Security and Resilience Vulnerabilities in the UK's Telecoms Networks

A review of the risks posed to the regulated Telecoms Industry by non-deliberate threat, conducted by BAE Systems Detica on behalf of Ofcom

Matt Willsher, Dan Carr, Luke Stevenson and Phil Huggins

29 April 2013

Our reference: CYCA1289

91 pages including cover

Detica

BAE SYSTEMS

Version history

Version	Date	Author	Action
0.1	28 Mar 2013	MW	Draft Final Report
0.2	29 April 2013	MW	Final Report

Copyright statement

Document control

This section is optional and is used to describe any specific handling and deliverability requirements for the document and to whom the document has been distributed. This is usually only needed for a classified document.

Executive summary

Detica have been asked by the Office of Communications (Ofcom) to conduct a security and resilience assessment of the UK telecoms network to non-deliberate threat. This request is the result of an evolution in European Union's (EU) focus on regulation, ensuring providers are taking appropriate measures to manage the security and resilience of their networks. This legislation is applied in the UK via Section 105, parts A-D of the Communications Act 2003. Ofcom have a desire to better understand the security and resilience vulnerabilities that currently exist, or could be anticipated in the telecoms network.

Conducting our assessment required us to research and analyse a wide range of sources to establish two insights into the telecoms industry. These were:

1. To identify the key relevant existing, evolving and emerging trends within the telecoms industry; and
2. External factors which either currently impact or might impact on the industry in the future.

To identify the key existing, evolving or emerging trends we engaged with the internal subject matter expert (SME) community within Detica. We also conducted one-to-one interviews with key industry stakeholders as well as open source research. From our research we identified a total of 18 relevant key trends within the telecoms industry; of which nine were considered existing, four evolving and the remaining five emerging. From these trends we identified five that pose a relatively high degree of influence, and as such, should be monitored more closely by Ofcom moving forward. These covered:

1. The poor levels of knowledge and asset management within the industry that means key information is not effectively captured or efficiently shared within or between service providers. Resulting in a lack of understanding of the core infrastructure and its interdependencies – most notably at the network layer;
2. Limited network insight of providers, especially around the connections with, and reliance upon, additional networks and infrastructure outside of the direct boundaries of its own network. This largely leaves providers blind to the status of their network beyond functioning or not;
3. Vendor diversity and the efforts made by providers to introduce resilience into their networks by using different suppliers either by geography or component;
4. The industry trend to save costs by leveraging infrastructure. Encompassing a wide range of cost saving measures has consolidated network infrastructure, reducing diversity and subsequently resilience, thus increasing the impact of incidents; and
5. Outsourcing and offshoring delivery of support and other services deemed non-essential by providers in an effort to reduce the costs associated with service provision.

Next, we identified external factors that, whilst non-malicious in their intent, could have the consequence of currently or in the future exploiting security or resilience vulnerabilities in telecoms networks. For this we used the PESTLE framework covering: Political; Economic; Social; Technological; Legal; and Environmental factors to obtain a view of the entire environment in which service providers operate. From our research we were able to identify a wide range of external factors the telecoms industry faces covering issues such as: cable theft and its associated impact; user demands for service providers

to offer enhanced services at the same cost; increased reliance on the telecoms network for service delivery, invariably in the absence of alternative options; and rapid technological evolution and innovation that require the industry to adapt and change quickly.

These two sources of information were assessed and analysed to generate a list of 48 security and resilience vulnerabilities within the telecoms network. This list was further categorised into those vulnerabilities that exist currently, totalling 30, and those that are anticipated – accounting for the remaining 18. Each vulnerability was rated for: its potential impact to the network in the event that it is realised; and the likelihood of it being realised. The two scores were combined to give an overall vulnerability rating that permitted us to rank the vulnerabilities. A total of five vulnerabilities fell into the highest level of ranking, three of which were assessed as being current and two as anticipated. These are listed below - with the first three considered current:

1. The increasingly ageing infrastructure that the network is reliant on. This includes components that are no longer supported and deemed to be end-of-life.
2. A lack of complete understanding of internal network interconnections and dependencies that means not only are incidents more likely but when they do occur they will have a larger impact than if the level of understanding was higher.
3. An irregularity of disaster recovery function and process testing. While procedures might be in place, for example back-ups, these are generally not tested to ensure they function correctly. Similarly disaster recovery plans may exist but the lack of knowledge of the network means the plan only covers an element of the component functionality.
4. An increasing dependency on small specialist SME companies that perform critical functions but have no competition meaning in the event of their failure there is no alternative supplier available to service providers.
5. Less resilient vendor equipment. The drive down of core service provision costs is filtering through to equipment vendors who are correspondingly evolving to meeting core requirements at the lowest possible cost.

These five vulnerabilities also form the basis of five scenarios created. These also draw on a wide range of other, contributing trends, to highlight a set of five instances where vulnerabilities in the network might be realised and the corresponding incident that might be generated. These help ‘bring to life’ much of the earlier work in the report.

Finally, we put forward a number of recommendations which we propose could either help to mitigate the most impactive or most likely vulnerabilities being realised or more widely assist the telecoms industry to become more resilient. Of these the recommendations offering the greatest potential are:

1. That Ofcom consider developing their internal strategy on validating appropriate technical and organisational measures to manage risks to the network in line with breach reporting; and
2. The telecoms industry should be encouraged to improve their knowledge of the intra- and inter-dependencies that exist in the network.

In summary, the majority of vulnerabilities present within the telecoms networks are as a direct consequence of continually merging infrastructures and bolting on functionality. This is mitigated to an extent by the good community of sharing within the core telecoms providers, coupled with a genuine desire to manage and address resilience and security

issues that not only affect their own networks, but also the wider infrastructure. As the industry has to deal with technological evolution and innovation coupled with a less predictable set of consumer requirements the challenges are only set to continue.

List of contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose & Objectives

Detica have been asked by the Office of Communications (Ofcom) to undertake a study identifying security or resilience vulnerabilities in the UK Telecoms Network which could be exploited by non-deliberate threats. In meeting this requirement Ofcom set Detica five key objectives:

1. Summarise relevant key trends that currently exist or are emerging in modern telecoms networks, as well as their associated vulnerabilities;
2. Provide an assessment of whether these trends could introduce new vulnerabilities into the network or cause existing vulnerabilities to evolve;
3. Undertake an horizon scanning exercise to inform an assessment of the likely future trends and any additional vulnerabilities these may introduce to the telecoms networks;
4. Detail the level of awareness and recognition within the telecoms industry of the vulnerabilities identified, as well as assessing the maturity and effectiveness of their respective countermeasures; and
5. Provide an indication of both the likelihood and associated scale of impact in the event that an identified vulnerability be exploited.

The foundations of this study were built upon information obtained from the following sources:

- Detica's extensive network of telecoms Subject Matter Experts (SMEs);
- One-to-one interviews with key industry stakeholders covering: network operators, hardware and software vendors, and industry bodies involved in resilience; and
- Open source research, including from news articles, blogs, forums, and whitepapers, academic and other studies.

1.2 Context & Scope

Changes initiated by the EU are causing the framework governing communications regulation to evolve from a focus on market supply and competition to ensuring providers are taking appropriate measures to manage the security and resilience of their networks. This requirement is legislated in the UK through the addition of Section 105, parts A-D of the Communications Act 2003 requiring regulated companies to:

- Take appropriate technical and organisational measures to manage risks to the security of public electronic communications networks and public electronic communications services;
- Notify Ofcom of any security breach or reduction in the availability of the public electronic communications network which has a significant impact on the network; and
- Submit to an audit of the measures taken to manage the security risks conducted either by Ofcom or an Ofcom-nominated person.

This report is intended to inform Ofcom's understanding of the security and resilience vulnerabilities that could be exploited by non-deliberate threats (see Section 1.3). This includes those that are currently prevalent within the network, and those that may evolve

or be introduced over the coming decade due to emerging industry trends. It is important to note that this report does not cover those threats considered to be either malicious or deliberate, and is primarily focussed on the telecoms networks ability to provide an adequate level of service availability.

The scope of the report was initially defined in the Ofcom invitation to tender published on 6 December 2012 (Ofcom, 2012). It was later refined in a kick-off meeting held with Ofcom on 11 February 2013. Subsequently, the output from these events has limited the scope of this report to the regulated UK telecoms sector.

1.3 Key Terms & Definitions

A number of terms are heavily utilised through our report. To aid readers we have provided the key terms and their associated definitions in this section.

In recent years there have been numerous studies into the security and resilience of both networks and systems; however these have tended to focus on threats considered to be deliberate or malicious. As such, this has led to various interpretations of what constitutes a deliberate threat. For the purpose of this report, a deliberate or malicious threat is defined as:

> *Deliberate Threat –an action carried out by an individual, or group of individuals, that either directly or indirectly results in intentional harm, damages or losses to their target.*

For example, launching a Distributed Denial of Service (DDoS) attack against a Home Location Register (HLR) designed to drastically reduce service availability. However, as mentioned previously, this report is primarily focussed on non-deliberate or non-malicious threats, defined as:

> *Non-deliberate Threat – an action or event that either directly or indirectly results in unintentional harm, damages, or losses.*

For example, a high-profile news event – such as the London 7/7 bombings – resulting in a significant increase in network traffic with the potential to render certain network segments unusable. There are also circumstances where these definitions may be slightly blurred. Some threats considered deliberate can also have unforeseen consequences that are outside the original intentions of the perpetrator. For example, cable theft where the deliberate act of stealing copper can also result in an unforeseen loss of availability where critical fibre cables have been damaged to gain access to the copper.

Incidents occur when a threat is realised, in order to do so they must exploit vulnerabilities, defined as:

> *Vulnerability – an entity or process exposed to deliberate or non-deliberate threats, susceptible to compromise.*

This report is primarily concerned with the resilience of the UK Telecoms Networks, defined as:

> *Resilience – the property of a system or entity that enables it to resume its original state in the event an incident occurs.*

By joining together the concepts of both resilience and vulnerability, resilience vulnerabilities can be defined as:

> *Resilience Vulnerability – an entity or process exposed to deliberate or non-deliberate threats that, if realised, will affect the system's ability to resume its original state in the event an incident occurs.*

In addition, security vulnerabilities are defined as:

> *Security Vulnerability – an entity or process exposed to deliberate or non-deliberate threats that, if realised, will result in a loss of a system's information assurance.*

1.4 Approach

Our approach to meeting Ofcom's requirements can be broken into five phases. These are outlined in further detail below. Our high-level methodology illustrating how the five phases link and their respective constituent components is also shown in Figure 1, below. It is important to note that the activities are neither mutually exclusive nor dependant; certain activities trailed and led into other stages.

Phase 1: Discover & Build Initial Model

The initial phase was based around a focussed workshop involving the project team and Detica's internal SMEs. The key objectives of the workshop were to identify the following:

- key industry stakeholders;
- high-level industry strategy and objectives;
- initial trends and areas of potential vulnerability;
- potential factors that could impact upon the above, utilising the PESTLE (Political, Economic, Social, Technological, Legal and Environmental) analysis tool; and
- any knowledge gaps requiring industry clarification or confirmation.

Phase 2: Enrich Data & Interview Experts

In phase two we utilised the output of phase one to construct a set of targeted questions aimed at key industry stakeholders and SMEs. We primarily used face-to-face interviews and when this was not possible questionnaires and teleconferencing was used.

The questions were designed to achieve the following:

- confirm or refute external factors identified in the PESTLE analysis;
- confirm or refute industry trends and vulnerabilities identified; and
- identify any additional trends and vulnerabilities yet to be recognised.

In addition to the industry engagement outlined above, this phase also included the cultivation of open-source research to support our findings. This was primarily focussing on the following areas:

- publically reported telecoms industry incidents;
- publically reported incidents in other industries;
- telecoms industry statistics;
- historical trends; and
- emerging and future trends.

Based on the initial findings generated during this phase we were able to generate a draft table of contents comprising the major headings our report would include. In accordance with listed deliverables required in this project we shared this with Ofcom by email on 22 February 2013 and talked through the draft table of contents in a meeting on 27 February 2013.

Phase 3: Risk Assessment

Following the collection of data from within the internal Detica SME community, wider telecoms industry and open sources phase three entailed collating the data set into an authoritative list of relevant key industry trends and external factors. These key trends and external factors were then analysed to generate a list of industry security and resilience vulnerabilities. They also formed the basis of our interim presentation to Ofcom, delivered on 14 March 2013 providing the opportunity for Ofcom to validate our research conducted to this point.

With validation of the key trends and external factors we then assessed their impact on the vulnerabilities identified and whether they may alter their susceptibility to compromise. Finally, each vulnerability was then critically assessed to provide an indication of how likely a potential compromise may be and the extent of the damage should an incident occur. Our methodology for calculating potential impact and likelihood is outlined in Section 1.6, below.

Phase 4: Refine & Populate Final Model

During this phase the project team re-engaged with appropriate SMEs across Detica to validate the trends and vulnerabilities previously identified. In addition, the team carried out a general sensitivity analysis to attribute a level of confidence in the findings and the potential impact of any bias.

Five of the key vulnerabilities were extrapolated into more developed risk scenarios, providing a narrative approach describing their causes and impacts. A series of foresight predictions were also generated for each of the key trends to give an indication of how these might develop.

Finally, a number of key recommendations were formed to give Ofcom some potential high-level solutions that could reduce either the likelihood or impact of the most critical vulnerabilities.

Phase 5: Report

In the final phase of this project we brought together all the component parts of our research and assessment into a final report. A description of the structure of our report is provided in Section 1.6, below.

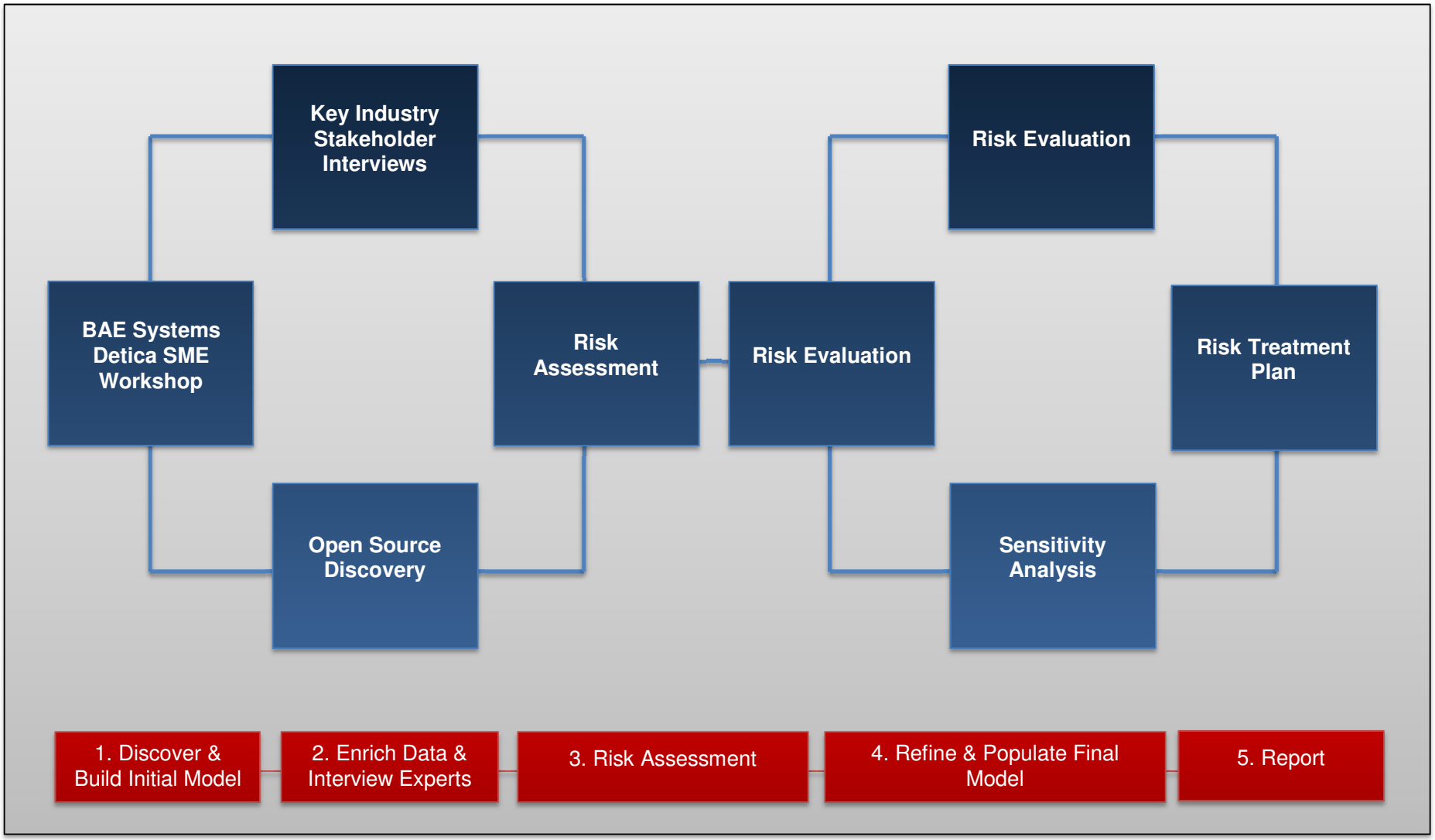

Figure 1 – Methodology Overview

1.5 Document Structure

The report is set out in such a way as to lead the reader logically through our research and assessments to show how we identified the security and resilience vulnerabilities that we did.

In section 2 we detail the information obtained from our internal SME community, interviews conducted with industry and open source research and the associated relevant key industry trends we identified from this. The section is split into three sub-sections based on whether the key trend currently exists, exists but is evolving or can be considered an emerging trend. Each trend is entered into the following template to capture the complete range of relevant associated information.

ID #:	**Title:**	
Coverage:	**Categories:**	**Recommended Focus:**
Description:		
Future State:		

Table 1 – High-level Trend Structure

A full description of the table structure is provided in Section 2.2, below.

Section 3 captures the results of our PESTLE analysis and the resulting external factors that we identified as posing a potential non-deliberate threat to the telecoms network. It includes external factors that may impact upon the telecoms industry's ability to deliver services; exacerbate the exposure of existing vulnerabilities; cause additional vulnerabilities to exist; or result in resilience/security incidents occurring.

The various factors are broken into the following sub-headings: Political, Environmental, Social, Technical, Legal, and Economical. Although certain factors are placed within a given heading, it is feasible that they could equally sit within one of the other high-level areas. Where factors sit is not of paramount importance, PESTLE is designed to aid analysis and the identification of factors as opposed to a strict process of categorisation. Each external factor has a potential impact to the telecoms network and likelihood or occurrence score assigned. Descriptions of the levels of each are detailed in Section 1.6, below.

The results of our analysis of the key trends and external factors are borne out in Section 4 which details the security and resilience vulnerabilities we have identified. Each trend is detailed in isolation explaining how the existence of one or more of the key trends present in the telecoms industry has either resulted in or could cause vulnerabilities in the network infrastructure. We provide traceability back to the vulnerability's contributory trends from Section 1. In addition, any external factors that may either result in realisation of the vulnerability, or exacerbate its impact or likelihood – as described previously in the PESTLE analysis – are covered.

We have also assigned impact and likelihood ratings to each vulnerability which we combine to give an overall vulnerability rating. A full description of the methodology behind the ratings is given in Section 1.6, below.

Section 5 extrapolates a number of key vulnerabilities listed in Section 4 to generate five distinct risk scenarios. Each scenario is described, outlining the vulnerabilities exploited,

how this was achieved, and what the impact could be in real terms. The scenarios are designed to demonstrate worst-case events, whilst maintaining realism and plausibility.

In Section 6 we list our recommendations, at a high level, of how industry and/or Ofcom may address the most critical vulnerabilities identified in Section 4. The recommendations are particularly focussed on areas where we believe either: Ofcom or industry stakeholders could achieve quick-wins in terms of reducing vulnerability exposure, without great expense; or how mitigation of vulnerabilities identified as high-risk, i.e. those that would result in widespread loss of service and/or resilience, can be achieved.

Finally, in Section 7 we present our conclusion, drawing together the main findings of the report as well as any subsequent recommendations into a final summary, drawing the report naturally to a close.

1.6 Calculating Impact & Likelihood

One of the key objectives of this report is to give Ofcom an indication of both the likelihood and associated scale of impact in the event that an identified vulnerability is exploited. In the absence of a pre-existing tool or template for calculating impact and likelihood within Ofcom we were free to use our own. We regularly conduct risk assessments on behalf of our clients as have a well-established framework for calculating both impact and likelihood.

For Ofcom we adapted this framework to enable us to calculate impact and likelihood at a generic industry scale rather than against specific technical or business components. We describe each level in the framework in the three tables below.

Impact Severity	Description
Insignificant	There is a minimal service disruption that a limited number of customers may experience or that may occur for a short period of time. It is unlikely the incident will be reported and investigating and remediating the fault is relatively quick and simple with no impact to service provision.
Minor	Exploit of the vulnerability has a limited impact on some customers, for a limited period of time or a combination of both. The incident results in minor financial and reputational damage to the service provider and goes largely unreported except on customer or specialist blogs, forums and chat rooms. Investigating and remediating the vulnerability is relatively simple and can be fixed with minimal outlay or disruption to the service.
Moderate	Realisation of the vulnerability will have an impact on service delivery to a significant but constrained (either by geography or service) number of users or for a noticeable duration. The impact will cause a large financial and reputational loss to the service provider and be reported in specialist and trade press. Remediation is relatively quick to implement but causes some disruption to normal service provision.
Major	Vulnerability exploit causes significant loss of service either by number of customers affected, length of service outage or a combination of the both. The impact will cause major financial and reputational loss to the service provider entailing coverage in the national press. Investigating and remediating the vulnerability requires large levels of resource and may cause disruption to service provision.
Catastrophic	Exploit of vulnerability results in catastrophic loss of service to customers by both number of customers affected and duration. The impact will cause large financial and reputational loss to the service provider entailing widespread coverage in national and international press. Investigating and remediating the vulnerability requires the application of significant levels of resource for considerable time and causes major disruption to service provision.

Table 2 – Impact of Occurrence

Likelihood	Description
Extremely Unlikely	May occur only in exceptional circumstances. There are no known instances or anecdotes from across the industry of any incident occurring. Anticipated to occur once in more than 100 years.
Unlikely	Not expected to occur with very few instances or anecdotes of incidents industry-wide. Little opportunity, reason or means for incident to occur. May occur once in 100 years.
Possible	May occur at some time with irregular examples and anecdotes of incidents raised within the industry. Some opportunity, reason or means for incident to occur. May occur once in 20 years.
Likely	Considered likely to occur with regular recorded incidents in the industry and strong anecdotal evidence. Significant opportunity, reason or means for incident to occur. May occur once in 7 years.
Very Likely	Expectation that an incident will occur in the next year across the industry.

Table 3 – Likelihood Description

By cross-referencing the impact and likelihood ratings we are able to establish an overall vulnerability rating. As illustrated by the coloured grids in the matrix below, the ratings fall into one of five categories: critical; high; medium; low; and negligible.

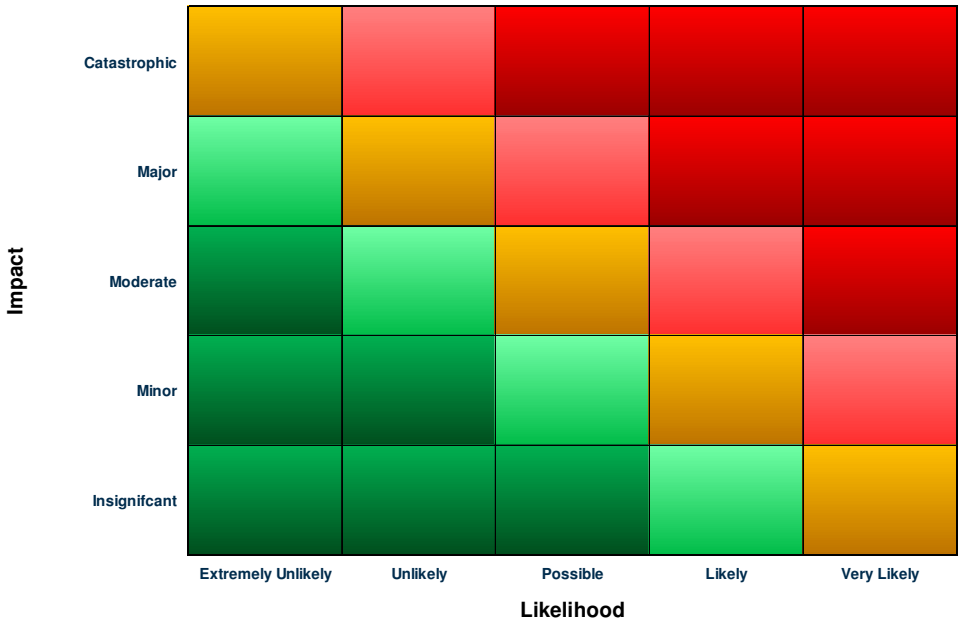

Figure 2 – Example Vulnerability Matrix

1.7 Assumptions & Dependencies

This study was designed to meet a specific requirement from Ofcom (see Section 1.1), and therefore has a number of important limitations to its scope. In addition, there were a number of dependencies required by to be able to successfully meet Ofcom's requirement. These are listed below.

The following assumptions were made in relation to this project:

1. That the telecoms network constitutes both the fixed-line and radio network infrastructure. Satellites and other telecommunications technology was considered to be less of a concern;
2. No distinction is made within the sector between elements comprising the Critical National Infrastructure (CNI) and those considered outside. In instances where we have been made aware of trends or vulnerabilities that cross over into non-regulated portions of the telecoms sector these have been detailed within the report;
3. Application service providers, for example Skype and LoveFilm, constitute a significant and growing part of the telecoms industry and potentially fall within the regulatory scope of Ofcom. However, they were not of primary concern to our research;
4. That all stakeholders engaged in the production of this report operated with integrity, providing honest and accurate information. We have not sought to test or verify any of the statements recorded in the interviews we have taken;
5. Due to the relatively short timescale in which this piece of work was conducted the findings should not be considered exhaustive or complete;
6. This report will be used to help inform Ofcom's knowledge of trends within the telecoms industry and any potential existing or emerging vulnerabilities; and
7. This project will not inform part of any audit process or program for Ofcom.

In addition, this assessment took place under the following dependencies:

1. The Project Authority will appoint a suitably empowered individual to help Detica arrange and prioritise interviews with service providers and equipment vendors;
2. At the end of week two of the project Detica and the Project Authority will review progress in meeting industry stakeholders. In the event that the target number of face-to-face meetings is not met a decision will be taken whether to use questionnaires to elicit industry response;
3. In the event questionnaires are used the project authority will draft a cover letter to accompany these;
4. The Project Authority is required to confirm the risk model to be used to calculate likelihood and scape of impact within two weeks of the commencement date;
5. The accuracy of the results portrayed within this paper is heavily reliant upon the accuracy and completeness of the information provided from key industry stakeholders.

2 Key Trends

This section of the report describes the relevant key trends that exist, are evolving or emerging in the telecoms industry. It also details the extent to which they are prevalent across the industry and gives an indicative recommendation of how much focus Ofcom should give to each trend going forward.

2.1 Approach

The key trends identified within this study were originally captured during the discovery phase, i.e. via one-to-one stakeholder interviews, SME workshops, open source research, and team workshops (see Section 1.4). In order to provide structure and facilitate the information gathering exercise, we targeted questions and analysis on general trends followed by a pseudo-procurement lifecycle to ensure complete coverage across the lifespan of a telecommunications network and/or service. The lifecycle is illustrated in the seven-stage diagram below.

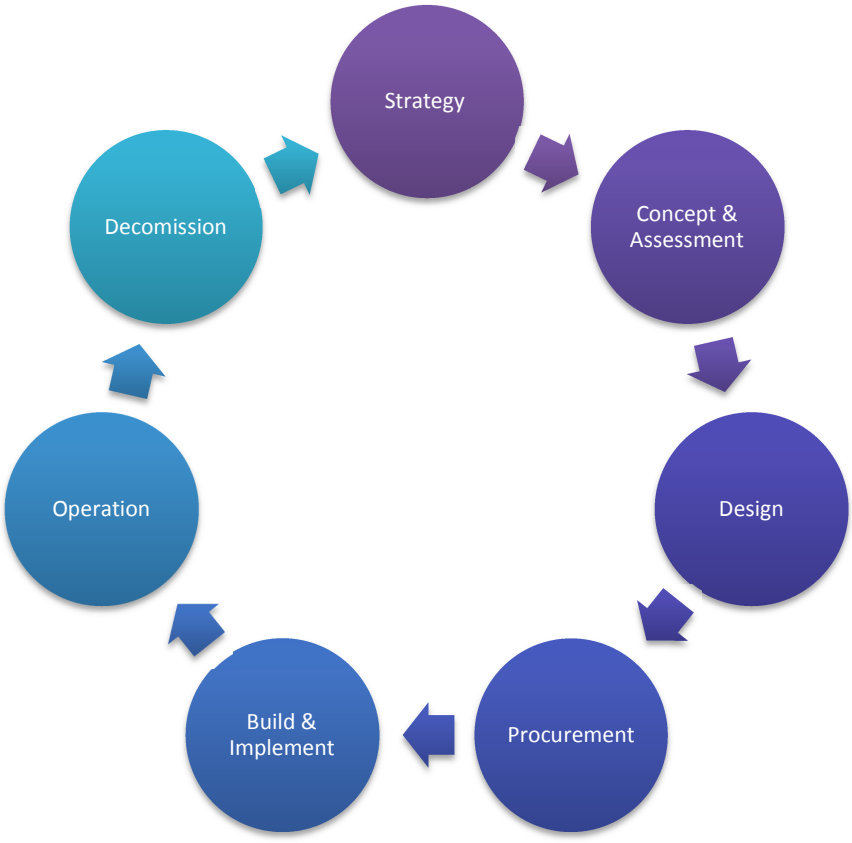

Figure 3 – Trend Lifecycle

Our description for each lifecycle stage is as follows:

1. Strategy: The key aims and objectives for the telecoms industry and how organisations are taking steps towards realising them;
2. Design: The process of designing networks to deliver their strategic objectives;
3. Procurement: How telecoms organisations are procuring hardware and software in support of their service offerings;

4. Build & implement: The process of turning designs and procured equipment into physical usable infrastructure;
5. Operation: How telecoms networks are ran, operated, and maintained day-to-day, encompassing everything go live to shut down;
6. Decommission: How networks and/or equipment is removed from the infrastructure when it reaches the end of its usable life; and
7. General/Other: A catch-all category that covers aspects where a trend exists but it doesn't logically or neatly sit directly in any of the categories outlined above.

After identifying all of the existing, evolving or emerging trends in the telecoms industry we consolidated and refined them into the definitive list contained in this report. This process of amalgamation was designed to group similar and adjacent trends with a view to keeping them at a high enough level to ensure they remain digestible to the reader.

Each trend was aligned with one or more of the lifecycle stages to give the reader an indication of where it may exist chronologically.

2.2 Trend Structure

The trends outlined in the remainder of this section follow the table structure described in Figure 4 – Trend Table Structure, below.

ID: 1	**Title:** Lean Service Provision	
Coverage: Industry-wide	**Categories:** Design, Procurement, Build & Implementation, and Operation.	**Recommended Focus:** Medium
Description:		
The telecoms industry is mature with market saturation and achieving differentiation of relatively commoditised services is proving challenging. Consequently, this has led to telecoms organisations seeking to increase their profit margins by further identifying and exploiting areas in which they can reduce cost. Transparent pricing schedules and thin margins – primarily of core network connections in both the fixed-line and mobile sectors – have resulted in a desire to increase the Average Revenue Per User (ARPU). There is a general perception that operators will only perform functions that they are obliged to by law; a defensive measure in order to prevent against spending money on functionality that is not deemed essential. This has an impact from a service availability perspective in terms of a bottle neck in the event that additional data capture and provision is required. Most recently, this has been achieved through the outsourcing and offshoring of key core business processes and services, even in areas such as back-end infrastructure support. This can cause significant resilience issues if not handled correctly – as highlighted during the recent 2E2 events. In addition, although the mobile sector is modernising their infrastructure, the potential to turn off legacy 2G networks sooner rather than later – in favour of cost savings – is a seemingly attractive proposition. The balance between cost reduction and maintainability/resilience is becoming increasingly unclear; how much resilience will be sacrificed in the race for cost savings has yet to be determined. Therefore, it is important to note that the cheapest supplier is not necessarily the best. This trend also had wider implications for the industry as a whole, specifically in terms of the quality of vendor equipment and of the underlying general infrastructure.		
Future State:		
In the absence of any great step-change in either the telecom operator/provider's business model or approach, this trend is likely to both continue and progressively increase over the coming years. The threat of the growth of IP services and the snowballing of user bandwidth demands will continue to put significant pressure of service and operational costs, culminating in a less resilient infrastructure than the one currently in place.		

Figure 4 – Trend Table Structure

Each table section is intended to describe the following:

- **ID –** A unique reference number for each trend, providing traceability within subsequent report sections.
- **Title –** A short and unique trend title.
- **Coverage –** Which areas of the industry this particular trend relates to, e.g. industry-wide, primarily mobile, primarily fixed-line, etc.
- **Categories –** Which categories outlined in Section 2.1 above the trend relates to.
- **Recommended Focus –** An indication of how much effort Detica recommends Ofcom expend on monitoring the future development of the trend.
- **Description –** An in-depth description of the trend and what it encompasses, including any corresponding evidence or examples highlighted during this study.
- **Future State –** Detica's perception of how this this trend is likely to develop over the coming years.

2.3 Existing Trends

ID: 1	**Title:** Lean Service Provision	
Coverage: Industry-wide	**Categories:** Design, Procurement, Build & Implementation, and Operation.	**Recommended Focus:** Medium
Description:		
The telecoms industry in the UK is mature and has achieved market saturation. Service providers face the challenge of transparent pricing schedules, thin margins and rising expectations from consumers. Against this backdrop providers are keen to increase their profit margins by reducing costs associated with service provision on the one have and increase the Average Revenue Per User (ARPU) on the other. The trend in cost reduction to-date has been led through outsourcing and offshoring of support services which has the potential to introduce significant resilience issues if not handled correctly, as highlighted by the recent 2E2 failure. This trend of focussing on core provision has extended to create a defensive posture within the industry to only perform functions that they are obliged to by law; a defensive measure in order to prevent spending money on functionality not deemed essential. There is the potential this trend will have an impact on service availability by creating a bottle neck in the event that additional data capture and provision is required. It remains to be seen how this trend to offer services in as lean a manner as possible will affect resilience or the extent to which resilience will be sacrificed in the drive for savings. This trend also had wider implications for the industry in terms of the quality of vendor equipment and of the underlying general infrastructure.		
Future State:		
In the absence of any great step-change in either the telecom operator/provider's business model or approach, this trend is likely to both continue and progressively increase over the coming years. The threat of the growth of IP services and the snowballing of user bandwidth demands will continue to put significant pressure of service and operational costs, potentially culminating in a less resilient infrastructure than the one currently in place.		

Table 4 – Trend: Lean Service Provision

ID: 2	Title: Poor Knowledge & Asset Management	
Coverage: Industry-wide	**Categories:** Design, Operation and Decommissioning	**Recommended Focus:** High

Description:

There is a clear trend across the industry of poor knowledge and asset management in relation to the network infrastructure. One of the most critical areas of this lack of knowledge is in the lack of understanding of the core infrastructure and its interdependencies, most notably at the network layer. This is a function of historic mergers and acquisitions within the industry accompanied by the subsequent integration and rationalisation. The situation is further compounded by the sheer scale and complexity of the network as it exists currently, one that is only set to increase.

As networks have grown and evolved a lack of effective knowledge management and failure to retain staff knowledge on their departure has created a situation where operators have little understanding of the full extent of the assets they possess, their function or their location. The result of this trend is that in the event of an incident there are often significant delays in determining the root cause, with examples of six hours just to determine the problem before remediation can start. This lack of awareness and understanding feeds into a reluctance to decommission network components for fear of causing unintended service outages.

The trend manifests itself in a wide range of practical applications as well. A lack of up to date network diagrams and reliance on paper copies of technical architecture leads to engineering teams digging in the wrong area, potentially damaging network infrastructure. The importance of this issue is highlighted by the fact operator's deal with an average of five hundred changes a month. Similarly not knowing the number of available ports on any given switch introduces issues for provisioning new customers onto the network. Once lost it is resource intensive to re-learn this level of detail about the network.

Operators and providers can also find themselves being the last to find out about incidents occurring; especially those who are reselling their infrastructure to multiple MVNOs and MVNEs whose customers tend to inform them first. Ironically, the industry itself has never had as much access to timely and accurate logging information, but the sheer volume of logging/audit data the network generates means it is exceptionally hard to process.

Future State:

Although there are threats to significant skills loss, i.e. due to externalising of key skills/knowledge outside of the direct organisation, this could also be the catalyst to change. Outsourcing aspects requires more streamlined and definitive processes to be in place in order to allow the third party to deliver their service, therefore there can be an expectation that the processes will have to mature and improve in order to make this model effective. In addition, the modernisation of the networks currently underway provides a relatively clean slate by which to start building a new infrastructure that is both mapped and recorded.

Table 5 – Trend: Poor Knowledge & Asset Management

ID: 3	Title: Operating Legacy Estates	
Coverage: Industry-wide	**Categories:** Operation	**Recommended Focus:** Medium

Description:

Telecoms networks are commonly comprised of multiple networks of varying age, design, and technology. This has typically been the result of historic mergers – and the subsequent integration and rationalisation of infrastructures – as well as the introduction of new capability aimed at delivering new-age services and built on top of existing solutions. The process of mergers has tended be on a cost-effective basis, so although the networks may have been perfectly resilient in isolation, once joined up the primary focus was ensuring they could function in tandem at reasonable cost, as opposed to maintaining an equal degree of resiliency. Ultimately, any new system introduced will likely interoperate with infrastructure that has been in place for tens of years, particularly within the backbone of the fixed-line networks. A particular example in the mobile space relates to a data centre in Ireland that is responsible for supporting the billing systems of northern Europe. Despite being years old, there is a reluctance to replace the kit for fear of breaking the process it underpins.

This legacy infrastructure is comprised of network components that are often unsupported, making obtaining replacement parts a significant challenge. Coupled with the fact the industry no longer stockpiles significant volumes of components and has limited levels of network insight, this can often lead to systems being continued past their expected service life due to the fear of what may happen should attempts be made to upgrade or replace them.

Future State:

Recent network modernisation will begin to slowly decrease the impact of this trend. However, the sheer scale of the networks and infrastructure in place makes it impossible to do a complete refresh at any given period. As such, there will always be certain parts of the infrastructure that are older, likely unsupported, and less resilient.

Table 6 – Trend: Operating Legacy Estates

ID: 4	Title: Lack of Third Party Insight	
Coverage: Industry-wide	**Categories:** Operation	**Recommended Focus:** Medium

Description:

In spite of the reliance of many telecoms service providers on third parties to deliver elements of their network services, they lack any real insight into the specific operational approach to security and resilience of these third parties. Although covered by Service Level Agreements (SLAs) these tend to only specify operational requirements and associated financial penalties for non-compliance. Furthermore, the industry generally lacks business continuity plans to mitigate the failure of one or more of their third parties, as demonstrated by the recent passing of 2E2 into administration. In this example the trend was perfectly demonstrated – service operators lacked the ability to operate independently of 2E2 forcing them to continue funding operations until such time as they could find alternatives.

This trend is exacerbated by the lack of diversity in infrastructure ownership; with the exception of 3 there are only two groups operating infrastructure (EE – consisting of Orange and T-Mobile's – and O2/Vodafone). As we have already seen in trend 2 this can mean they can be the last to know of issues. It also means there are a growing number of niche companies vital to the process of connecting calls (e.g. Truephone) but due to their size, they are operating under tighter budgetary constraints which often imply a reduced level of redundancy.

On the whole the telecoms industry tends to follow standards-based implementations and architectures to commonly agreed technology; there may be minor nuances in terms of interpretation but nothing that would likely drastically threaten resilience. Relatively mature resilience Key Performance Indicators (KPIs) are also embedded within requirements addressed during the design phase. These tend to be typically cost-benefit based, for example any component with more than five thousand users behind it will likely have dual resilience as a minimum. In addition, the minimum baselines in place around interoperability between networks are growing – such as ND1643 – but the extent in which they are being fully implemented and tested remains unclear.

Future State:

We anticipate the level of third-party insight increasing in future, largely due to the relatively forthcoming industry forums and the widespread impact of the recent 2E2 incident. It remains to be seen if this will act as the catalyst needed for operators to ensure the third-parties they contract build in resiliency, both in the network and as a business. Countering this, the proliferation of MVNOs and MVNEs is likely to increase further over the coming years, as will the number of dynamic and small organisations that provide very specialist and bespoke parts of the telecoms ecosystem. These niche providers will still be operating under tight budgetary constraints which are likely to cause an overall increase in number and diversity of weak spots in the underlying infrastructure.

Table 7 – Trend: Lack of Third Party Insight

ID: 5	Title: Poor Decommissioning	
Coverage: Industry-wide	**Categories:** Operation, Decommissioning	**Recommended Focus:** Medium

Description:

A function of operating legacy estates, coupled with poor asset management means the industry is unable to decommission infrastructure effectively as they do not understand the effect of removing constituent parts of the system. Industry perceives the risk to be lower to maintain an aging network than to identify and decommission parts deemed redundant or past their service life. Supporting this trend are numerous examples of components of network infrastructure being left through a lack of understanding as to the true nature or full extent of the services it provided.

The trend of poor decommissioning is supported by a tradition within the industry of storing any spare component parts within exchanges, engineering vans and other infrastructure nodes. In the event of component failure engineers would be able to perform like-for-like swaps, even in the event the component was no longer supported by the manufacturer.

When live traffic is transiting the device it can be easier to identify the impact of its removal. However, when it remains dormant industry tends to hesitate as it could be a critical component of a process not operating at the time of observation.

Future State:

As legacy infrastructure is progressively modernised and replaced, as current initiatives would suggest, this should slowly reduce the impact of this trend. However, this will take time and a shift in culture internally to want to fully understand, capture and grasp the new infrastructure being implemented. The replacement of existing kit in the interim period will continue to be challenging, especially where spare parts are now difficult to obtain or where there is a lack of knowledge of their function on the network.

Table 8 – Trend: Poor Decommissioning

ID: 6	Title: Limited Network Insight	
Coverage: Industry-wide	**Categories:** Operation	**Recommended Focus:** High

Description:

This trend is closely linked with limited third-party insight and poor knowledge management and sharing. Although a given owner of a network segment may have exceptional knowledge of its internal links and dependencies, it is highly unlikely that they understand the complex nature of its reliance on additional networks and infrastructure outside of its direct boundaries. The result of not understanding how varying network elements connect, interact and ultimately deliver services means operators are largely blind to the status of their network beyond functioning or not. In the event the network is not functioning, this significantly impacts the length of time taken to identify root causes of incidents, irrespective of relatively consistent and commoditised operational metrics. There are also examples of incidents causing a 'domino' effect due to the criticality of operations of neighbouring networks which also subsequently fail. A recent theft from a MTX exchange resulted in a national incident, as opposed to the small geographical area expected. The lack of knowledge of how equipment and network interconnect can result in what is perceived to be a relatively non-critical piece of equipment having a huge impact, especially when fibre connections need to be rebuilt.

Although networks may have significant levels of resilience built in – specifically in the core of the fixed-line infrastructure – understanding when this resilience has come into effect is lacking. Examples exist of networks falling back onto secondary lines but notification of this is lost in the volume of other automated alerts generated by the network. The failure to restore the primary line can result in exceeding capacity on the secondary line - which in theory could also be the primary line for other services - and in the event the secondary line also fails, the network impact is significantly higher. Most operators would struggle to say at any given time how many redundant links are being used, and where they are located. These tend to be resold between operators often being oversubscribed.

Future State:

As networks are upgraded and monitoring and logging solutions mature, the visibility of the network's state should become clearer. However, these benefits could also be counterbalanced by the growth and increased diversity of services and data transiting the network. The expected uplift of user demands could introduce ever increasing levels of system complexity, offsetting the benefits of centralisation. It is also important to note that although there may be fewer systems to be concerned with, centralisation ensures that should they be unavailable the impact of their loss will be significantly higher than a more diverse infrastructure. This will be particularly prevalent in the mobile space with the continued reliance on the Home Location Register (HLR).

Table 9 – Trend: Limited Network Insight

ID: 7	Title: Network Geo-location & Focus	
Coverage: Industry-wide/Mobile	**Categories:** Design, Build & Implementation, and Operation	**Recommended Focus:** Low

Description:

Currently the telecoms industry faces a trend of competing pressures users on the one hand wanting ever quicker services and government on the other pushing for greater and more even coverage. Historically, networks have focussed on delivering higher speed to urban areas. This trend is being challenged by the UK government's desire to see extension of the telecoms network to remote rural areas to help drive and support economic development. This trend has the potential to distract the industry from its core strategy in the event it has to re-focus in line with government requirements.

In the mobile sector developing infrastructure in the city has proved challenging, due to effects such as propagation loss. To counteract this mobile providers commonly choose building roofs for enhanced coverage. This trend has been impacted for the last five years by the number of retailers passing into administration since the start of the credit crunch in 2008. This has the adverse effect that network operators struggle to gain access to the equipment housed on the roofs of premises now vacant.

The final trend for geo-location by the telecoms industry is the apparent clustering of service operations. For example, the South East hosts primary and backup data centres meaning a geographically constrained event has the potential to result in nationwide impact for customers.

Future State:

Although the pressure to increase coverage will continue, it is expected the primary focus will remain on increased speed as the telecoms industry has the potential to make greater returns on investment from this. While wider coverage would be to the benefit of society as a whole, expending large sums of capital to reach a small subset of the population is not the most financially viable proposition for the industry.

The rise of equipment access issues will likely increase in the short-term as more premises close, but with the introduction of more flexible and ad-hoc infrastructure technology, such as femto cells, will likely cause a reduction in its impact.

Table 10 – Trend: Network Geo-location & Focus

ID: 8	**Title:** Vendor Diversity in Network Implementations	
Coverage: Primarily Fixed-line	**Categories:** Design, Build & Implementation, Operation	**Recommended Focus:** High

Description:

Modern telecoms networks are extremely complex, comprising many different makes and models of both hardware and software. This complexity is further compounded by a general trend of reliance on other providers' networks in order to connect with subscribers, introducing significant intra- and inter-operability issues due to variances in standards.

This level of diversity does introduce a degree of resilience but this has arguably come about by chance rather than a considered approach. For example, one operator may choose to use a specific vendor for a specific functional component of their network such as all edge routers are CISCO-manufactured and all switches from Alcatel. This implies a relative amount of diversity between distinct layers of the stack. However, others may choose to purchase all equipment from a given vendor for a given geographical region, driven by cost centres and the prospect of economies of scale. Resilience and vendor diversity is considered during the process of selecting a vendor, but as the drive for cost reduction increases this will likely become less critical with respect to potential savings achieved via bulk ordering.

In the mobile network infrastructure this trend is less obvious and correspondingly less of a direct concern as diversity is more evenly distributed. However, both sectors have a minimal level of understanding in terms of the low-level implementation of the equipment. This closed-source practice leads to a large level of dependency on vendors, especially for support.

Future State:

The diversity of vendor choice and component selection is likely to reduce further over the coming years. At present, it is rumoured some of the high-profile vendors are struggling financially, as a consequence this could cause mergers/acquisitions to occur, or disappear. A reduction in vendor choice would further limit an operator's ability to spread resilience risk throughout their infrastructure. Their approach taken historically is likely to remain, i.e. choosing vendors for specific network functions and/or geographical regions. However, as the drive for cost savings continues to increase the scope and size of single-vendor agreements is likely to continue to grow. This should be watched carefully, especially for components deemed critical for the operation of the core underlying infrastructure.

Table 11 – Trend: Vendor Diversity in Network Implementations

ID: 9	Title: Pre-production limitations	
Coverage: Industry-wide	**Categories:** Operation	**Recommended Focus:** Medium

Description:

There has been a long-standing trend for the telecoms industry to develop as comprehensive test environment as possible. However, for economic reasons it will never be viable to replicate the live production environment. As such there will always be an element of doubt and uncertainty as to the impact of implementing a new component into the network. The trend has largely removed implementation error, which tends to be the consequence of human mistakes. Rather, it will most likely be the operational element of the component that fails.

In support of testing there is a clear trend across the industry for associated policies and procedures to be in place around implementation and operation. However, with the trend of outsourcing means it is invariably third parties expected to abide by these policies and procedures. In many cases they are either unaware of the existence or content of the policies and procedures or choose to ignore them.

This results in a lack of understanding as to the implications of either removing or introducing components into the infrastructure that is not carried out with the desired level of assurance. This can lead to additional resilience incidents in times of change.

The general approach to testing processes, e.g. Disaster Recovery (DR) and Business Continuity (BC) is less than is probably necessary. As a whole, the industry may test backup procedures (as an example) but the regularity in which they do so, and the degree of confidence that they will work when required is generally low.

Future State:

It is anticipated that test environments will develop over the coming years, increasingly moving towards mirror images of the core infrastructure. However, it has been suggested that when this time comes, operators may then seek for the test environment to become the backup network and/or additional contingency network capacity. This should be watched carefully to ensure that an adequate degree of resilience is still available.

Table 12 – Trend: Pre-production Limitations

2.4 Evolving Trends

ID: 10	**Title:** Network Upgrade	
Coverage: Primarily Mobile	**Categories:** Design, Build & Implementation, and Operation	**Recommended Focus:** Medium
Description:		
In an effort to reduce the cost of maintaining networks, service providers are increasingly centralising their operations as part of the network upgrade process. This trend has in part been encouraged by Ofcom in order to aid competition by the centralisation of the URN (Unique Reference Number) database. In the wider context of centralisation the industry is seeking to implement the concept of unified entity, i.e. a single version of the truth where possible. Operators that offer services in both the fixed-line and mobile space have centralised their customer databases. Consequently, any impact to the database will impact upon all the services they provide, as opposed to just the one when these systems used to be operated in isolation. As a result of decreasing margins on core service provision providers are keen to both better understand the profile of their customers in order to tailor the selling of additional and more profitable services whilst also increasing their loyalty. This trend also offers some protection against proposed legislation around the 'right to forget'. While there is a desire to upgrade the network this is tempered by a culture within the industry of general reluctance and hesitancy to deploy new components into the existing network. This is reinforced by their lack of knowledge of what the introduction may do the networks ability to remain operational.		
Future State:		
The trend for centralisation of infrastructure and services is expected to continue over the coming years, coupled with an increased level of co-operation and collaboration between operators. This collaboration will largely be driven by the potential prospect of cost savings and efficiencies. The introduction of completely new standalone infrastructures during the modernisation of the network may reduce the reluctance to deploy new technology as the understanding of the network and its implementation should be better captured and shared accordingly.		

Table 13 – Trend: Network Upgrade

ID: 11	Title: Utilisation of Mixed & Shared Infrastructure	
Coverage: Primarily Mobile	**Categories:** Design, Build & Implementation, and Operation	**Recommended Focus:** Medium
Description:		
As network operators have evolved they now have to operate multiple generations of infrastructures in order to accommodate the full range of services they currently offer. The evolving trend is for service providers to use 2G for voice, 3G for data and 4G for speed; although there is a desire in the industry to decommission 2G networks to save on the associated cost of maintenance and potentially free up the spectrum for other services. The evolution to 4G networks will pose some interesting issues in relation to network integration. Currently, it is unclear whether the industry is pursuing a mixed network approach, as mentioned above, or will alternatively seek to offload some delivery to technologies such as WiFi. There is also a trend to move towards the sharing of physical infrastructure. For example O2 and Vodafone share masts as do Orange and T-Mobile (post-Everything Everywhere merger). Subsequently, any incident affecting the physical infrastructure will now impact a much wider community of users that previously would have been avoided with each operator using their own infrastructure.		
Future State:		
The trend for sharing of infrastructure and resources is likely to continue over the coming years. One service provider is exploring the possibility of developing a proposition for an industry-wide shared virtual infrastructure, similar to that offered by Amazon in the Cloud but for telecommunications services. In terms of maintaining mixed infrastructures this is likely to remain for the next few years; and despite the attraction to switch off certain networks this will only likely happen once there has been significant uptake of 4G.		

Table 14 – Trend: Utilisation of Mixed Infrastructure

ID: 12	Title: Leveraging of Infrastructure	
Coverage: Primarily Mobile	**Categories:** Operation	**Recommended Focus:** High
Description:		
Many service providers do not want to have to operate or support associated infrastructure. Rather, there is a trend for them to operate as virtual operators, utilising some or the entire existing infrastructure belonging to competitors. This cost-reduction trend also extends to the increased use of Commercial Off-The-Shelf (COTS) equipment as opposed to bespoke implementations. A consequence of this trend is that the telecoms industry in the UK has limited involvement in the research and development of new equipment. There is also as a trend for increasingly using contracting staff over permanent skilled employees. Currently contractor rates are declining as the skills required are relatively commoditised due to the age of the services/networks currently in place. This requirement for external skills introduces a dependency on outside experience and training. An example of this is the use of ex-Army personnel who are used almost exclusively to provide network upgrades on a contracting basis due to the skills they acquired during service. However, the telecoms industry has no guarantee the Army will continue to develop or require such a skillset, potentially losing a specialist pool of resource.		
Future State:		
The introduction of new technologies and the modernisation of the infrastructure is likely to refresh the skills required, leading to an increase in contractor rates. However, market conditions should be monitored to ensure that these skills remain available to the industry as a whole. The use of COTS products is also likely to continue as organisations seek to make additional cost savings and efficiencies as well as reducing interoperability issues.		

Table 15 – Trend: Leveraging of Infrastructure

ID: 13	Title: Machine-to-Machine Services	
Coverage: Industry-wide	**Categories:** Operation	**Recommended Focus:** Medium
Description:		
There is an evolving trend for utilising the telecoms network to enable machines to communicate automatically with other machines. Examples of this currently include the use of electronic tags to monitor individuals under curfew and to remove humans from the operational process, and on a much larger scale the anticipated Smart Grid. This is progressively removing the human from the loop, a process also seen in the network infrastructure by unmanning exchanges and other key physical infrastructure sites, though not key core exchanges. For those exchanges that are unmanned, there tends to be a 4-hour call out period for engineers. The growth of machine-to-machine services means the core network infrastructure is being utilised for an ever-increasing and capacity consuming number of uses, potentially increasing the nation's reliance on its ability to operate effectively. This also implies an increased level of remote monitoring and/or management as there is reduced direct human-device interaction. The associated rise in network traffic presents an evolving challenge to operators to be able to effectively monitor and analyse results, potentially leading to difficulties in terms of identifying incidents that previously would have been identified by a human at its inception.		
Future State:		
Machine-to-machine services are anticipated to grow over the coming years, for example in vehicles and remote healthcare solutions. Again, as operators seek to obtain cost savings it is likely that humans will be slowly replaced in the search for automation and cost efficiencies.		

Table 16 – Trend: Machine-to-Machine Services

2.5 Emerging Trends

ID: 14	**Title:** Outsourcing & Offshoring	
Coverage: Industry-wide	**Categories:** Design, Procurement, Build & Implementation, Operation	**Recommended Focus:** High
Description:		
In an effort to minimise non-core service provision costs, there is a growing trend to outsource and offshore as much of the support service functionality as possible. The lever of outsourcing is now so attractive and extensive that many service providers have lost the knowledge of how their networks are designed, built and operated, especially at the network layer. Theoretically, outsource companies could provide this information, but should they encounter significant staff turnover it will take even longer to understand the fundamentals of the network in the event of a failure. Offshoring introduces additional complexities and vulnerabilities, for example in the event international communications links are unavailable or denied for political reasons. Offshoring has been encouraged by the number of pan-EU telecoms operators centralising their support functions away from traditional UK-based centres. There is a counter-argument that this trend increases diversity and differentiation across the industry. However, there has been no formal study undertaken to-date confirming this. In the event a study is conducted it may highlight offshore and outsourced companies providing these services all use the same tools and techniques, ultimately increasing the level of conformity, and therefore decreasing security and resilience, across the industry. Although many service providers are increasingly using outsourced services there is poor understanding of the associated dependencies and consequences. This was highlighted recently when 2E2 went into administration; multiple operators were exposed as lacking business continuity plans forced to fund 2E2's continued operation in the short-term – at great expense – despite having service level agreements in place that were likely viewed as adequate cover, at least financially.		
Future State:		
It is believed that this trend will continue to develop as the industry pursues additional cost savings, potentially removing key industry knowledge from providers. It is also believed that the types of services that are outsourced will evolve, e.g. leveraging offshored resource to provide more cost-efficient code development.		

Table 17 – Trend: Outsourcing & Offshoring

ID: 15	Title: Cloud & Virtualisation Utilisation	
Coverage: Industry-wide	**Categories:** Design, Procurement, Build & Implementation, Operation	**Recommended Focus:** Low
Description:		
With virtualisation and cloud computing offering the functionality of traditional infrastructure deployments without the distinct physical hardware costs and space implications, the telecoms industry is searching to see how these features can be most effectively applied. Currently a general consensus has yet to be formed by service providers as to how this can be achieved, but there is a drive to leverage its capabilities in whatever way possible – either by proprietary implementation or via a third party. This trend is most apparent when looking at MVNO's and MVNE's. As they tend to be smaller organisations seeking to setup cheap and efficient solutions cloud and virtualisation services meet their requirements perfectly. At present the most common services that will utilise cloud/virtualisation tend to be support-based, such as billing, CRM, and customer mediation portals. However, the primary concern with cloud services is their resilience and this could have significant implications for service availability. This concern id diminished for private virtualised clouds which leverage existing infrastructure.		
Future State:		
It is anticipated that industry uptake of both cloud and virtualisation will continue to grow, though how this will look in reality is still open to debate. As we have mentioned the intention is clear and the potential cost reductions to be leveraged are attractive to service providers but the precise nature of the use and subsequent reliance on cloud and virtualisation services remain uncertain. The most likely approach – and ultimately the most resilient – will be to develop and offer internal private cloud services; which is entirely possible given the scale of their existing infrastructure. In addition, network operators there is the potential service providers will seek to offer cloud services to their customers in an attempt to diversify their offering.		

Table 18 – Trend: Cloud & Virtualisation Utilisation

ID: 16	Title: Growing importance of IP	
Coverage: Industry-wide	**Categories:** Design, Procurement, Build & Implementation, Operation	**Recommended Focus:** Medium

Description:

There is a clear trend emerging from the telecoms industry that IP becoming the protocol of choice for both services and applications. This is supported by a corresponding trend of growing amounts of IP-supporting technology in the network infrastructure. This is an evolution from traditional fixed-line infrastructures built using permanent virtual circuit ATM technology requiring manually configured routes. The industry has sought to counter this trend to an extent due to a desire to retain familiarity with network architecture and operation. For example, forcing packet-switching Ethernet and IP to act in the same manner as PVC technology by defining definitive routing paths as this concept is more familiar.

This resistance is increasingly diminishing with the uptake of 4G by the mobile sector and with recognition that fixed-line operators can introduce disruptive services into the mobile sector, for example with apps enabling VoIP calls chargeable to them instead of the mobile service provider. This trend therefore has the potential to introduce both threats and opportunities for service providers. Many service providers are currently exploring new business models in order to maintain their profitability with some introducing their own IP-services to remain competitive. For example, O2's 'To Go' application.

As well as introducing disruptive opportunities within the telecoms industry the increased proliferation of IP-based services and applications transiting traditional telecoms networks poses a threat to the revenues of operators from external sources as well. While the technology should theoretically provide a more resilient and dynamic infrastructure but this is yet to be fully utilised. In the meantime the trend is helping to raise user expectations regarding their IP-based applications, in turn increasing the criticality of the application layer to service providers.

Future State:

IP services and applications running off IP-based networks are only expected to increase in operation. This has the potential to give network operators a higher degree of flexibility in how they manage and route traffic and opening up the possibility of utilising QoS. This could potentially impact upon certain user groups and/or service types depending on its implementation.

As IP-based applications become increasingly important, there will also be additional challenges around providing the same level of quality expected from customers on traditional technologies. For example, VoIP applications simply cannot provide the same call quality as traditional networks as they were not designed for that type of service. However, this is unlikely to perturb user demands or application providers from continuing to push the boundaries of what can be provided over IP infrastructures.

Table 19 – Trend: Growing Importance of IP

ID: 17	Title: Utilisation of New & Mixed Technology	
Coverage: Primarily Mobile	**Categories:** Build & Implementation, Operation	**Recommended Focus:** Low
Description:		
In an effort to increase flexibility and adaptability in the network, there is a trend for service providers to adopt new technologies such as femto cells and non-fixed location base stations to dynamically boost capacity. To-date this has been in areas of geographic concentration of users and for periods of anticipated high activity – as demonstrated during the Olympics. The attraction of service providers using femto cells is that they provide a cheap and effective way of providing guaranteed mobile signal over an alternative communications channel. There has also been an increase in the implementation of small cell technology in areas such as football stadiums, where the stadium owner tends to own the in-stadium infrastructure. The utilisation of WiFi is also on the rise, piggybacking onto mobile networks to provide traditional services in areas where conventional mobile services are strained by signal quality or demand. Another associated trend emerging in the telecoms industry is that of flexible infrastructures such as spider cloud.		
Future State:		
We expect a growth in the uptake of more mixed technology networks in the coming years. This introduces specific queries as to the predictability and management of network interdependencies. For example, creating additional ad-hoc mobile cells for high-profile sporting events may offset against the radio access networks inability to handle the traffic load, but that traffic must join the fixed-line infrastructure at some stage; likely routing through a central router or switch. If this has not been planned for it may place additional strain on the fixed-line infrastructure if not managed correctly. Femto cells will also continue to rise due to their ease of installation. However, it is considered unlikely they will have much more than a minimal impact on the overall resilience of the network as each femto cell only tends to service a small number of users.		

Table 20 – Trend: Utilisation of New & Mixed Technology

ID: 18	Title: Appearance of New Commercial Models & Services	
Coverage: Industry-wide	**Categories:** Operation	**Recommended Focus:** Medium

Description:

As the industry evolves we are seeing the emergence of new commercial models that adapt to other industry trends such as the reduction or removal of handset subsidies. Other associated key trends can be seen in the emergence of increasing numbers of MVNO and MVNE operators. However, the mobile industry is wary of becoming simply a 'dumb pipe' connecting content generators with end-users. Therefore, we are seeing efforts to differentiate service offering filtering through into new commercial models. Examples include O2's 'To Go' application, but it remains to be seen whether the quality of service meets user expectations or how the model will affect the traditional Call Duration Register model for cross-charging.

In the fixed-line sector there is evidence of operators introducing new services such as cloud and data centre services; as demonstrated in the government G-Cloud and PSN procurements. There is also an increased focus on cross-selling, especially in the consumer space in an effort to enable more targeted selling of services and increasing contract length. Examples include negotiation with content providers to provide preferential services for brokering the relationship between content providers and customers. For example, Orange offered a Sky Sports package through via their 3G network utilising mobile handsets.

In the enterprise space providers have an increased focus on providing packaged and managed services – allowing their customers to outsource the management, support, and upgrading of their estates. For example, the recently tendered GCF contract for shared e-mail services to Other Government Departments (OGDs).

Future State:

The aspiration to offer differentiated and new services will continue, potentially putting a strain on the available spectrum as new services will want to be tailored to the most appropriate part of the spectrum to achieve better throughput and reduced propagation loss, risking spectrum interference. This is especially prevalent around crossover margins in urban areas that suffer from significant levels of attenuation requiring more lines of sight.

The growth of MVNOs and MVNEs will also continue to rise because of the low barriers to entry. However, the rate at which they leave the marketplace will also increase as there simply will not be enough demand and the market will become quickly saturated, potentially to the disruption of customers.

The likelihood that content providers will gain closer relationships with operators remains to be seen as the content provider has little to gain commercially from the arrangement; customers do not generally expect a specific service level from them, it tends to be more focussed towards their network provider.

The introduction of more IP and Ethernet technologies and services could introduce the potential for operators to begin to offer Quality of Service (QoS) functionality; potentially to the detriment of some user groups and/or types of traffic, e.g. to prevent excessive downloads of large files (e.g. double HD).

Table 21 – Trend: Appearance of New Commercial Models

2.6 Trend Summary

Trend ID	Title	Coverage	Trend State	Recommended Focus
1	Lean Service Provision	Industry-wide	Existing	Medium
2	Poor Knowledge & Asset Management	Industry-wide	Existing	High
3	Operating Legacy Estates	Industry-wide	Existing	Medium
4	Lack of Third Party Insight	Industry-wide	Existing	Medium
5	Poor Decommissioning	Industry-wide	Existing	Medium
6	Limited Network Insight	Industry-wide	Existing	High
7	Network Geo-location & Focus	Industry-wide/ Mobile	Existing	Low
8	Vendor Diversity in Network Implementations	Primarily Fixed-Line	Existing	High
9	Pre-Production Limitations	Industry-wide	Existing	Medium
10	Network Upgrade	Primarily Mobile	Evolving	Medium
11	Utilisation of Mixed & Shared Infrastructure	Primarily Mobile	Evolving	Medium
12	Leveraging of Infrastructure	Primarily Mobile	Evolving	High
13	Machine-to-Machine Services	Industry-wide	Evolving	Medium
14	Outsourcing & Offshoring	Industry-wide	Emerging	High
15	Cloud & Virtualisation Utilisation	Industry-wide	Emerging	Low
16	Growing Importance of IP	Industry-wide	Emerging	Medium
17	Utilisation of New & Mixed Technology	Primarily Mobile	Emerging	Low
18	Appearance of New Commercial Models & Services	Industry-wide	Emerging	Medium

Table 22 – Trend Summary

3 PESTLE Analysis

In order to identify non-deliberate threat to the telecoms industry we required a tool capable of exposing external factors that, while non-malicious in their intent, could have the consequence of exploiting security or resilience vulnerabilities in telecoms networks. We used the PESTLE framework covering: Political; Economic; Social; Technological; Legal; and Environmental factors to obtain a view of the entire environment in which telecoms organisations operate. The relevant external factors and their potential to be non-deliberate threats are detailed in the six sub-sections detailed below.

At the end of each sub section the external factors are summarised in a table and their respective potential impact to the telecoms network and likelihood of occurrence is captured. Each table section is intended to describe the following:

- **ID –** A unique reference number for each external factor.
- **Title –** A short and unique title of the external factor.
- **Summary –** A brief description of what the title of the external threat covers.
- **Impact** – an indication of the impact should the vulnerability be exploited/realised.
- **Likelihood** – an indication of how likely the vulnerability is to be exploited/realised.

3.1 Political Factors

Modern telecoms networks are reliant on cross-border co-operation for transmission of IP, even for some intra-country calls. And while it is considered extremely unlikely that service availability would ever be affected by inter-government relationships the extended nature of the network is deemed to present an external threat. Data packages have to leave the UK, most likely via undersea cable, transit a network in another country before returning to the UK, again via undersea cable. This route poses two key threats: the undersea cable could be broken and resilience of the foreign network might not be as strong as is the case in the UK. Disruptions to the overseas network might also be subject different service level agreements to those in the UK, potentially extending the duration of a service outage.

The potential break-up of the European Union and devolution vote in Scotland in 2014 are two external factors that might impact on the telecoms network in the UK. While neither event should prevent the delivery of services it will cause significant impact on the inter-connectedness between service operators. Call duration records will be increasingly complex to take into account the various different currencies that need to be accommodated in the event of the break-up of the EU. Similarly, the devolution of Scotland should not affect resilience directly but may require additional investment in compliance that might otherwise have been spent on security and resilience efforts.

A number of governments around the world have placed bans or restrictions on the use of equipment from certain vendors on the grounds of security and intelligence concerns. The most well-known of these examples is the ban of equipment from Chinese-registered companies Huawei and ZTE in the US, but also India and other countries.

There is the potential that economic and security concerns combine to prompt nationalisation of vendors as governments intervene in failing telecoms equipment vendors. This restriction on equipment that can or can’t be used could reduce the diversity of the network increasing the impact of a vulnerability being exploited as more of the network is affected. Though, currently there is no trend of networks that already have this kit installed swapping it out for performance or resilience reasons.

Within the UK there is a drive by government to increase the range of services provided online with the intended benefit of reducing cost. Examples cited include to justify this include the cost of renewing car tax online as 20 times cheaper than by telephone, 30 times cheaper than by post and 50 times cheaper than in person. This increasing dependence on network availability and a corresponding lack of alternative sources of these services makes the potential impact of a network outage greater.

ID	Title	Summary	Impact	Likelihood
1	Government relations	Break down in inter-government relations disrupts international transmission of telecoms traffic	Minor	Extremely unlikely
2	Differing resilience standards	Use of international networks for routing exposes UK traffic to varying levels of network resilience and SLAs	Minor	Unlikely
3	Break-up of the EU	A break-up of the EU would disrupt network security and resilience harmonisation efforts	Major	Possible
4	Devolution of Scotland	The gaining of independence by Scotland may cause service provision issues	Minor	Possible
5	Vendor restrictions	Government security concerns restrict the number of hardware and software vendors	Moderate	Likely
6	Political will for increased service provision	Increased use of internet to deliver government services at expense of alternative sources	Minor	Possible

Table 23 – External Political Factors

3.2 Economic Factors

The maturity of the telecoms sector and thin margins on providing core services has introduced two key trends: becoming as lean as possible in the provision of core services by offshoring and outsourcing all non-essential managed support services; and focussing on increasing revenue per unit and creating market differentiators by providing additional services such as content provision.

The first of these trends introduces an external threat to the resilience of the network from reduced variance in diversity. As there is a ‘race to the bottom’ of the cost in providing core network service providers utilise more commercial off the shelf (COTS) hardware and software in place of bespoke items to reduce costs. This increased use of COTS components results in consolidation in the hardware and software market to achieve economies of scale. In the event of a threat causing a network outage there is the potential that a larger proportion of the network might be affected as a result.

It also introduces bottlenecks in the supply chain as multiple providers’ source from the same providers. In the event of a network outage or other event that requires increased demand for network components there may not be the capacity in the supply chain to meet this demand, increasing the impact of the outage. It also means that in the event of a supplier not being able to operate a much larger number of providers will be affected.

Broader external economic threats are tied to the credit crunch that first came to the fore in 2008. These include the potential collapse of the Euro currency causing telecoms providers to have to re-configure call duration records to accommodate each new currency. It could also disrupt the EU efforts to harmonise the roaming charges for users crossing national borders.

The collapse in consumer spending has also significantly increased the number of high street retailers passing into administration. In the event that providers have towers located on the roofs of these premises they are no longer able to access them until the unit is re-let and access can be granted.

As the price of commodities has increased due to global demand so there has been a corresponding increase in the theft of network infrastructure that can be re-sold. Most commonly this has been copper cable that formed the backbone of the legacy telecoms network. The impact to modern networks is the result of modern fibre cables following the same geographic architecture and being laid over the copper. This means it is either cut or broken in the removal of the copper below by criminals.

Other elements of the telecoms network are also attractive to criminals because of the high-value, low-weight and small component size. Examples include organised crime groups targeting articulated lorries carrying specialist components. The problem is compounded by the geographic spread of the network making it uneconomic to physically secure every part of infrastructure. Rather, the industry attempts to learn from every theft to identify priority areas of network infrastructure that should be physically secured, most notably nodes in the network where fibre connections are made.

Cost of running multi-generational networks put the industry under financial pressure to decommission historic networks to save on cost of operation and maintenance.

ID	Title	Summary	Impact	Likelihood
7	Reduced functionality	Vendors following suit from telecoms industry and driving down cost in hardware	Moderate	Possible
8	Supply chain bottlenecks	Increase use of COTS places greater dependence on the supply chain	Minor	Possible
9	Collapse of €	Impacts the call duration records	Minor	Possible
10	Increase in vacant retail units	Masts on roofs of vacant retails units not accessible	Insignificant	Extremely Likely
11	Commodity price increase	Commodity price rises increase the chance of copper and fibre cable theft	Moderate	Extremely Likely
12	Organised crime	Targeting of high value network components	Moderate	Possible

Table 24 – External Economic Factors

3.3 Social Factors

User's interaction and reliance on the telecoms network has evolved significantly since the emergence of mobile telephone and again with the introduction of 3G. Since then there has been huge growth in consumer demand for internet access. A study conducted

by the Office for National Statistics in 2011 found that 45% of people used a mobile phone to access the internet and 6 million users had accessed the internet via a mobile phone in the last 12 months.

This ever increasing demand by consumers for bandwidth-consuming services places a range of external factors on the telecoms industry that they have to accommodate in their network infrastructure. The telecoms industry finds itself in the middle of huge demand from its user base and a more than willing supply of material from content generators with little influence over either side.

Furthermore, content generators are exploiting technological development to offer enhanced material such as double-HD that the telecoms industry has to accommodate. At the moment it is unclear exactly how the network will accommodate this demand though utilising mixed networks is common. This meets the requirement but introduces dependencies within the network that are unknown and have the potential to exacerbate the impact of any outage. It also increases the loading on other elements of the network in the event that any part fails.

As a result the telecoms industry has seen a transition by its user base from a relatively stable and predictable base of fixed line telephony usage to a constantly evolving and disruptive market. An historic model catering for three minutes of calls by subscribers per day with predictable busy periods and hot spots is no longer valid. Rather, service providers must today content with more random voice, video and data requirements from subscribers and other entities.

At the same time reliance on the infrastructure to deliver services, increasingly in the absence of alternative options, heightens the need for resilience and increases the impact of any outage. This external factor can be identified in the use of the telecoms network as the primary delivery channel by corporations to support remote working and also governments for the delivery of services. The reliance of the network to-date has helped compound the potential issue by creating an expectation in users that they will always be contactable and correspondingly able to connect.

As modern handsets are more akin to computers than traditional telephones there is a huge potential threat from the emergence of mobile malware. Despite their similarity to PCs user expectation regarding security of the handset is largely misplaced. The expectation that security is a service provider issue risks the mobile industry being hugely exposed to malware that could cause significant losses to users or service disruptions through the exploitation of handset bots to launch voice or data denial of service attacks.

Linked to the huge demand for bandwidth services are the potential spikes in service demand at both predictable times, such as sporting and music events, as well as unexpected ones such as the July 2007 bombings in London. These spikes have the potential to cause minor disruptions such as packets of data being dropped through to complete network failure.

At present the industry is waiting for the trigger for mass adoption of 4G. For 3G this was the advent of applications that made the data element a key requisite that 2G was unable to provide. In the event that this trigger is found we can expect a similar rush to 4G that service providers and the underlying infrastructure has to be able to support this or risk facing resilience issues.

ID	Title	Summary	Impact	Likelihood
13	Consumer demand	Consumers have a seemingly ever-increasing demand for bandwidth-consuming services	Minor	Likely
14	Consumer expectations	Consumers have an expectation that service providers will provide security of their device	Moderate	Likely
15	Content generation	Service providers have little influence over the volume of content generate for consumers	Insignificant	Likely
16	Constantly evolving market	Phone functionality means it is increasingly hard to predict consumer behaviour	Moderate	Possible
17	Consumer dependence	Consumers increasingly rely on their mobile phone for enabling services	Minor	Possible
18	Potential 4G use	Uncertainty over the nature and scale of adoption of 4G services	Insignificant	Extremely Likely

Table 25 – External Social Factors

3.4 Technological Factors

The external technological factors probably introduce the greatest number of non-deliberate threats that might result in outages or resilience issues for telecoms networks.

The telecoms infrastructure is a paradox of historic legacy elements and the latest modern technology. This is indicative of the industry having to run three generations of technology to support core services - offer users the latest technology or risk falling behind the competition - and support communications to, from and between increasingly diverse content generators and end points.

The result of this combination are hugely complex networks, often compounded by the fact they rely on multiple network operators to facilitate service provision. This introduces differences in levels of security and resilience as well as standards between varying parts of the network. It also increases the number of points of potential failure such as any variance in the network synchronicity or timing.

Automated reporting of more modern technology permits the unmanning of exchanges as component parts are able to feedback performance electronically. However, this introduces a huge volume of network performance data that has to be effectively managed and requires effective response to anomalous behaviour or automated alerts. As with many other industries, telecoms providers have to be able to master big data, generated from both their own network infrastructure and user base, or risk being swamped under the volume of data generated.

For elements of the legacy networks both hardware and software can be end-of-life and as such no longer supported by the manufacturer. Vulnerabilities will no longer be patched leaving the technology vulnerable to any exploits subsequently identified. It also means that in the event of failure the service provider either has to own or be able to source spares or the component needs to be completely replaced with any associated disruption.

Rapid evolution of the industry places the network under greater strain. It now has to cater for modern services running off increasingly powerful servers, drawing more electricity than was historically the case. This trend is set to continue and will place increasing strain on the Data Centres and exchanges housing the infrastructure. Ensuring an adequate supply of power to the network is essential to its resilience with brown-outs posing a potential external threat in the event that the power supply is unable to keep pace with demand.

Not only does the telecoms network have to cope with increasing bandwidth consumption from users but also increasingly from machine-to-machine connectivity. The number of connected devices in the UK is expected to double by 2020. This trend has already started in the utility industry with the current trialling of smart meter devices that is expected to result in the deployment of 53 million devices by 2019.

In addition to smart meters there is also a trend for a wide range of other items to also contain the ability to connect including cameras, household appliances and motor vehicles. All of this adds traffic to the network that consumes additional bandwidth.

This demand must be taken into account when designing network coverage, especially as modern 4G networks 'breath' in order to accommodate user demand; service provision expands and contracts as required. While less of an issue for rural areas there are potential implications in high-density urban areas. In the event that user demand is greater than service provision there is the potential for disconnect between user expectation and service provision. 4G is also new, and as such is not as comprehensively tried and tested. There is the potential that, at least in the short term, there will be more outages as problems are ironed out.

As the telecoms industry increasingly adopts IP as the protocol of choice this unlocks a range of new non-deliberate threats. The prime example of this is the introduction of disruptive influences such as apps that use IP to allow voice calls to utilise data channels and deny the mobile service provider the opportunity to collect revenue for the call.

The final technological factor is posed by spectral interference. Official estimates have suggested that 4G transmissions in the 800MHz band could create interference to terrestrial television services for a small proportion of UK citizens. OFCOM estimates suggest approximately 2.6 million households will be affected. Plans are already in place to mitigate the effects of this interference.

By way of mitigation the industry has contingency plans to support the 4G rollout and has set up Digital Mobile Spectrum Limited to assist households affected by interference; a further independent group the TV/4G Coexistence Oversight Board will offer advice to this company.

ID	Title	Summary	Impact	Likelihood
19	Increasing network complexity	The connections between legacy and modern network infrastructure	Moderate	Possible
20	Increasing range of content generators	More and more devices are connected including smart metering and white goods	Minor	Likely
21	Automated reporting	Network components are increasingly able to report their status for monitoring	Insignificant	Likely

22	Heavier draw on electricity	Increased computing power of modern network components demands higher power usage	Moderate	Possible
23	Breathing coverage	Modern cells 'breath' in keeping with service demand	Insignificant	Extremely Likely
24	Spectral interference	Increasing demands on the spectrum leave less free space between blocks	Minor	Unlikely

Table 26 – External Technological Factors

3.5 Legal Factors

A range of legal Acts exist to cover the telecoms industry, the most prominent of which is the Communications Act 2003. The introduction of new legislation has the potential to impact the strategic direction of the industry and help introduce new trends that might in turn cause existing vulnerabilities to evolve or introduce entirely new ones.

An existing external legal factor affecting the industry is the effort to harmonise charges across international boundaries. As the ability to make wider profit margins from travellers using their phones overseas diminishes, providers accelerate their efforts to have as lean an operation as possible in providing core services as cost cutting becomes the primary function to increase profit margins.

In keeping with many other industries service providers are required to make compulsory breach notifications, for example in the event of service outages or breach of data protection. While it is unlikely that these laws would introduce resilience issues in their own right they could affect trends within the industry which do; for example, by increasing spending on compliance over security and resilience.

The industry also faces possible future legislation that might require further capital investment by the industry. Examples include: the proposed EU legislation requiring providers to be able to fulfil a user's 'right to be forgotten'; and UK legislation covering access by law enforcement and the security services to deep packet inspection data.

One legal factor which could impact network resilience would be laws restricting the location of cell towers. This would force providers to concentrate their infrastructure. In the event of a tower being destroyed or unavailable the impact is exacerbated.

ID	Title	Summary	Impact	Likelihood
25	Introduction of new legislation	Any new communications-related legislation will impact on the telecoms industry	Insignificant	Possible
26	Roaming charges	Harmonisation of EU roaming charges	Minor	Likely
27	Breach notification	Forcing spending on compliance over resilience	Minor	Possible
28	'Right to be forgotten'	Creating legal right for consumers details to be permanently removed from all databases	Minor	Likely

29	Location restrictions	Legal blocks on location telecoms infrastructure in certain geographies	Insignificant	Possible

Table 27 – External Legal Factors

3.6 Environmental Factors

The telecoms network, similar to any other, comprises physical components that if damaged will cause service outages. This threat is heightened in the telecoms network because so much of the network is unmanned and leverages existing infrastructure – such as cables traversing road and rail tunnels.

This places the infrastructure of the telecoms network at risk of disruption caused by extreme weather events such as flooding but also accidental destruction. There are numerous examples of outages caused by unrelated accidents, such as fires in tunnels and shipping cutting undersea cables. There are also examples of extreme weather causing an indirect impact due to the disruption of supply chains.

Some components in the telecoms network are dependent upon finite raw materials such as rare earth. There is a potential disruptive factor from the availability on the open market of some of these raw materials. In many cases, these supplies can be subject to internal disputes in the countries in which they are sourced. They are also vulnerable to geo-political factors, with some nations seeing them as key to the current and long term growth of their economies.

The supply and demand effects on the commodity market can also have direct consequences on the telecoms network infrastructure. We have already explored this in the economic factors section (above) in respect of copper and other cables. This threat also extends to silica used to make fibre optic cables which can also be attractive to criminals.

In conjunction with the external legal factor covered, the environmental concerns around telecoms masts can restrict their placement. This limitation can cause a concentration of service providers on the masts permitted. In the event that one of these masts is destroyed, rendered inaccessible, or stops operating there are two potential outcomes: a greater number of users are affected as a result of the concentration of providers linked to the mast; or the area of coverage affected is greater as the geographic placement of masts is increasingly distributed.

ID	Title	Summary	Impact	Likelihood
30	Exposure to natural disaster	Disruption to service as a result of natural disaster or accidents	Major	Possible
31	Use of finite raw materials	Requirement for rare raw materials in network components exposes industry to supply and demand issues	Minor	Unlikely
32	Location restrictions	Legal blocks on location telecoms infrastructure in certain geographies	Insignificant	Possible

Table 28 – External Environmental Factors

4 Security & Resilience Vulnerabilities

4.1 Approach

This section was formed as part of phases three and four of the methodology, see Section 1.4 for further detail. The trends identified and outlined in Section 2 were cross-examined with the factors described in the PESTLE analysis (Section 3) to produce a list of associated vulnerabilities. Each vulnerability was then assessed to determine how likely it is to be realised and/or exploited, and an indication of its subsequent impact. For a deeper explanation of the metrics used and the approach taken see Section 1.6.

Having identified a list of associated vulnerabilities these were then subsequently split into two sections: current and anticipated. These categories are reflected in the preceding structure of this section of the report. The section labelled *Current* outlines the vulnerabilities in place in the infrastructure as it stands. Conversely, the section labelled *Anticipated* describes vulnerabilities that may exist in the future due to changes in external factors (as outlined in the PESTLE analysis - Section 3), the emergence and evolution of industry trends, or the failure to mitigate the increasing levels of exposure of pre-existing vulnerabilities.

4.2 Table Structure

The table structure outlined in Figure 5 – Vulnerability Table Structure, contains the following items for each vulnerability:

- **ID** – a unique identifier.
- **Title** – a unique high-level descriptor.
- **Description** – a detailed description of the vulnerability.
- **Related Trends** – which industry trends contribute or relate to the vulnerability.
- **Vulnerability Level** – a rating calculated on the impact and likelihood metrics.
- **Impact** – an indication of the impact should the vulnerability be exploited/realised.
- **Likelihood** – an indication of how likely the vulnerability is to be exploited/realised.
- **Rationale** – a description of why the associated impact and likelihood values have been awarded.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale

Figure 5 – Vulnerability Table Structure

The vulnerability level falls into one of five categories of increasing importance:

1. Negligible
2. Low
3. Medium
4. High
5. Critical

4.3 Matrix Structure

At the beginning of both Section 4.5 (Current) and Section 4.6 (Anticipated) a vulnerability matrix – like the one shown in Figure 6 – Vulnerability Matrix Structure below – provides a high level illustration of where the vulnerabilities currently reside in relation to their impact and likelihood scales. The matrix is primarily used as a tool to allow the highest ranking vulnerabilities to be easily drawn out for analysis. In addition, it provides a well-rounded high-level overview of the current state of the telecoms industry to manage their vulnerabilities exposed to non-malicious threat. The scale increases in criticality from the bottom left corner to the top right, i.e. those in the 'red' area are deemed to be more critical than those found in the green.

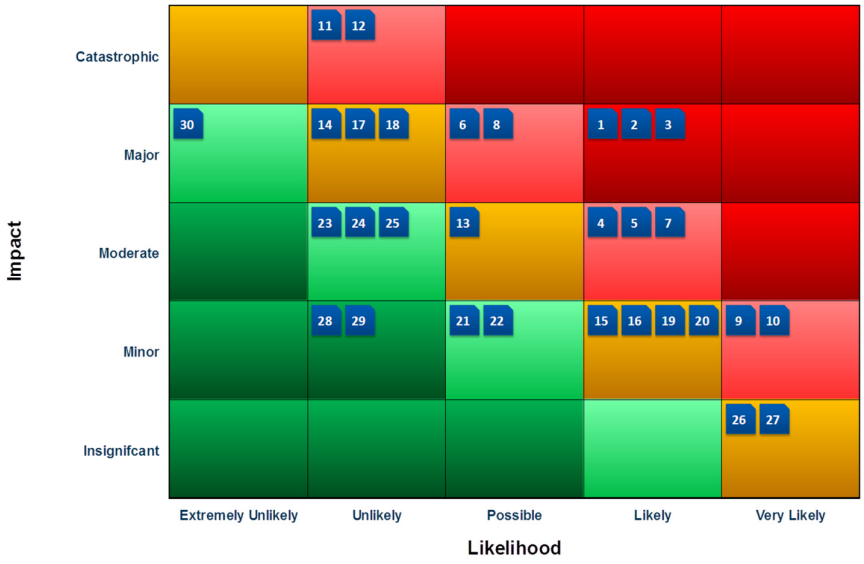

Figure 6 – Vulnerability Matrix Structure

4.4 Sensitivity Analysis

In order to attribute a level of confidence to the vulnerabilities generated and reduce the impact of any bias in their creation, we undertook a range of activities designed to test the sensitivity of the impact and likelihood ratings. These included:

- Utilising the Ofcom reporting thresholds for service outages in generating our impact table;
- Where they were available, drawing on the anecdotes and real-world examples we highlighted during both interviews and our open source research to ensure the vulnerabilities listed were primarily based on practical as opposed to theoretical circumstances;
- Ensuring the process by which we generated the vulnerabilities – as well as their corresponding impact and likelihood ratings – was as transparent as possible. In doing so we have explained our methodology and detailed the rationale for the ratings attributed to each vulnerability; and
- Having the vulnerabilities pass through a rigorous quality assurance process prior to their inclusion in the final report.

4.5 Current

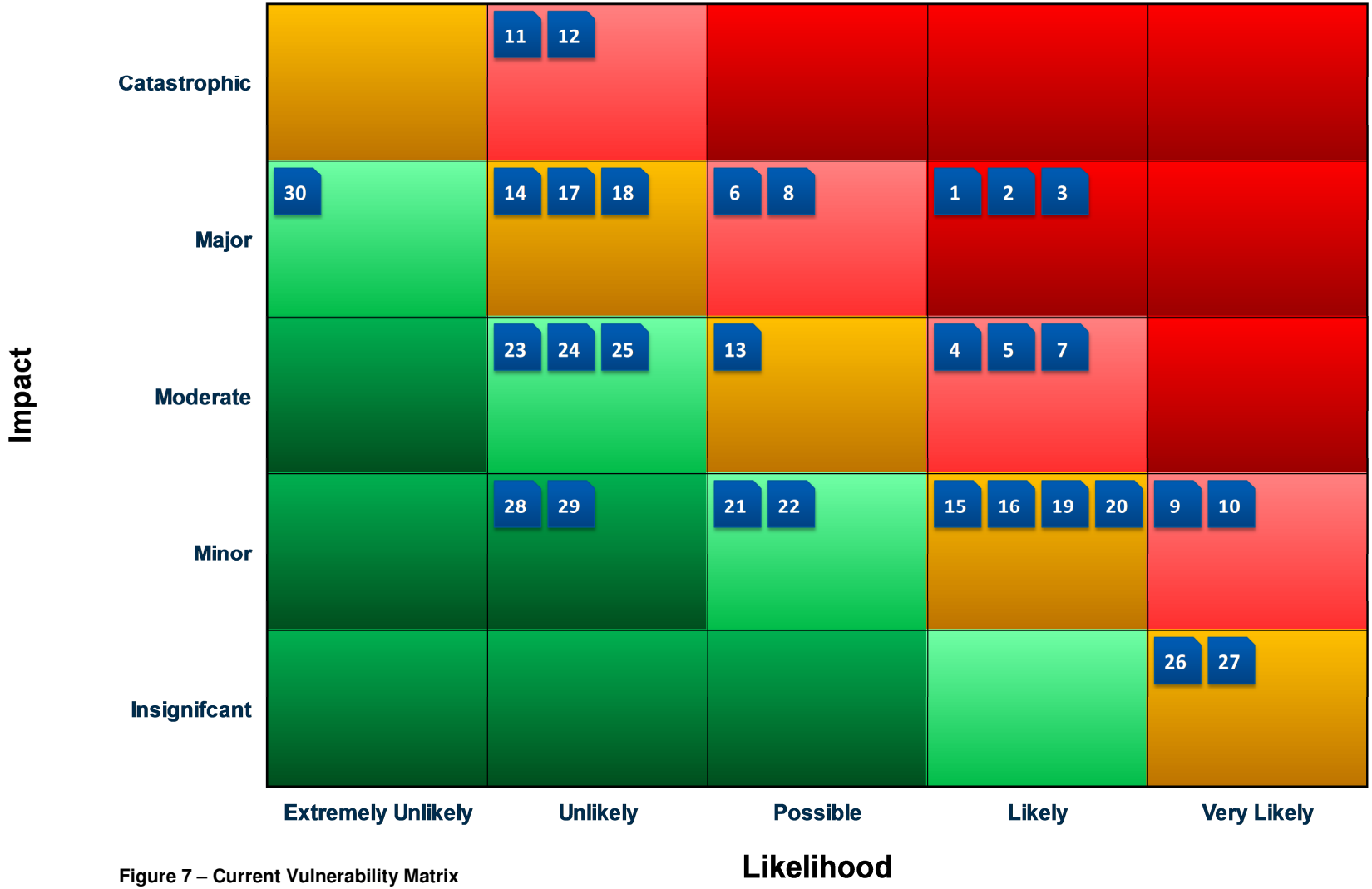

Figure 7 – Current Vulnerability Matrix

4.5.1 High Priority

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
1	Increasingly aging infrastructure	The telecoms industry does not tend have a mature or consistent approach to the decommissioning of its infrastructure. As a result, parts of the network are progressively getting older making them more susceptible to faults and failure. This is not necessarily due to design faults, simply aging components. Consequently, over time this is likely to increasingly lead to more and more incidents occurring.	3, 5, 11	**High**	Major	Likely	There are examples in recent history of critical components that are at the end of their realistic service life. However, the threat of decommissioning with limited knowledge of its functionality and technical dependencies has resulted in a reluctance to either touch or upgrade it, for fear of the consequences. Unfortunately inevitably it fail at some stage and depending on the criticality of the system(s) in question, could cause a major impact to the service.
2	Lack of complete understanding of internal network interconnections and dependencies	The telecoms industry has a poor and incomplete view of each of their respective networks and how they interconnect. This lack of knowledge can result in incidents that have unforeseen consequences and extend the process of discovery and root cause analysis.	2, 3, 6, 11, 17	**High**	Major	Likely	Any incident will be contained to a single network, but depending on the criticality of the component in question it could lead to a major impact.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
3	Irregularity of disaster recovery (DR) function and process testing	The telecoms industry is inconsistent in terms of how often they actually test their disaster recovery procedures, in particular backups. Consequently, although backups are taking place (at varying intervals) whether they would actually work in practice is uncertain. As such, data could be lost and significant delays could be introduced when returning the network to its previous operating state.	1, 3	**High**	Major	Likely	Unfortunately components are likely to fail at any point, irrespective of how regularly they are tested. It is hard to continually have full assurance that procedures will operate effectively in a real-life scenario. However, given the breadth of testing the impact would likely remain on a relatively small scale, but could be major depending wholly on the criticality of the system(s) in which it provides redundancy to.

Table 29 – Current High Priority Vulnerabilities

4.5.2 Medium Priority

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
4	Level of unobtainable infrastructure parts	Infrastructure components have progressively aged, coupled with the limited level of limited decommissioning throughout the industry, means there are numerous pieces of equipment that are neither still manufactured nor available for purchase. Consequently, this has led to industry having to source replacement components from online auction services or foreign nations with long lead-times. In addition, the replacement component will also have aged, providing limited assurance of how long it will function as anticipated.	3, 6, 17	Medium	Moderate	Likely	The impact is once again implied by the system/application affected. As there is now so much legacy equipment on the infrastructure the likelihood is deemed to be likely. However, if there were major issues with obtaining a replacement or a widespread flaw that is no longer rectifiable, the option always remains for wholesale replacements and/or upgrades.
5	Variable and indirect reporting chains	The telecoms industry can have a relatively convoluted reporting chain for incidents. The existing and growing model of reselling infrastructural services , e.g. via MVNOs and MVNEs means that when an incident occurs the first to know about it are virtual operators as their customers are expecting them to deliver their service. However, these organisations have little influence on the operating infrastructure and must pass on the fault to the core operator. This process of relaying messages can introduce additional delay into highlighting incidents.	11, 12, 15, 16	Medium	Moderate	Likely	The number of parties involved in incident reporting is constantly on the rise, which can result in delays to incident resolution. This is particularly an issue in the mobile sector. Customers do not understand the commercial model or the full network stack, so they tend to contact their service provider directly. However, if an incident was sufficiently large enough to be classified as major or higher the operator is likely to identify it themselves.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
6	Lack of complete understanding of external network interconnections and dependencies	The telecoms industry has a poor and incomplete view of how their infrastructure interoperates with external networks, as well as their respective dependencies. This lack of cross-industry view of the effect of network changes and/or knock-on effects of incidents can often result in impacts that far exceed what was expected. This 'domino' effect and lack of knowledge can also lead to significant delays in incident resolution as the industry may not know which parties need to be involved or how, significantly extending the process of discovery.	11, 12, 15, 17	**Medium**	Major	Possible	This is deemed possible as there are numerous network interoperabilities in place which are likely to continue for the foreseeable future. In addition, individual operators do not have a full grasp of their own infrastructure and as such neither do operators who depend on its operation. There are examples of such a vulnerability being realised in both the UK and France highlighting the potential scale of its impact.
7	Completeness of disaster recovery (DR) procedures	The telecoms industry does not have a complete picture of how their networks are composed, both internally and externally. As such, any disaster recovery procedures in place will have a reduced level of assurance that they can actually operate effectively in the face of a real-life disaster, irrespective of any testing regimes. This could significantly impact upon the industry's ability to recover and remediate disasters.	2, 5, 6	**Medium**	Moderate	Likely	The lack of knowledge and asset management in the industry implies that you may plan for a component failure but once it actually occurs you discover it is a more critical component of the infrastructure with 50% more functionality than you were previously aware of.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
8	Vendor diversity of network infrastructure	The telecoms industry has varying levels of vendor diversity within their core infrastructure. Although less of an issue in the mobile radio access network, when choosing vendors resilience considerations tends to come second to the potential cost benefits achieved through economies of scale. Historically, single vendors have supplied individual geographical regions or specific network functions, e.g. edge routers, or a combination of the two. Should a given vendor go bust they would be unsupported. In addition, the volume of users impacted through faults to a specific piece of equipment is greatly increased.	1, 8	**Medium**	Major	Possible	While networks operators have the intention of having a diverse network, in reality this has proved to be difficult to implement consistently – particularly in the fixed-line sector. Consequently, this has resulted in a lack of diversity and geographical pockets of vulnerability. This is likely to increase over the coming years as the potential benefits of economies of scale become ever more attractive.
9	Lack of understanding of non-critical resilience incidents	The telecoms industry only tends to fully understand incidents that are high-profile and/or critical. The lack of knowledge around smaller-scale incidents can preclude the industry from identifying issues before they snowball to result in critical incidents.	2, 6	**Medium**	Minor	Very Likely	The lack of network insight and complexity of interconnections, in conjunction with numerous examples cited in the course of conducting this assessment, means this is likely to be occurring already but the industry simply does not detect them as it stands. However, it is considered to be relatively minor because anything considered more so would be flagged and subsequently addressed.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
10	Wide geographical coverage of infrastructure network	The telecoms industry's networks are so large and dispersed that it makes it exceptionally hard for them to physically secured and protected. As such, they are more vulnerable to theft and damage. This occurs most commonly in the form of cable theft due to the rising value of copper. Although the theft is malicious, there are unintentional consequences of stealing key pieces of infrastructure and the associated impact it has on operators' ability to operate the network. In addition, fibre cables are also often damaged as thieves aim to get at the copper underneath.	3, 7	**Medium**	Minor	Very Likely	Historical trend and media coverage proves the level of frequency of this issue as is stands. However, the impact is relatively minor as the most sensitive/critical sites have been appropriately secured as a direct consequence of the frequency and impact of historical attacks. Despite this, attacks are likely to continue and increase, especially considering the growing value of precious metals, but it is not economically viable to entirely mitigate this vulnerability.
11	Geographical distance between key infrastructural components	The telecoms industry does not necessarily have large geographical distances between their primary and redundant sites. For example, although a primary site may be in Reading the DR site is located in Slough. Consequently, should there be a significant incident that affects the whole of the south-east would prevent the operator from using both its primary and secondary sites.	7	**Medium**	Catastrophic	Unlikely	This is deemed to be unlikely given the geographical coverage and severity an incident required to directly result in a regional outage. However, the impact itself is likely to the criticality of the services connected in the event of such an incident occurring.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
12	Reliance on cloud availability for service delivery	The telecoms industry, particularly virtual operators have a reliance on cloud platforms in order to deliver their service capability. Should their providers go down and/or be unavailable for a significant period this would prevent users from accessing their service(s), despite the fact the core network infrastructure remains operational.	15, 16, 17, 18	Medium	Catastrophic	Unlikely	Although there is an increased use of the cloud and the primary concern with them is their availability, the likelihood of their services being unavailable is low given their distributed and dispersed architecture. However, if they were to be unavailable and the system hosted was highly critical, it could have a catastrophic impact to services.
13	Reliance on vendors for technical equipment expertise and support	The telecoms industry does not have the skills in-house to maintain and support vendor equipment. In the event that a given vendor was to enter administration, or are simply unavailable to provide support – e.g. during a widespread incident where they do not have the capacity to service all their customers simultaneously – could lead to delays for incident resolution or unsupported infrastructure. As such, operators would be incapable of resolving and rectifying incidents.	1, 14	Medium	Moderate	Possible	The lack of in-house skills could lead to a delay in responding to incidents and reduce an operators' ability to resolve them. However, in the event that a particular vendor's circumstances renders portions of the operators' networks unsupported the option for replacing the equipment still remains, albeit with the potential for great expense. However, the vendors currently used are large and well established organisations providing a degree of assurance they will remain stable, at least in the short-term.

Table 30 – Current Medium Priority Vulnerabilities

4.5.3 Low Priority

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
14	Reliance on outsourced core-infrastructure support services (in country)	The telecoms industry has an increased reliance upon third-party suppliers in order to maintain and support their infrastructure, particularly in the mobile sector. This has the potential to result in skills loss as operators can no longer influence or control the retention of knowledge within third party organisations. Consequently, this could potentially lead to an inability to rectify large scale incidents as suppliers may be incapable of providing sufficient resource to resolve catastrophic failures.	1, 14	**Low**	Major	Unlikely	The impact of this vulnerability is mitigated by the fact that the third-party support provider still remains in country. Although skills are no longer retained in-house, if an incident considered catastrophic was to occur the wider resource would still be available to operators – potentially through the contractor market. Alternatively, they could simply insource but this would need to be identified and acted upon quickly.
15	Lack of resilience to third-party failure	The telecoms industry is also heavily reliant on third-parties to provide support and business services to their users. In the event that a third-party supplier was to enter administration the telecoms industry as a whole has immature and underdeveloped continuity plans to bring certain activities back in-house or move to alternate suppliers.	1, 4, 14	**Low**	Minor	Likely	Although this is relatively likely, as recent events with 2E2 have demonstrated, there is always the option of paying the administrator to maintain the service while an alternative provider or approach is identified. However, this will have additional cost to operators.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
16	Lack of understanding of third-party delivery model (and risks)	Although SLAs are in place for third-parties, the transparency and understanding of how organisations actually go about meeting them is not necessarily clear or understood. Consequently, as providers do not understand the risks of their third-parties it makes it challenging to prepare for or manage them in the event they are transferred when a third-party can no longer satisfy their SLAs, e.g. should they go bust.	1, 4, 14	**Low**	Minor	Likely	While SLAs are in place they provide a degree of financial cover and contingency to the operator. However, in the event that a third-party enters administration these are effectively meaningless and provide no way of actually ensuring the operator can maintain their service to their users. However, the impact is considered minor as there is always the potential to either continue the service at the operator's cost or to switch to an alternative provider.
17	Reduced infrastructure diversity	The telecoms industry is increasingly using more and more COTS equipment; as opposed to traditional bespoke kit. Consequently, technology is converging – reducing the variance in the infrastructure which implies any fault or failure with a specific COTS product/component will have a much wider impact.	1, 2, 8	**Low**	Major	Unlikely	Although there would be an increased impact to any vulnerability, due to the scale of support provided by commercial vendors implies these would be quickly rectified. In addition, the chance of equipment failing is reduced as COTS products are often more widely reviewed and assured.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
18	Level of unsupported infrastructure	A by-product of failing to decommission and the cost of wholesale infrastructure refreshes is a significant amount of unsupported legacy equipment being used within communications infrastructure. In addition, this has also led to a lack of knowledge as to how it should be supported and how it interconnects and interfaces with other equipment. Consequently, the equipment is no longer patched and any new vulnerability at the component level will remain. In the event that the equipment begins to fail or it cannot handle interoperability with new technology this cannot be addressed.	2, 3, 6	**Low**	Major	Unlikely	As with other vulnerabilities the impact is largely dependent upon the system and/or applications affected by its compromise. This is deemed unlikely as although there are widespread levels of legacy components in the infrastructure, critical systems have high levels of in-built resiliency and fall-back options. Despite this, on the rare occasion this isn't the case, it could result in a major impact as it would be extremely difficult to resolve and could potentially require extensive replacement of equipment.
19	Reliance on paper-based technical architecture	The telecoms industry is heavily reliant upon the use of old paper-based systems to depict their network architecture. The drawings themselves are more susceptible to damage or loss and do not necessarily represent an accurate or complete view of the network. This - coupled with the fact engineers have to have hard copies of them in order to carry out their work - can lead to significant delays to incident resolution and unplanned work, as well as upgrades.	2, 3, 6, 7	**Low**	Minor	Likely	This is likely to be realised given the lack of knowledge of the existing infrastructure and the completeness of the paper-based records. However, this would only lead to delays to existing incidents, rather than exacerbate or create additional ones.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
20	Understanding of physical asset location and quantity	The telecoms industry has significant gaps in their knowledge of where they have previously installed key infrastructure components, most notably fibre cables. This can lead to engineers digging in the wrong location and/or causing additional accidental damage when attempting to resolve issues. It potentially renders multiple fibre cables redundant which could have become critical in the future during periods of high demand.	2, 3, 6	**Low**	Minor	Likely	The sheer scale of the telecoms networks and the gaps in knowledge of where particular components are is likely to lead to delays in resolving incidents. Despite this the impact is relatively minor other than cases where a key fibre-line may be damaged accidentally. However, given the spatial distance between each key line the chances of hitting these accidentally are relatively slim.
21	Reliance on third-party business-support services	The telecoms industry has a degree of reliance on third-party organisations to provide business support services, e.g. billing systems. Outsourcing non-critical services to third-parties could result in users losing access should they fail or the organisation enters administration.	1, 4, 14	**Low**	Minor	Possible	This is considered to be possible as we know there is a trend to outsource support service; one which we expect to grow over the coming years. However, the impact will likely be minor as critical core services still remain in-house.
22	Reliance on third-party network infrastructure (in country)	Each respective telecoms provider is heavily reliant on their competitors and third-parties to maintain their service throughout the country. Although individually they have far reaching infrastructure, none of the providers have complete national coverage. As such, each is dependent on the other to provide complete end-to-end services.	1, 7, 11, 12, 17	**Low**	Minor	Possible	This is considered possible as there is network interdependency in place which inherently brings with it an associated degree of underlying risk. However, the impact is believed to be relatively minor because should one link fail, there are numerous alternative routes that will allow you to re-route via another course.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
23	Reliance on third-party network infrastructure (internationally)	The telecoms industry is reliant on international third-party network infrastructure in order to maintain service. Although they may be able to collaboratively manage and control national communications and connectivity, globally they rely on infrastructure operated and maintained externally. Consequently, if the UK was to experience damage to an underground IP cable this could impact upon the UK's ability to deliver global communications services.	1, 7, 11, 12	**Low**	Moderate	Unlikely	The chances of a given national being cut off due to political/geo-political reasons are extremely unlikely due to its economic impact. However, there is potential for an undersea cable to be accidentally cut, especially if it is on a shipping lane, removing a key route to deliver IP services. Despite this, most nations now have multiple routes in/out of their country so there should still be potential to re-route traffic, albeit with the possibility of a slight degradation in the quality of service.
24	Finite spectral capacity	The telecoms industry is consistently trying to offer additional services requiring more bandwidth and/or range. Consequently, the electromagnetic spectrum is becoming increasing crowded - especially on publically available unlicensed frequencies (such as 2.4GHz). Consequently, as more and more services are introduced there is potential for increased levels of interference, especially on spectral boundaries. In extreme cases this could lead to a loss of service.	15, 16, 17, 18	**Low**	Moderate	Unlikely	Although this has the potential to introduce issues into the operation of telecoms networks, the management and licensing of the electromagnetic spectrum is relatively well managed. Although it is a finite resource, should a service be deemed critical it should have its own frequency allocated to prevent any issues with interference. However, recent examples relating to 4G and Freeview television have demonstrated the impact such issues can have to users of non-critical services.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
25	Concentrated physical infrastructure	The telecoms industry has reduced their level of diversity in terms of distinct physical infrastructure. This is especially prevalent in the mobile sector, where traditionally there were multiple operators with their own masts; this has now reduced down to what are effectively two sets - with the exception of 3. EE (Orange and T-Mobile) is using one set of masts, and O2 and Vodafone are using another. Consequently, any event affecting the physical infrastructure will affect an increasingly wider customer base.	1, 7, 11, 12, 17	**Low**	Moderate	Unlikely	Although multiple operators are now sharing the same infrastructure and cells, the overlap in mast coverage and the ease and cost of building in mobile redundancy tends to drastically mitigate the likelihood of this vulnerability being realised. However, in the event that these circumstances do not hold true, there is potential for a relatively large number of users to be affected.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
26	Lack of control over content generation	The telecoms industry has little influence over the generators of content transiting their network and its associated quality/bandwidth requirements. In addition, users are continually pushing for increased bandwidth, faster connections, and higher quality data services. Unfortunately, application providers and content generators have little concern with the telco industry's ability to match the demand. Consequently, in the future this could lead to an inability to deliver services to a sufficient quality and increased demand could significantly strain the network infrastructure.	18	**Low**	Insignificant	Very Likely	The generation of content and its associated demands for bandwidth and speed is only going to increase. However, although content generators are not directly responsible for the impact their data has to operators' ability to maintain their networks, it is still a symbiotic relationship. The content generators rely on the network operators to exist in order to deliver their services, not necessarily to a given quality standard. In the event that an operator can no longer support content generators and its customers it will be to the detriment of both parties. Therefore, it is highly unlikely that it will reach a point where either party fails under these circumstances.
27	Lack of intelligible incident trending	The telecoms industry does not necessarily have a collaborative and in-depth understanding of the frequency of common incidents. Consequently, this means predicting and managing them again in future -as well as prioritising effort - becomes difficult.	2, 6, 13	**Low**	Insignificant	Very Likely	At present there is good and open information sharing within the industry of issues deemed critical. However, this is not necessarily the case when it comes to the underlying small-scale incidents that contribute or lead to critical events. This is either because they are not recognised or shared due to their perceived insignificance.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
28	Reliance on third-party for field teams (engineering)	The telecoms industry heavily relies on skills obtained externally to deliver key infrastructure upgrades and remediation. The most pertinent example being the British Army and their training of ex-forces to carry out drilling and network infrastructure implementations. There is the potential that should these skills no longer be taught externally, the telecoms industry would struggle to have access to the skilled workforce required for tasks of this nature.	1, 2	**Low**	Minor	Unlikely	This is considered to be unlikely as the demand for the skillset externally is likely to remain for the foreseeable future. In the event that this no longer remains the case and this becomes a critical issue for industry there is scope for this to be picked up and addressed internally. In summary, as long as there is a market for this work externally it is unlikely that that eventuality will come to pass.
29	Limited pre-implementation assurance capability	The telecoms industry's level of testing capability varies substantially from organisation to organisation. Coupled with the limited understanding of how the operating infrastructure is implemented and its associated interconnections means it is difficult to fully test and anticipate the full effects of configuration or infrastructural changes prior to implementation. Consequently, changes of this nature can lead to unintentional incidents.	1, 9	**Low**	Major	Unlikely	This is considered to unlikely due to the fact that testing environments are generally as robust as they can be; the more critical the component the greater the volume of testing it will undergo prior to implementation. However, testing is no guarantee of the subsequent effect its implementation may have on the production network and historic examples indicate level the level of resultant impact, for example O2's difficulties following introduction of their new HLR system.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
30	Inability to plan and test crisis management	The telecoms industry cannot write procedures for events that have yet to happen, or are difficult to test/simulate. Similarly, in order to physically test large-scale critical incidents potentially impacting the entire telecommunications network infrastructure, you would have to disable the service. Financially this simply isn't viable for either the operators or the nation. Consequently, the industry will never know precisely how they should handle large-scale crisis.	2	**Low**	Major	Extremely Unlikely	A crisis by nature will entail a major event. However, calculating the scale of impact of such an event is difficult to capture or plan for given that it is not possible to conduct any network testing around crisis scenarios.

Table 31 – Current Low Priority Vulnerabilities

4.6 Anticipated

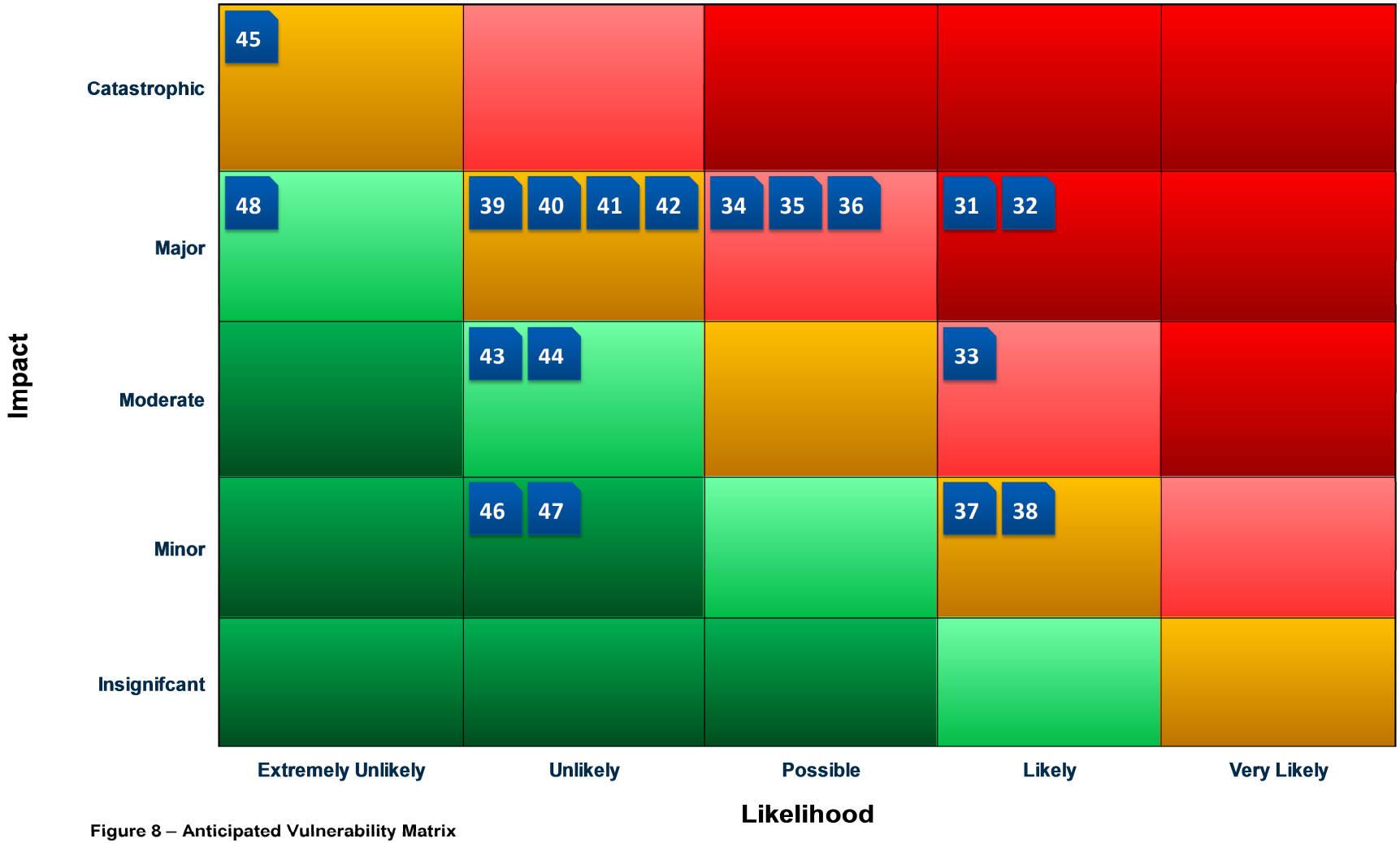

Figure 8 – Anticipated Vulnerability Matrix

4.6.1 High Priority

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
31	Dependency on small specialist SME companies	As telecoms networks have become more complex there has been an emergence of small specialist companies to support niche areas. This introduces a vulnerability that service providers are overly reliant on these small companies, lacking the in-house skills and capability themselves to run elements of their network. The vulnerability extends to the potential that as a small company there is a greater risk that in the event they fail there will not an adequate market of alternative suppliers to fill the gap. Should this vulnerability be exploited service will be impacted until the service provider is able to source the appropriate skills and capability to rectify the issue.	1, 4, 6, 10, 14, 18	**High**	Major	Likely	The UK government is keen to see small and medium-sized companies commanding a greater share of the economy and this fits well with the trend in the telecoms industry. These SME companies with their deeply specialist capability can support critical parts of the infrastructure but lack the support of an extensive trading history or wide range of contracts.
32	Less resilient vendor equipment	The trend of reducing costs as much as possible in core service provision is filtering through to vendors. Instead of a focus on providing high-quality products it is instead moving more towards meeting core requirements at the lowest cost. This introduces a vulnerability that the security and resilience aspects of the components will not be as high resulting in greater chances of failure and corresponding service outage.	1, 4, 8	**High**	Major	Likely	It is not just the failure of a specific component in the network that underpins this vulnerability but the fact that service operators will implement single vendor components by geography or functionality. In the event the component is found to have a security or resilience flaw it has the potential to cause a major impact.

Table 32 – Anticipated High Priority Vulnerabilities

4.6.2 Medium Priority

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
33	Less resilient code and applications	The growing trend of using outsourced or offshored development capability for saving costs has the potential to introduce vulnerabilities in the security and resilience of code and applications. This would be the result of a potential disconnect between the requirements of the service provider and the motivations of the developers. The outcome of this could be code that while meeting the functional requirements specified, is less secure or resilient as the developers have no incentive to ensure these aspects. Less secure or resilient code and applications may fail more frequently and be easier to break accidentally resulting in more frequent incidents and service failures.	1, 4, 8, 9, 14	**Medium**	Moderate	Likely	It is likely that cheaper code and application development will result in a reduction in quality, with less focus on security and resilience. There is also the chance that there will be less oversight and assurance of the development as well. The pre-production testing regime in the telecoms industry should help mitigate a proportion of the risk posed prior to implementation in the production network.
34	Reliance on offshored support services	In an effort to reduce costs associated with core service provision telecoms providers will increase their use of offshore support services. This introduces a vulnerability that the service provider loses the skills to understand how the support services are delivered. In addition, there is vulnerability that in the event of an incident the skills and capability to resolve it exist offshore introducing potential time zone differences and a lengthening of the time it takes to resolve an incident.	1, 2, 4, 6, 14	**Medium**	Major	Possible	The trend for offshoring is such that a large number of network support services are now performed outside the country. In the event these support services are located in countries with network resilience issues themselves this could impact operation in the UK. As a minimum the difference in time zones has the potential to enhance the impact of a UK-based incident.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
35	Unforeseen consequences of multi-generational intraoperability	Service providers now have to operate and maintain multi-generational networks. This introduces a vulnerability that providers are unable to predict how these mixed networks will work together. There are already examples of intra-and inter-operability failure leading to impacts of service provision and it is anticipated that as another network generation (4G) is implemented and legacy networks (2G) remain, so the dependencies will only increase. As the consequences are unforeseen it is difficult to predict what they might be. This will largely be dependent on the service(s) affected.	2, 3, 6, 10, 11, 17	**Medium**	Major	Possible	The level of impact is not just limited to the failure of components to be able to operate together; it also means one half of the operation has to be changed. This has the potential to introduce a new relationship to the network that, if not tested appropriately, could result in another, different, incident.
36	Inability of existing infrastructure and applications to adequately support future technological developments and implementations	As telecoms networks have developed they have utilised infrastructure and applications available at the time. In many instances legacy infrastructure and applications is being utilised or re-purposed to support more modern network provision and applications. This introduces a vulnerability that legacy infrastructure or applications are unsuitable to support more modern technology making it less secure and resilient and more prone to failure.	2, 6, 9, 10, 11, 12, 17	**Medium**	Major	Possible	In the event a failure is realised or the vulnerability exploited it is the more modern service that is impacted making it more likely to affect a greater proportion of the subscriber base. Because it is legacy infrastructure or application the service provider has to implement an alternative network component which potentially introduces further vulnerability.

Table 33 – Anticipated Medium Priority Vulnerabilities

4.6.3 Low Priority

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
37	Manageability of network performance data volumes	The industry faces a juxtaposition of never having had so much data on network performance yet at the same time being so blind to issues on the network. This is a function of having too much data and being unable to manage it, especially with regard to proactively identifying incidents. Instead the volume of data helps hide minor incidents that have to progress to critical status before they are picked up. This introduces the vulnerability that minor incidents are allowed to progress to critical status before being addressed affecting the investigation and resolution time.	6, 10, 13, 17	**Low**	Minor	Likely	There are plenty of examples of networks missing minor network incidents because the associated alert levels are lost in the volume of traffic being received. However, critical alerts are picked up and investigated and this should only improve as data management improves with time.
38	Inability to predict spikes in bandwidth consumption	Being unable to predict bandwidth consumption leaves service providers potentially facing service outages. Trends creating this vulnerability include more mobile network infrastructure in place of fixed stations. Additional capability can be provided for known spikes in service requirement such as sporting and music events. However, it leaves the network potentially easy to overload in the event of unexpected spikes. This vulnerability is even greater in light of vulnerability ID12.	2, 6, 7, 12	**Low**	Minor	Likely	It is not so much the inability to predict spikes that cause service outages as the inability to handle them. However, not knowing when or where spikes will occur can leave geographically constrained elements of the network without service until the spike is managed. Because of the geographic constraint this should be relatively quick.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
39	Centralised network infrastructure	Centralising network infrastructure entails the consolidation of periphery functions into a single central function. For example, services previously provided via multiple databases across the network now run from a single database held centrally. While it is recognised there should be a corresponding increase in the resilience and redundancy of this single database there is still a vulnerability created should the single database crash or be unavailable as there are no alternatives to draw on. We observed this vulnerability primarily in the mobile industry though the trend is becoming increasingly common across the entire industry. The full impact of the vulnerability being realised is largely dependent on the type of centralised service affected but in a worst case scenario could affect the entire subscriber set for a substantial length of time.	1, 10, 12, 17, 18	**Low**	Major	Unlikely	Centralising introduces an obvious vulnerability in that instead of multiple versions or variants within the network there is now a single instance. This should have appropriately higher levels of resilience and redundancy built in but in the event there is a failure it has a correspondingly much large impact.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
40	Levels of direct physical infrastructure interaction	As the level of manual observation and management of the network decreases this is replaced with corresponding levels of automation and remote device management. The vulnerability this introduces is that the automated data reduces knowledge of exactly how the component works and that it also introduces a requirement to have management of the network performance data.	3, 6, 12, 13	**Low**	Major	Unlikely	Realising these vulnerabilities could mean that incidents are missed because the automated data feeds are not appropriately managed, or in the event of an incident that the root cause is not understood because automated reporting does not provide the full range of information required. There is also the risk that it is not possible to gain remote access requiring physical access to resolve the fault with any associated delay.
41	Reliance on offshored development	The vulnerability introduced is that reliance leads to a lack of internal knowledge as to the workings of the code or application developments created offshore. In the event of an incident there is an inability to address any development issues without consulting with the third party creating two potential issues: delay in the response and subsequent remediation; and risk that the third party does not have the knowledge management or transfer to be able to address the issue either.	1, 4, 14	**Low**	Major	Unlikely	The realisation of this vulnerability is considered unlikely as skills will likely exist in the local market, if not wider, to be able to resolve the issue. There is a minor risk that the component affected is critical but old enough that there is only a small market of expertise though this should only affect the contractor rates.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
42	Reliance on contractors	In an effort to reduce costs associated with core service provision infrastructure owners will increasingly rely on contractors to perform an increasing range of rolls. At present contractor rates are relatively low. However, reliance on contractors leaves the industry vulnerable to losing the skills and experience internally to be able to effectively and efficiently investigate and resolve incidents themselves	1	**Low**	Major	Unlikely	The local contractor market will expand and contract as market forces dictate. In reality the skillset required will always be available, rather it becomes a question of the price that has to be paid to acquire it.
43	Inability to handle spikes in bandwidth consumption	It is anticipated that spikes in bandwidth consumption will be increasingly common as users move further away from the traditional model of 3 minutes per day per users at predictable times. This puts pressure on the service providers to build in capacity and resilience to accommodate these unexpected spikes. The vulnerability is that the network infrastructure is unable to withstand these spikes leading to packets being dropped or service dropped entirely.	2, 3, 6, 7, 11, 17	**Low**	Moderate	Unlikely	Modern fibre cable offers significant volumes of bandwidth which can be relatively easily supplemented. However, examples such as the immediate aftermath of the July 2007 bombings in London indicate the impact to service availability that an inability to handle spikes in traffic. The growth in the use of IP will help introduce greater capacity by enabling more dynamic routing.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
44	Lack of home-grown skills to proficiently implement technological developments	Telecoms networks require specialist skills in order to be correctly implemented and enable both users and service provider's to leverage the benefits each new instance of technology is capable of. There is a vulnerability that these benefits will not be realised in the UK as we lack the home-grown skills to proficiently implement technological developments. The impact of this is that appropriate levels of security and resilience are not introduced leaving the network vulnerable to service outages. Furthermore, resolving these issues will take longer as there will not be the skills and capability to investigate and remediate incidents appropriately.	14, 15, 16	**Low**	Moderate	Unlikely	It is considered unlikely the UK will ever find itself in a position that it is unable to attract the requisite skilled workforce to implement the latest telecoms technology. There is a small associated risk that the workforce is not as skilled as it could be resulting in a less secure or resilient implementation.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
45	Ability to maintain profitability in the face of proliferating IP services and applications	Commercial models in the telecoms industry are evolving, largely facilitated by the ability to use IP to transmit voice in the same way as data. We are already seeing some disruptive influences in the market with apps enabling VoIP calls to be made from handsets that are not charged back to the subscriber's service provider. With margins on core service provision already eroded this vulnerability further erodes the potential revenue per unit to service providers. With less revenue there is increased pressure on network investment with the potential that security and resilience will receive less. In turn this will result in increased numbers of incidents as components are kept inline longer leading to increased frequency in breakdowns and in the event they become end-of-life open to exploit from any security vulnerabilities identified subsequently.	16, 18	**Low**	Catastrophic	Extremely Unlikely	While the telecoms industry is coming under pressure from a broader range of competitors because of the proliferation of IP services and applications these new joiners to the market are still reliant on the underlying infrastructure. It is therefore a symbiotic relationship that all parties would work to rescue in the event of potential failure by a network operator.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
46	Inability to access network infrastructure	Being unable to access network infrastructure means service providers are unable to correct faults in the event they occur. This vulnerability has been highlighted following the credit crunch and the corresponding failure of numerous high street retailers. With many telecoms masts located on the roofs of high street retail units these have been inaccessible when occupiers have passed into administration. Other examples of this include masts located in secure compounds.	2, 7, 12	**Low**	Minor	Unlikely	While it is unlikely there would ever be a case access is impossible there is the potential that incidents are prolonged by the delay cause in gaining access to affected infrastructure because it is hosted in an area accessible only via a third party.
47	Inability to handle growth of bandwidth consumption	The telecoms industry faces ever increasing demand for bandwidth from both suppliers and users. On the supply side content generators are utilising latest technological developments to offer content requiring higher bandwidth, for example double-HD. Also on the supply side are increasingly diverse data generators such as smart meters, household white goods and vehicles. In the event that the infrastructure network is unable to grow at a corresponding rate it introduces a vulnerability of the bandwidth capacity being exhausted.	3, 7, 10, 12, 13, 6, 17	**Low**	Minor	Unlikely	Realising this vulnerability is unlikely because of the lead times available to identify the trend and implement mitigating measures to be able to deal with it.

ID	Title	Description	Related Trends	Vulnerability Level	Impact	Likelihood	Rationale
48	Unknown consequences of new application services	Each new application has the potential to introduce vulnerabilities into the network because of the unknown consequences it brings. As we have seen it is impossible to test fully every potential aspect of the production network. The vulnerability is even more pertinent for two key reasons: service providers are keen to move into application services to help increase profits; and introducing new applications onto legacy estates overlays new on old with no clear understanding of whether the legacy elements of the network will be able to cope.	3, 6, 9, 10, 17	**Low**	Major	Extremely Unlikely	It is extremely unlikely this vulnerability would ever be realised because it would be contained at the network layer and associated traffic passing over traditional and known protocols. In the event there is a failure it would cause compatibility issues and could result in network components failing with a corresponding major impact.

Table 34 – Anticipated Low Priority Vulnerabilities

5 Risk scenarios

5.1 Scenario 1 – Lack of Network Insight

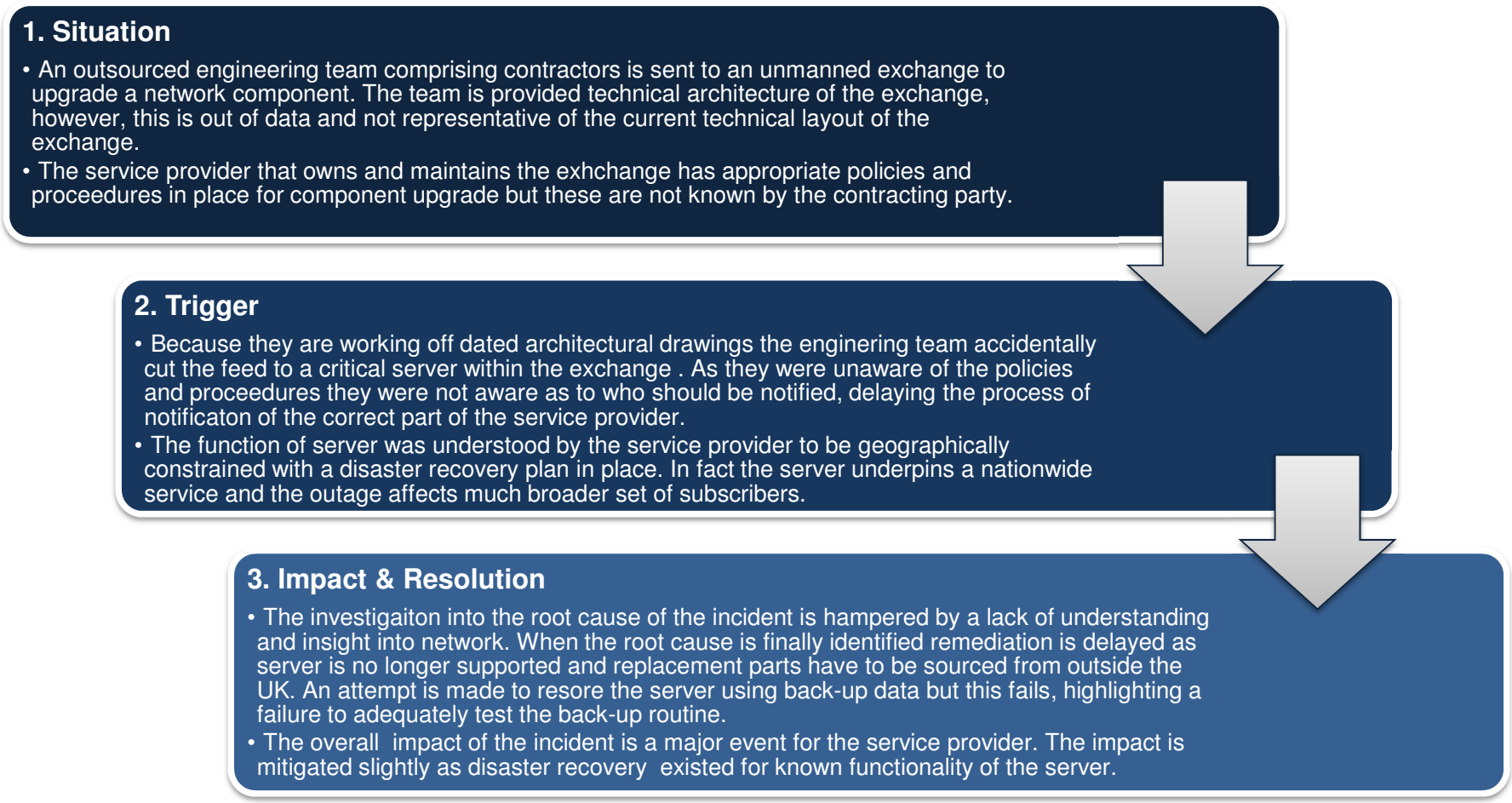

Figure 9 – Lack of Network Insight Scenario

5.2 Scenario 2 – Increasingly Ageing Estate

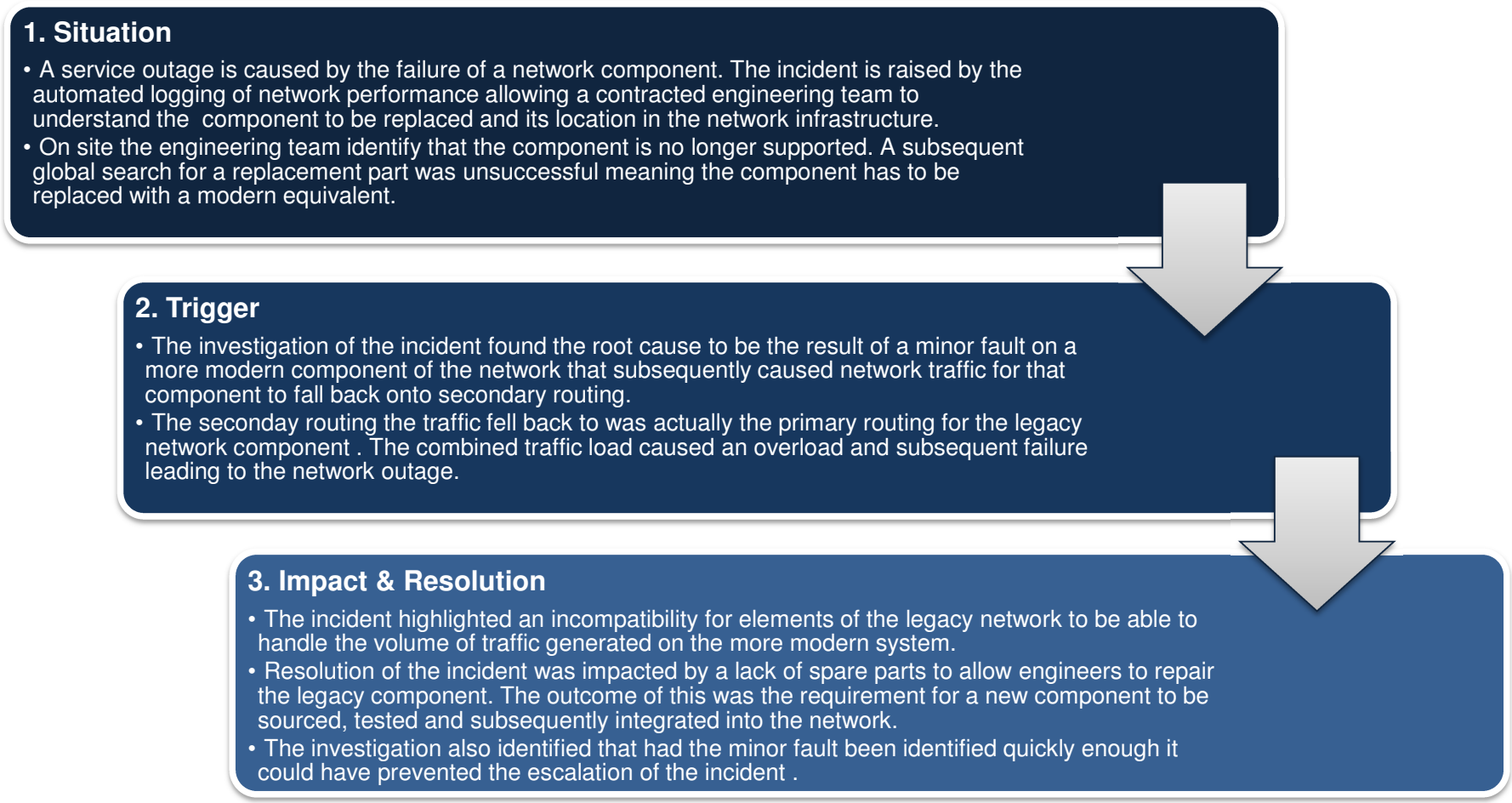

Figure 10 – Increasingly Ageing Estate Scenario

5.3 Scenario 3 – Lack of Vendor Variance

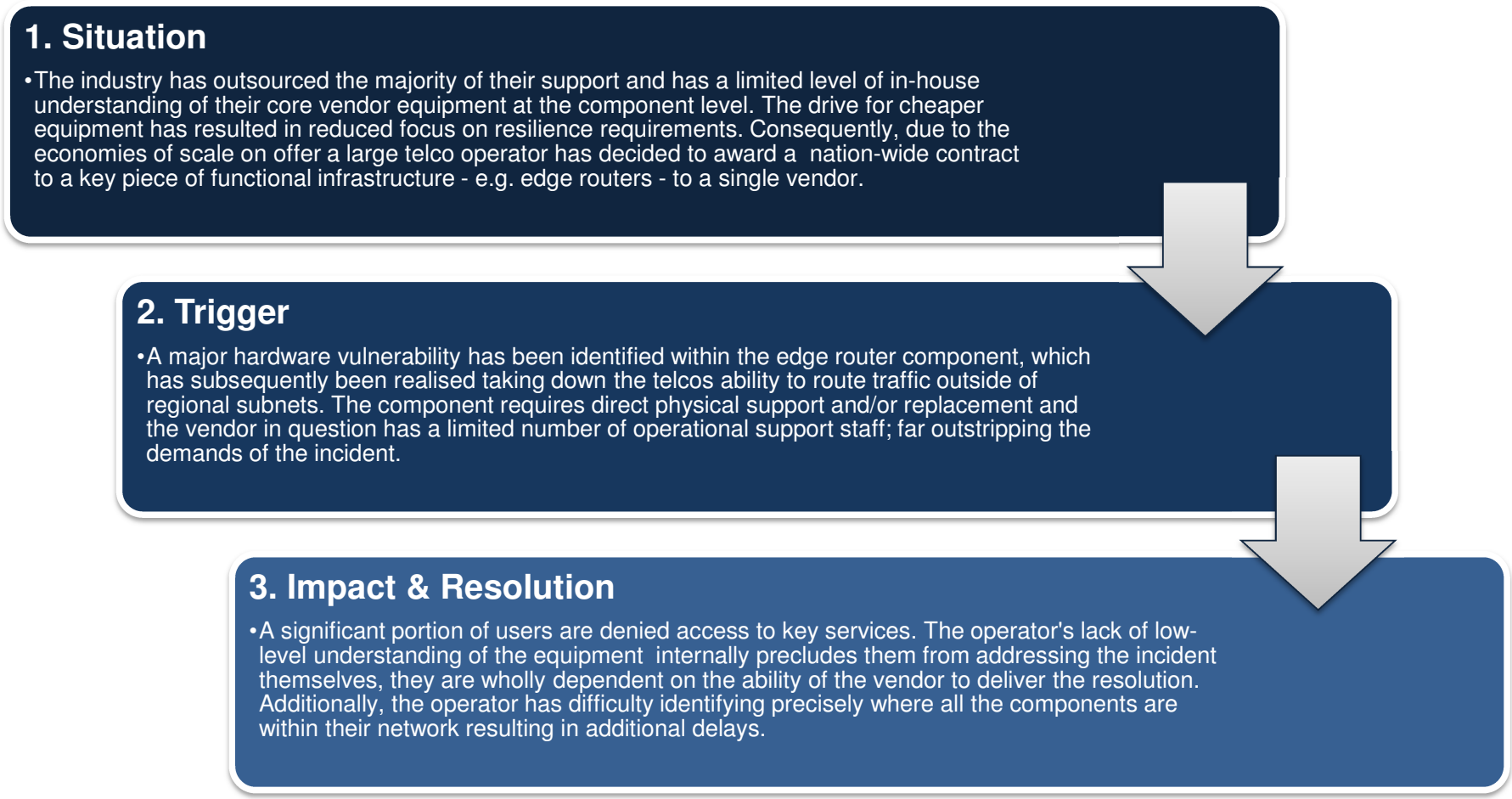

Figure 11 – Lack of Vendor Variance Scenario

5.4 Scenario 4 – Dependency on Small SME Companies

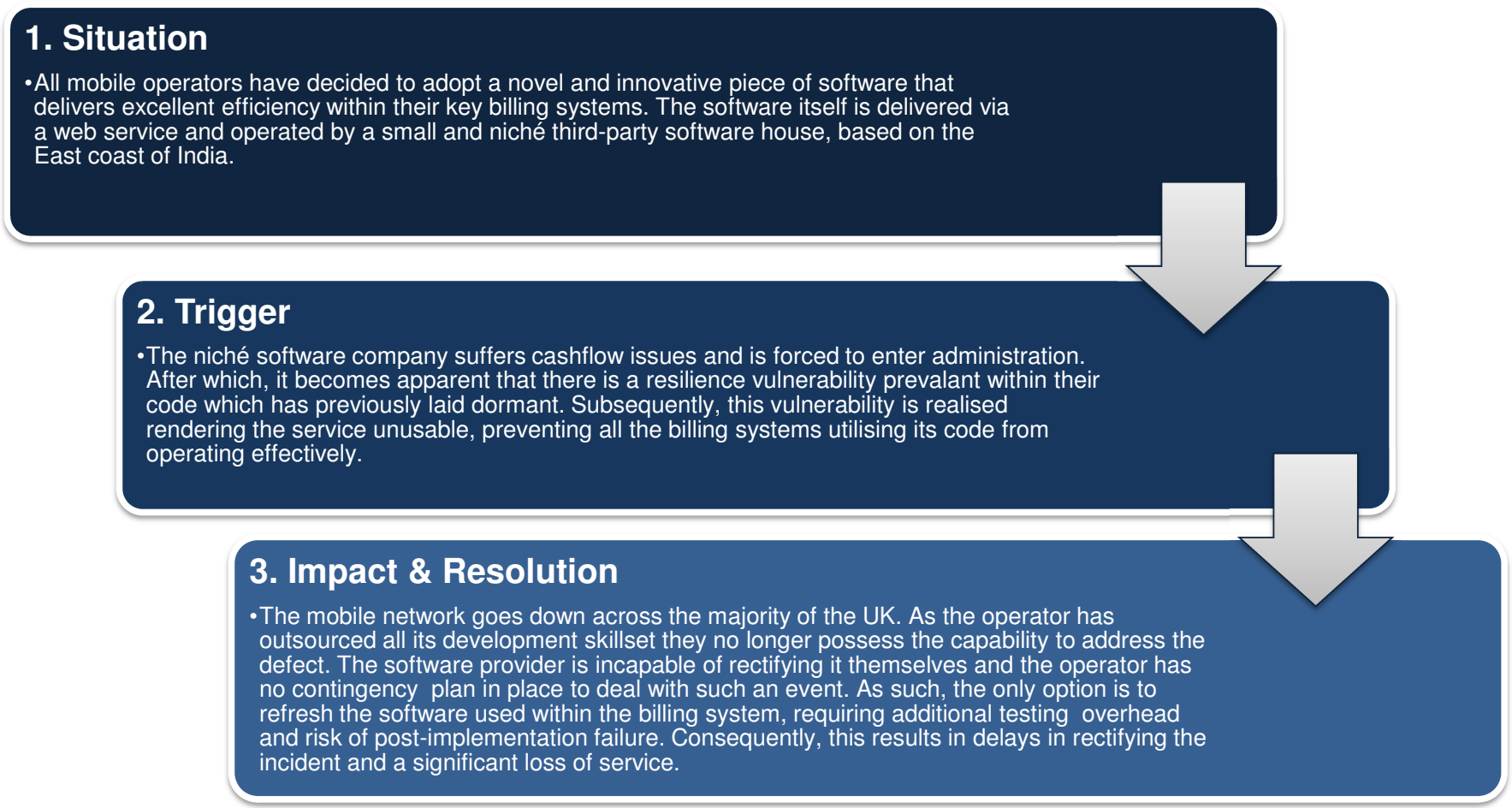

Figure 12 – Dependency on Small SME Companies Scenario

5.5 Scenario 5 – Unanticipated Disruption

Figure 13 - Unanticipated Disruption Scenario

6 Recommendations

We have made a number of recommendations for potentially addressing the vulnerabilities introduced as a result of the key industry trends and external factors identified through this report. These recommendations are purposefully set at a high level leaving Ofcom free to set the finer detail in a manner they feel to be most appropriate to the telecoms industry in the event the recommendation is adopted. We have split our recommendations into two categories based on the criticality of the vulnerability or issue they address and potential impact they might have in mitigating this.

6.1 Priority 1 Recommendations

1. Ofcom has issued a formal response to the addition of Section 105, parts A-D of the Communications Act 2003 and established a reporting process for telecoms providers to notify of security breaches. However, internal strategy on validating appropriate technical and organisational measures to manage risks to the network is not as developed. Ofcom may wish to consider progressing its approach to this element of the legislation in line with the breach reporting element.
2. The telecoms industry should be encouraged to improve their knowledge of the intra- and inter-dependencies that exist in the network. This should also incorporate understanding the full range of functionality of key components and ensuring there is appropriate disaster recovery and business continuity management in the event of component failure.
3. Ofcom could produce a list of security and resilience questions to be answered as part of the due diligence process of engaging with third parties either in the UK or offshore. This list could include specific sections addressing the most common functions contracted out to third parties such as code and application development and support services. It could also include a section on business continuity management plans in the event of the failure of the third party.
4. An information sharing initiative should be considered for network operators to centralise and archive their technical architecture. This would address a wide range of issues including the vulnerabilities associated with the current reliance on hard copy drawings;
5. A strategic threat assessment researching the nature and scale of reliance on hardware and software that is unsupported or deemed to be end-of-life should be considered.
6. An investigation into the extent of implementation and corresponding compliance, including capturing exemption registers to industry standards such as ND1643 should be considered.

6.2 Priority 2 Recommendations

1. Ofcom should consider requesting updates from service providers as to their expectations of the additional demand to be created by machine-to-machine services and their plans to mitigate this.
2. Ofcom could undertake a review of vendor diversification across the industry for evidence of risks posed by increasing uniformity. If needed this could be conducted at a number of different levels and also incorporate awareness and assessment of issues such as resilience in the supply chain.
3. A formal review of the regulators response to the introduction of EU legislation in each member country could be completed to inform Ofcom of the variance in response by country and the potential implications for network resilience where

transmissions originating in the UK are dependent on foreign networks; and of the range of options for consideration in enforcing Section 105, parts A-D.

4. In consultation with the industry and BIS Ofcom could help formulate a strategy to increase the skilled workforce to ensure the UK is able to fully exploit the potential benefits of a digital economy. This can include increasing awareness of the use and dependence on IP and the implications for networks from the introduction of 4G.
5. As network data is increasingly nebulous, for example stored in servers located outside the UK or in the Cloud this poses challenges to the traditional regulator model. Ofcom should consider undertaking a regular review of the extent to which regulated service providers adopt this model. It could also encompass recognition of the emergence of unregulated entities, either unique to telecoms provision or established in another industry and acting as a disruptive influence in the telecoms sector.

7 Conclusion

This assessment has uncovered 18 key existing, evolving and emerging trends within the telecoms industry as well as a diverse range of external factors that the industry has little or no control over their developments. Combined, these two fields, in conjunction with insights gained from interviews with our internal SME community and industry experts culminated in the identification of 30 existing and 18 anticipated vulnerabilities within the telecoms industry. In many instances anecdotal evidence exists that indicate these vulnerabilities have already been realised. The number of emerging trends and anticipated vulnerabilities suggests that the industry will continue to suffer, or worse still experience an increase, in the exploitation or realisation of vulnerabilities exposed to non-deliberate threats.

The telecoms industry is facing a turbulent time in the coming years due to the roll out of 4G across the UK and the on-going development of social and technological trends. In many ways the industry is becoming increasingly vulnerable to non-deliberate threats and the rapid pace of technological innovation and change should only serve to exacerbate their exposure. However, the industry largely recognises both the increasing threat environment and the importance of network – and correspondingly service – resilience to their business model. This is driving efforts to mitigate the most critical vulnerabilities but it does not appear to address the vast majority of vulnerabilities that are well established throughout the telecoms industry.

Many of the vulnerabilities can trace their foundations back to the multiple variants of networks that have been pieced together through historic mergers and technological developments. While the watch phrase for the industry could be ‘first do no harm to the network’, once components are successfully integrated the knowledge and asset management maturity of the industry means this is largely forgotten. The result today is a concoction of legacy and modern equipment that nobody is quite sure how it all fits together, or the full extent of functionality held by each respective component.

While the testing regime for new components is as comprehensive and thorough as the testing environment permits, it can never replicate the complexity and dependencies that exist in the production network. As the UK prepares for the implementation of another generation of network refreshes these intra- and inter-dependencies within the network are only going to increase in both number and complexity.

Positively there are signs that network insight is increasing. More modern components invariably include automated logging to monitor their performance and behaviour. The major challenge the telecoms industry faces is being able to successfully manage and interpret the ever increasing volumes of network logs. These have the potential to enable the industry to move from a position of reactivity in terms of incident response to a more proactive approach to management of issues. Effective and efficient log management will allow incident trends to be identified and addressed before they escalate into a critical incident affecting significant number of users with long investigative and remediation overheads.

Reducing the number and severity of security and resilience vulnerabilities in the telecoms network will require a combination of both the technology outlined above but also an evolution in culture. Legacy estates and bolt-on networks are in part a result of technological evolution but also symbolic of the poor rates of decommissioning within the industry. This also introduces issues with running components that are either end-of-life or no longer supported.

The second key culture change required is in the level of understanding held by the industry of the location, function and dependencies of their key components. The lack of this knowledge directly contributes to the creation of vulnerabilities that can subsequently be exploited and realised by non-deliberate threats. In the event of incidents occurring, this lack of knowledge is also contributing to extended investigation and resolution times. Better insight into the network will help enable the industry to recognise vulnerabilities and make the case for either accepting them or introducing mitigating countermeasures.

In summary, the majority of vulnerabilities present within the telecoms networks are as a direct consequence of continually merging infrastructures and bolting on functionality. However, this cannot be overly lambasted as it has likely been the only feasible approach to operate and deliver networks and infrastructure of this scale. As it stands there is a good community of sharing within the core telecoms providers, coupled with a genuine desire to manage and address resilience and security issues that not only affect their own networks, but also the wider infrastructure. After all, maintaining the availability of the wider network is paramount to their ability to remain profitable and deliver services to their customers.

Although there are likely to be numerous challenges ahead the industry has a focus and will to both recognise and address them wherever pragmatically possible. However, what must be kept in mind is that in the midst of growing media coverage and focus of malicious threats, vulnerabilities realised via non-malicious threat can have equally devastating consequences to operators, businesses, end-users, and ultimately the nation. The industry must ensure they do not lose sight of this, especially in light of the increasing national dependence on the long-standing operation of the core telecommunications infrastructure.

8 Abbreviations

Abbreviation	Definition
CNI	Critical National Infrastructure
DDoS	Distributed Denial of Service
HLR	Home Location Register
SME	Subject Matter Expert
MVNO	Mobile Virtual Network Operator
MVNE	Mobile Virtual Network Enabler
BC	Business Continuity
DR	Disaster Recovery
KPI	Key Performance Indicator
URN	Unique Reference Number
COTS	Commercial Off-the-Shelf
CDR	Call Duration Register
GCF	GSI Governance Framework
GSi	Government Secure Intranet
QoS	Quality of Service
HD	High Definition
PSN	Public Services Network
ATM	Asynchronous Transfer Mode

References

Aaudestad, J. a., 2003. Vulnerability of the Telecommunications. *Telektronikk*, Issue 1.

Baines, L. C. M. D., 2003. *The National Telecommunications Infrastructure: A 21st Century Organizational,* s.l.: U.S. Army War College.

Cowan, J., 2012. *http://www.m2mnow.biz/2012/07/17/6496-o2-uks-major-network-outage-is-put-down-to-hlr-systems-failure/.* [Online].

Engineering, R. A. o., n.d. *Extreme space weather: impacts on engineered systems and infrastructure,* s.l.: Royal Academy of Engineering.

Enisa, 2011. *Enabling and managing end-to-end resilience,* s.l.: Enisa.

George H. Baker III, P., n.d. A Vulnerability Assessment Methodology for Critical Infrastructure Facilities.

Group, E. C. R. &. R., n.d. *Telecommunications Networks – a vital part of the Critical National Infrastructure,* s.l.: s.n.

International Journal of Control and Automation, 2008. Common Threats and Vulnerabilities of Critical. Volume 1.

Ofcom, 2012. *Ofcom Tender No: ITT 27/2012.* s.l.:s.n.

Richard A. Caralli, J. H. A. P. D. C. D. W. W. &. L. R. Y., 2012. *CERT® Resilience Management Model,* s.l.: Software Engineering Institute.

Rontti, J.-M. T. &. T., 2011. *Unknown Vulnerability Management for.* s.l., s.n.

Secretariat, C. C., n.d. *ENSURING RESILIENT TELECOMMUNICATIONS,* s.l.: Cabinet Office.

T. H. Shake, B. H. D. M., n.d. Assessing Network Infrastructure Vulnerabilities to Physical Layer Attacks.

9 Annexes

9.1 Team Structure

The Detica team delivering this review comprised two full-time staff and two part-time specialist staff. The project team drew heavily on the SME pool within Detica as well as interviews with Telco Industry individuals. Ian Baglow acted as the commercial account manager for this engagement. Phil Huggins provided oversight of the project and in addition to his review the final deliverable was subject to review by an expert panel from Detica. This structure is shown in the diagram below.

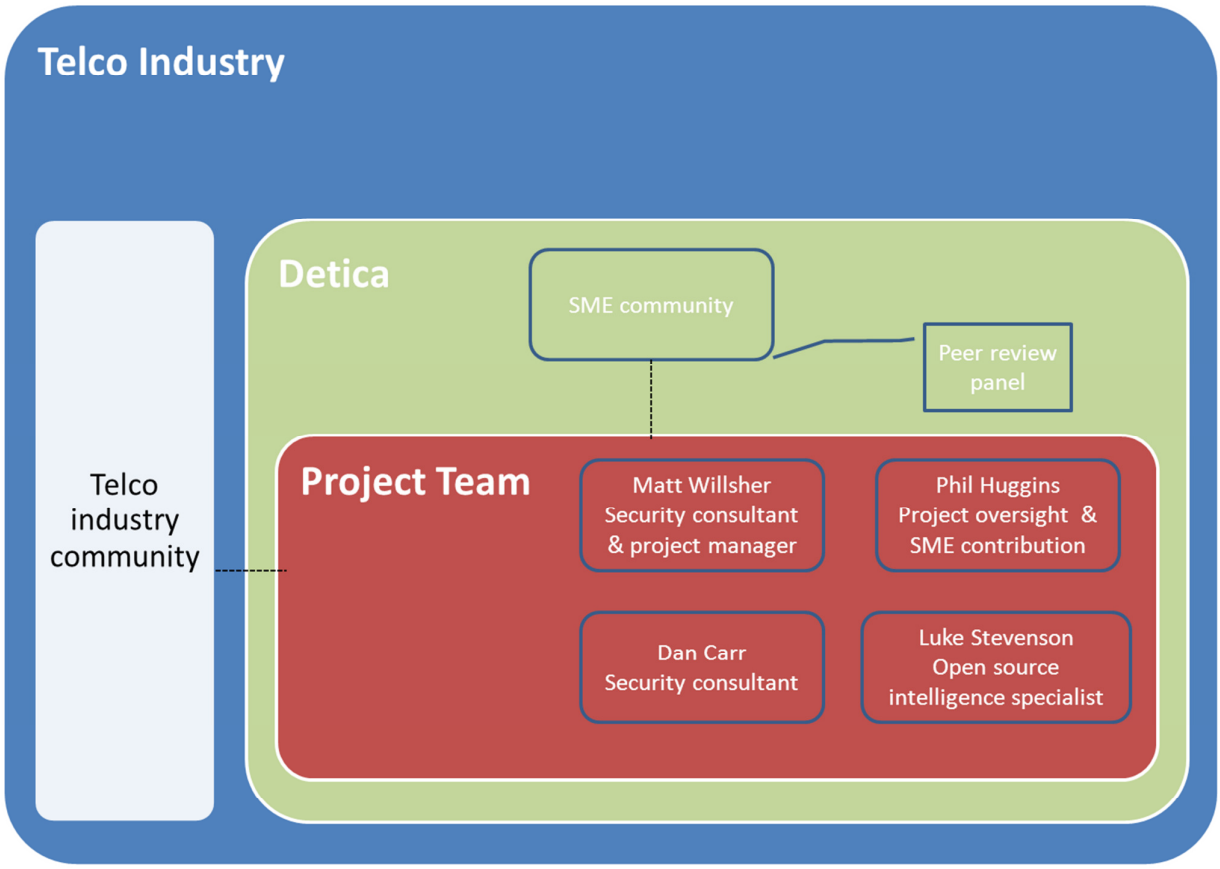

Figure 14 - Team Structure

9.2 Tables

9.2.1 Likelihood Table

Likelihood	Description
Extremely Unlikely	May occur only in exceptional circumstances. There are no known instances or anecdotes from across the industry of any incident occurring. Anticipated to occur once in more than 100 years.
Unlikely	Not expected to occur with very few instances or anecdotes of incidents industry-wide. Little opportunity, reason or means for incident to occur. May occur once in 100 years.
Possible	May occur at some time with irregular examples and anecdotes of incidents raised within the industry. Some opportunity, reason or means for incident to occur. May occur once in 20 years.
Likely	Considered likely to occur with regular recorded incidents in the industry and strong anecdotal evidence. Significant opportunity, reason or means for incident to occur. May occur once in 7 years.
Very Likely	Expectation that an incident will occur in the next year across the industry.

9.2.2 Impact Table

Impact Severity	Description
Insignificant	There is a minimal service disruption that a limited number of customers may experience or that may occur for a short period of time. It is unlikely the incident will be reported and investigating and remediating the fault is relatively quick and simple with no impact to service provision.
Minor	Exploit of the vulnerability has a limited impact on some customers, for a limited period of time or a combination of both. The incident results in minor financial and reputational damage to the service provider and goes largely unreported except on customer or specialist blogs, forums and chat rooms. Investigating and remediating the vulnerability is relatively simple and can be fixed with minimal outlay or disruption to the service.
Moderate	Realisation of the vulnerability will have an impact on service delivery to a significant but constrained (either by geography or service) number of users or for a noticeable duration. The impact will cause a large financial and reputational loss to the service provider and be reported in specialist and trade press. Remediation is relatively quick to implement but causes some disruption to normal service provision.
Major	Vulnerability exploit causes significant loss of service either by number of customers affected, length of service outage or a combination of the both. The impact will cause major financial and reputational loss to the service provider entailing coverage in the national press. Investigating and remediating the vulnerability requires large levels of resource and may cause disruption to service provision.
Catastrophic	Exploit of vulnerability results in catastrophic loss of service to customers by both number of customers affected and duration. The impact will cause large financial and reputational loss to the service provider entailing widespread coverage in national and international press. Investigating and remediating the vulnerability requires the application of significant levels of resource for considerable time and causes major disruption to service provision.