

MAXIMIZING THE BENEFITS OF A PENETRATION TEST

Penetration Tests Minimize the Real Costs of an Attack Against your Network

According to a survey conducted in 2005 of U.S. corporations, government agencies, universities, and financial and medical institutions:

- Respondents reported more than \$130.1 billion in financial losses from computer security breaches
- The most serious financial losses occurred through virus attacks (more than \$42.7 billion), unauthorized access (more than \$31.2 billion), and theft of proprietary information (more than \$30.9 billion)
- 65% of respondents detected system penetration from the outside



Organizations that have implemented effective network security solutions may still have vulnerabilities, or holes, within their network. New vulnerabilities in networking devices, operating systems and applications, are regularly identified and reported in the media. Explicit details on how to exploit these vulnerabilities are rapidly available in numerous online locations, and are freely available to hackers and disgruntled employees alike.

To detect these vulnerabilities, many organizations rely on automated *vulnerability scans* using tools such as eEye's Retina, or Nessus. Although these cans provide a quick estimate of overall security, they are prone to false results, and require skilled interpretation to provide value to the organization.

Penetration tests, sometimes referred to as "ethical hacking" pick up where scanning products leave off.

A penetration test is a controlled and managed model of an actual system intrusion by a trusted tester. It gives a realistic demonstration of an attempted break-in into your network, showing the real threats that you face from an outside intruder or an internal employee or business partner.

The Benefits of Penetration Testing

As a component of your organization's defence-in-depth security strategy, penetration testing provides several benefits:

- Identifies systems that are prone to attack, or that may already have been compromised
- Identifies gaps in the overall implementation of security, allowing organizations to rapidly implement the most cost-effective action plan to mediate risks
- Helps managers to create and support business decisions, focusing their security budget or other resources on where they are needed most

- Develops trust with strategic partners, suppliers, customers and others upon whom business depends
- Fulfills requirements for regulatory compliance
- Independent security audits are becoming a requirement for obtaining cyber-security insurance

When to Conduct a Penetration Test

Penetration testing, like all elements of corporate security and privacy operations, is a business function. Before initiating penetration testing, the organization must have an Information Security Policy in place to provide the necessary strategic guidance. In addition, it should have identified the most valuable corporate assets through a formal risk assessment process.

Once these steps have been completed, penetration testing that directly supports the business can be put in place. Testing can occur at several points, including:

- Periodic repeat testing – An organization should regularly schedule penetration tests of the network at least two times per year. These tests should be conducted by at least two different testers (internal and external third parties, or multiple external third parties) to maximize the chance of identifying different vulnerabilities
- Deployment of new network infrastructure - Every new network infrastructure should be thoroughly with both external and internal tests. In addition, the introduction of new technologies such as wireless or Voice over IP should be tested

- Changes/upgrade to existing infrastructure - Whenever the existing infrastructure is changed, it should be tested again to ensure that new vulnerabilities have been introduced. The amount of testing required will depend on the nature and level of the changes made to the infrastructure. This is particularly important when new partners gain access to your network, particularly in the from a corporate merger or acquisition
- Implementing or changing a business critical application - New applications (whether Internet facing or Intranet hosted) must be tested before they are put into production, particularly if a risk assessment identifies the application as being business critical. Major changes involving the functionality of the application should be thoroughly retested
- Major HR challenge – Following dismissal of an employee with privileged access (system administrator, database administrator, information security operator), the security of the network should be confirmed and documented

Penetration Testing Strategies

When considering the strategy to select when designing a penetration test, there are three parameters to consider – the attacker/defender knowledge profile, and the attack route, and the scope.

The attacker/defender knowledge profile applies is concerned with the base knowledge of the “attacker”, or tester, and the “defender” (the employee responsible for monitoring the network to guard against intrusions). Several perspectives can be chosen:

In a “**white box test**”, the tester has complete knowledge of the internal network’s architecture, operating systems, and applications prior to testing. This strategy mimics the worst-case scenario where the attacker has complete knowledge of the network.

DigitalDefence recommends that organizations employ this strategy at least once per year to maximize the number of vulnerabilities identified during testing

A **black box**, or “blind”, testing strategy aims at simulating the actions of a real hacker. The tester has no prior knowledge of the target network. The tester might be given a website address or IP address and told to attempt to crack the website as if he were a hacker. The results of this testing methodology highlight identified vulnerabilities in a very compelling manner!

The impact of this testing strategy is lessened by the fact that it is more time consuming and expensive than full knowledge testing because of the effort required by the testing team to research the target.

More importantly, by focusing on a single attack path that was successfully used during testing, it may neglect other direct and indirect paths to the targets that might be used by attackers. Therefore, DigitalDefence recommends that this strategy not be employed until a full-knowledge test has been conducted to identify the maximum number of vulnerabilities.

A **double blind testing strategy** is an extension of the blind testing strategy. The organization’s IT and security staff are not notified of the testing beforehand – they themselves are “blind” to the testing activities. This strategy can be used to test the organization’s security monitoring and incident identification, escalation and response procedures.

Double blind tests must be carefully monitored to ensure that the organization’s incident response procedure is responsive, and terminated before it can escalate to involve law enforcement

Some testing strategies utilize a **gray-box** or **crystal-box** approach, in which the tester simulates an inside employee with an account on the internal network and standard access privileges. This test assesses internal threats from employees within the company.

The attack route describes the perspective being used by the tester to “attack” the target network. There are two attack routes:

An **external testing strategy** refers to attacks on the organization’s network perimeter using procedures performed from outside the organization’s systems (Internet or Extranet). It should be noted that a tester who successfully attacks a device on the perimeter can usually escalate the attack to devices on the interior of the network.

Internal testing is performed from within the organization’s technology environment. This test mimics an attack on the internal network by a disgruntled employee or an authorized visitor. The focus is to understand what could happen if the network perimeter were successfully penetrated or what an authorized user could do to penetrate specific information resources within the organization’s network.

Testing strategies can also be described in terms of scope, which generally refers to how much of the organization’s network is allowed to be tested.

A **full-scale**, or network, strategy generally allows all parts of a network to be tested (with the exception of components defined as being out of scope). This broad strategy allows the attacker to focus on a particular vulnerability, and then extend it to attack multiple points within the network.

In contrast, a **targeted testing strategy** typically involves both the organization’s IT team and the penetration testers. A targeted testing approach may be most efficient and cost-effective when the objective of the test is focused on a particular technology (e.g. remote access/VPN), or a business critical application.

Types of Testing

Penetration testing constitutes a broad range of testing methodologies and types. Different approaches will be used to review an “average network” versus testing of a specialized technology or particular application. Some of the different types of penetration testing are defined below:

- Application security tests evaluate the logic of a particular application as it interacts with the existing network in support of the business objectives. It may include a source code review, which looks for poor programming techniques that may introduce later vulnerabilities, such as buffer overflows. It also ensures that there are no “back-doors” put in place by the programmers to allow for later access into an application
- Denial of Service, DoS testing assesses your network’s ability to withstand an attack that would render it unavailable for use by its legitimate users

NOTE: DigitalDefence does not endorse the use of this type of testing. A DoS test can cause a production network to fail. Furthermore, given the number of ways to introduce a DoS state, it is virtually impossible to conduct a test and identify a network as being vulnerable or not vulnerable to a DoS

- Firewall testing reviews the physical and logical configuration of a firewall to ensure that it complies with corporate security and privacy objectives and that the rule set is providing an adequate amount of protection to the organization
- Remote access tests ensure that the means that remote employees and partners are using to access the network are secure, no confidential data is leaking from the network, and that all ingress and egress points are protected against human and automated attacks

- Physical assessments ensure that the “walls, doors, and locks” used to secure networks are doing their job, and that physical controls in place are adequate to ensure both personnel and material safety
- War dialing identifies the network resources that are vulnerable to attack through telephony systems such as analogue modems
- Wireless network security is a matter of significant concern, as considerable leakage of data can occur if the wireless network is not as secure as the wired network
- Social engineering is the practice of obtaining network access by manipulating people. It is considered the easiest way to gain access because people are generally trusting.

In-House or Third Party Testers?

Should the penetration testers be employees of the organization, or an external third party that performs testing as a service?

Generally, in-house testers (employees) are used when the organization lacks the funds for a third party tester, or when corporate data is judged to be too sensitive for an external agency to see. They are also an excellent resource when the testing is relatively minor (e.g.: introduction of a new file server) or the testing is of limited breadth, such as testing for the presence of a newly reported vulnerability

Employees usually lack the training and experience required to be effective penetration testers. By hiring an external third party that is skilled in this type of test, you are maximizing the number of vulnerabilities that will be found. In addition, their reliance on a defined methodology and practice in providing this service will generally result in a faster, more effective, and cheaper penetration test.

External third parties are mandated to comply with some regulatory agencies (the financial services industry in particular). As well, by outsourcing the

penetration testing, you are outsourcing potential liability as well.

The best perspective is to consider the penetration testing arrangement with an external third party as “partner sourcing” – ensure that there is the maximum transfer of knowledge to internal employees so that they can understand and participate in the penetration testing process. At the same time, ensure that all parties understand and accept the limitations of internal testers, and know when to involve a skilled third party

The Penetration Testing Process

Although the exact penetration testing methodologies will vary among testers, they generally follow the same series of phases:

- Discovery, in which information is gathered on the target organization through Web sites and mail servers, public records and databases
- Enumeration in which the penetration tester actively tries to obtain user names, network share information and application version information of running services
- Vulnerability mapping in which the test team maps the profile of the environment to publicly know vulnerabilities
- Exploitation; in which the test team will attempt to gain privileged access to a target system by exploiting the identified vulnerabilities

The Risks Associated with Penetration Testing

Any penetration test is subject to the following limitations:

- A penetration test is a “point-in-time” snapshot; it can never be considered to be 100% comprehensive. If a new vulnerability is identified following completion of the test, then that vulnerability must be tested against the network
- The testing activities may inadvertently trigger events or responses that may not have been anticipated or planned for (some tests may result in network or server failure, or employees may notify law enforcement authorities)
- Sensitive security information may be disclosed, increasing the risk of the organization. For example, the testers will usually identify weak userID / password combinations, which could be used to compromise a network if accidentally released

Controlling Risks – The Secrets of a Successful Penetration Test

In order to ensure success, DigitalDefence has identified 10 critical success factors:

1. Manage the Penetration Test as a Formal Business Project

Penetration testing, like all aspects of information security, is a business process. Therefore, it must be managed as a business process.

It is important to have the scope, objectives and terms of the penetration testing engagement clearly and fully articulated in writing. The roles and responsibilities of each participant in the project should be clearly defined. Project management, activity monitoring, ongoing communication expectations and how incident management will be handled should be formally documented.

If penetration testers are corporate employees, their actions should be documented in advance, and penetration testing should be conducted as a routine business process

When external 3rd penetration testers are employed, the business expectations should be documented prior to vendor selection in the Request for Proposal (RFP) document

The vendor should then create a statement of work (SOW) based on the RFP that specifies its rules of engagement that all parties agree on

Create detailed confidentiality agreements and nondisclosure agreements, and verify these with an attorney

2. Ensure the Penetration Test Conforms to the Corporate Information Security Policy

The corporate Information Security policy is the executive-approved document that articulates the organization’s security strategy and its practices for complying with that strategy

The final deliverables from a penetration test should directly support the security policy and corporate strategy; the results should not emphasize tactical-level or short-term technologies or practices.

Therefore, the testers should be familiar with the corporate Information Security Policy. External testers should ask to see the security policy in advance of the testing.

3. Identify Legal and Regulatory Requirements

Compromise of sensitive or confidential data, and failure to prove the practice of due diligence in securing such data can lead to fines and even jail time for the company officers responsible. For Canadian companies engaged in cross-border data transfers, compliance with regulations such as the Sarbanes-Oxley Act can be critical.

The penetration testers must be fully cognizant of security and privacy laws in all jurisdictions in which your business is operating.

In addition, they should be knowledgeable in the regulations that may govern the industry vertical to which your organization belongs.

4. Define the Terms of Engagement (TOE)

The Terms of Engagement identify the “rules” governing the testing activities; they define the activities that are permitted, and the activities that are prohibited

At the very least, the TOE should include:

- Objective(s) of the penetration test
- Provisions for the business-focused management of the penetration test: change control procedures, escalation and dispute resolution procedures; representations, warranties and remedies; as well as defining liability if anything goes wrong
- Responsibilities of the organization, and the tester (internal or third party)
- Types of tests to be performed, including known risks of the tests being performed
- Description of what activities are in bounds, out-of-bounds
- Timeframe for testing
- Criteria for “success” of the penetration test
- Criteria for classifying vulnerabilities (low, medium, high)
- What to do if sensitive information (e.g.: passwords, client transactional information) is discovered, or high-level vulnerabilities

The objective of the test may be any one of the following:

- Breach, or by-pass, the perimeter of the test network
- Gain access to any hosts or databases that are accessible from the Internet, or targets that are accessible from the inside of the network
- Identify known actual or potential vulnerabilities in a network, host, or desktop, or an application
- Any or all of the above (unrestricted)

Responsibilities of the Organization

The organization will supply the following information to the tester:

- A list of target IP addresses and / or address ranges
- A list of target domain names (blind scans only)
- Any specific targets (domains, hosts, databases, applications) that will receive a special emphasis during testing
- Targets within the specified target range that are specifically excluded from the penetration test
- Restrictions on date and time of testing
- Defined escalation process to deal with "high" level vulnerabilities, or other network or testing issues

If testing is being conducted on-site the organization must provide the tester with appropriate connectivity and a physical location to test from.

If testing is being conducted from a remote location, the organization must ensure that the tester has sufficient authentication to complete the tests.

Some additional points to consider during penetration testing:

- Avoid introducing major network changes while the test is occurring — the test should reflect a stable network, and introducing new changes to your network infrastructure will produce inaccurate results
- Perform backups of critical systems prior to testing to ensure recovery should data become damaged
- Decide who in your organization will know about the test – it is best to have few personnel know about the test so that employees are not tempted to modify the network's security configuration
- Define a Point of Contact, POC, person. This should be the single person for the tester to contact for all matters. The POC should be knowledgeable regarding the testing being conducted, the network being tested, and should have the authority to initiate or halt the corporate incident response. Have a defined escalation path for the tester to follow if the POC is unavailable, with full contact information for all parties

Tester Responsibilities

The tester will provide a Primary Point of Contact and backup points that can be reached immediately so that all testing activity can be stopped in case of problems encountered during testing

For remote testing, the tester must supply the IP address or range(s) that will be used to scan or attack the organization's sites

The tester will use the accepted corporate methodology or the methodology documented in their reply to the Request for Proposal to perform the Penetration test

All vulnerabilities identified will be reported to the organization; vulnerabilities judged as being of "high" or "medium" criticality will be manually confirmed to eliminate false-positive results

If a third party tester is used, they will use the most qualified staff within their company to perform penetration tests; the business should retain the right to approve each member of the team performing the test, and to review their CV to assess qualifications and experience

In order to avoid business interruptions, the test items that are out of scope must be fully identified. These may include some or all of the following:

- Placing any executable application or script on a network device or host
- Gaining control (administrator root access) of any network device or host
- Removing or altering any file (configuration, content, or any other file) located on a network device or host
- Any Denial of Service (DoS) testing or other testing that could cause an increase in network activity, or otherwise impact network or server performance
- Physical access to the premises for the purpose of gaining information or actual access to the network by any means (unless physical access testing is specifically identified as an element being tested during the penetration test)



The TOE must be approved by the business organization's executive or senior management, and the tester must accept and agree to abide by all conditions of the TOE prior to the beginning of any testing.

5. Define Deliverables in Advance of the Testing

Before starting the penetration test, review reports previously delivered by the tester to a client. These reports should be “sanitized” to remove references to company identities, IP addresses, or host names.

Overall, the deliverables should focus as much as possible on providing quantifiable information (e.g.: number of low, medium, high vulnerabilities) that will allow the business to focus on achieving a measurable improvement with each successive penetration test

If the reports do not support the business objective of the penetration test, both parties should work to develop a format that is acceptable

In general, the business should expect two separate reports, each aligning the penetration test with the corporate Information Security Policy – the Executive Summary and the Technical Report.

The Executive Summary (2 to 3 pages) will consist of at least the following items, stated in a brief, high-level format:

- A brief opening statement that “a penetration test was conducted against <the business’s external network / internal network / specific application/ source code on <date> by <tester> using the following methodology <briefly describe>”
- A statement comparing the business tested to its industry peers (this may not be used in cases of targeted testing, or application-specific tests)
- A statement regarding the strategic level of security that was observed during testing
- General statements regarding the number of vulnerabilities identified
- Recommendations to mediate the identified vulnerabilities
- Any other material deemed relevant in a high-level executive summary

The Technical Report will consist of at least the following items:

- A statement comparing the business tested to its industry peers (this may not be used in cases of targeted testing, or application-specific tests)
- A detailed overview of the testing methodology used, including an attack-flow description and/or diagram
- A detailed findings section, which includes a full description of all terms used. For each vulnerability that is identified, the following should be presented in a separate Table or Excel spreadsheet : Name / CVE number (if available) for each vulnerability identified; description of the vulnerability; demonstration of the vulnerability (if available) using screen; systems affected (list ALL systems affected by IP address and/or system name); risk analysis – impact if exploited (high / medium / low); ease of exploitation (high / medium / low); steps to mediate the risk – these steps should be detailed enough so that a reasonably skilled network administrator can follow them, and mediate the identified vulnerability; ease of mediation – direct financial cost of mediation (high / medium / low); personnel and time costs to mediate vulnerability (high / medium / low)
- Supporting Appendices, such as administrative contacts during the test, a list of all IP addresses assessed during conduct of the test, a list of all tools (open source, proprietary) used during testing, including version numbers used, and other material as required

When reviewing the format of the documentation, also review the final deliverables will be released to the company in a secure manner.

In addition, it is the responsibility of the business to secure access to these documents once they are received from the tester

6. Ensure the Appropriateness of the Selected Vendor

Make sure your tester possesses the skill and experience to test every component of your network. If not, either consider another tester or look into using multiple testers. If you select multiple testers, select one to manage the project, and have that tester subcontract with the others

Ask for references — although many penetration testing clients do not want their name given for security or privacy reasons, some companies are willing to discuss their experience with penetration testing vendors.

Make sure the tester possesses adequate liability insurance in the event of unapproved damaging consequences of testing

7. Fully Evaluate the Individual Tester(s)

A penetration test is only as good as the individual doing the testing; therefore, when working with an external third party, ensure that you are comfortable with the individuals as much as with the third party vendor!

Identify what security certifications the testers hold. Common security certifications include CCIE: Security, CEH, CISSP, CCSP, GIAC, OPSTA, and Security+. Alone, these certifications do not guarantee that an individual is a good tester – consider them to be a baseline defining “acceptable testers”, and then evaluate each individual’s experience (previous engagements, references, ability to respond to technical questions)

Beware of the “bait-and-switch” – approving one third party for testing based on the experience of a key individual, and then having that individual replaced at the time of testing. Ensure that the Terms of Engagement give you the right to approve of substitutions

Confirm whether the vendor hires former black-hat hackers — it is best to avoid testing firms that advertise hired hackers because you cannot be sure the hacker is going to be completely ethical in his or her behavior

The tester should either provide you with documentation on criminal background checks of employees, or you should perform your own background check on their employees

Finally, as always, ask for references

8. Identify the Test Methodology and Tools Used

The penetration tester should always use a documented, repeatable methodology. This increases the quality of the test because it minimizes repeated or missed steps. It also allows the business to review the methodology at a later point in time to confirm whether a new vulnerability would have been identified in a previous test

Ideally, tests will be based on an acknowledged standard such as the Open-Source Security Testing Methodology Manual (OSSTMM), or a documented and internal approach

All penetration testers rely on tools to assist them in assessing the network. If open source tools or exploit code is used against your production network, ensure that the tester has validated these tools in a lab prior to use ensure their safety

A redundant suite of tools should be used to minimize or eliminate false results

A list of all tools used, including license information, should be included in the Technical Report

9. Ensure Control of Raw Test Data and Final Results

Penetration testers typically have access to extremely sensitive security information about a business's network. Until any identified vulnerabilities are mediated, the

Technical Report is a "road map" of how to hack your network

In working with a tester to design a penetration test, you should consider the following:

- How and where will information that is collected, including working paper files, be stored? In electronic form? In physical form?
- Who has, or will have, custody of this information?
- How much information will the final reports and executive summaries contain?
- How will notes, working papers and other forms of information be retained or destroyed?

DigitalDefence recommends that all raw data, drafts, and final reports be encrypted during storage and transport to the client. Strong encryption (128 bit AES) should be used.

When the testing is finished, and the business has taken possession of the final results, the tester will either retain a copy of the test report for archival purposes and trend analysis, or destroy all material pertaining to the client. Any retained material must be stored in an encrypted state. If customer material is to be destroyed, a Certificate of Destruction should be issued to the client to provide assurance that no confidential material remains

10. Integrate Penetration Testing Results into a Vulnerability Management Process

The greatest failure of penetration tests is not the discovery of vulnerabilities, but the lack of an auditable process to eradicate them.

In contrast to penetration tests, vulnerability management is the business process that provides for a security program with a budget and resources to address and mediate the discovered vulnerabilities

A vulnerability management process is a manual or automated process for:

- Regularly obtaining threat and vulnerability information pertaining to the business's network
- Scanning and/or supporting penetration tests to identify vulnerabilities
- Storing vulnerability and mediation information to support trend analysis
- Managing trouble tickets pertaining to vulnerabilities
- Managing the implementation of patches and security fixes in hardware, software, and applications
- Generating both executive and technical level reports
- Supporting audit requirements to ensure compliance

Vulnerability management is a requirement to ensure that all security holes identified during a penetration test are fully addressed by the organization

Conclusion

The proliferation of threats, from both the outside and the inside of the network, have ensured that penetration testing will be a required component of all network security programs

However, penetration testing on its own will not secure a network. Organizations have to ensure that the final step of "patching the holes" is completed, and that that mediation is fully documented

Most importantly, organizations have to change their focus from identifying vulnerabilities to identifying *WHY* there are vulnerabilities – if penetration testing is part of the security and business strategy, what part of the strategy or the underlying process can be improved to minimize the occurrence and impact of vulnerabilities?

DigitalDefence – Penetration Testing Support

DigitalDefence offers penetration testing to our clients as a professional service; it builds on our unique strengths as an industry leader:

- Deep knowledge of existing vulnerabilities - ISIS, our proprietary database, contains over 20,000+ known vulnerabilities and their exploits, as well as the means for fixing them
- Redundant testing environment - We scan for vulnerabilities with commercial, open source, and proprietary tools that re-scan for vulnerabilities to fully identify false positives and negatives
- Modular design - Some optional tests that we may conduct in consultation with you include:

Password Audit - Under strict supervision of our client, we will harvest and attempt to crack user and administrator passwords in order to evaluate the strength of passwords chosen by employees

Wardialing - Using a modem to dial a range of phone numbers used by your organization, we will attempt to locate insecure modems that can be used to access your network

Firewall / IDS audit - DigitalDefence will conduct an audit of your perimeter security controls, ensuring that they are configured to enforce your Information Security policy

Social engineering - DigitalDefence will attempt to by-pass the people who enforce your security through a variety of means, such as looking over their shoulders while they enter data ("shoulder surfing"), looking for data that has been disposed of ("dumpster diving"), and asking for users to give up passwords or other confidential information

Website integrity assessment - Defacing websites for political reasons, or even as a form of graffiti, is the most common security breach occurring today. DigitalDefence will help you to guard against attack on your website

Application assessment - We will assess the security of particular business critical applications, such as web servers, mail servers, ftp servers, databases, and others

- Scorecard approach - allows organizations to track their progress towards achieving a more secure network
- Intelligent reporting - Written vulnerability reports are created and assessed by a experienced consultants, not automated scripts that may contain false results
- Customer-tailored reports - Separate versions are prepared for executive and technical staff. The final report can be used as a decision-making tool to identify the probability and potential impact of network intrusions

Additional information is available at:
http://www.digitaldefence.ca/index.php?pro_pentest

DigitalDefence is also an industry leader in providing organizations with cost-effective training to implement their own penetration testing program

Our Attack and Defence of the Network is an intensive course delivered over 5 days. It delivers these vital objectives to IT and security practitioners:

- Provides a business-driven assessment methodology that ensures technical processes are fully aligned with the business strategy and practices
- Provides the skills to manage internal and external testers, maximizing the value of their testing for your organization
- Builds a strong awareness of the risks and threats faced by your organization
- Teaches the real-world techniques used to attack networks and systems; students use the same methodology employed by DigitalDefence consultants as part of the Penetration Testing service
- Provides clients with the understanding and practical skills required to defend against these attacks

When they have completed this course, students will know how to generate effective reports that will help their organization to improve security.

The Attack and Defence of the Network course is available at both the Foundation and Advanced Levels; additional information is available online at:
<http://www.digitaldefence.ca/index.php?id=6>



DigitalDefence – Your Partner in Security

Founded in 2001, DigitalDefence is the premier provider for Information Security, Privacy and compliance solutions in Canada. From the development of a corporate security strategy through the delivery and management of services, DigitalDefence helps organizations to conduct business in a secure and trustworthy fashion.

The benefits of partnering with DigitalDefence include:

Canadian Focus - DigitalDefence is focused solely on our Canadian clients and how they do business in the Canadian business environment. We know the marketplace, and the unique issues that we all face

Business-Focused - All of our consultants have extensive industry experience, and many of our consulting engineers have MBAs and other financial qualifications in addition to their strong technical expertise.

At DigitalDefence, business requirements drive the technology of our security solutions - not the other way around

Standards-Based Solutions - By basing our security solutions on the international Information Security management standard, ISO 17799, we adhere to the globally accepted best practice for the management of Information Security

End-to-End Methodology - We follow a documented, repeatable methodology that is driven by your business requirements. The methodology follows the lifecycle of the service or solution through the plan, design, implement, and management stages

Thought Leadership - DigitalDefence is dedicated to becoming the knowledge leader of the present environment and future trends in Information Security in Canada. We frequently speak on security at public events, and are proud to be a co-founder and sponsor of Canada's largest security user group, TASK (www.task.to)

Technology Leadership - DigitalDefence supports strong research and development program with continuous training of our Information Security specialists. We strive to continually advance our knowledge and practical skills

Vendor Neutrality - We recommend solutions without any bias towards product vendors.



DigitalDefence is Canada's trusted provider of Information Security services to protect priceless information assets from internal and external compromise, enabling enterprises to focus their resources on their business objectives. Our Information Security Management Model encompasses the complete life cycle of your projects – planning, design, implementation, and management. This foundation supports the professional services, managed services, and the training we employ to rapidly and cost-effectively secure your business, maximizing your return on investment. DigitalDefence provides the support to protect your strategic information resources, and focus on your core competency – your business.

© DigitalDefence, Inc. 2005. All rights reserved.
This data sheet is for informational purposes only. DIGITALDEFENCE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.
DigitalDefence, Inc. • First Canadian Place, 100 King Street West • Toronto, ON M5X 1K7 • Canada
(416) 306-5775 – voice (416) 644-8801 - fax
www.digitaldefence.ca