



**NISCC Assurance Report for
“The CNI Organisation”
Generic Example
June 2004**



**NISCC Assurance Report for
“The CNI Organisation”
June 2004**

NISCC acknowledges the assistance of “The CNI Organisation” in providing the input into this process and thanks them for their efforts and co-operation.

Document History	Version	Date of Issue
AR Template for NISCC use	V5	Feb 2004
Generic Example for NISCC Website	V6	June 2004

HANDLING of the Report

Commercially sensitive information provided by “The CNI Organisation” will be protected by NISCC and, on completion, this report will be given the governmental ‘protective marking’ of RESTRICTED COMMERCIAL. In turn, NISCC will draw on sensitive material to produce the threat and vulnerability information, and “The CNI Organisation” is requested to share this report only with those in the company who need to see it, and to ensure that is stored securely, under lock and key, when not in use.

DISCLAIMER

Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NISCC. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

NISCC shall also accept no responsibility for any errors or omissions contained within this document. In particular, NISCC shall not be liable for any loss or damage whatsoever, arising from the usage of information contained in this document.

Contents

1	EXECUTIVE SUMMARY	5
1.1	CRITICALITY OF ORGANISATION	5
1.2	KEY FINDINGS; ASSURANCE POSITION	5
1.3	THREAT OVERVIEW	5
1.4	SIGNIFICANT RECOMMENDATIONS	5
1.5	REVIEW PLAN.....	5
2	NISCC	6
2.1	AIM	6
2.2	NISCC COMPOSITION	6
2.3	PROMOTING PROTECTION & ASSURANCE (PPA).....	6
2.4	THE ASSURANCE REPORT	6
2.5	NISCC & “THE CNI ORGANISATION”	7
3	THE ORGANISATION	8
3.1	FUNCTION	8
3.2	LOCATION	8
3.3	OWNERSHIP.....	8
3.4	SIZE.....	8
3.5	OTHER GOVERNMENT RELATIONSHIPS TO THE ORGANISATION	8
3.6	ORGANISATION’S INFORMATION INFRASTRUCTURE.....	8
4	THE ORGANISATION’S PLACE IN THE CNI	9
4.1	DEFINITION OF CNI.....	9
4.2	CRITICALITY OF “THE CNI ORGANISATION”	9
4.3	IMPACT OF LOSS.....	9
4.4	ORGANISATIONAL DEPENDENCIES	9
4.5	DEPENDENCE ON IT.....	9
5	CORPORATE ASSURANCE INDICATORS	10
5.1	INFORMATION SECURITY POLICY	10
5.2	BUSINESS CONTINUITY AND DR PLANS.....	10
5.3	ISO17799 (INFORMATION SECURITY) ACCREDITATION.....	10
5.4	IT HEALTH CHECKS / PENETRATION TESTS.....	10
5.5	USE OF UNIRAS AND OTHER CERTS	10
5.6	CONTACTS WITH EXTERNAL SECURITY GROUPS & FORA	11
5.7	CONTACTS WITH EXTERNAL SECURITY SPECIALISTS	11
5.8	RECRUITMENT VERIFICATION CHECKS.....	11
5.9	ISO 9000/1 (QUALITY MANAGEMENT) ACCREDITATION	11
5.10	SENIOR MANAGEMENT COMMITMENT	11
6	DESCRIPTION OF CRITICAL SYSTEMS	12
6.1	PURPOSE	12
6.2	NETWORK ARCHITECTURE.....	12
6.3	TECHNICAL, HARDWARE, SOFTWARE, PROTOCOLS	12
6.4	BLOCK DIAGRAM.....	12
6.5	CRITICAL SYSTEMS’ DEPENDENCIES	12

7	ASSURANCE INDICATORS FOR EACH CRITICAL SYSTEM.....	13
7.1	SECURITY POLICY.....	13
7.2	SYSTEM ACCESS POINTS	13
7.3	PROTECTION OF NETWORK SERVICES	13
7.4	SOFTWARE PATCHES	13
7.5	ANTI-VIRUS PROTECTION.....	13
7.6	PASSWORD POLICY	13
7.7	IDS / FAULT DETECTION.....	13
7.8	AUDITING OR PENETRATION TESTING OF SYSTEM	13
7.9	SYSTEM DEPENDENCIES	13
7.10	CHANGE CONTROL PROCEDURES	13
7.11	INFORMATION BACKUP PROCEDURES	13
7.12	SYSTEM RESILIENCE & AVAILABILITY.....	13
8	VULNERABILITY ASSESSMENT.....	14
8.1	ATTACK TECHNIQUES	14
8.2	AVENUES OF ATTACK	15
8.3	TECHNICAL VULNERABILITIES.....	15
9	THREAT ASSESSMENT	16
9.1	THREAT SOURCES	16
9.2	ASSESSMENTS FOR ORGANISATION	17
9.3	THREAT SUMMARY	17
9.4	THREAT LEVEL DEFINITIONS	17
10	SUMMARY OF RECOMMENDATIONS	18
10.1	LIST OF ALL RECOMMENDATIONS, IN PRIORITY ORDER.....	18
11	REVIEW PLANS.....	18
11.1	PLANNED CHANGES IN ORGANISATION’S ARCHITECTURE.....	18
11.2	RECOMMENDED DATE FOR NEXT ASSURANCE VISIT	18
12	GLOSSARY	18
13	ANNEX A - ASSURANCE INDICATORS	19
13.1	CORPORATE ASSURANCE INDICATORS.....	19
13.2	ASSURANCE INDICATORS FOR CRITICAL SYSTEMS.....	20
14	ANNEX B – UNIRAS REPORTING GUIDELINES	21

1 Executive Summary

This includes a high level, and brief, description of the main findings of the Assurance Report. Specific issues are summarised in this chapter, which will be more fully described later in Assurance Report.

1.1 Criticality of Organisation

A short statement to describe the impact of loss of the organisation's critical service/s or operations, both on the organisation itself and the wider economy and community.

1.2 Key Findings; Assurance position

A summary of the conclusions from the Assurance Process, and a general overview of how robust the organisation's security policies and practices are, in relation to their critical systems and operations.

1.3 Threat overview

A summary of the key findings from the Threat Assessment, specifically regarding the threat of electronic attack against the company. Identify the highest threat source.

1.4 Significant recommendations

As identified through the Assurance Process, and already discussed with the organisation. Not a comprehensive list (which is at Chapter 10) but just the most significant.

1.5 Review plan

A record of the key dates in the Assurance Process, with dates committed by both NISCC and the partner organisation, to establish which recommendations have been accepted, which implemented, and a commitment to revisit and review the Assurance Report at a future, specified, date.

2 NISCC

2.1 Aim

The National Infrastructure Security Co-ordination Centre (NISCC) was established by the Home Secretary to promote the protection of the UK's Critical National Infrastructure (CNI) from electronic attack, and to report on the level of protection in place. For further information on NISCC please see www.niscc.gov.uk

2.2 NISCC Composition

NISCC is an inter-departmental centre which co-ordinates activity in support of this aim across a range of organisations. Each of these contributes resources and expertise to NISCC's programme of work according to its own remit, its own priorities, in relation to the challenge in hand, and depending on what value it can add. Contributing departments are The Security Service; CESG; The Home Office; Cabinet Office Security Policy Division; the Civil Contingencies Secretariat; The Central Sponsor for Information Assurance; MoD; the National Hi-Tech Crime Unit (NHTCU); DTI; and DSTL.

2.3 Promoting Protection & Assurance (PPA)

In order to fulfil its remit, NISCC seeks to undertake an assurance process with CNI organisations to assess the level of protection afforded to critical systems; provide information on threats and vulnerabilities to enable the management of risk; and make recommendations to promote proportionate protection. This assurance process is high-level using a standard set of assurance indicators, and does not amount to accreditation. The primary deliverable of the process is the NISCC Assurance Report.

2.4 The Assurance Report

The assurance process enables NISCC, and the partner organisation with whom the process is being undertaken, to focus in a structured way on a variety of "Assurance Indicators", shown in the form of matrices, against which the security policies and practices at both a corporate level, and for those individual systems which are identified as critical, can be compared with the accepted best practice.

This is not a formal auditing process, but it allows NISCC to offer an independent review of infrastructure, policies and processes using a standard set of common criteria. However, it does give NISCC, with the unique ability to access specialist resources as necessary, an opportunity to offer advice, comments and recommendations on the aspects of Information Security and IT protection which are covered in the process. The conclusion of the NISCC assurance process is the publication of an Assurance Report, comprising:

- An Impact Assessment, which defines the criticality of "The CNI Organisation" within the CNI by outlining the impact of loss or failure of each critical service provided by the Organisation (Chapter 4);
- An assessment of the assurance level of "The CNI Organisation", using a set of "corporate assurance indicators" (Chapter 5);

- An identification of critical IT or computer systems, and first-level dependencies on other organisations and equipment suppliers (Chapter 6);
- An assessment of the assurance level of each critical system or network, using a set of “critical systems’ assurance indicators” (Chapter 7);
- A Vulnerability Assessment, which describes any known vulnerabilities in the critical services or supporting critical systems, with recommendations for their mitigation, and discusses avenues of attack to which the systems may be susceptible (Chapter 8);
- A Threat Assessment which describes the threat groups and gives an assessment of the level of threat facing “The CNI Organisation”, with respect to the vulnerabilities and attack avenues already identified (Chapter 9);
- A set of specific recommendations regarding the appropriateness of the protective measures in place, commensurate with the results of the Impact, Vulnerability and Threat Assessments (summarised in Chapter 10).
- Proposals for future engagement of NISCC with the company (Chapter 11).

All NISCC Assurance Reports are treated as confidential and are not discussed with any third party, even for the comparison of results. However, the report, and scope of recommendations within it, will give a very good guide to the relative effectiveness of the corporate Assurance Strategy. The NISCC Assurance Matrices in particular can be used to measure effectiveness in any specific area of assurance. Subsequent reviews can be used to measure year-on-year progress or levels of improvement.

2.5 NISCC & “The CNI Organisation”

Any comments about our specific relationship to the organisation.

3 The Organisation

3.1 Function

The core function or business of the organisation.

3.2 Location

Headquarters; major sites; geographical spread.

3.3 Ownership

Whether the organisation is UK owned, foreign or multi-national. Part of a wider group etc.

3.4 Size

Size in terms of employees, market share etc. - in absolute terms and in comparison to peers within the sector.

3.5 Other Government Relationships to the Organisation

This will include the company's relationship to the National Security Advice Centre (NSAC), and whether any company sites are receiving NSAC advice. There may be a recommendation to NSAC that certain physical sites identified in the NISCC assurance process should be considered by NSAC as well.

Identification and explanation of any other Government relationships with the organisation, including relevant regulators, security advisors and whether they have regular contact with the Civil Contingencies Secretariat or National Hi-Tech Crime Unit.

3.6 Organisation's Information Infrastructure

Very high-level overview of major components of their infrastructure, including a summary of how IT security is managed, whether there is an IT security team and the identification of an appropriate IT security contact.

4 The Organisation's Place in the CNI

4.1 Definition of CNI

The Government views the CNI as those assets, services and systems that support the economic, political and social life of the UK whose importance is such that any entire or partial loss or compromise could:

- cause large scale loss of life;
- have a serious impact on the national economy;
- have other grave social consequences for the community, or any substantial part of the community; or
- be of immediate concern to the national government.

4.2 Criticality of "The CNI Organisation"

In defining an organisation or company's business as being part of the CNI, NISCC will identify those *services* that the company provides which are assessed as critical, using the definition above. For each of these services, agreement has to be reached on which underlying IT systems or networks are critical to the service i.e. systems whose loss would have a substantial impact on the delivery of that service. Each service may also depend on systems provided by other companies and any critical dependencies of this sort will also be identified.

This section is a description of why the organisation is assessed as being within the CNI, based on the services or resources it provides which are regarded as critical and an explanation as to why they are critical.

4.3 Impact of Loss

Impact of failure or degradation of critical services over time, in terms of economic, social, political and life-threatening consequences.

4.4 Organisational Dependencies

Overview of independent companies or organisations upon which the subject of the Report depends to deliver its critical services. This is a high-level list of the key services and external service providers (such as telecommunications and other utilities providers) on which the organisation depends.

4.5 Dependence on IT

IT or Control Systems that are vital to support critical services.

Of all the systems described in 3.6, which are critical to support the critical services described in 4.2. Brief list. Each critical system is analysed in Chapter 6.

5 Corporate Assurance Indicators

These ten ‘assurance indicators’ relate to “The CNI Organisation” as a company – corporate policies and practices that are ‘indicators’ to the level of information assurance in the company.

5.1 Information security policy

An information security policy is a crucial element for providing direction and support for overall information security and protection. This paragraph should cover issues such as whether such a policy is established within the organisation, that it has been agreed by a member of the organisation’s Board, that it is available to and accepted by all staff and that there is a regular review and updating policy.

5.2 Business Continuity and DR plans

Critical business processes need to be protected from the effects of major failures or disasters. This paragraph covers basic issues such as whether effective business continuity plans have been developed and are in place, whether a nominated individual is responsible for managing the continuity process, whether a business impact analysis is carried out to identify the events that can cause interruptions, whether business recovery strategies have been defined and are regularly tested.

5.3 ISO17799 (Information Security) Accreditation

Has the organisation achieved accreditation to ISO 17799 for its critical systems, or is it planning to? Short of formal accreditation, the company may have designed its networks and procedures in accordance with 17799, without aiming for accreditation.

5.4 IT Health Checks / Penetration Tests

A well planned, consistent, programme of internal IT audits will ensure that measures deployed to enhance infosec will remain effective, and that any new vulnerabilities are identified and managed. Issues such as whether the company undertakes a regular programme of IT audits, to measure ongoing compliance with corporate requirements, and whether technical testing is carried out in accordance with CHECK standards, will be covered in this paragraph.

5.5 Use of UNIRAS and other CERTs

The effective reporting of incidents and the use of accurate and reliable information resources will minimise the damage from security incidents, and ensure that lessons are learnt and ongoing issues are monitored. This section, therefore, covers the organisation’s involvement with UNIRAS or any other CERT and, if they subscribe to any CERT services, whether the alerts and messages are disseminated appropriately within the company; that any IT security incidents are reported to UNIRAS or another CERT; and areas such as whether lessons are learnt from incidents.

Recommendation 5.5 “The CNI Organisation” should report significant electronic attack incidents to UNIRAS. Guidance on what UNIRAS would like to receive is at Annex B, under section 14 below.

5.6 Contacts with External Security Groups & Fora

Is “The CNI Organisation” a member of any forum specialising in information security or assurance, such as NISCC’s Information Exchanges; ISACs; i4, ISF, IAAC, industry SIGs etc.

5.7 Contacts with External Security Specialists

Specialist infosec advice is likely to be sought or required by a majority of organisations. Contact should be made with suitable external experts whose required quality of work is well defined. This paragraph covers issues such as whether the organisation outsources any elements of network security and, if so, that the security requirements are defined and agreed with the third party and form part of a contract.

5.8 Recruitment Verification checks

To reduce the risk to the organisation of individuals perpetrating fraud or misusing system resources, the rigorous vetting and training of staff should be applied, including proof of identity and security checks. This paragraph covers points such as whether verification checks are carried out for key staff, and whether these checks are compliant with BS 7858. The requirement for employees to sign an acceptance of the company’s security policy through the inclusion of security responsibilities into their terms and conditions can also be covered in this section.

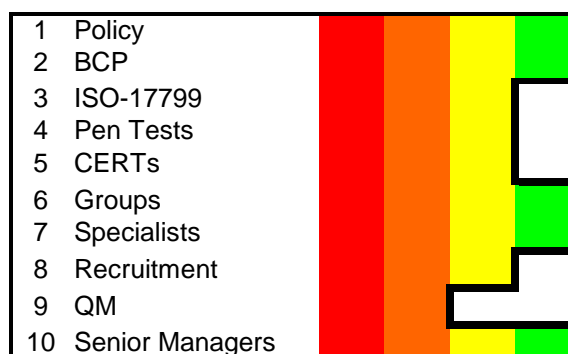
5.9 ISO 9000/1 (Quality Management) Accreditation

ISO 9000/1 is a generic name given to a set of standards developed to provide a framework around which a quality management system can effectively be implemented. Its primary aim is to provide an organisation with a set of processes that ensure a common sense approach to the management of the organisation. It is not essential for all organisations to be accredited to this specific standard, but this paragraph should identify whether their internal policies, procedures and principles, both manual and electronic, are audited.

5.10 Senior Management Commitment

It is essential that senior management, preferably at Board level, are fully committed to the concept of information security. This means that they should support any internal security policies and procedures, including business continuity arrangements, and should be prepared to support and implement significant recommendations even if there are financial or other resource implications.

Graphical summary of the Assurance Matrix ‘scores’ – in accordance with the Matrix definitions at Annex A.



6 Description of Critical Systems

In this chapter, the systems which are deemed to be critical are considered from the perspective of the organisational management – their awareness, appropriate support and response arrangements in the event of loss or failure.

This chapter should include a detailed technical description of the system, including the hardware and software used. A block diagram of the network and details of the critical systems' dependencies (ie those on which continuation of the service is reliant) should also be included.

6.1 Purpose

What this IT or Scada system, or network does.

6.2 Network Architecture

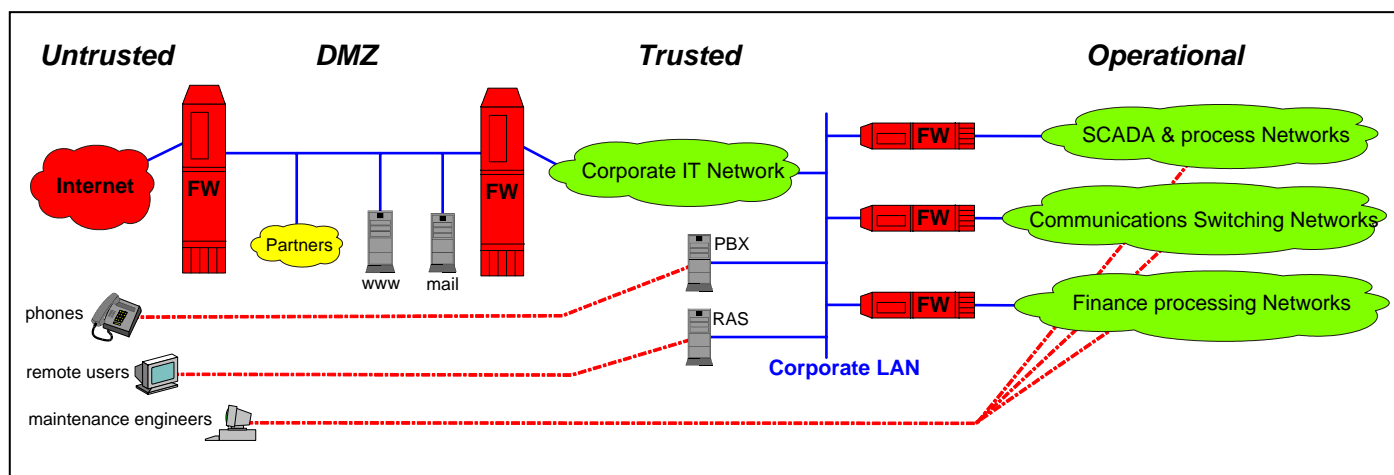
Description of network architecture – is it a LAN, WAN, global VPN, a stand-alone server etc.; is it connected to the Internet. etc.

6.3 Technical, hardware, software, protocols

Key elements – such as main servers or critical components. Is it running TCP/IP; is it based on X.25; is it a Scada network running ModBus etc.

6.4 Block diagram

A picture is worth a thousand words. All network diagrams become part of the NISCC CNI Mapping project, to capture interdependencies between organisations.



6.5 Critical Systems' Dependencies

If not covered adequately in the Corporate section (4.4), there may be specific dependencies for a system – eg upon a technology vendor.

7 Assurance Indicators for each Critical System

See also the Assurance Indicators matrix at section 13 below. These indicators are to measure whether the company has a policy or practice in place.

7.1 Security policy

Does the company have one for this specific system?

7.2 System Access Points

Has the company identified and managed access points?

7.3 Protection of network services

Are network services (like Internet access, external email, printer sharing, network drive mapping, RPC, telnet, SNMP, ping, network scanning, external media etc) restricted or switched-off if not needed?

7.4 Software Patches

How does the company implement patches?

7.5 Anti-virus Protection

Is it run centrally, on clients, not at all etc.

7.6 Password Policy

What is it? Is it adequate?

7.7 IDS / Fault Detection

Is it run on the critical network under review?

7.8 Auditing or penetration testing of System

Is this done regularly? Internally, or by external companies? Are external companies CHECK approved? CHECK is the CESG-accredited The IT Health Check Service.

7.9 System dependencies

Has the company identified and managed the dependencies for this system? Power, water, telecoms etc.

7.10 Change control procedures

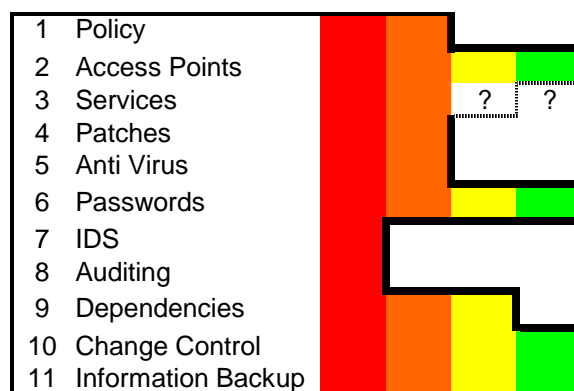
Any formal procedures for this system?

7.11 Information backup procedures

Any formal procedures for this system?

7.12 System resilience & availability

Any availability standards or commitments



Graphical Matrix Summary

8 Vulnerability Assessment

8.1 Attack Techniques

Threat groups have a range of electronic attack techniques or tools at their disposal. We separate these attacks into categories: denial of service; network intrusion; viruses and worms; Trojan software; and malicious hardware. This is for ease of explanation - in reality the boundaries between the types of attack are often blurred. In the case of operational and process control systems (for example, SCADA), we can also add operator spoofing as an attack method.

8.1.1 DOS

Denial of service (DOS) attacks are designed to render a system unusable, often without actually penetrating it. For example, attackers often cause denial of service by flooding target systems with unwanted data, effectively blocking legitimate use. In some cases an attacker will simultaneously flood a victim from multiple sources. This is called a distributed denial of service attack (DDoS). It is also possible to cause denial of service by exploiting vulnerabilities. A historic example of this is WinNuke, a program that sends a single packet of data that will cause vulnerable windows machines to crash immediately.

8.1.2 Network Intrusion

Network intrusion is the term that we use to describe situations where an attacker remotely penetrates a system: to cause a malfunction or damage; simply to scope the system and identify its vulnerabilities; or to remove data surreptitiously and deniably. This is commonly achieved by exploiting vulnerabilities in software on the target machine, but may also rely on techniques such as password guessing, wireless hacking or “war dialling” where the attacker dials lots of telephone numbers in an attempt to find a modem that will accept an inbound connection.

8.1.3 Viruses and worms

Viruses and worms are self-replicating programs. The term virus is used to describe programs that infect individual files, while worms are stand-alone programs that copy themselves to victim machines. A typical virus works by attaching itself to an executable file and then infecting other executable files whenever the infected one is executed.

The most common form of worm is a mass mailing worm. When executed by a victim, a mass mailing worm emails itself to everybody in the victim’s address book with a message to tempt these new victims to execute the worm and spread it further. Other kinds of worm, like Code Red, do not rely on gullible users, but instead they will automatically locate, exploit and copy themselves to vulnerable systems.

8.1.4 Trojans

Trojan software is often regarded as a kind of virus. Trojans can be apparently useful or fun programs, e-mails or even web-pages that contain a hidden malicious payload. This payload can be executed by opening e-mails, attachments to e-mails, by being drawn into or automatically connected to infected web-sites. Often this payload opens a back door on the system to give the attacker access to the victim, but other payloads are possible. A Trojan could delete or change files or cause a serious malfunction to a system which might cause it to crash under certain pre-set conditions.

8.1.5 Malicious Hardware

Viruses, worms and Trojans are sometimes called malicious software. It is not often recognised that attacks can also be executed using malicious hardware. One example is a key logger. An attacker can covertly attach this small device to a target computer keyboard, where it will then record keystrokes. The attacker can then covertly remove the key logger and download the contents, revealing all of the passwords and usernames typed on the target machine.

8.1.6 Operator Spoofing

Operator Spoofing is the term used to describe the operator being tricked into taking imprudent action based on spurious or false signals apparently from field devices. This attack is more complex as the attacker is required to access and modify the system to change the data points on the screen graphics in order to deceive operators and stimulate an event eg an emergency shutdown. This requires understanding of the system and the process control (SCADA) software in use; the network address of the server(s), the ability to access and modify files on the server(s), including access through the company network (if necessary) plus necessary administrator privileges. Insider knowledge of the network would help significantly in this type of attack.

8.2 Avenues of Attack

This section identifies possible avenues of attack on the architecture – how an attacker might gain access to the critical systems from the Internet. Examples might include the following:

8.2.1 Attack through Office Network

From Internet, via email or web-browsing, into the corporate LAN, and from there to the critical servers or networks.

8.2.2 Attack from a Partner Network

A ‘trusted’ network interconnected to the company’s network – eg a trading partner, telecoms company etc.

8.2.3 Attack through physical access

Gain unauthorised access to a terminal or network access point.

8.2.4 Use of Insider

Threat actor recruits an insider or contractor to gain access

8.3 Technical Vulnerabilities

Specific vulnerabilities in hardware, software, network or communications protocols used by the organisation.

9 Threat Assessment

9.1 Threat Sources

The electronic attack (eA) threat to “The CNI Organisation” arises from a range of potential attackers. At one end of the scale are *foreign states* that have hostile intentions towards the UK and at the other are *script kiddies*. In the middle we have a mix of threat groups: *terrorists*, who may be seeking to add electronic attack to their existing capabilities; *activists* conducting publicity-seeking attacks; *criminals* engaged in electronic crime; disgruntled *employees*, *hackers*, *crackers* and *virus writers*.

9.1.1 Foreign states

Foreign states are increasingly recognising the value of electronic attack. Any such attacks are likely to be carried out by specialists working for military or intelligence agencies. Attacks could have two possible motives. Firstly, to gather intelligence; there is evidence that states with electronic capability are actively seeking to acquire economic and financial intelligence. Secondly, attackers may seek details of systems, including any vulnerabilities which, in time of crisis could be used to mount attacks designed to disrupt the UK’s critical infrastructures.

9.1.2 Terrorists

There are several *terrorist groups* who currently have the intention to damage UK infrastructures. However, despite the fact that groups are making increasing use of computers, we assess that for the time being they will continue to favour traditional physical attacks rather than using electronic means. We also assess that, although there is varied capability within terrorist groups, they are unlikely to be able to carry out widespread and damaging electronic attacks, though low level attacks such as defacements are always a possibility. Insider knowledge or assistance would add significantly to the chance of success of any electronic attack.

9.1.3 Hacktivists

Activist groups, also known as hacktivists, have been known to carry out denial of service attacks, website defacements and electronic ‘sit-ins’. Electronic attack/computer protest has centred on issues such as global capitalism, the war in Iraq and pollution. Generally speaking, such protestors have not shown the intent or capability seriously to harm the UK’s critical infrastructure, although the potential for information theft must also be borne in mind.

9.1.4 Criminals

Criminals represent a threat to the CNI, though the exact nature will vary depending on the sector and nature of business of the individual organisation. There are numerous examples of criminals using eA for fraud and extortion. Reports of any such criminal activity should be reported to the National Hi-Tech Crime Unit (NHTCU); NISCC has no law enforcement powers.

9.1.5 Hackers, Crackers & Virus Writers

There is considerable disagreement about the meaning of the term *hacker*. In this report, we use the term to describe a person or group motivated by a desire to analyse and explore other people’s systems. While this activity is likely to be illegal, we separate this group from criminals because of the difference in motive. They are

discrete from *crackers* who break into computer systems with malicious intent. Some hackers would simply try to penetrate critical systems to gain prestige within the hacker community, or because it provided an interesting technical challenge. Others may have an interest in deliberately damaging computer systems for a variety of reasons e.g. because of a personal grudge or protest against a company. There will inevitably be a wide range of skill levels amongst the hacking community and at the upper end of the scale there is a high degree of capability. *Virus Writers* have different skills, not only creating the virus, but also in deploying new, creative and more effective means of propagation.

9.1.6 Individuals with legitimate access

There is a real threat, albeit difficult to quantify, from a *disgruntled employee* (or other contractor, visitor or consultant with privileged access) who, for whatever reason, could use their individual expertise and level of access maliciously to damage systems or cause disruption. The type of attack and its potential damage will vary significantly from employee to employee, and any hostile motivation is likely to be for personal reasons, rather than ideological. In documented cases of insider attacks for personal reasons, issues such as impending redundancy, perceived employment rights infringement, or greed were the triggers for attacks on their employees. “The CNI Organisation” is likely to be better placed than NISCC to assess this threat.

9.1.7 Script Kiddies

The final threat source is commonly described as “*script kiddies*”. They are probably probing Internet facing portals for vulnerabilities in many commercial and government systems on a daily basis. These unskilled attackers scan the entire Internet in search of vulnerable victims, and then run hacking tools, which they have often downloaded from the Internet, against them. Such individuals may succeed in penetrating office networks or mounting limited denial of service attacks.

9.2 Assessments for organisation

This section will identify the threat level, specific to the organisation, for each avenue of attack identified in Chapter 8, and for each threat source (for example, the threat level for the office network or process control systems within the organisation).

9.3 Threat Summary

A summary of the assessment of the threat for each group and each avenue of attack, based on available intelligence about the threat groups, and our experience of their past activities.

9.4 Threat Level definitions

The definitions referred to elsewhere in Chapter 9 are summarised in tabular form.

10 Summary of Recommendations

10.1 List of all recommendations, in priority order

Each recommendation throughout the report is uniquely numbered, using the paragraph number for the relevant recommendation. This section acts as a central ‘checklist’ or catalogue of recommendations we have made. This will make review at a later date easier.

For example:

Recommendation 5.5 “The CNI Organisation” should report significant electronic attack incidents to UNIRAS. Guidance on what UNIRAS would like to receive is at Annex B, under section 14 below.

11 Review Plans

11.1 Planned changes in Organisation’s Architecture

Significant changes that are planned may trigger NISCC to re-visit. For example, if the company is to migrate from X25 to TCP/IP next year, the vulnerability of the network will probably change.

11.2 Recommended Date for Next Assurance Visit

This should include dates to see whether NISCC’s recommendations have been accepted; been actioned; if there are architectural changes ahead; and finally, for a review in 2 or 3 years’ time.

12 Glossary

Include a glossary in the Report if it helps. NISCC is building up a glossary of information assurance, InfoSec, telecommunications, networking and process control terms, from which relevant ones can be drawn for each Assurance Report.

13 Annex A - Assurance Indicators

When assessing the level of assurance in this Report, we use two consistent sets of assurance indicators, as described in paragraph 2.4 above. The tables below list these indicators, and the five levels of assurance ‘maturity’ associated with each.

13.1 Corporate Assurance Indicators

No	Assurance Indicator	Little or no progress to best practice	Some progress	Significant progress	Recommended best practice
1	Information Security Policy	No published policy document	Published policy document	Published policy document, available to all users responsible for security.	Published policy document, approved by board, regularly reviewed, accepted by all users responsible for security
2	Business continuity and Disaster Recovery plans	No plans	Plans being developed	Plans in place	Plans in place and tested regularly
3	Compliance with BS7799 or other similar standards	Unaware of 7799 and other similar standards	Aware of 7799 – compliance with this or similar standard has been considered.	Compliance with some aspects of 7799 or equivalent standard	Certification / full compliance with 7799 or equivalent standard
4	IT Health Checks or penetration tests	No recent IT Health Check	Recent IT Health check of CNI systems (no regular schedule)	Regular Health Checks of CNI IT systems – standard unknown	Regular CHECK standard Health Checks of CNI IT systems
5	Use of UNIRAS or other CERTs,	Not involved in any CERTs	Member of UNIRAS or other CERT	UNIRAS/CERT messages disseminated appropriately in company	Contributing to UNIRAS or other appropriate CERTs,
6	Contacts with external security groups or fora or Information Exchanges	No contacts	Some contact with relevant groups	Membership of a limited number of relevant groups	Membership of wide range of relevant groups and member of an Information Exchange.
7	Contacts with external security specialists	No contacts	Occasional contact with one or more specialists	Regular contact with limited range of specialists	Regular contacts with a wide range of specialists
8	Recruitment verification checks	Little consideration of verification checks	Developing verification checks for key staff	Has verification checks for key staff	Compliance with BS7858
9	ISO 9000/1 – Quality Management	Unaware of ISO 9000 and similar standards	Some consideration of quality standards	Compliance with some aspects of ISO 9000/1 or similar standard	Hold ISO 9000/1 or similar quality standard

13.2 Assurance Indicators for Critical Systems

No	Assurance Indicator	Little or no progress to best practice	Some progress	Significant progress	Recommended best practice
1	Security Policy	Policy not in place	System security policy being developed or inappropriate	Appropriate system security policy in place but implementation needs improvement	Appropriate system security policy implemented effectively
2	Identification of system access points	Little/no consideration of access points	Some access points identified/documentated	Most access points identified/documentated	All access points identified /documentated
3	Protection of networked Services	No protective measures in place	Few protective measures in place	Some protective measures – could be more effective	Appropriate protection in place
4	Application of software patches	No policy – patches not applied routinely	Policy under consideration	Policy on patches exists – implementation could be more effective	Policy of prompt application of software patches – implemented effectively.
5	Anti-virus protection	No anti-virus protection.	Anti-virus protection being considered	Some anti-virus measures – could be more effective.	Appropriate anti-virus policy and effective implementation.
6	Password Policy	No password policy	Password policy in development or inappropriate	Appropriate password policy but little evidence of implementation.	Appropriate password policy implemented effectively
7	Intrusion Detection Procedures	No intrusion detection procedures in place.	Intrusion detection procedures being considered	Some intrusion detection procedures – could be more effective.	Appropriate intrusion detection procedures in place
8	Auditing of system	No auditing of system	Auditing under consideration	Occasional auditing	System regularly audited
9	System dependencies	Dependencies not identified	Some dependencies identified	Most critical dependencies identified	All critical dependencies identified / SLAs in place with other system owners
	Colour Code	RED	ORANGE	YELLOW	GREEN

14 Annex B – UNIRAS Reporting Guidelines

UNIRAS, the CERT (computer emergency response team) within NISCC, is responsible for reporting and disseminating computer and network security incidents for its community. Originally just government departments, the UNIRAS community has been expanded to include companies that hold sensitive government data, and organisations that are in the CNI.

“The CNI Organisation” receive UNIRAS reporting, and are invited to submit incidents to UNIRAS, which will be held in strictest confidence. The wider the reporting base to UNIRAS, the more comprehensive the threat and warning information UNIRAS can report back to its members.

The table below gives guidance on the sort of incidents that UNIRAS would ideally like “The CNI Organisation” to report. UNIRAS operates 24x7: their telephone number is 020 7821 1330. Further contact details and reporting mechanisms can be found at www.uniras.gov.uk.

No	Attack Type	Examples and description	Reporting guideline
1	Hacking attack	attacks resulting in data theft; modification; corruption or illegitimate access.	report all as soon as possible
2	Denial of Service	Malicious or deliberate DOS attack resulting in reduced service	report all as soon as possible
3	Data interception or monitoring	network data intercepted, for example unauthorised packet sniffing or password capturing	report all as soon as possible
4	Malicious software	infection of the network by malicious software – virus, worm or Trojan	report all as soon as possible
5	IDS hits	attacks or behaviour that trigger intrusion detection systems	report those that are above the corporate thresholds configured for the IDS, and are not immediately accounted for
6	Scans	scanning or probes on the external borders or firewalls	only those scans or probes that are anomalous, or are against novel ports
7	Other	Anomalous system or network behaviour that may impact security but does not result from known software or hardware failure	report anything inexplicable, or consult UNIRAS for advice
8	Malicious software	Where malicious software is stopped at gateways by AV or firewalls	report monthly synopsis or trend analysis, if available