported capabilities include monitoring keystrokes and mouse movements, accessing webcams and USB drives, searching and replacing local files and maintaining a persistent connection.

The signatures and Indicators of Compromise (IoCs) included in this advisory will assist in detecting APT28 malware. Network based signatures alone will not guarantee successful identification of APT28 in a network. Many of the communication modules used by the actor are wrapped in protocols such as SSL/TLS, with the intention of evading content-based signatures.

Please use the indicators in this NCSC advisory to check for the presence of this malware on your platforms and networks.

https://www.ncsc.gov.uk/content/files/protected_files/article_files/Indicators%20of%20Compromise%20for%20Malware%20used%20by%20APT28%20v.4.pdf

4.2 Spend Boundaries

The investment in cyber security covers both operational and non-operational IT systems and covers the necessary resources and technology to Identify, Protect, Detect, Respond & Recover from Cyber Security Threats in line with the NIST Cyber Framework with the objective of compliance to the EU NIS Directive.

Security

5 Probability of Failure

The probability of failure of our ability to secure and protect our infrastructure from Cyber Threat has been identified as part of UK Government's risk assessment on Cyber Threats to Critical National Infrastructure.

5.1 Probability of Failure Data Assurance

The text below is an extract from UK Government's risk assessment of Cyber Threat to Critical National Infrastructure.
The UK Government identifies 'cyber' as one of six Tier 1 threats to national security. This note focuses on the cyber threat to the UK's critical national infrastructure, describes measures to improve cyber security and challenges in how to implement them. It also examines national and international policy and legislation. Computer systems increasingly underpin UK CNI. Examples include inter-bank payment systems, NHS data networks and industrial control systems that monitor and operate physical infrastructure (such as nuclear power plants or railway signals). Such systems are increasingly connected into large networks to allow centralised monitoring and remote or automated control, to make operation and maintenance more efficient. These networks often connect to the internet, either directly or indirectly via the operators' other networks. As more industrial control systems connect to computer networks, the potential for cyber-attacks to cause physical effects increases. The extent of connected computer systems in CNI is likely to continue to grow. For example, the Government is leading a roll-out of smart energy meters, and the NHS is aiming to digitise all medical records by 2020. Computer-based CNI systems are vulnerable to electronic failure, design flaws, operator error, physical damage and cyber-attack. Cyber-attacks can be delivered physically (for example via a USB stick) or via the internet. Internet-based attacks range from simple scam emails sent in large numbers, to advanced attacks targeting specific institutions. Sophisticated attacks progress in multiple stages, probing the network after an initial breach to gain information and control over periods that can last years.

http://researchbriefings.files.parliament.uk/documents/POST-PN-0554/POST-PN-0554.pdf

6 Consequence of Failure

SGN' ability to manage its IT and OT estate is paramount to continue to safely operate our gas network and Security :

- Regulatory and Compliance risk: Security
- Lack of Resiliency in Critical Systems risk: Security
- Inability to Keep Up with Digital Business Projects risk: Security
- Third-Party Risk: Security
- Reputational Risk: Security
- Emerging Technology Risk: Security
- Loss of Intellectual Property: Security

7 Options Considered

7.1 Option 1 – Minimum investment to maintain our cyber security infrastructure

Minimum investment in Cyber to maintain a safe & reliable network. Implement the necessary resources and technology to Identify, Protect, Detect, Respond & Recover from Cyber Security Threats in line with the NIST Cyber Framework with the objective of compliance to the EU NIS Directive Cyber Assessment Framework.

7.2 Baseline Option – Security

Security

7.3 Options Technical Summary Table

We have identified the following specific initiatives which help manage the threats identified in line with the framework mentioned in Sections above. It should be noted that this is based on our current threat assessment and as we move into each year of GD2, an assessment will be undertaken on the threat level and adjustments made to the level of investment if the threat position changes.

Table 1: Technical Initiatives

Cyber Initiative	Type	Tier	Option 1 - Minimum Investment to maintain a safe & reliable network	Option 2 - Do Nothing – Point Initiatives reacting to Emerging Cyber Threats
Security			X	N/A
			X	N/A
			X	N/A
			X	N/A
			X	N/A
			X	N/A
			X	N/A
			X	N/A
			X	N/A
			X	N/A
			X	N/A
			X	N/A
			X	N/A

Security

		X	N/A
		X	N/A
		X	N/A
		X	N/A
		X	N/A
		X	N/A
		X	N/A
		X	N/A
		X	N/A
		X	N/A
		X	N/A
		X	N/A
		X	N/A
		X	N/A
		X	N/A
		X	N/A
		X	N/A
		X	N/A
		X	N/A
		X	N/A
		X	N/A
		X	N/A

Notes:

Project – Specific investment in Cyber with finite start and end time and dedicated resources assigned to implement the investment.

Initiative – Investment in Cyber using shared resources with specific funding to implement the investment.

Tier 1 – Projects & Initiatives associated with the current significant risks recorded within the SGN risk register and or recommendations from previous external audits.

Tier 2 – Projects & Initiatives associated with industry and government good practice that support the overall risk reduction for SGN but may not be referenceable.

Tier 3 - Projects & Initiatives associated with industry and government good practice that support the overall risk reduction for SGN but may not be referenceable and have been prioritised to support project delivery capacity.

Transition from GD1 to GD2

SGN is currently going through a technology driven transformational change and as a result there are several security improvement projects in progress. These cover elements related to people, process and technology. As part of GD2 submissions we have created three different categories for the projects required to close gaps in cyber security and ensure SGN achieve the relevant level of Cyber Resilience. These categories are based on timelines for delivery, dependency on other projects and criticality. Following the engagement of the Advisory team at Ofgem and feedback provided, we have provided a summary of the current activities within GD1 and the tactical approaches taken in preparation for GD2 funding. The current plans submitted as part of GD2 do not reflect the recently revised guidelines provided by Ofgem in October 2019.

The feedback received from Ofgem has been productive, and we will continue to work with the competent authority and engage the Cyber advisory team wherever and whenever required. The following Tier 1 projects have been identified as areas of initial focus:

OT Asset Management

Security

IT Asset Management

Security

Attack Path Mapping

Security

Security

Privileged Access Management implementation

Security

Active Directory (AD) separation

Security

Cyber Security Team Training

Security

Cloud Migration: Security

APM action remediation: Security

Endpoint Protection: Security

Table 2: Options Technical Summary

Security

7.4 Options Cost Summary

Table 3: Options Cost Summary

Option	Template	Cost Breakdown	Total Cost (£m)
Invest in Cyber Security	IT Capex	Resources Software Hardware Contingency	Commercial Confidenti
		Total	**14.73**
Invest in Cyber Security	IT Opex	Equipment Civils Engineering Costs Contingency	Commercial Confiden
		Total	**7.58**

The following table broadly summarises the cost of alternative options in comparison to the minimum investment required to maintain a safe and reliable Network. Further detail can be found in the associated cost benefit analysis document for each of the investment areas.

Table 4: Alternative Options

Security

Security

Please note the costs outlined in the Options Technical Summary Table are based on the following assumptions:

Option 1 assumptions:

- Commercial Confidentiality
- Commercial Confidentiality
- Commercial Confidentiality

Option 2 assumptions:

- Security

- Security
- Security
- Security

Security

- Security
- Security

Security

Security

8 Business Case Outline and Discussion

This investment enables our ability to continue to secure our IT & OT technology infrastructure.

8.1 Key Business Case Drivers Description

Table 5: Summary of Key Value Drivers

Option No.	Option Description	Key Value Driver
1	Minimum Investment to maintain a safe & reliable network	Ability for SGN to continue to maintain the security of our Cyber investment and support business processes. Enables us to meet our outputs and license conditions Incremental change to address obsolescence.
2	Do nothing	Not recommended

The case to proceed for Cyber should be considered in comparison with a 'do-nothing' option Security

As mentioned in the previous section, where real-life examples of problems which could be encountered if adequate investment is not made to secure our cyber assets, we have identified the minimum investment necessary to maintain a safe & reliable network.

SGN's license to operate requires us to be compliant with the Uniform Network Code and the Supply Point Administration Agreement. It is critical that we can comply with legislation regarding how we manage our organisation and run operations daily. Failure to invest in Cyber security would compromise our ability to comply, which in turn could lead to a breach of license conditions leading to significant fines or a failure to comply with the law which could lead to fines and / or legal action being taken against SGN.

As well as the above meeting stakeholder expectations regarding keeping the gas flowing safely, sustaining our future, keeping energy affordable, improving our service and supporting our communities is wholly dependent on investment enabling us to respond to legislative and regulatory requirements impacting our systems in the most effective way.

Our Architectural Principles and IT strategy advocates a cloud first, buy not build approach ensuring that the total cost of ownership for any solution is best value for money when comparing to options that are available. Our programme and project governance structure will ensure that appropriate business case development and options analysis is done at the point of change in GD2 to underpin customer, OFGEM, National Cyber Security Centre & UK Government expectations regarding maintaining appropriate levels of protection from new and emerging cyber security risks throughout the GD2 period.

Progress and benefits will be measured through evidence of improved trends from key security metrics and capability to measure them. These include but not limited to:

Operational security metrics:

- Patch coverage and latency e.g. number of critical patches applied within a period,
- Antivirus coverage e.g. percentage coverage of Antivirus across the estate

Security Incident Management:

- Total number of security incidents reported monthly
- Total number of incidents addressed within agreed timescales

Compliance:

- Percentage of total number of critical systems or processes audited
- Number of very high or high risk issues as an outcome of audits

Access Control:

- Number of privileged access accounts that have been inactive for a set number of days
- Number of accounts that have not been disabled for leavers

Metrics stated above are a subset of current operational reports in line with current governance structure and is not an exhaustive list.

Table 6: Summary of CBA Results

Option No.	Desc. of Option	Preferred Option (Y/N)	Total Forecast Expenditure (£m)	Total NPV	2030	2035	2040	2050

8.2 Business Case Summary

This paper recommends the expenditure of £22.318 million over five years starting in April 2021. The scope of this investment covers project activity necessary to ensure that SGN can continue investing to secure our cyber assets to maintain a safe & reliable network.

We will continue to measure our investment in Cyber Security against the maturity levels as set out in the CAF framework and the Threats levels as provided to us by our partners and industry bodies.

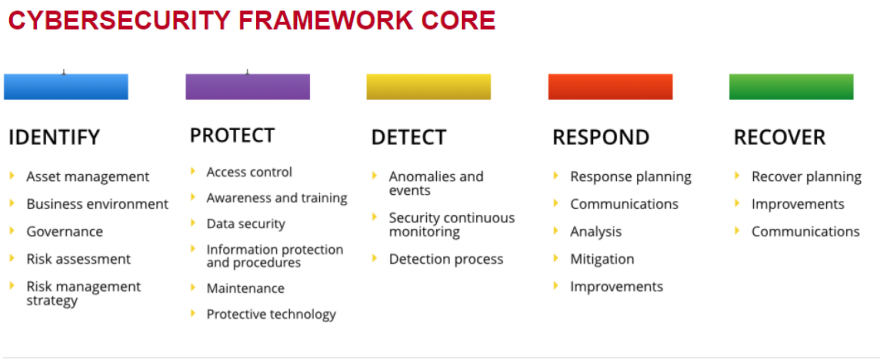


Table 7: Business Case Matrix

	Invest in Cyber Security
GD2 Capex (£m)	
Number of Interventions	
Carbon Savings ktCO2e (GD2)	
Carbon Savings ktCO2e /yr	
Carbon Emission Savings (35yr PV, £m)	
Other Environmental Savings (35yr PV, £m)	
Safety Benefits (35yr PV, £m)	
Other Benefits (35yr PV, £m)	
Direct Costs (35yr PV, £m)	
NPV (35yr PV, £m)	
High Carbon Scenario	
Carbon Emission Savings (35yr PV, £m)	
High Carbon NPV (35yr PV, £m)	

9 Preferred Option Scope and Project Plan

9.1 Preferred option

Our recommendation is to progress with Option 1: Implement the necessary resources and technology to Identify, Protect, Detect, Respond & Recover from Cyber Security Threats in line with the NIST Cyber Framework with the objective of compliance to the EU NIS Directive Cyber Assessment Framework. We have identified specific initiatives which help manage cyber threats in Section 6. It should be noted that this is based on our current threat assessment and as we move into each year of GD2, an assessment will be undertaken on the threat level and adjustments made to the level of investment if the threat position changes.

9.2 Asset Health Spend Profile

Table 8: Asset Health Spend Profile

Asset Health Spend Profile (£m)						
	2021/22	2022/23	2023/24	2024/25	2025/26	Post GD2
Commercial Confidentiality						Investment profile continues post GD2

The CAF framework, risks identified, and treatments recommended can be found in the attached power-point deck, which describes the methodology in more detail.

Security

9.3 Investment Risk Discussion

Risk Description	Impact	Likelihood	Mitigation/Controls	Comments
Changing threat profile, significantly changes proposed investment plans and value of investment	Medium	>80% & <=100%	Internal and external Cyber Threat Management processes and regular review and re-prioritisation of project activity throughout GD2	We have highlighted through the paper that cyber threats change, and we need to be flexible.
Impact of cyber projects on business as usual impacting ability to meet regulatory standards	High	<=20%	Thorough Project Management, design and testing, risk and issue management. Appropriate budget assigned for delivery considering lessons learnt from previous upgrades.	We will continue to monitor the business strategy and impact of technology change on the business and amend accordingly.

Changing technology trends including operating systems and applications impact the cost and timelines for delivery of the option	Medium	>40% & <=60%	Investment in technology roadmaps, ensuring early sight of any changes.	We have got advice from the industry while identifying costs for our current investments and will continue to do so.

Table 9: Sensitivity Results for the Preferred Option

Cyber Security	Low	Mid	High
Capex (£m) Number of Interventions Carbon Savings ktCO2e (GD2) Carbon Savings ktCO2e /yr	Commercial Confidentiality		
Carbon Emission Savings (30yr PV, £m) Other Environmental Savings (30yr PV, £m) Safety Benefits (30yr PV, £m) Other Benefits (30yr PV, £m) Direct Costs (30yr PV, £m)			
NPV (30yr PV, £m)			

Low case: The low case is the same as the mid case as investment in Cyber Security is mandatory. No sensitivity has been applied to this case.

Mid case: No changes have been applied.

High case: SGN have applied an increase of 50% to the costs. This is somewhat likely. Cyber threat continues to evolve and become more difficult to detect and prevent.

Project payback has not been carried out as part of this analysis due to the effect of the Spackman approach. For a cash-flow traditional project payback period please see scenario 4 of our Capitalisation Sensitivity table.

Capitalisation Sensitivity

Consumers fund our Totex in two ways – opex is charged immediately though bills (fast money – no capitalisation) and capex / repex is funded by bills over 45 years (slow money – 100% capitalisation). The amount deferred over 45 years represents the capitalisation rate. Traditionally in 'project' CBA's the cashflows are shown as they are incurred (with the investment up front which essentially is a zero capitalisation rate). Therefore, we have developed scenarios that reflect both ways of looking at the investment – from a consumer and a 'project'.

The scenarios are summarised as follows:

- Scenario 1 - we have used the blended average of 65%, used in previous iterations of this analysis.
- Scenario 2 - we have represented the Capex and Opex blend for the two networks, as per guidance.
- Scenario 3 - addresses our concerns on capitalisation rates whereby Repex and Capex spend is deferred (100% capitalisation rate) and Opex is paid for upfront (0% capitalisation rate).

- Scenario 4 - this reflects the payback period in 'project' / cash-flow terms and provides a project payback.

We have taken a view of the NPV in each of the scenarios, except for scenario 4, at the 20, 35 and 45 Year points, to demonstrate the effect of Capitalisation Rate on this value.

Table 10: Capitalisation Rate Variation

Scenario	1	2 SGN	3	4
Capex (%)	65	41	100	0
Opex (%)	65	41	0	0
Repex (%)	100	100	100	0
Output				
NPV (20yr PV, £m)	112.34	105.16	122.80	
NPV (35yr PV, £m)	80.41	75.25	87.95	
NPV (45yr PV, £m)	64.39	60.74	69.72	
Payback	3.00	3.00	3.00	3.00

Appendix A - Acronyms

Acronym	Description
APT	Advanced Persistent Threat
BEIS	Department for Business Energy and Industrial Strategy
CAF	Cyber Assessment Framework
E3CC	Energy, Emergency Executive Cyber Committee
GDPR	General Data Protection Regulation
IoC	Indicators of Compromise
IT	Information Technology Business Systems as identified by OFGEM in the Cyber Resilience guidelines
MSP	Managed Service Providers
MWR	MWR InfoSecurity
NCSC	National Cyber Security Centre
NIDS	Network-based Intrusion Detection System
NIS	Network & Information Systems
NIST	National Institute of Standards and Technology
NCCIC	National Cybersecurity and Communications Integration Centre
OFGEM	Office of Gas and Electricity Markets
OT	Operational Technology as identified by OFGEM in the Cyber Resilience guideli
TA	Technical Alert
TTP	Tactics, Techniques, and Procedures
SSL/TLS	Secure Sockets Layer / Transport Layer Security