



eEye Digital Security and ECSC Ltd Whitepaper

Attaining BS7799 Compliance with Retina[®] Vulnerability Assessment Technology

Information Security Risk Assessments *The Special Case of IT Vulnerability Assessments*

For more information about eEye's Enterprise Vulnerability Assessment and Remediation Management Solutions, visit:
www.eeye.com

For more information about ECSC's full range of information security services, visit:
www.ecsc.co.uk





© 2004 eEye Digital Security
and ECSC Ltd
All Rights Reserved.

This document contains information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of eEye Digital Security and ECSC Ltd.

Collateral Information

eEye Digital Security Whitepaper
Information Security Risk Assessments
(WPBS7799BN)
Revision level 2.2

For the latest updates to this document, please visit:

<http://www.eeye.com>

or

<http://www.ecsc.co.uk>

Warranty

This document is supplied on an "as is" basis with no warranty and no support.

Limitations of Liability

In no event shall eEye Digital Security or ECSC Ltd be liable for errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

The information contained in this document is subject to change without notice.

No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this whitepaper.

Disclaimer

All brand names and product names used in this document are trademarks, registered trademarks, or trade names of their respective holders. eEye Digital Security and ECSC Ltd are not associated with any other vendors or products mentioned in this document.

ECSC only recommends specific vendor product solutions following a wider consultation process with its clients.

Although the initial standards work behind BS7799 dates back more than ten years, it has been thrust into the spotlight recently, and many organisations are finding themselves considering the benefits of compliance or full certification. It is clear that no single product can provide a complete solution to BS7799 compliance – organisations need to apply a combination of process management, security products and solutions, and expert advice to achieve their goals.

The following paper discusses the special case of Information Technology vulnerabilities within the wider framework of information security, and outlines a best practice approach to meet the challenge.

“Security requirements are identified by a methodical assessment of security risk.”

Source: BS7799-1:1999

Overview of BS7799

BS7799 was originally conceived as a “code of practice for information security management” that can be applied to any organisation. The current standard emphasises a sensible approach which is both grounded in pure risk management, and self-improving to adapt to new threats and a constantly changing security landscape.

Since its inception, it has been accepted as an ISO standard - ISO/IEC17799 - and has also been expanded by the release of BS7799-2:2002, which is a set of measurable criteria that can be used to grant certification to organisations with a compliant structure. In plain terms, ISO/IEC17799 (the code of practice) is a list of sensible things to do to manage security. BS7799-2:2002 (the certification criteria) is a set of measurable requirements which must be met to attain a certified Information Security Management System (ISMS) and thus gain BS7799 certification.

Organisations seek BS7799 certification for a variety of reasons – whether to assure business partners of their level of internal security, to comply with regulatory or legislative requirements such as the Data Protection Act (1998), or simply to ensure themselves and investors that they are following best practice with regards to information security. However, it should be remembered that the overall goal of BS7799 is to help organisations manage security, and not simply to gain certification.



The Information Security Management System (ISMS)

The concept of an Information Security Management System is at the heart of BS7799-2:2002, and the key criteria for compliance or full certification. An ISMS should manage all facets of information security, including people, processes and Information Technology (IT) systems. Key to a successful ISMS is that it be based on a feedback loop to provide continual improvement, and that it take a structured approach to asset and risk management. The Information Security Management System encompasses all the controls that the organisation puts in place to ensure information security, across the following 10 domains:

“The [risk assessment] approach adopted should aim to focus security effort and resources in a cost-effective and efficient way”

Source: BS7799-2:2002

- Security policy
- Security organisation
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance

Independent BS7799 consultants ECSC, one of the few consultancies with a fully certified BS7799 ISMS, are helping many organisations through the development process leading to compliance or full certification. The risk assessment process is particularly challenging for most organisations. Typically, staff with formal risk management expertise have little experience with IT security and IT staff have had little opportunity to contribute to a structured risk assessment process. External consultation is one way to facilitate fusion between the two respective fields of expertise – building capacity within the organisation that will be invaluable in the long term.

The Link Between Vulnerability Assessment and Risk Management

In traditional risk management terms, there are three components to any Risk – a Vulnerability, a Threat and a Potential Loss, or negative outcome. The combination of these three factors is then assessed in terms of likelihood and frequency, and assigned a monetary value, usually on an annualised basis.

One corollary of this, which is often overlooked, is that it is impossible to perform accurate risk assessment without quantifying vulnerabilities. When applied to Information Technology (IT) systems, this then implies that some kind of Vulnerability Assessment System is essential to assessing risk, and thus a critical part of a BS7799 compliant ISMS, or indeed any best practice information security infrastructure.



IT Vulnerabilities – A Special Case

“[The] shrinking window of remediation opportunity demands processes that are timely, accurate and verifiable.”

In contrast to more conventional information security risks, the case of IT vulnerabilities is unique. The traditional risks such as fire, theft and break-in with regards to information security are relatively well understood by practitioners, and can be assessed on an annual basis, or thereabouts. In contrast, the CERT® Coordination Center (CERT/CC) (Carnegie Mellon Software Engineering Institute) recorded almost 8000 new IT vulnerabilities in 2002-2003. Every new vulnerability presents a potential risk to information security within the IT structure, and must thus be assessed; with appropriate remediation activities undertaken to control the concomitant risk.

A further impetus to perform more frequent assessment of IT vulnerabilities is the shrinking window between the publication of new vulnerabilities and the “exploit code” or attack programs. While earlier worms such as Nimda or SQL/Slammer struck some months after the publication of the exploit, MS-Blaster, in August 2003, emerged a mere 26 days after the vulnerability was published. This shrinking window of remediation opportunity demands processes that are timely, accurate and verifiable.

One sound approach is to have an asset-centric system of pre-calculated risk profiles for your information assets situated within IT systems.

The Combined Risk Value (CRV) methodology has been developed by ECSC to systematically apply these principles to allow an organisation to implement a comprehensive risk management system. The approach places appropriate weightings to the following:

- Impact on the business, either through unauthorised viewing, corruption or loss
- Number of attackers with potential access
- Opportunity for an attack to be launched
- Exposure of the system, in terms of relative publicity
- Motivation of potential attackers, and any attack history
- Skill levels of the security administrators
- Protection given by the existing technical countermeasures
- Vulnerability history of the system

Each IT system can then be scored and prioritised from a risk perspective.



“The advantage of a capable Vulnerability Management system is that it can use vulnerability scanning to constantly monitor the network for exposure to known vulnerabilities, and thus inform the risk management and risk reduction processes included in the ISMS in near real-time”

The above assessment of your relative risks within IT systems can then be combined with an effective system for quickly identifying new vulnerabilities - whilst helping plan appropriate actions to contain the associated risks.

With the constant flood of new vulnerabilities, organisations should consider software tools to streamline and optimise this area of their security management. Vulnerability Management tools have been identified by most analysts and many companies as being key to overall IT risk reduction strategies. The advantage of a capable Vulnerability Management system is that it can use vulnerability scanning to constantly monitor the network for exposure to known vulnerabilities, and thus inform the risk management and risk reduction processes included in the ISMS in near real-time.

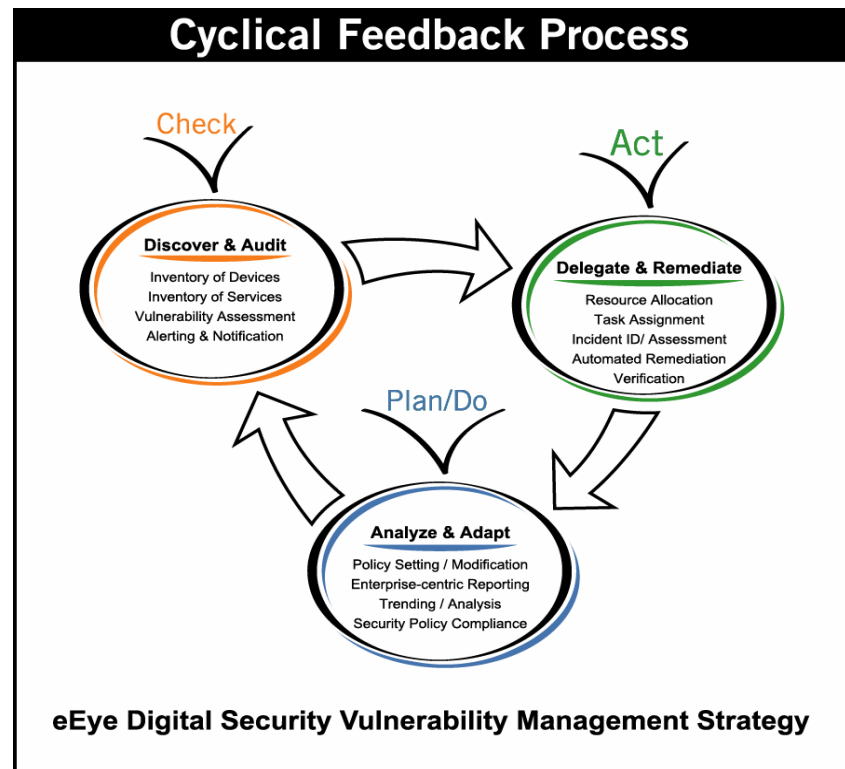
Attempting to perform such assessments with manual scanning tools, or regular external audits and penetration tests, is no longer viable due to the proliferation of new vulnerabilities and the shrinking window between vulnerability publication and the public release of exploit code. Enterprise solutions, such as eEye Digital Security’s Enterprise Vulnerability Assessment and Remediation tools, enable organisations to effectively meet this challenge.

Plan – Do – Check – Act

A well-established ISO methodology for process management is PDCA, or Plan Do Check Act. PDCA has also been incorporated as a best practice approach to security process management for BS7799 compliant ISMS. One of the core concepts behind PDCA is that it is a cyclical feedback process, using “lessons learned” to drive improvement through each iteration of the cycle.



With respect to the special case of IT vulnerabilities, eEye Digital Security have defined a three phase Vulnerability Management Cycle which incorporates all aspects of a vulnerability-focused IT risk reduction process. The eEye Vulnerability Management Cycle is fully supported by its Remote Enterprise Manager (REM) software, in conjunction with Retina, the industry leading network vulnerability scanner. This process can be directly mapped to the ISO and BS7799 Plan Do Check Act structure as follows:



Three Phases of Vulnerability Assessment & Remediation

Using eEye’s advanced network vulnerability scanner, Retina, eEye’s Vulnerability Assessment and Remediation solution handles the complete process – from the asset identification and auditing phase, through the review and remediation stage, to final verification of fixes. eEye’s complete Enterprise Vulnerability Assessment solution incorporates Retina and a sophisticated events management system to manage the entire process and minimise resources needed to undertake this critical security initiative.



Phase 1: Discovery & Auditing

In order for an organisation to assess its networks, it is important to understand its constituent digital assets. Therefore, the first step in the vulnerability assessment and remediation process is asset

identification. Though elementary, the Discovery Phase is an important first step in understanding the range of devices on a network. Retina quickly identifies and maps all of these elements in a centralised database.

As previously discussed, an indispensable component of information security risk management is auditing your entire network for vulnerabilities. Retina Network Security Scanner offers comprehensive auditing capabilities and unparalleled speed, accuracy, and ease of use. With thousands of Retina scanners deployed worldwide, Retina has evolved to be the industry's most effective scanning engine.

Phase 2: Delegate and Remediate

Upon discovery of network issues, the task of assigning vulnerabilities for remediation can be simplified with an automated solution that incorporates a security events management system. eEye's Enterprise Vulnerability Assessment solution is designed for large, distributed enterprises that have expansive networks that must be protected. For smaller organisations, the stand-alone capabilities within Retina meet the delegation needs of IT and network security personnel.

The Remediation Phase encompasses the "fixing" of the issue. eEye's technology provides hands-on fixes that resolve issues correctly – the first time. Detailed remediation instructions guide administrators through the process of correcting network vulnerabilities before an attacker can exploit them. After a patch or fix has been applied, a follow-up Retina scan serves as verification that the issue has been addressed and corrected.

Phase 3: Analyze & Adapt

Reporting, trend analysis, policy settings, and resource management are all part of the Analyze & Adapt Phase of the vulnerability assessment and remediation management process. In accordance with a BS7799 compliant ISMS, this stage provides the necessary documentation to prove that the proper security measures are being completed on a regular, ongoing basis.

With comprehensive auditing tools like Retina Network Security Scanner, the unification of process and technology is simplified. Most importantly, implementing eEye's solution yields results and measurable security value for organisations of all sizes that are moving towards BS7799 compliance or full certification.



Summary

“[eEye’s Enterprise Vulnerability Assessment solution] becomes more than just useful for the enterprise; it becomes an asset. This is a product worth having.”

Source: *InfoWorld* (2/21/03)

- Although BS7799 compliant organisations must address the gamut of information security issues, software vulnerabilities and misconfigurations are a special case, due to the constantly changing vulnerability landscape.
- While more conventional business risks can be assessed on a periodic basis, near continuous vulnerability scanning is required to stay ahead of the curve of software vulnerabilities and misconfigurations.
- According to the CERT® Coordination Center, 99% of attacks are based on known vulnerabilities for which countermeasures exist. Organisations that implement a comprehensive Vulnerability Management system, in conjunction with a BS7799 Information Security Management System, will be able to control these vulnerabilities and substantially reduce their attack surface.
- This special case of IT vulnerabilities can only be addressed with specific tools that provide accurate vulnerability scanning as well as features to manage the process of remediation and business workflow.
- Solutions such as eEye Digital Security’s Enterprise Vulnerability Assessment and Remediation solution meet the needs of companies seeking BS7799 compliance, or full certification, by providing a comprehensive, process based approach to managing the risk of IT vulnerabilities.

To learn more about eEye Digital Security’s Enterprise Vulnerability Assessment and remediation management solution, visit:

<http://www.eeye.com/html/Solutions/EnterpriseVA/index.html>



For more information about ECSC’s full range of information security services, visit:

www.ecsc.co.uk

