EC-RRG
Electronic Communications
Resilience & Response Group
Protecting Communications

EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure

Updated August 2018

Contents

1 Introduction

The purpose of these guidelines is to bring together a wide range of advice and guidance on agreed best practice in the establishment and maintenance of resilience within telecommunications networks and services, for those Communications Providers which are considered to be part of the UK's Critical National Infrastructure (CNI), either because of the scale of their operations or because they provide key services to other parts of the CNI. However, these guidelines do not represent regulatory guidance. In particular, it does not seek to clarify compliance with current UK regulation relating to Publically Available Telephone Services, since such services are provided by a wider group of Communications Providers than form part of the CNI. However, and for the avoidance of doubt, the voluntary guidelines are relevant to both fixed and mobile providers and networks.

These guidelines are not intended to cover all the actions that might be required in the event that resilience has been compromised and emergency remedial action across multiple providers and/or government is required. This topic is covered by the UK Telecommunications Industry Emergency Plan[1].
They are also not intended to cover any Orders that might be made by government in times of emergency, for example, those made under Part 2 of the Civil Contingencies Act, under Section 94 of the Telecommunications Act or Section 132 of the Communications Act.

These guidelines are not intended to be used to specify contractual obligations between Communications Providers and their customers and should not be used for this purpose. However, the Centre for the Protection of the National Infrastructure (CPNI) has published helpful guidance to customers on Telecommunications Resilience [2] and how to approach Communications Providers when seeking to procure resilient services.

2 Definitions

In these guidelines, the following definitions apply:

2.1 Resilience

The word 'Resilience' is to be interpreted in the broadest sense as the ability of an organization, resource or structure to be resistant to a range of internal and external threats, to withstand the effects of a partial loss of capability and to recover and resume its provision of service with the minimum reasonable loss of performance.

2.2 Communication Provider (CP)

"Communications Provider" means-

(a) a provider of a public electronic communications network;
(b) a provider of a public electronic communications service; or
(c) a person who makes available facilities that are associated facilities by reference to a public electronic communications network or a public electronic communications service;

AND who is considered to form part of the CNI.

[1] UK Telecommunications Industry Emergency Plan.
There is a national industry wide emergency plan which is owned and managed by the EC-RRG.

[2] Telecommunications Resilience:
https://www.gov.uk/guidance/telecoms-resilience

2.3 Public Electronic Communications Network (PECN)

"public electronic communications network" means an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public;

2.4 Public Electronic Communications Service (PECS)

"public electronic communications service" means any electronic communications service that is provided so as to be available for use by members of the public;

2.5 Electronic Communications Network (ECN)

"electronic communications network" means-

(a) a transmission system for the conveyance, by the use of electrical, magnetic, optical or electro-magnetic energy, of signals of any description; and
(b) such of the following as are used, by the person providing the system and in association with it, for the conveyance of the signals:
    (i) apparatus comprised in the system;
    (ii) apparatus used for the switching or routing of the signals; and
    (iii) software and stored data.

2.6 Electronic Communications Service (ECS)

"electronic communications service" means a service consisting in, or having as its principal feature, the conveyance by means of an electronic communications network of signals, except in so far as it is a content service.

2.7 Associated Facility

"associated facility" means a facility which-

(a) is available for use in association with the use of an electronic communications network or electronic communications service (whether or not one provided by the person making the facility available); and
(b) is so available for the purpose of:
    (i) making the provision of that network or service possible;
    (ii) making possible the provision of other services provided by means of that network or service; or
    (iii) supporting the provision of such other services.

3 Revision

These guidelines will be subject to review and amendment following consultation with the EC-RRG membership.

4 Guiding principles

Given the broad definition of Resilience, it can be seen to embrace:

(a) Good network design;
(b) Effective operational processes for normal network operations, management and maintenance;
(c) Appropriate processes to respond to a range of contingent risks.

All Communications Providers should maintain an ongoing programme of risk assessment and make plans and investments commensurate with the identified risks, taking into account both the likelihood of events and the impact of their occurrence. Communications Providers should take a holistic view of Resilience, so that it is seen as an integral part of a set of wider company processes, for example:

(a) Overall company Risk Management (ISO31000)
(b) Quality Management (ISO9001)
(c) Information Security (ISO27001)
(d) Business Continuity Management (ISO22301)

There should be management commitment to all these processes, with a clear line of responsibility and chain of command from the Board level right down to operational delivery.

In many cases, Communications Providers are not wholly responsible for all parts of the service they deliver. For example, they will often rely on interconnecting networks to reach all their customers, or be reliant on some common external facilities (e.g. the DNS system), or may procure underlying network services or infrastructure from other providers. In such cases, the overall resilience of their service is dependent on these other parties.

Communications Providers may seek Service Level Agreements and contractual arrangements to meet their overall resilience requirements, but it is far more effective to ensure that all such external suppliers take a similar and complementary approach to resilience management, as legally binding commitments might be of little real value in a crisis.

However endeavours should be made to regularly review these topics with their suppliers, partners or peers with a view to jointly understanding risk and agreeing the optimal management of those risks.

(a) Security and Resilience
(b) Business Continuity
(c) Disaster Recovery
(d) Quality of Service management
(e) Emergency Planning[3]

[3] Providers of Publicly Available Telephone Services have obligations relating to Emergency Planning under Condition 5 of the Conditions of Entitlement. They also have obligations under the Civil Contingencies Act 2004 as Category 2 responders.

5 Regulation

The national regulator for the communications sector in the UK is Ofcom, who will decide whether any given provider is compliant with obligations that are set out in UK legislation.

These guidelines do not address compliance to this legislation or regulations.

6 Risks to Resilience

While it will be for each provider to assess its own risks and appropriate measures to provide and maintain resilience, there are a widely accepted set of risks that Communications Providers face.

In summary, they can be grouped into 6 headings:

(a) Physical Threats
(b) Personnel Threats
(c) Cyber or Technological vulnerabilities
(d) Loss of key inputs
(e) System/Logical failings
(f) Electronic 'interference'

Industry should continue to be guided by the planning assumptions relevant to national risks such as major power loss or pandemics. [4]

6.1.1 Physical Threats

These include:

(a) Natural phenomena (Extreme weather, earthquake, flood and lightning);
(b) Fire
(c) Explosions, in particular those caused by gas leaks;
(d) Damage caused by accidents, vandalism, internal sabotage and terrorism.

6.1.2 Personnel Threats

These include:

(a) Insider threat (including the supply chain)
(b) Human Error
(c) Training, key skills, knowledge or resource availability
(d) Malicious acts and Hostile reconnaissance
(e) Negligence

---

http://www.legislation.gov.uk/ukpga/2004/36/contents

[4] National Risk Register
https://www.gov.uk/government/collections/national-risk-register-of-civil-emergencies

6.1.3 Cyber or Technological vulnerabilities

These include:

(a) System vulnerabilities (including software)
(b) Interworking or cascade vulnerabilities
(c) Capacity management/Overload controls
(d) Inappropriate protective controls to protect sensitive assets
(e) Separation or Segregation of networks, particularly management or control networks
(f) Review, testing and management of change (detection and prevention of misconfiguration)
(g) Hacking, Electronic interference (malicious or accidental)
(h) TEMPEST or other malicious acts

6.1.4 Loss of key inputs

Telecommunications depends on the continuous availability of many ‘key inputs’, amongst which the most critical are:

(a) Electrical Power
(b) Fuel (for backup generators and vehicle fleet)
(c) Human access (to operational installations)
(d) Materials

6.1.5 System/Logical failings

To prevent being vulnerable to the failure of a single part of the system, telecommunications companies are advised to assess the risks and invest, where practical, in duplicate or triplicate back-ups for their equipment (redundancy) and diverse transmission routings. Thus the ‘logical’ architecture of the service will be more resilient than the simple physical layout. But sometimes, due often to human error, these logical configurations can themselves fail to provide the expected level of security. The key is to avoid, wherever possible, ‘single points of failure’.

However, not all parts of the network can be made resilient and in these cases, the complementary processes of restoration and repair have to be strengthened.

6.1.6 Software failures

All telecommunications networks are reliant on software controlled equipment, and no software is immune from errors and operational failings. Unlike personal computers, it is not acceptable for a telecommunications network to crash and stop responding altogether.

A particularly worrying form of software failure is called a ‘systemic’ or ‘common-mode’ failure, where a software error in one network node causes the same fault to occur in other connected nodes, leading to a ‘runaway’ failure of an entire network.

6.1.7 Hacking, Electronic interference (malicious or accidental)

Telecommunications networks, especially those increasingly using IP technology, can be vulnerable to conditions entering the system via the network itself. Increasingly, these can be malicious in intent.

A wide range of types of threat fall into this category, including:

(a) Inappropriate signals injected by users, either too high a voltage or at the wrong frequency;
(b) Electromagnetic Pulses and Emissions (EMP and TEMPEST [5])
(c) Similar signal pickup problems caused by radio interference, e.g. from amateur radio transmissions;
(d) Traffic overloads, often stimulated by advertising campaigns and TV based promotions;
(e) Denial of Service attacks – malicious attempts to damage a service, sometimes by traffic overload, sometimes by the transmission of 'malware' (malicious software);
(f) Other impacts of 'malware' , such as viruses, worms and Trojans;
(g) Hacking, including attempts to subvert the proper operation of the billing system in networks;
(h) The transmission of specifically crafted signalling messages, designed to cause mis-operation of the network

7 Specific Recommendations

7.1 Design considerations

7.1.1 Physical

(a) A secure environment is a key factor in the maintenance of an adequate telecommunications service. The protection given to a building should be assessed and complement other controls in the "Security Procedures Telecommunications Systems and Services" [6]
(b) Wherever reasonable, essential equipment should not be concentrated, particularly in one building, to the extent that overall network security is jeopardised. Where essential equipment is co-located (for example, at multiprocessor sites), priority should be given to physical separation, such as a fire break, to reduce the possibility of common mode failure.
(c) Underground line plant, buried at a depth where intrusions are unlikely, is preferable to aerial line plant.
(d) The location of all external line plant such as underground and aerial cables should be notified to the relevant authorities as and when appropriate.
(e) Suitable processes should be in place to co-ordinate the activities of the various utilities and highway authorities to ensure that risk of damage is minimised.
(f) All sites, including radio mast sites, need to be secured against malicious attack and other forms of physical interference. Sites should also be capable of withstanding relevant environmental conditions. In particular, antenna masts should be designed to withstand likely wind and ice loading.
(g) Where appropriate, diverse entry and exit points, e.g. to sites or buildings, should be provided (including cable entries).

[5] TEMPEST and Electromagnetic Security
https://www.ncsc.gov.uk/scheme/tempest-and-electromagnetic-security

[6] Security Procedures Telecommunications Systems and Services
https://www.ncsc.gov.uk/content/files/Security_Procedures_Telecommunication_Systems_and_Services__-_issue_3.0_Dec_2015.pdf

(h) Where appropriate, use should be made of diverse duct tracks or routes (NB: Physical separation on its own does not deliver guaranteed availability, and this is usually achieved by a combination of physical separation, redundancy and resilience.
(i) Public telephone boxes should be positioned to minimise risk, for example from road accidents or vandalism. Street furniture such as cabinets should be similarly positioned and also be locked or sealed.
(j) Poles should ideally be placed in the lowest risk positions consistent with their use. The positioning of aerial cables and drop-wires is subject to broader regulation and must be installed to ensure adequate clearance of vehicles, land and buildings. Poles should be regularly surveyed to ensure their physical integrity and to assess new risks, e.g. tree growth.
(k) Where ventilation or air conditioning is used, single failure should not hazard the facility.
(l) Essential cooling for facilities should be appropriately secured against failure.
(m) Buildings should be secure against entry by unauthorised people. An adequate level of building security shall be demonstrable and commensurate with to the assessment of levels of risk and vulnerability. Secure entry systems, movement detectors and video surveillance may be necessary, and both perimeter and cellular security may be appropriate in large buildings.
(n) Equipment should be carefully sited within buildings to provide physical separation and protection where required.
(o) Processes should be in place to reduce the risk of equipment failure due to building and civil engineering works. Communications Providers should make information available on planning consents and cable routing (where necessary providing a helpline to deal with inquiries). Communications Providers should keep themselves informed about activities of other parties which may present a risk to network security.
(p) Where appropriate, suitable detection and extinguishing systems for fire, detection systems for explosive and asphyxiating gases and floods are recommended. For fire detection, current experience suggests that aspirating systems are superior to fixed head detectors, particularly where airflows are influenced by forced air conditioning. Fire extinguishing systems (for example water, misting or gas dumping) may be appropriate in certain circumstances but current experience suggests that none of these are particularly suitable for very large operational areas.
(q) Where normal maintenance access to a site may be jeopardised because of bad weather, arrangements for use of suitable alternative transport should be covered by the contingency plan (e.g. four-wheel drive vehicles, 'snowcats' and helicopters]. At sites prone to flooding, building utilisation should be such that the least critical functions are performed in the areas of highest risk.
(r) For sites hosting or supporting critical services, where these locations are within the Environment Agencies Extended Flood Outline, or where sites have experienced flooding historically, special considerations should be made to ensure the critical services can be maintained during a flooding incident (the service may be supported by delivery from an alternative site which should not be exposed to the same set of risks as the primary site) the impacts of flooding to key inputs should also be considered (Energy inputs such as Electricity, Fuel oil and Human access)

7.1.2 Key inputs: Power

Key inputs: Fuel

(a) The power supply to key equipment should not be interrupted in the event of a mains power supply failure.

(b) The mains supply should be secure and steps taken to ensure that it is reliable. For major sites, it may be appropriate to acquire diverse feeds of mains supply.
(c) The standby power supply should be of sufficient capacity to fully support the operational power load in the period between power failure and the cut over to any alternative supply which is available.
(d) Where power is provided by batteries, the battery capacity should be specified to maintain service for an appropriate duration at any stage in the battery design life.
(e) The duration and reason for the chosen duration should be documented. All batteries should be maintained to manufacturers' recommendations, taking account of expected lives as well as any recommendation to fully discharge batteries on a regular basis.
(f) Standby power systems should be exercised to ensure that they perform satisfactorily under failure conditions. Wherever possible, the security of mains supply should be supplemented with an alternative supply, e.g. diesel generators. These should be regularly tested and supported by an appropriate maintenance regime.
(g) Supporting processes should be in place to support extended power supply failures, for 7 days minimum for disruption to power supplies.
(h) At sites where it is not practical to provide an alternative on-site supply (i.e. diesel generators), battery capacity should be designed to cover the maximum likely interruption of the mains supply or the time to travel to site with portable generating equipment.
(i) There should be adequate arrangements to ensure that a supply of fuel for back-up generators is available, with contracts in place for replenishment.[7]

7.1.3 Key inputs: Human access

Systems should be designed to maximise the potential for remote operation. Designs for redundant networks should take into account the possibility of loss of human access to a site. In cases where human access is temporarily restricted, procedures should be in place to notify staff who would normally work at a given building or site. Contingency plans should cover the liaison with emergency responders[8] concerning access to maintain essential services. Considerations should also be made to the risks identified in the National Risk Register, for example Human pandemics which may have a direct bearing, but also Animal health (which may result in control cordons restricting access) or Volcanic activity (which may result in people being stranded or prevented from travelling to site or spare part availability)

When designing provision for alternative sites for fallback of control centres or other operational centres, consultation is recommended with the communication service provider to ensure expectations of communications provision or coverage are realised at the fallback site for the scale of fallback anticipated.

[7] Preparing for and responding to energy emergencies
https://www.gov.uk/guidance/preparing-for-and-responding-to-energy-emergencies

[8] Preparation and planning for emergencies: responsibilities of responder agencies and others
https://www.gov.uk/guidance/preparation-and-planning-for-emergencies-responsibilities-of-responder-agencies-and-others

7.1.4 Key inputs: Materials

Adequate stocks of spare parts and consumable materials should be kept on site or at a convenient depot within a short travelling time to site. Additionally, contracts may be in place with suppliers to hold buffer stocks on behalf of the Provider. Particular care should be taken for items sourced from overseas in case of transport disruptions.
Security risks posed by the supply chain should be considered.[9]

7.1.5 System/Logical failings

Overall resilience of the network and services should be delivered through an appropriate combination of resilient equipment, redundancy, restoration and repair:

(a) Resilient equipment means that it is designed to be inherently reliable, secured against obvious external threats and capable of withstanding some degree of damage;
(b) Redundancy means that back-up systems duplicating the functionality of the systems are available to take over in the event of failure;
(c) Restoration means that the capabilities are in place to replace a failed system with a working one;
(d) Where redundancy and restoration are not possible, repair processes are critical; and
(e) It is acknowledged that redundant design is easier to achieve in the core or long distance networks, where switches can provide mutual redundancy. Closer to the customer (for example at a local concentrator or multiplexer), fast restoration and repair become more critical.
In particular, Communications Providers should:

(i) Use reliable apparatus and systems (sourced from capable suppliers) designed to prevent or withstand the effects of extreme conditions, including the loss of public power supplies;
(ii) Give particular attention to the security of 999/112 emergency and safety of life traffic, for example by using techniques such as priority routing, repeat attempts, alternative routing and trunk reservation, and by avoiding dependence on a single set of premises for dealing with emergency traffic;
(iii) Have a recovery plan in place against the event that network failure occurs; and
(iv) Consider the security of both traffic and signalling links.

Signalling routings should be engineered to avoid known problems caused by asymmetric and circular routings, which can occur where Signal Transfer Points (STPs) are used.

[9] Supply Chain security risks
https://www.cpni.gov.uk/supply-chain
https://www.ncsc.gov.uk/guidance/cyber-security-risks-supply-chain

7.1.6 Software failures

Where equipment is software controlled, the software should be designed to be 'non-stop' or to restart automatically. It should be designed to minimise the possibility of a software error propagating throughout the system or to other equipment and be secured against unintended external interference.
In order to avoid 'common mode' or cascade failures, consideration should be given to dual plane or dual meshed networks provided by different suppliers.

7.1.7 Electronic 'interference'

(a) Communications Providers should plan accordingly to mitigate these threats. Such threats include:
    (i) electrical conditions – It is expected that Communications Providers will use apparatus at network interfaces that can withstand or prevent onward transmission of electrical signals or conditions that are outside normally expected operating values;
    (ii) signalling – It is expected that Communications Providers will minimise the impact of inappropriate signalling messages which may cause mis-operation of the network or billing systems; and
    (iii) traffic loads – It is expected that Communications Providers will apply network management controls to limit the impact and onward transmission of excessive traffic volumes, but no more than is reasonably required to maximise the establishment of effective calls or timely data connections.

(b) Communications Providers should consider what protection may be necessary on metallic circuits from accidentally applied voltages, current surges associated with earth potential differences[10] and lightning strikes.
(c) Terminal equipment (TE) may cause a safety hazard by presenting an excessive voltage to the network. The presentation of high voltage to the network termination is clearly only applicable to fixed networks and should only occur after serious TE failure. The threat this presents to the network should be limited to the local loop, as the network should be self-protecting to prevent more extensive damage and reduce the risk to network maintenance staff.
(d) Communications Providers should be aware that TE may under certain circumstances inject incorrect signalling information. Conducted or radiated emissions including those from TE may affect fixed networks. They should penetrate no further than the local loop, albeit possibly affecting adjacent circuits.
(e) Communications Providers should also be aware that under certain circumstances, service-affecting problems can be caused by ingress into the telecommunications system of radio signals. The use of mitigating measures (e.g. filters) may be useful to resolve such problems.

[10] Rise of Earth Potential at Electricity Stations
http://www.energynetworks.org/assets/files/electricity/engineering/telecoms/eitc/restricted/Specification_edits/S36/s36.pdf

http://www.energynetworks.org/assets/files/electricity/engineering/telecoms/eitc/restricted/eitc_docs/eitc38m/OpenReach%20EROP.pdf

7.1.8 Inappropriate use of signalling protocols

(a) Communications Providers should comply with any relevant technical networking standards, incorrect signals received from outside can interfere with the correct operation of the network. Such signals might be benign in intent and be caused by accidental miss-operation of other equipment. However, they may also be caused by deliberate attempts to interfere with the network, for example to avoid the proper charging for network services (phone fraud), to deny service to others, or to corrupt stored data or software. Multiple levels of security may be needed to counter such threats, including signalling 'policing', firewalls, etc. including liaison with relevant information exchanges[11]

(b) TE may under certain circumstances inject incorrect signalling information. The network should be self-protecting and ignore incorrect signalling from TE which does not conform to the expected protocols. Nonetheless, such signals may interfere with or mask legitimate information. Correctly formatted but erroneous signalling may be more dangerous to the network, for example malfunctioning automatic dialling equipment congesting the network with unwanted calls.

(c) Communications Providers are encouraged to implement Calling Line Identity (CLI) in accordance with relevant Codes of Practice to assist, with tracing the source of interfering signals and fraudulent or malicious calls.

(d) Communications Providers should consider appropriate measures to ensure that their networks can be protected from signalling problems in an interconnected network. Screening (also known as policing) is a technique that can be used, if appropriate, at the edge of the network to protect it from mis-operation of connected networks. Candidate areas for screening that Communications Providers should consider as necessary might be:

(i) Interconnect screening – there are good grounds for providing screening of an interconnect link so that only agreed use of the interconnect is allowed; and

(ii) Policing is also used to reduce the incidence of false 112/999 calls to Emergency Organisations. Communications Providers should ensure that genuine emergency calls are not rejected by this policing.

(e) Intra-network signalling screening may not be necessary as modern protocol specifications contain sufficiently robust error handling procedures. Access screening may be inherent in the protocol conversion done in the traditional telephone network by the local exchange, but with more transparent IP networks, specific access screening measures may be needed.

7.1.9 Resilience issues for IP networks

(a) IP based networks (and some other data systems) present an increased level of threat from electronic interference because there is no physical separation of the communications paths and signalling paths as there is in traditional telephone networks with common channel signalling.

(b) Traditional IP networks exhibit significant levels of inherent resilience, but nevertheless like any network can have single points of failure, particularly at the edge. The resilience of IP networks is also traditionally dependent on the whole resource of the public Internet, much of which may be outside the management control of a given Communications Provider. Changes in routing patterns to reflect available resources can take a considerable time to stabilise (convergence time) and this can be

[11] Telecommunications Fraud Forum
http://www.tuff.co.uk/

detrimental to services requiring very high levels of availability. Communications Providers should therefore plan their resilience measures to provide managed domains under their own control with predictable and rapid configuration arrangements. IP reconfiguration can be avoided, in part, by utilising the restoration capabilities of any underlying transport layer, whether traditional SDH/ATM or Optical Switching, but steps should be taken to prevent 'races' between the different restoration arrangements.

(c) Although IP networks can work with random interconnectivity, resilience is assisted by providing a defined hierarchical architecture to the network, as between, for example, edge, metro and core nodes. Similar links within the hierarchy should use similar bandwidths, or the value of restoration routings will be diminished. 'Short cuts' across the hierarchy should be avoided. By creating network routings which are inherently predictable, Communications Providers can avoid the need for complex modelling of network behaviour.

(d) Core managed domains benefit from the use of Interior Gateway Protocols with link state routing protocols such as IS-IS and OSPF. Load sharing across multiple equal cost paths should be used wherever possible. Link costings and metrics should be designed so that routers lower in the hierarchy are never used to tandem traffic between routers higher in the hierarchy.

(e) Border gateways not only separate internal and external routingdomains, but can provide important firewall capabilities. Deep packet inspection can be used to provide more detailed screening.

(f) Aside from its other advantages, Multi-Protocol Label Switching (MPLS) can aid resilience by separating traffic of different levels of importance and providing highly predictable network routings.

(g) Communications Providers should take full account of advice and warnings promulgated by the government's Computer Emergency Response Team (CERT) now part of the National Cyber Security Centre NCSC [12]

(h) Communications Providers should take full account of guidance on the deployment and management of Border Gateway Protocol, used in the Internet [13]

(i) Communications Providers should take appropriate precautions to guard against and respond to hacking and electronic attack. Communications Providers are encouraged to make use of appropriate industry fora to co-operate on these issues, in particular the CPNI Security Information Exchanges [14]

7.1.10 Terminal equipment

Instances have been given above where TE may pose a threat to network integrity. Physical disconnection of fixed line TE can protect the integrity of the network from risks posed by TE.

[12] NCSC
https://www.ncsc.gov.uk/

[13] BGP guidance
https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-54.pdf

[14] General guidance
https://www.cpni.gov.uk/content/identify-threats
https://www.ncsc.gov.uk/cisp
https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

7.1.11 Excessive traffic loads

(a) Networks need to be protected from traffic overload conditions. Network traffic management (NTM) is a set of tools and techniques for detecting, monitoring and controlling network traffic to protect the network from abnormal loads, while at the same time optimising network performance. While NTM is capable of dealing with mass calling behaviour, it is recognised that complete service denial or disconnection may be required to control excessive traffic from (or to) a single customer.
(b) Communications Providers should adhere to the following NTM principles in protection of essential service:

    (i) Maximise the number of trunks filled with effective calls (i.e. calls which can be carried to their destination), rather than non-effective calls (i.e. calls which encounter congestion and cannot be carried to their destination);
    (ii) Give priority to single link calls, rather than calls going via alternative routes. During overload, more calls attempt to go by alternative multi-route links, which greatly increases the possibility of these calls blocking other call attempts. All or a portion of alternative route traffic can be blocked;
    (iii) During abnormal overload conditions, use any temporary idle capacity in the network to reroute traffic;
    (iv) Prevent switching congestion caused by large traffic or data volumes, to prevent the spread of congestion to connected systems; and
    (v) Give priority to terminating traffic over origination of new traffic or data flows.

(c) Communications Providers should give effect to these principles by:
    (i) Protective controls that remove traffic from the network as close as possible to its origins during overload, such as ‘call gapping’; and
    (ii) Expansive controls that re-route traffic from overloaded routes or failures to other parts of networks that are under-loaded with traffic because of different busy hours, such as ‘alternative routing’.

(d) Communications Providers should ensure a technical congestion control processes are in place to enable graceful control of overload or congestion events, further details are below which encompasses the non-technical preventative measures.
(e) Communications Providers should have:
    (i) An NTM centre to provide real time surveillance of the access and transport network and to implement traffic controls;
    (ii) Arrangements in place with their customers for the notification of planned mass calling events e.g. TV show phone-ins;
    (iii) Arrangements in place to inform interconnected Communications Providers of planned and detected mass calling events;
    (iv) Knowledge of national holidays and festivals (e.g. Christmas Day, New Year’s Eve);
    (v) Knowledge of holidays and festivals in distant countries to which they operate direct links; and
    (vi) An awareness of, in real time, news reports that may stimulate traffic (e.g. natural disasters).

(f) It is accepted that in some cases, Communications Providers with small networks consisting of only one or two switches may choose not to invest in NTM facilities but instead rely on controlling their interconnect with other networks that do provide NTM.

(g) It is recognized that congestion can be created in one network, and have an impact on a competitor's network due to network interconnection. If steps are taken in the affected network to reduce the impact of excessive traffic, typically by call-gapping, it is conceivable that another Communications Provider may have cause to complain that its ability to carry revenue-earning traffic is restricted. Conversely if no action is taken the affected network could fail. It is important for Communications Providers to understand that good network traffic management actually maximises the effective (i.e. revenue-generating) call capacity of the network. It is therefore expected that:
    (i) All Communications Providers will document what congestion protection measures will be used (for example: call gapping, alternative routing and priority techniques) and in what circumstances. Any such documentation should be made available to other Communications Providers with a legitimate interest;
    (ii) All Communications Providers will also document what measures will be used to ensure the priority of 999/112 traffic, particularly during congestion periods; and
    (iii) Signalling links will be dimensioned to avoid congestion and will in general have much lower occupancy than traffic links. This is due to the importance of minimising the risk of losing signalling messages and the need to reduce signalling latency. The number of signalling links should be established for normal and failure conditions, and some form of planning tool may be required to determine the signalling relationships supported by a given linkset except in very small networks.

(h) The above advice relates mainly to traditional circuit-switched telephone networks. In future, it may also be relevant to the control of session-based connections in IP networks, such as telephony. However, there are a number of differences with generic IP networks. These include:
    (i) To a degree, the TCP/IP protocol has an inbuilt ability to pace connections according to the load on the system;
    (ii) Unlike telephone networks, IP networks may be carrying many classes of traffic, with different holding times and arrival behaviours (often fractal in character);
    (iii) Different Qualities of Service may be defined for different classes of service, so pre-emption is a possible technique to manage excessive loads, with delay tolerant services giving way to ‘real-time’ services.

7.2 Operational Processes

7.2.1 Network management systems

(embracing operations, administration and maintenance) allow the remote control and surveillance of communications networks. Network management plays a vital role in maintaining resilience by providing data on events and alarms in the network, allowing the Communications Provider to take corrective actions as required. The appropriate use of statistical data collection is an essential part of network management. Properly designed network management and procedures should mitigate losses due to internal and external events.

7.2.2 Operational Processes

Communications Providers should have effective operational processes in place, covering at least the following areas:

(a) fault management;
(b) planned works and planned maintenance;
(c) configuration/change management;
(d) performance management;
(e) security management; and
(f) traffic management.

7.2.3 Fault Management

For fault management to be effective, Communications Providers should have systems and processes for fault detection, fault monitoring, finding the cause of faults (Root Cause Analysis), bypassing faults to maintain network performance and fault fixing.

It is considered that:

(a) Communications Providers should be fully informed about the status of its network at all times, including the status of the network itself and all related buildings and equipment on which the network is dependent;
(b) Communications Providers should make use of information derived from customer-reported faults and complaints to identify network faults;
(c) competent personnel, data and technical equipment should be available for fault management 24 hours a day;
(d) there should be points of contact and escalation procedures to guarantee an equitable and timely response to faults;
(e) a clear process should be in place for the systematic analysis of the causes of faults, for example: observation of symptoms, development of a hypothesis, testing of the hypothesis and the formation of conclusions;
(f) Communications Providers should develop and operate a maintenance manual including agreed response times for different fault conditions as well as indicative restoration or repair times and procedures; and
(g) Communications Providers should prioritise service restoration over clearance of faults not affecting service.
(h) In the case of interconnected Communications Providers, it is expected that:

(i) any party becoming aware of an interconnect service fault will inform all other associated operators, and
(ii) in such an event, prompt action to resolve the fault should be taken by the party in whose system the fault has arisen.
(iii) The management of planned maintenance and faults between interconnected operators should be part of more general operations and maintenance (O&M) procedures between interconnected operators.

7.2.4 Notice Periods

Communications Providers should provide reasonable notice to the affected parties of any planned work (including maintenance) that carries significant risk of impairment to essential services.[15] Except is when an emergency change is required to maintain the security or stability of the network.

[15] Planned outage notification to customers ITU-T M.1541
https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-M.1541-201101-I!!PDF-E&type=items

7.2.5 Change and Configuration Management

Good configuration/change management entails keeping a reliable inventory of network resources and having documented robust processes for the allocation of resources and management of changes that may pose significant risks to the continued delivery of services.

7.2.6 Performance Management

Effective performance management involves the use of data from the network management system and elsewhere to monitor network performance, to gauge performance against specified standards and to manage call carrying capacity to meet specified grades of service. On this point, reference should be made to other sections in these guidelines relating to traffic management.

7.2.7 Security Management

Effective security management in this context involves personnel, systems and processes that control access to both the network itself and the network management system and related assets. This includes user authentication, encryption, and access management processes. The security management regime should have a holistic approach across Physical, Personnel and Technological or Cyber realms.[16]

7.2.8 Risk Management

Effective risk management in this context involves assessing the design requirements of process, procedure, networks, systems and services, identifying any vulnerabilities or shortfalls assessing potential impacts and where appropriate designing mitigating controls to manage those risks where they have been assessed as posing a significant threat to continued operations.

7.2.9 Traffic Management

Real time traffic management involves the ability to gather data from various parts of the network to allow judgements to be made concerning real time call routing options. This may also include the gathering of data from signalling links, PSTN/Internet gateways and interconnect routes with other Communications Providers.
A network management centre should not be a potential cause of catastrophic failure of the network. Communications Providers should consider the desirability of geographically separate network management centres, based on an analysis of costs, benefits and risks.

7.2.10 Testing

Communications Providers should have procedures for testing the network, including provocative testing of network components as appropriate. It is recognised that it is impossible to test something as complicated as a modern telecommunications network with complete certainty. Therefore Communications Providers should be able to demonstrate that potential failure scenarios have been envisaged and that contingency plans for service restoration have been prepared tested and are in place. The objective of the contingency plan should be to maintain the Communications Provider's ability to fulfil, as a minimum its service obligations in the event of network failure.

[16] Security guidance
http://www.cpni.gov.uk and http://ncsc.gov.uk

8 Business Continuity and Emergency Planning

It is not intended that these guidelines covers all aspects of Business Continuity and Emergency Planning.

The EC-RRG has developed a series of Best Practice statements in this area. These are appended at Annex A. Many of these are similar to statements within these guidelines, but cover more aspects of Business Continuity and Emergency Planning.

9 Conclusions

These guidelines should provide appropriate guidance for Communications Providers to decide how to establish and maintain appropriate levels of resilience in their networks consistent with being part of the CNI.

10 Annex A

Business Continuity and Emergency Planning

Industry Standards

ID	Industry Standard
UKBC 1-1	Network Operators and Service Providers should formally document their Business Continuity process. Key areas for consideration include: Process Description, Plan Scope, Assumptions, Dependencies, Responsibility, Risk Assessment, Business Impact Analysis, Prioritisation, Plan Testing, Training and Plan Maintenance.
UKBC 1-2	A successful Business Continuity Plan requires executive support and oversight. Network Operators and Service Providers should establish an executive steering committee (composed of executive managers and business process owners) to provide guidance and direction to the planning team.
UKBC 1-3	The Business Continuity Plan for Network Operators and Service Providers should address critical business processes (e.g., Call Completion, 999 Emergency Services, Provisioning, Maintenance, etc.), support functions (IT, Sourcing, Logistics, Buildings, etc.), Revenue Collection with the key business partners.
UKBC 1-4	The Business Continuity Plan for Network Operators and Service Providers should be formally reviewed on an annual basis to ensure that the plans are up-to-date, relevant to current objectives of the business and can be executed as written.
UKBC 1-5	The Business Continuity Plan for Service Providers and Network Operators should include a Business Impact Analysis (BIA) of the loss of critical operational support systems and/or applications and a Risk Assessment of potential loss due to man-made and natural disasters.
UKBC 1-6	During Incidents which result in the invoking of the Business Continuity Plan, Service Providers and Network Operators should establish a designated Emergency Operations Centre. This centre should contain tools for coordination of service restoration including UPS, alternate means of communications, maps, and documented procedures to manage business interruptions and/or disasters.
UKBC 1-7	Service Providers and Network Operators should establish a geographically diverse back-up Emergency Operations Centre. The diverse centre must have no dependency on the main designated Emergency Operations Centre, and the two centres must have no risks which could simultaneous affect both centres.
UKBC 1-8	Incident coordination and control in the emergency operations centre and at the incident site should be achieved through mirroring the three-tier Incident Command System used by the Emergency Services in the UK.

ID	Industry Standard
UKBC 1-9	Service Providers and Network Operators should regularly exercise their Disaster Recovery Plans. Exercise scenarios should include natural (e.g. flooding, fire) and man-made (e.g., nuclear, biological, and chemical) disasters.
UKBC 1-10	Service Providers and Network Operators should designate personnel to be responsible for producing and maintaining the Disaster Recovery Plans.
UKBC 1-11	Service Providers and Network Operators should make use of multiple alternative communication devices, systems and service providers for use by their critical people during emergencies.
UKBC 1-12	Service Providers and Network Operators should develop company specific protective measures that correlate with the threat levels identified by the UK Security Services.
UKBC 1-13	Service Providers and Network Operators should review their insurance requirements in order to maintain Business Continuity in the event of massive property damage or loss, incapacitation of senior officers, and other interruptive situations.
UKBC 1-14	Service Providers and Network Operators should conduct risk and threat analysis at critical network sites.
UKBC 1-15	Diagrams and drawings of network sites should be included in Business Continuity plan documentation. Drawings should be kept up to date as network changes occur.
UKBC 1-16	Service Providers and Network Operators should develop processes or plans to quickly account for all employees in or near the impact area of a disaster.
UKBC 1-17	Service Providers and Network Operators should have documented plans or processes to assess the damage to network elements, external plant, building infrastructure, etc. for implementation immediately following a disaster.
UKBC 1-18	Service Providers and Network Operators should always emphasise employee and public safety during all phases of recovery from an incident or disaster.
UKBC 1-19	Service Providers and Network Operators should maintain their participation in The UK Telecommunications Industry Emergency Planning Forum (EC-RRG) which includes advisory sessions, exercises, and training. They should review existing and proposed best practices and consider implementation.
UKBC 1-20	Service Providers and Network Operators establish liaison points with the relevant authorities (for example, Lead government department via EC-RRG or Local resilience forum's), such that in the event of a CBRNe related incident, response may be appropriately co-ordinated and trained responders engaged by those agencies may support any required installation/repair or related activity.
UKBC 1-21	Service Providers and Network Operators should provide disaster recovery contact information to the Industry Regulator for inclusion in the UK Plan for the Telecommunications Sector, and update this contact information as changes occur or at the request of the Regulator.
UKBC 1-22	Service Providers and Network Operators should implement development of a vital records program to protect those records that may be critical to restoration efforts.
UKBC 1-23	Service Providers and Network Operators should identify key individuals within their organisations that are critical to disaster recovery efforts. Planning should consider maximizing the availability of these individuals.
UKBC 1-24	Service Providers and Network Operators should develop disaster recovery plans that consider simultaneous Industrial Action during a period of disaster recovery.
UKBC 1-25	Service Providers and Network Operators should consider creating a threat and risk assessment team to quickly determine appropriate actions both pro-active or re-active to address potential or real threats
UKBC 1-26	Service Providers and Network Operators should create a remote system access strategy for use during disaster recovery.
UKBC 1-27	Exchange buildings should be equipped with on-site UPS systems and emergency power generation capability to provide an ongoing power supply in the event that commercial power is interrupted in order to ensure continuity of services. Periodic maintenance routines of the batteries and power generators including, but not limited to engine runs should be performed to assure stand-by power reliability

ID	Industry Standard
UKBC 1-28	Service Providers and Network Operators should run preventative maintenance programs for network site support systems including emergency generators, UPS, DC plant, HV, and fire suppression systems.
UKBC 1-29	Service Providers and Network Operators should ensure that an adequate number of portable power generators are available consistent with the size of the company's network operation and with due regard to the regularity of mains power failure.
UKBC 1-30	Service Providers and Network Operators should ensure adequate fuel, emergency maintenance and a defined re-supply plan are available for emergency power.
UKBC 1-31	Service Providers and Network Operators should enter into Mutual Aid agreements with partners best able to assist them in a disaster situation.
UKBC 1-32	The Business Continuity Plan for Service Providers and Network Operators should include a list of critical Equipment and third-party suppliers and business partners. In addition, it should contain an assessment of their ability to respond to a disaster and a review of individual contracts to determine what level of service is available during a disaster.
UKBC 1-33	Network Operators should develop a strategy for the deployment of emergency mobile assets such as switch equipment, transmission, cellular equipment, masts, microwave radio assets, Power Generators, for emergency deployment and service augmentation.
UKBC 1-34	Network Operators should ensure that all emergency mobile assets are maintained at the same level as the existing network infrastructure. Hardware and software maintenance should be assigned to designated technicians with the expectation that the emergency mobile assets will always have the most current hardware and software and be immediately available for deployment.
UKBC 1-35	Disaster Recovery exercises should include trial deployment of emergency mobile assets and should be conducted to train as many technicians and support personnel as possible in as realistic a manner as possible.
UKBC 1-36	Each Network Operator should determine in advance whether they will use line of sight systems (microwave radio, satellite communications systems etc.) to re-establish communications. If these technologies are to be deployed it is recommended that contingency designs be developed for each technology in advance, with personnel trained to install and optimize the systems. Lists of key personnel and telephone numbers for site access should be established to satisfy the ability to access this requirement.
UKBC 1-37	Service Providers and Network Operators should make use of disaster recovery management models with escalation procedures that provide a clear escalation path to executive levels both internally and externally.
UKBC 1-38	Service Providers and Network Operators should, during times of disaster, communicate the disaster response status frequently and consistently to all appropriate employees - so that they all understand what processes have been put in place to support customers and what priorities have been established in the response.
UKBC 1-39	Service Providers and Network Operators should verify that their Equipment Suppliers have escalation processes for support during disasters, including contacts with Logistics (who know what spare equipment is available in various depots, and how to ship it), Manufacturing (who may need to adjust the priority of what's being built and/or shipped) and Sales (who need to communicate their response plan and determine the customers' needs).
UKBC 1-40	Service Providers and Network Operators should have contact lists for the various specialist functions needed during disasters, so that equipment and skilled specialists can be deployed to disaster sites in the most significant cases.
UKBC 1-41	Service Provides and Network Operators should ensure their Equipment Suppliers provide a "Disaster Information Checklist", which will provide a set of questions which the Service Provider would address immediately after a disaster and then inform the Equipment Supplier to facilitate equipment delivery.
UKBC 1-42	Service Providers and Network Operator should consider deploying advanced technologies to address critical needs when responding to disasters.
UKBC 1-43	Service Providers and Network Operators should ask their Equipment Suppliers, during their response to major disasters, to ensure that the escalation point within their organisation has a specific channel for dealing with requests relating to disaster events.

ID	Industry Standard
UKBC 1-44	Service Providers and Network Operators should ask their Equipment Suppliers to provide a "Disaster Recovery Services Checklist" giving a listing of all the Equipment Supplier's professional services which the Service Provider or Network Operator may require during an event.
UKBC 1-45	Service Providers and Network Operators should develop plans or processes so that resource needs, identified through damage and resource assessments, can be escalated up the company chain of command, with suppliers, or through mutual-aid partners.
UKBC 1-46	Service Providers and Network Operators should consider, when/where feasible, maintaining sufficient hardware spares for critical elements to continue service after an incident without the need to obtain spares from Equipment Suppliers.
UKBC 1-47	Service Providers and Network Operators should develop processes to routinely archive system media backups and provide for storage in a "secure off-site" facility which would provide geographical diversity.
UKBC 1-48	Service Providers and Network Operators should consider supplementing media backup storage with full system restoration capability for media with documented restoration procedures that can be utilized at an alternate "hot site", in case of total failure of the primary service site.
UKBC 1-49	Service Providers and Network Operators should consider, where feasible, utilizing multiple communication carriers to provide diverse connectivity between service nodes reducing single points of failure.
UKBC 1-50	Service Providers should consider alternative carrier/transport methods such as satellite, microwave or wireless to further reduce point of failures or as "hot transport" backup facilities.
UKBC 1-51	Service Providers and Network Operators should periodically test new and existing business critical systems for capability limitations to avoid impaired operation during disasters.
UKBC 1-52	Service Providers and Network Operators should engage in pre-construction site selection processes to ensure network sites are not built in locations at a high risk of natural or man-made hazards.
UKBC 1-53	Fire detection and suppression systems should be installed at all network sites.
UKBC 1-54	Service Providers should use applicable engineering and construction standards in the building of network facilities.
UKBC 1-55	In recovery situations network build standards should be such that they do not interfere with other infrastructure.
UKBC 1-56	Service Providers and Network Operators should ensure deployment of resilient communication systems to appropriate Disaster Recovery personnel.
UKBC 1-57	Service Providers and Network Operators should work collectively with local, regional and central government organisations and other utilities to develop processes for efficient communications and coordination, as required under the regulations and guidance arising from the Civil Contingencies Act 2004.[17]
UKBC 1-58	Service Providers and Network Operators should work with government and other utilities in the development of any Emergency Communications Networks in order to provide a process for key utilities and government emergency responders to communicate during disaster events.
UKBC 1-59	Service Providers and Network Operators should make information available to contractors and other bodies on cable routes, in order to minimise the likelihood of damage and cable cuts when excavation is undertaken.
UKBC 1-60	Service Providers and Network Operators should ensure that Service Level Agreements for repair are reviewed and the records and data bases are reconciled annually.
UKBC 1-61	Service Providers and Network Operators should establish and maintain an interface with local, regional and central government agencies to ensure effective support is available upon request as part of disaster recovery.
UKBC 1-62	All Service Providers and Network Operators should introduce network controls on public networks in order to control congestion and ensure that emergency calls (999) receive proper priority during emergency situations.

[17] Emergency Preparedness
https://www.gov.uk/government/publications/emergency-preparedness

ID	Industry Standard
UKBC 1-63	Service Providers and Network Operators should implement consistent network management controls between operators, in order to promote reliability of the interconnected network.
UKBC 1-64	Network Operators and Service Providers should identify and manage critical network elements and architecture that are essential for network connectivity and customer services. In each case, considering security, redundancy and diversity.
UKBC 1-65	In order to facilitate asset management and increase the likelihood of having usable spares in emergency restorations, Network Operators and Service Providers should maintain "hot spares" (circuit packs electronically plugged in and interfacing with any element management system, as opposed to being stored in a cabinet) for mission critical elements. To determine appropriateness of this standard, certain factors should be considered, including redundancy, single points of failures for critical customers, etc.
UKBC 1-66	In preparation for predicted natural events, e.g., ice, snow, flood, hurricane, Service Providers and Network Operators should consider preparing and moving standby generating capacity and verifying the proper operation of all their subsystems.

11 Document Control

Document History	Comment	Version	Date of Issue
Draft 1	For comment	v0.1	15 June 2005
Draft 2	Minor amendments	v0.1	25 July 2005
		v0.2	24 October 2005
Draft 3	Document renamed and relationship to regulation clarified. Further minor amendments for IP environment.	v0.3	11 January 2006
Removal of OFCOM Ownership comments		v0.3	12 January 2006
TI-EPF Comments: Addition of Optical (Section 2.5) Explicit inclusion of Fixed and Mobile		v0.4	30 March 2006
Change Title		v0.5	3 April 2006
Add TI-EPF Logo		v0.6	24 April 2006
Update for EC-RRG		v0.7	March 2008
Update for EC-RRG	To be moved to Version 1.0	v0.8	TBC
Updated spring 2018 and agreed by EC-RRG June Plenary 2108	Latest version marked updated August 2018 on front cover	v2.0	30 August 2018 (Rob Willis DCMS)

12 References

[1] UK Telecommunications Industry Emergency Plan.
There is a national industry wide emergency plan which is owned and managed by the EC-RRG.

[2] Telecommunications Resilience:
https://www.gov.uk/guidance/telecoms-resilience

[3] Providers of Publicly Available Telephone Services have obligations relating to Emergency Planning under Condition 5 of the Conditions of Entitlement. They also have obligations under the Civil Contingencies Act 2004 as Category 2 responders.
http://www.legislation.gov.uk/ukpga/2004/36/contents

[4] National Risk Register
https://www.gov.uk/government/collections/national-risk-register-of-civil-emergencies

[5] TEMPEST and Electromagnetic Security
https://www.ncsc.gov.uk/scheme/tempest-and-electromagnetic-security

[6] Security Procedures Telecommunications Systems and Services
https://www.ncsc.gov.uk/content/files/Security_Procedures_Telecommunication_Systems_and_Services__-_issue_3.0_Dec_2015.pdf

[7] Preparing for and responding to energy emergencies
https://www.gov.uk/guidance/preparing-for-and-responding-to-energy-emergencies

[8] Preparation and planning for emergencies: responsibilities of responder agencies and others
https://www.gov.uk/guidance/preparation-and-planning-for-emergencies-responsibilities-of-responder-agencies-and-others

[9] Supply Chain security risks
https://www.cpni.gov.uk/supply-chain
https://www.ncsc.gov.uk/guidance/cyber-security-risks-supply-chain

[10] Rise of Earth Potential at Electricity Stations
http://www.energynetworks.org/assets/files/electricity/engineering/telecoms/eitc/restricted/Specification_edits/S36/s36.pdf

http://www.energynetworks.org/assets/files/electricity/engineering/telecoms/eitc/restricted/eitc_docs/eitc38m/OpenReach%20EROP.pdf

[11] Telecommunications Fraud Forum
http://www.tuff.co.uk/

[12] NCSC
https://www.ncsc.gov.uk/

[13] BGP guidance
https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-54.pdf

[14] General guidance
https://www.cpni.gov.uk/content/identify-threats
https://www.ncsc.gov.uk/cisp
https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

[15] Planned outage notification to customers ITU-T M.1541
https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-M.1541-201101-I!!PDF-E&type=items

[16] Security guidance
http://www.cpni.gov.uk and http://ncsc.gov.uk

[17] Emergency Preparedness
https://www.gov.uk/government/publications/emergency-preparedness