



NISCC Technical Note 04/04

Issued 25 March 2004

Organisational Vulnerability Management Process

Key Points

- **This technical note is of use to all organisations who use IT**
- **This technical note is the first aimed at developing response capability**
- **A minimal method for assessing risk is suggested**
- **Active monitoring vulnerability information is important**
- **Guidance on deploying patches and workarounds is provided**

**National Infrastructure
Security Co-Ordination Centre**
PO Box 832
London
SW1P 1BG

Tel: 020 7821 1330 Ext 4511
Fax: 020 7821 1686
Email: enquiries@niscc.gov.uk
Web: www.niscc.gov.uk

Introduction

1. This Technical Note addresses the processes involved for an organisation to identify the risks associated with a vulnerability and to perform appropriate remedial action (which includes not remediating the vulnerability).
2. Intended audience are those in an organisation responsible for IT security, typically the departmental or company security officer.
3. Managing a response to vulnerabilities is an essential part of evaluating and managing the risks to the business of an organisation. Managing risk is, in turn, an essential part of operating any business successfully, whether the risk relates to operational issues or to supporting business processes.
4. There are certain general areas of organisational security which this paper does not address that will assist in reducing the risks from vulnerabilities. It is prudent for example to design systems with security in mind, selecting products with a record of few vulnerabilities or, at least, rapid and reliable patching of vulnerabilities. However there may be a cost associated with this choice in terms of decreased functionality or increased hardware or software costs. Nevertheless, putting security measures in place (such as firewalls) to prevent vulnerabilities being exploited is strongly recommended. Equally important, and again not addressed here, is the culture of security in an organisation: that is, formulating and applying security policies, processes and procedures.

Definitions

5. The following table contains some definitions of common terms used throughout this paper:

TERM	DEFINITION
Vulnerability	A group of conditions which, taken together, can leave a system open to unwanted access or unauthorised use by an intruder or denies availability of the system
Threat	The capability and intention that intruders have to attack a system by means of a vulnerability
Likelihood	A probabilistic measure of an event occurring

Cost	A financial measure associated with a vulnerability
Impact	The effects on all aspects of the business of a successful exploitation of a vulnerability
Risk	At minimum a qualitative measure of the potential for attack against a system by means of a vulnerability. Risk is a function of likelihood of successful attack, cost and impact (see below).

Assessing Risk

6. An analysis of the numerous risk assessment methodologies is beyond the scope of this paper, but it is important to note that each methodology has been developed for specific business environments and therefore may not apply completely to your organisation. This Technical Note does not advocate a particular quantitative risk assessment method, but it does enumerate factors which should be considered when assessing risks from vulnerabilities. The use of a risk assessment process that conforms to an appropriate organisational, national or international standard is strongly recommended as part of business management. (Infosec Standard No. 1 provides the risk assessment method for UK central government; ISO 17799 provides an international standard for IT security management.)

7. Risk to an organisation from a vulnerability is generally considered to be a function of:

- The likelihood that an organisation's system will be attacked (which is a function of the threat to the system)
- The likelihood that the vulnerability will be exploited (which is a function of the availability of countermeasures for the vulnerability)
- The impact of exploiting the vulnerability
- The costs associated with a successful exploitation of the vulnerability

8. In summary, managing risks relating to vulnerability therefore requires assessing the likelihood of a successful attack, the impact and the cost. Cost in this context includes costs associated with loss of information assets, costs associated with loss of service, costs of system recovery, reduction in share valuations and intangible costs such as damage to reputation. The costs of implementing preventative and mitigating security measures need to be measured against the costs of a successful attack. In some environments it is not possible to measure the costs associated with exploiting a vulnerability. In those environments the risk from a vulnerability may be taken to be a function of the likelihood of there being an attack ("threat") which is successful ("vulnerability") and the impact of a successful attack.

Requirements

9. In order to ensure that the vulnerability management process can be implemented, the following steps should be taken:
- Ensure that there is senior management buy-in for the importance of vulnerability handling in terms of reducing risk to the business and that users are aware of the issues
 - Maintain an inventory of systems in the organisation including a definition of each system and an up-to-date list of products in each system
 - For each product record the version, patch level and the location of the product
 - For each product assess the value of the product and the value of information stored by that product
 - For each system in the organisation determine the criticality of the system in terms of availability of service, confidentiality of data, integrity of data and cost
 - Have a policy for business continuity management including system backup and recovery to meet a security management standard such as ISO 17799 which is regularly applied and tested

Likelihood of Vulnerability being Exploited

10. The following steps can be used to assess the likelihood of successful attack through exploiting a vulnerability:

STEP	LIKELIHOOD OF SUCCESSFUL ATTACK
Determine whether the products in use in the system are affected	The likelihood of successful attack becomes zero if the products are not affected
Determine whether the versions of the products in use in the system are affected	The likelihood of successful attack becomes zero if the versions of the products are not affected
Determine whether there are security measures in place in systems that prevent the vulnerability being exploited	The likelihood of successful attack becomes zero if security measures prevent exploitation
Determine whether there are known exploits for the vulnerability	The likelihood of successful attack decreases if there are no known exploits
Determine how difficult exploitation of the vulnerability is in terms of expertise, equipment and time	The harder a vulnerability is to exploit, the lower the likelihood of successful attack; although sophisticated attackers are still a concern if an exploit is practicable
Determine whether workarounds are available and implemented in the organisations' systems	The likelihood of successful attack decreases if workarounds are implemented

If workarounds are not available, determine when, if at all, workarounds will be available	The likelihood of attack increases the longer workarounds are not available unless a patch is available
Determine whether patches are available and implemented in the organisations' system	The likelihood of successful attack becomes zero if patches remediating the vulnerability are implemented
If patches are not available, determine when, if at all, patches will be available	The likelihood of successful attack increases the longer patches are not available unless a workaround is available

11. Organisations may be made aware of patches and workarounds through alerts issued by Computer Security Incident Response Teams (CSIRTs) and through industry groups.

Likelihood of Attack

12. If there is no possibility of successful attack by means of a particular vulnerability, then there is no risk from exploitation of that vulnerability, and it is unnecessary to determine the likelihood of attack or the impact from exploiting the vulnerability in question. (Risk assessments from classes of vulnerabilities are still recommended of course.)

13. The following steps can be used to assess the likelihood of attack associated with exploiting a vulnerability:

STEP	LIKELIHOOD OF ATTACK
Determine, if possible, what sources are likely to attack your system and what would motivate their attack	The likelihood of attack increases as the number and sophistication of the attackers increases
Determine whether there is evidence of scanning or probing of the organisation's systems related to the vulnerability	The likelihood of attack increases if there is scanning or probing of the organisation
Determine whether there is evidence in the public domain of scanning or probing of other organisations' systems related to the vulnerability	The likelihood of attack increases if there is scanning or probing elsewhere
Determine whether there is evidence in the public domain of attackers exploiting the vulnerability	The likelihood of attack increases if the vulnerability is being exploited elsewhere

14. Organisations may be made aware of patches and workarounds through alerts issued by CSIRTs and through industry groups.

Impact

15. The following steps can then be used to assess the impact of exploiting a vulnerability:

STEP	IMPACT
<p>Determine the likely results of exploiting the vulnerability,</p> <ul style="list-style-type: none"> • Denial of service • Data disclosure (eg ability to read files) • Data interception or modification (eg man in the middle attacks, session hijacking) • System compromise at user level • System compromise at system or administrator level 	<ul style="list-style-type: none"> • There is an impact on organisational security under "denial of service" if availability is important • There is an impact on organisational security under "data disclosure" if confidentiality is important • There is an impact on organisational security under "data interception" if confidentiality or integrity is important • There is an impact on organisational security under "user level system compromise" if confidentiality or integrity is important • There is an impact on organisational security under "system level compromise" if confidentiality or integrity is important

Cost

16. The following steps can be used to assess the costs associated with a vulnerability:

STEP	COST
<p>Determine the value of the information that would be disclosed or lost if the vulnerability was exploited</p>	<p>Cost increases as the value of information disclosed increases</p>
<p>Determine the value of service availability lost if the vulnerability was exploited</p>	<p>Cost increases as the value of service availability lost increases (although the service availability requirement will vary depending on the criticality of the service to the organisation)</p>
<p>Determine the value of products damaged if the vulnerability was exploited</p>	<p>Cost increases as the value of products damaged increases</p>
<p>Determine the cost of recovering the system if the vulnerability was exploited</p>	<p>Cost increases as the value of system recovery increases</p>

Determine the cost of patching the vulnerability or implementing workarounds	The costs of remediating the vulnerability need to be balanced against the costs of not doing so, namely the costs associated with the vulnerability being exploited
Determine, if possible, the value of indirect costs, such as loss of share valuations and damage to reputation	Cost increases as severity of attack and public awareness increases

Regular Activities

17. The foregoing steps identified in the tables above can be used to determine the risks to an organisation in qualitative terms at an instance in time, but certain activities need to be carried out regularly and frequently in order to maintain a current view of the risks. These activities are:

- Monitoring the publication of vulnerabilities
- Monitoring the publication of exploits for the vulnerability
- Monitoring the publication of patches and workarounds
- Monitoring outward facing organisational network perimeters and public sources, and CSIRTs and industry groups for evidence of attackers probing for the vulnerability

18. It is useful for organisations to establish relationships with CSIRTs and Critical National Infrastructure Protection (CNIP) organisations to share information on product vulnerabilities and exploits.

Vulnerability Remediation

19. Once the risk associated with a vulnerability has been assessed, whatever metrics are chosen to provide a quantitative measure, the following steps should be taken if the risk justifies remediating the vulnerability:

- Identify and locate affected systems (using the inventory)
- Apply workarounds on non-operational systems and understand side effects
- Deploy patches on non-operational systems and understand side effects
- If the workaround or patches do not significantly impact on the system stability and do remediate the vulnerability, the appropriate remedial steps (workarounds or patches) should be applied to all of the organisation's operational systems, using enterprise wide electronic delivery of updates where appropriate
- If patches do not work or result in system instabilities and there are no workarounds, it may be necessary to employ a further countermeasure such as limiting access to the affected product or service by use of a firewall
- Depending on the difficulty of applying workarounds or patches to all affected systems in the organisation, it may be appropriate to apply a

remediation policy based on risk to particular systems and devices (eg routers in the network interior tend to be less vulnerable to external attack than routers on the network boundary and may in some circumstances be patched after those on the boundary or not be patched at all if they are not vulnerable)

- Depending on the difficulty of applying workarounds or patches to all affected systems in the organisation, it may be appropriate to employ temporary security measures (such as blocking a service at the organisational perimeter)

20. Again, the process of remediating vulnerabilities is not static; patches and workarounds may be updated by vendors. It is important to monitor such developments.

System Recovery

21. In the event that a successful attack takes place before remedial steps can be taken, a recovery plan should be implemented. The details of this plan will vary from organisation to organisation, but it should include the concept of a “known good backup” of the system, where the system administrator is confident that the data on the system has not been subject to an attack. Analysis of accounting logs, and integrity checking and intrusion detection software tools can help in identifying the date when the attack took place and therefore in identifying the appropriate backup to use.