

NCRA Questionnaire Explanatory Notes

*These explanatory notes should be edited to suit the user’s purpose in conducting a NCRA*

CONTEXT

A National Cyber Risk Assessment (**NCRA**)has been commissioned by <name of commissioning organisation> to help to plan for further investment in cyber security and resilience that may be necessary.

The reason for conducting this National Cyber Risk Assessment is as follows:

* The economic and social development of <country name> will depend on significant levels of connectivity through cyber space. As in many nations where digitalisation is being introduced on a significant scale, the economy, the administration of government and the provision of essential services will increasingly rely on the integrity of cyberspace and on the infrastructure, systems and data which underpin it. This brings with it opportunities for innovation, growth and efficiency, but is likely to bring risks of societal and economic disruption.
* Introduction of the hardware and software to facilitate this interconnected digital environment has sometimes 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 shortcomings. The Government requires assurance that systems being obtained from the commercial market will provide adequate levels of business continuity through cyber security and resilience.

The Government can bring its resources to bear to address cyber threats. But the scale and dynamic nature of cyber threats mean that no Government can directly provide for all aspects of cyber security and resilience. Instead, an approach is needed where industry, infrastructure providers and other partners in the development of the country, collaborate with each other and government in securing networks, services and data. The purpose of this NCRA is therefore

* To provide the Government with a rational basis for prioritizing its own investment in national cyber security
* To assist with the communication of identified risks to key stakeholders to create a culture of cyber risk management, security and resilience.

METHOD

The NCRA will begin with a Survey of significant cyber systems in use by organisations and businesses which use these systems to provide services that are essential for the economy, for Government and for the welfare of the population. These national infrastructure services are by definition.

*“facilities, systems, sites, information, people, networks and processes necessary for the country to function and upon which daily life depends. Typically, these would include: energy, food, water, health, transport, money supply, communications, emergency services and aspects of government including defence. They also include some functions, sites and organisations which are not critical to the maintenance of essential services but which need protection due to the potential danger to the public (chemical sites for example).”*

The NCRA uses a simplified method of qualitative risk assessment to identify those systems that entail the greatest risk of disruption to these essential services, the economy or society. A ‘screening risk assessment’ - entirely based on the answers given voluntarily by participants in the Survey (you) in response to this Confidential Questionnaire – may be followed by further confidential discussions to enable the Government to evaluate the highest risks.

THE QUESTIONNAIRE

* Answers to the Questionnaire will be confidential: it will be hosted on a [secure government web-site]; [other measures will be taken to protect information]; [detailed answers will not be shared with other participants]
* Participating organisations will be able to contact [the organisers] to clarify questions; and may be asked to meet with [the organisers] to clarify answers they have given
* Feedback will be given on a one-to-one basis to [all] participants in the survey, following the initial or final evaluation phase of the NCRA
* One questionnaire should be answered for every significant cyber-dependent service a participating organisation identifies as of interest to the Survey
* The questionnaire is not designed as an audit of cyber security but to inform a qualitative (not quantitative) national-level risk assessment
* The questionnaire uses multiple choices for the key (scoring answers) but allows for short text answers to be given in other cases; please keep answers short and do not include detailed descriptions or technical data.

The Questionnaire will ask you to estimate the nature of the cyber risk in your organisation, in five sections:

* Information about your organisation and critical cyber systems in use
* For each critical cyber system you identify:
	+ Critical system characteristics of each critical cyber asset
	+ Identification of the reasonable worst-case scenario illustrating the threats and hazards most likely to affect the system
	+ The impacts of a successful attack on or disruption of your critical cyber systems
	+ Your estimate of the cyber-security/resilience qualities of your critical cyber-systems

HOW CYBER RISKS ARE CALCULATED

The answers will be used to estimate the cyber risk to the country according to the following formula:

**QUESTIONNAIRE SECTION 1: INFORMATION ABOUT YOUR ORGANISATION**

**This section will be used to [record information about the organisation, which national infrastructure sector it belongs to, and what services it provides through the use of critical cyber systems.][For confidentiality reasons, the name of the organisation, and the cyber systems identified, will be codified before the information in Sections 2-5 is analysed and compared with information supplied by other participants, so that the collective risk assessment is anonymised]**

**In this survey, Cyber systems** are information systems and networks (hardware, software and associated infrastructure), the data on them, and the services they provide. **Cyber Security** refers to the protection of cyber systems from unauthorised access, harm or misuse. This includes harm caused intentionally by an operator of the system (the ‘insider threat’), or accidentally, as a result of failing to follow security procedures. **‘Cyber resilience’** refers to the ability to prepare for, detect, respond to and recover quickly from cyber-attacks or incidents and so to limit their impact*.*

1.1 Name of the organisation – self-explanatory.

1.2 List the services that your organisations provides: - please describe the range of services provided by the organisation which depend on cyber systems for which you are submitting a Questionnaire response (NB the Survey requires one complete Questionnaire response for each significant cyber system).

1.3 Which national infrastructure Sector does your organisation belong to? – the questionnaire lists the most commonly defined national infrastructure sectors, from which to choose; if none applies, please tick other (and specify which).

1.4 List critical cyber systems:- list only those cyber systems in use by your organisation to provide/support provision of services that are critical for the ‘public good’ (public welfare, the economy, essential services); this may be a number of linked systems with similar characteristics, in which case list these as one. Every system you list will need a full questionnaire to be completed – see Q 2.1.

1.5 Cyber security within the organisation – this question concerns the extent to which cyber risks are recognised at Board level (rather than at lower levels, which are covered by Section 5) within the organisation; and whether there is (or not) a Corporate Culture of cyber risk management.

**QUESTIONNAIRE SECTION 2: CRITICAL SYSTEM CHARACTERISTICS**

**This section focuses on one of your critical systems and captures the characteristics and functions of the system.**

2.1. Which of the cyber systems at 1.4 does this questionnaire describe? Which department, organisation or business is responsible for this system? Each questionnaire response should only describe one cyber system; if your organisation has identified more than one in response to Section 1, then you should identify which system this questionnaire refers to, and which department or part of your organisation is responsible for it.

2.2 Brief description of the system:- please describe the system and its functions briefly – technical details are not required.

2.3 Indicate briefly why this system has been identified by you as a significant system providing or supporting the provision of services that are essential for the country to function.

2.4 System connectivity – a significant element of the risk presented by cyber systems is the extent to which they are insulated from other systems or networks, and the extent to which ‘firewalls’ can become eroded over time; please consider whether your system is truly stand-alone or has become partly linked to other networks in use within or outside the organisation. Also consider the extent to which the system controls physical outcomes (as do, for example, SCADA systems, the ‘Internet of Things’) which affect daily life.

2.5 System hosting – self-explanatory

2.6 & 2.7. Responsibility for cyber security – if the system is not hosted on IT that is owned and managed by your organisation (see 2.3) then responsibility for security may be divided between your organisation and an external provider. In that case, please tick ‘No’ and explain in 2.7.

2.8 Internal business criticality - answers to this question should take account of the extent to which there is effective back-up/redundancy in your system, enabling the effects of disruption to be mitigated; if there is any doubt about the effectiveness of back-up systems (e.g. because they may be exposed to the same risk as the primary system) then the marking should reflect this.

2.9 External business criticality – this question considers only how many people and organisations depend on the service that you are providing, using the cyber system identified at 2.1, for their welfare, livelihood or businesses.

2.11 Outward dependencies: this question is specifically asking about cyber-dependencies – direct reliance on cyber systems (e.g. the Internet) which are operated by other organisations. Do not include dependence on non-cyber-services provided by others (e.g. electricity supply) even if you believe they are likely to rely on cyber-space

2.12 Inward dependencies: this question asks whether other systems operated by other organisations directly depend on the cyber system covered by this questionnaire.

**QUESTIONNAIRE SECTION 3: CYBER RISKS**

**This section is to identify the cyber risk, and to determine what would be a ‘reasonable worst-case scenario’ illustrating the risks to your system. The cyber risk is an event that affects objects of value (property, business continuity, profitability etc) to your organisations. The Survey identifies the risk by inviting you to construct a scenario representing the worst that could reasonably happen to your system given its function, the kinds of ‘threat actors’ who are known to be motivated to attack such systems, and the methods (‘threat vectors’) they have to do so.**

**See Annex A for extracts from the UK’s National Cyber Security Strategy describing the different kinds of threat actor and attack vector (methodology) and giving examples that may help to answer questions in this section.**

3.1 The three aspects of information security – this question asks you which of the following aspects is the most important to the system you have described in this questionnaire response. The definitions of the three aspects is as follows:

|  |  |
| --- | --- |
| Availability | information can be accessed by the user when it is needed |
| Integrity | information has not been changed accidentally, or deliberately, and is accurate and complete |
| Confidentiality | information is only available to those who have a right to know it |

The definitions of the scores used to assess the importance of the tree aspects of information security to your organisation is as follows:

|  |  |
| --- | --- |
| Low | This aspect of information security is not significant for the delivery of essential services and any disruption to system operation, loss of integrity or breach of confidential information will have little impact on the delivery of services or the reputation of the organisation. |
| Medium | This aspect of information security is important to the successful delivery of some services and any disruption to system operation, loss of integrity or breach of confidential information will have a limited and manageable impact of some key services and the reputation of the organisation. |
| High  | This aspect of information security is very important to the successful delivery of essential services and any disruption to system operation, loss of integrity or breach of confidential information will have a severe impact on some key services and the reputation of the organisation |
| Very High | This aspect of information security is critical to the successful delivery of essential services and any disruption to system operation, loss of integrity or breach of confidential information will have a severe, widespread and long-term impact on key services and the reputation of the organisation |

3.2 Importance of cyber threat intelligence – Organisations whose cyber systems are exposed to the threat of attack rely on up-to-date information about threat actors and threat methodologies to ensure that their systems remain secure, and to trigger effective incident response. These questions ask you how readily you are able to obtain up-to-date cyber threat information and how important you think it is to the security of the system that you are assessing. The definition of the scores used to assess the importance of threat intelligence to your organisation is as follows:

|  |  |
| --- | --- |
| 1 | Threat intelligence is not used as part of the organisations approach to cyber security |
| 2 | Threat intelligence is occasionally made available but is not an important aspect of the approach to cyber security  |
| 3 | Threat intelligence is sometimes sought and used on an ad-hoc basis to improve cyber security |
| 4 | Threat intelligence is an important part of the approach to cyber security and a process is in place to ensure that appropriate action is taken to respond to new or changing threats. |
| 5 | Threat intelligence is an essential part of the approach to cyber security and is used to provide timely response to changes in the cyber security threat environment |

3.4 The ability of your organisation to access threat intelligence is assessed as follows:

|  |  |
| --- | --- |
| 1 | Threat intelligence is not available |
| 2 | Threat intelligence is occasionally made available on an ad-hoc basis  |
| 3 | At least one source of relevant threat intelligence is accessed on a regular basis (e.g. monthly) |
| 4 | Several high-quality threat intelligence feeds are actively and frequently gathered and analysed (e.g. daily) |
| 5 | Multiple (all source) feeds of high-quality threat intelligence are actively gathered, analysed and used to provide a tailored near real time insight into the cyber security threat environment. |

3.5 – 3.6 Which cyber **threat actors** are you most concerned about? Which cyber **attack vectors** are you most concerned about? This question concerns only the cyber system being assessed: taking into consideration the relative importance of (see Question 3.1) availability, integrity, and confidentiality of the data on your system, which kind of threat actor (criminal, state/state-sponsored, hacktivists, terrorist) is most likely to be motivated and able to attack the system successfully; and which attack methodology would be of most concern to you. For some organisations/systems, accidental disruption is as big a concern as any malicious threat actor.

|  |  |
| --- | --- |
| **Threat Actor** | **Commonly associated threat vectors** |
| Cyber criminals | Cyber-**dependent** crimes (e.g. developing and propagating malware for financial gain, hacking to steal, damage distort or destroy data, networks; includes ransomware and threats of distributed denial of service – DDOS – for extortion |
|  | Cyber-**enabled** crimes – traditional crimes increased in scale by use of computers, networks or other forms of ICT (e.g. cyber-enabled fraud and data theft) |
| States and State-sponsored threat (generally covert) | Embarrassing outages of communications, IT and networked services etc |
|  | Espionage |
|  | Offensive cyber capabilities including destructive capabilities threatening security of CNI, industrial control systems, the ‘Internet of Things’, etc |
| Terrorists | Hitherto low technical capability, including defacements, ‘doxing’ (where hacked personal details are ‘leaked’ online) designed to attract media attention and intimidate victims |
|  | Future threat may increase as an increasingly computer-literate generation exploits possibilities of defacement or DDOS activity against States |
| Hacktivists, insiders and others  | Disruptive activity (website defacement; DDOS) and some more lasting damage by individuals with a grievance |
|  | Insider threat: theft of sensitive data and intellectual property; possible destructive DDOS |
| Accidental | Accidental damage by employees’ inadvertent infection of networked systems |

3.7 Reasonable worst case scenario: you are asked to use your ‘top’ answers to 3.1, 3.5 and 3.6 to construct a scenario, as follows:

“*The reasonable worst case scenario for this system is a successful attack by [top answer to 3.5] using [top answer to 3.6] resulting in a significant breach of [top answer to 3.1]”*

**QUESTIONNAIRE SECTION 4: IMPACTS**

**This Section asks you to estimate the scale of impact in the event of an attack according to the reasonable worst case scenario. Assume for the purposes of this Survey that the attack is successful, even if you consider that this is unlikely (the likelihood of a successful attack will be part of the assessment following completion of Section 5). You may find it useful to consider the case histories attached to this note which provide examples of organisations worldwide who have been successfully attacked.**

**Impacts are measured taking into account how widespread, how intense, and how long-lasting they are likely to be; the overall impact is taken into account. If the impact in one area is negligible, please use the ‘no impact’ column.**

4.1 Impact on people who use your services – the measure here is how many **people** who rely on your services would be affected by a successful attack.

4.2 Impact on other essential services – this question is trying to find out how many **other** essential services would be affected by a disruption to your cyber system. If the answer is that there are no knock-on consequences for other organisations in the national infrastructure sectors, then please mark ‘no impact’ against each.

* A ‘low impact’ is one where any impact is likely to be limited, localised in one area, and of short duration (minutes rather than hours).
* A ‘medium impact’ would be more intense, not localised but not nationwide, and of longer duration (hours).
* A ‘high impact’ would involve very significant and widespread disruption to the service, for a sustained period of time (days).

Case Study 3 (the 2013 Power Grid Attack in Ukraine) provides an example of a cyber attack that does not only affect direct customers of an organisation that is attacked, but also has indirect knock-on effects on a wider customer base through other national infrastructure owners.

4.3 Estimate the impact on industry and the economy. As can be seen from the case studies at Annex A, the financial damage can easily get into the $100millions. The scale used for this NCRA is accordingly

|  |  |  |
| --- | --- | --- |
| Scale | %age of GDP | $ equivalent [adjust for the size of the economy] or adopt the following figures |
| Low | Less the 0.01% | Less than $10 millions |
| Medium | 0.01-0.1% | $10-100 millions |
| High | 0.1-1% | $100-1,000 millions |
| Very High | More than 1% | More than $1 billion |

4.4 Estimate the impact on [non-material ‘objects of value’ to country X]. The judgements here will be subjective but you are invited to consider three dimensions of each impact type:

* Intensity - is the impact highly intensive or less so on a scale from 1-3
* Extent – is the impact localised, or widespread (nationwide), on a scale from 1-3
* Duration – is the impact short-lived (days), or long-lived (months), on a scale from 1-3

Combining the scores will give you an overall impact score of low (3-4), medium (5-6), or high (7-9)

[4.6 Reserved for the use of the NCRA to measure cyber risk to international events hosted by country x]

**QUESTIONNAIRE SECTION 5: SYSTEM VULNERABILITIES**

You are invited to self-assess the vulnerability of your cyber systems using a simplified approach based on the UK National Cyber Security Centre’s ’10 steps to cyber security’, which recommends a regime based on the 10 steps listed below:

**UK National Cyber Security Centre: 10 Steps to Cyber Security**

**1. Risk Management Regime.** Embed an appropriate risk management regime across the organisation. This should be supported by an empowered governance structure, which is actively supported by the board and senior managers. Clearly communicate your approach to risk management with the development of applicable policies and practices. These should aim to ensure that all employees, contractors and suppliers are aware of the approach, how decisions are made, and any applicable risk boundaries.

**2. Secure configuration.** Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching. Failure to do so is likely to result in increased risk of compromise of systems and information.

**3. Network security.** The connections from your networks to the Internet, and other partner networks, expose your systems and technologies to attack. By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organization). Your organization's networks almost certainly span many sites and the use of mobile or remote working, and cloud services, makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, think about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.

**4. Managing user privileges.** If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise of that users account will be more severe than it need be. All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges should be carefully controlled and managed. This principle is sometimes referred to as ‘least privilege’.

**5. User education and awareness.** Users have a critical role to play in their organization’s security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organization secure. This can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well as helping to establish a security-conscious culture.

**6. Incident management.** All organizations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact. You should identify recognised sources (internal or external) of specialist incident management expertise.

**7. Malware prevention.** Malicious software, or malware is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact your systems and services. The risk may be reduced by developing and implementing appropriate anti-malware policies as part of an overall 'defence in depth' approach.

**8. Monitoring.** System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements.

**9. Removable media controls.** Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls to its use.

**10. Home and mobile working.** Mobile working and remote system access offers great benefits, but exposes new risks that need to be managed. You should establish risk based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers. Train users on the secure use of their mobile devices in the environments they are likely to be working in.

**ANNEX A**

**CYBER THREATS AND HAZARDS**

**(Extract from the UK’s National Cyber Security Strategy, Chapter 3)**

**Cyber criminals**

This strategy deals with cyber-crime in the context of two interrelated forms of criminal activity:

**•** cyber-dependent crimes – crimes that can be committed only through the use of Information and Communications Technology (ICT) devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity); and fi

**•** cyber-enabled crimes – traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft).

Much of the most serious cyber-crime – mainly fraud, theft and extortion – against the UK continues to be perpetrated predominantly by financially motivated Russian-language organised criminal groups (OCGs) in Eastern Europe, with many of the criminal marketplace services being hosted in these countries. However, the threat also emanates from other countries and regions, and from inside the UK itself, with emerging threats from South Asia and West Africa of increasing concern.

Even when key individuals responsible for the most damaging cyber criminal activities against the UK are identified, it is often difficult for the UK and international law enforcement agencies to prosecute them when they are located in jurisdictions with limited, or no, extradition arrangements.

These OCGs are principally responsible for developing and deploying the increasingly advanced malware that infects the computers and networks of UK citizens, our industry and government. The impact is dispersed throughout
the UK, but the cumulative effect is significant. These attacks are becoming increasingly aggressive and confrontational, as illustrated by the increasing use of ransomware, and threats of distributed denial of service (DDoS) for extortion.

Whilst OCGs may pose a significant threat to our collective prosperity and security, equally of concern is the continuing threat from acts of less sophisticated but widespread cyber crimes carried out against individuals or smaller organisations.

**States and state-sponsored threats**

We regularly see attempts by states and state-sponsored groups to penetrate UK networks for political, diplomatic, technological, commercial and strategic advantage, with a principal focus on the government, defence, finance, energy and telecommunications sectors.

The capacity and impact of these state cyber programmes varies. The most advanced nations continue to improve their capabilities at pace, integrating encryption and anonymisation services into their tools in order to remain covert. While they have the technical capability to deploy sophisticated attacks, they can often achieve their aims using basic tools and techniques against vulnerable targets because the defences of their victims are poor.

Only a handful of states have the technical capabilities to pose a serious threat to the UK’s overall security and prosperity. But many other states are developing sophisticated cyber programmes that could pose a threat to UK interests in the near future. Many states seeking to develop cyber espionage capability can purchase computer network exploitation tools ‘off the shelf’ and repurpose these to conduct espionage.

Beyond the espionage threat, a small number of hostile foreign threat actors have developed and deployed offensive cyber capabilities, including destructive ones. These capabilities threaten the security of the UK’s critical national infrastructure and industrial control systems. Some states may use these capabilities in contravention of international law in the belief that they can do so with relative impunity, encouraging others to follow suit. Whilst destructive attacks around the world remain rare, they are rising in number and impact.

**Terrorists**

Terrorist groups continue to aspire to conduct damaging cyber activity against the UK and its interests. The current technical capability of terrorists is judged to be low. Nonetheless the impact of even low-capability activity against the UK to date has been disproportionately high: simple defacements and doxing activity (where hacked personal details are ‘leaked’ online) enable terrorist groups and their supporters to attract media attention and intimidate their victims.

The current assessment is that physical, rather than cyber, terrorist attacks will remain the priority for terrorist groups for the immediate future. As an increasingly computer-literate generation engages in extremism, potentially exchanging enhanced technical skills, we envisage a greater volume of low-sophistication (defacement or DDoS) disruptive activity against the UK. The potential for a number of skilled extremist lone actors to emerge will also increase, as will the risk that a terrorist organisation will seek to enlist an established insider. Terrorists will likely
use any cyber capability to achieve the maximum effect possible. Thus, even a moderate increase in terrorist capability may constitute a significant threat to the UK and its interests.

**Hacktivists**

Hacktivist groups are decentralised and issue-orientated. They form and select their targets in response to perceived grievances, introducing a vigilante quality to many of their acts. While the majority of hacktivist cyber activity is disruptive in nature (website defacement or DDoS), more able hacktivists have been able to in inflict greater and lasting damage on their victims.

**INSIDERS**

Insider threats remain a cyber risk to organisations in the UK. Malicious insiders, who are trusted employees of an organisation and have access to critical systems and data, pose the greatest threat. They can cause financial and reputational damage through the theft of sensitive data and intellectual property. They can also pose a destructive cyber threat if they use their privileged knowledge, or access, to facilitate, or launch, an attack to disrupt or degrade critical services on the network of their organisations, or wipe data from the network.

Of equal concern are those insiders or employees who accidentally cause cyber harm through inadvertent clicking on a phishing email, plugging an infected USB into a computer, or ignoring security procedures and downloading unsafe content from the Internet. Whilst they have no intention of deliberately harming the organisation, their privileged access to systems and data mean their actions can cause just as much damage as a malicious insider. These individuals are often the victims of social engineering – they can unwittingly provide access to the networks of their organisation or carry out instructions in good faith that benefit the fraudster.

The overall cyber risk to an organisation from insider threats is not just about unauthorised access to information systems and their content. The physical security controls protecting those systems from inappropriate access, or removal of sensitive data or proprietary information on different forms of media, are equally important. Similarly, a robust personnel security culture that is alive to the threat posed by disaffected employees, fraud in the workforce and industrial and other forms of espionage is an important element in a comprehensive approach to security.

**CASE STUDY 1: TALKTALK COMPROMISE**  On 21 October 2015, UK telecommunications provider TalkTalk reported a successful cyber attack and a possible breach of customer data. Subsequent investigation determined that a database containing customer details had been accessed via public- facing internet servers, with the records of approximately 157,000 customers at risk, including names, addresses and bank account details. On the same day, several TalkTalk employees received an email with a ransom demand for payment in Bitcoins. The attackers detailed the structure of the database as apparent proof that it had been accessed. TalkTalk’s report of the breach helped the police, supported by specialists at the National Crime Agency, to arrest the main suspects, all based in the UK, in October and November 2015.

The attack demonstrates that, even within large cyber-aware organisations, vulnerabilities can persist. Their exploitation can have a disproportionate effect in terms of reputational damage and operational disruption, and this incident generated substantial media attention. TalkTalk’s rapid reporting of the breach enabled law enforcement to respond in a timely manner, and both the public and government to mitigate the potential loss of sensitive data. The incident cost TalkTalk an estimated £60m and the loss of 95,000 customers, as well as a sharp drop in their share price.

**CASE STUDY 2: ATTACK ON BANGLADESH BANK’S SWIFT SYSTEM** The Society for Worldwide Interbank Financial Telecommunication (SWIFT) provides a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure way. As SWIFT sends payment orders which must be settled by correspondent accounts that the institutions have with each other, there has long been concern over any potential for this process to be compromised by cyber criminals or other malicious actors, seeking to inject illegitimate payment orders into the system or, in a worst case scenario, seeking to disable or disrupt the functionality of the SWIFT network itself.

In early February 2016, an attacker accessed the SWIFT payment system of the Bangladesh Bank and instructed the New York Federal Reserve bank to transfer money from Bangladesh Bank’s account to accounts in the Philippines. The attempted fraud was US$951 million. 30 transactions, worth US$850 million, were prevented by the banking system; however, five transactions worth US$101 million went through. US$20 million, traced to Sri Lanka, has since been recovered. The remaining US$81 million transferred to the Philippines was laundered through casinos and some of the funds were then forwarded to Hong Kong.

The forensic investigation launched by Bangladesh Bank discovered that malware had been installed on the bank’s systems and had been used to gather intelligence on the procedures used by the bank for international payments and fund transfers. Further analysis by BAE Systems of the malware linked to the attack uncovered sophisticated functionality for interacting with the local SWIFT Alliance Access software running in the Bangladesh Bank infrastructure. BAE concluded ‘that criminals are conducting more and more sophisticated attacks against victim organisations, particularly in the area of network intrusions’.

**CASE STUDY 3: UKRAINE POWER GRID ATTACK** A cyber attack on western Ukrainian electricity distribution companies Prykarpattya Oblenergo and Kyiv Oblenergo on 23 December 2015 caused a major power outage, with disruption to over 50 substations on the distribution networks. The region reportedly experienced a blackout for several hours and many other customers and areas sustained lesser disruptions to their power supplies, affecting more than 220,000 consumers. Use of the BlackEnergy3 malware has been blamed by some for the attack, after samples were identified on the network.

At least six months before the attack, attackers had sent phishing emails to the offices of power utility companies in the Ukraine containing malicious Microsoft Office documents. However, the malware was not likely to have been responsible for opening the circuit breakers which resulted in the outage. It is probable that the malware enabled the attackers to gather credentials that allowed them to gain direct remote control of aspects of the network, which would subsequently enable them to trigger the outage. This Ukraine incident is the first confirmed instance of a disruptive cyber attack on an electricity network. Instances such as this further demonstrate the need for good cyber security practices across all of Critical National Infrastructure (CNI).