

# THE COMPUTERWORLD HONORS PROGRAM

## CASE STUDY

LOCATION:  
*Boston, Massachusetts, United States*

YEAR:  
*2006*

STATUS:  
*Laureate*

CATEGORY:  
*Business and Related Services*

NOMINATING COMPANY:  
*Morgan Stanley*

### ORGANIZATION:

**Core Security Technologies**

### PROJECT NAME:

**CORE IMPACT**

### Summary

Core Security Technologies developed the first comprehensive penetration testing product for accurately identifying and exploiting specific network vulnerabilities. Until recently, organizations relied on expensive consulting firms or a patchwork of homegrown tools to test their network security stance. With the introduction of Core Security's CORE IMPACT, any system, security or network administrator can easily test the security of their network in an organized and repeatable environment, identify what resources are exposed, and determine if their current security investments are actually detecting and preventing attacks.

### Introductory Overview

Incorporated in 1996 by six founders with extensive backgrounds in information security, mathematics and communications, Core Security Technologies is now an international information security company with sales and marketing operations in Boston, Massachusetts and its development center in Buenos Aires, Argentina. During its history, Core has developed commercial software products for other security vendors, collaborated with leading consulting firms to provide information security expertise and published extensively in the industry. Core's nominated submission for this award focuses on the creation of CORE IMPACT, the first penetration testing product for identifying an organization's information security risks.

Penetration testing is a localized, time-constrained and authorized attempt to breach the architecture of a system using attacker techniques. It provides an accurate and comprehensive view of an information security stance, as it evaluates an entire system, exploiting vulnerabilities to determine precisely what information is at risk. The granular results of penetration testing make it possible to immediately prioritize corrective measures and to set the overall direction for an organization's security strategy.

Until recently the ability to perform a penetration test belonged to a select few specialists with years of experience. The testing process itself has historically been a manual, tedious, expensive and time-consuming procedure of applying public-domain or home-grown testing tools to determine how an attacker might gain access to a network and disrupt businesses. However, with



# THE COMPUTERWORLD HONORS PROGRAM

## CASE STUDY

**ORGANIZATION:**  
*Core Security Technologies*

**PROJECT NAME:**  
*CORE IMPACT*

**LOCATION:**  
*Boston, Massachusetts, United States*

**YEAR:**  
*2006*

**STATUS:**  
*Laureate*

**CATEGORY:**  
*Business and Related Services*

**NOMINATING COMPANY:**  
*Morgan Stanley*

the introduction of CORE IMPACT, that has all changed. Core has now made it easy, efficient and cost-effective for any network engineer or administrator to perform penetration tests.

CORE IMPACT is the first product that allows organizations to safely use actual attacker methodologies in real-world attack scenarios. With just a point and click, CORE IMPACT enables a user to actively exploit vulnerabilities within a network, replicating the kinds of access an intruder could achieve. CORE IMPACT easily and efficiently helps organizations safely understand their networks' vulnerabilities before an attacker does. With CORE IMPACT, organizations can now:

- \*Conduct all testing procedures methodically in one visual software package
- \*Test for external and internal vulnerabilities, including those that relate to how network components work together
- \*Compromise systems where vulnerabilities are found
- \*Advance from machine to machine, exploiting vulnerabilities and subsequent vulnerabilities that emerge from existing network relationships
- \*Report precisely where a network could be penetrated, as well as the associated security risks, and provide precise information so immediate corrective action can be taken
- \*Test their network on an on-going basis using frequent updates of exploits (attacks), which are provided regularly, typically 4-6 times per month.

### Benefits

A security breach by a malicious hacker, virus or worm can cost an enterprise or organization millions of dollars in damages as well as incalculable harm to its reputation. By safely, efficiently and quickly identifying how vulnerable assets can be breached, penetration testing gives security professionals the information they need to help them better secure their network. Core Security Technologies has significantly altered the way that penetration testing is conducted by companies with the introduction of CORE IMPACT. CORE IMPACT replaces expensive, inconsistent manual penetration testing performed at best once a year, with a professional, state-of-the-art automated penetration testing product that enables regular, on-going testing.

In the absence of commercial penetration-testing software, companies were previously limited to the following two options:

- \*Hiring a consultant who uses proprietary and publicly available software for penetration testing--This option is expensive and its results are not consistent across all environments. Furthermore, manual testing is not easily repeatable and the testing itself (due to costs and manpower allocation) is usually performed infrequently. Also, testing effectiveness depends on the skill of the tester, not the quality of the product.
- \*Internally develop their own penetration-testing capabilities--It is difficult and for companies to find security professionals with sufficient knowledge to develop safe attacks internally. This option requires a substantial time investment from highly specialized and costly individuals. Alternatively, using publicly available tools also poses significant challenges, as the code has not



# THE COMPUTERWORLD HONORS PROGRAM

## CASE STUDY

**ORGANIZATION:**  
*Core Security Technologies*

**PROJECT NAME:**  
*CORE IMPACT*

**LOCATION:**  
*Boston, Massachusetts, United States*

**YEAR:**  
*2006*

**STATUS:**  
*Laureate*

**CATEGORY:**  
*Business and Related Services*

**NOMINATING COMPANY:**  
*Morgan Stanley*

undergone rigorous quality assurance tests, which can sometimes lead to inaccurate test results or even damage to network assets.

Demonstrating a new direction from the above options, CORE IMPACT enabled First State Bank Assistant Vice President Jason James to replace his organization's need for consulting firms and full time experts. "Doing these penetration tests manually would have taken us forever," said James. With CORE IMPACT we were easily and quickly able to determine which of our network defenses were performing up to expectations. If I had tried to do this without CORE IMPACT, I would have had to hire a full-time specialist to do the work."

Additionally, CORE IMPACT helped James prioritize remediation efforts by eliminating unnecessary work on false positives. "CORE IMPACT is a tremendous value. It automated numerous time-consuming tasks, it simplified the work and it made my department and me more efficient."

Through its detailed reporting capabilities CORE IMPACT also helped First State Bank comply with all its regulatory requirements. "Not only was I able to meet the FDIC's and the Texas State Banking Commission's requirements, but also IMPACT helped me comply with my additional yearly external audit. With CORE IMPACT, I now have an unprecedented level of knowledge, confidence and proof in the security of my network."

CORE IMPACT is the only penetration testing product for IT personnel who must efficiently assesses the specific threats to their organization. Business benefits of CORE IMPACT include:

- \*Enabling a proactive rather than reactive approach to IT security decisions
- \*Avoiding the costs that result from network outages/downtime due to security breaches
- \*Ability to safeguard organizations' key assets by providing a comprehensive assessment of internal and external security risks
- \*Improving compliance with government and industry regulatory requirements, with upfront knowledge that your network is both secure and compliant
- \*Informing companies as to whether the security infrastructure (e.g., IPS, IDS, Firewalls) they have purchased are working and delivering the expected level of security
- \*Providing an objective way to test and justify additional security purchases;
- \*Improving remediation efforts by knowing the specific compromisable assets and being able to more intelligently prioritize remediation tasks

### The Importance of Technology

The ever-increasing threat of attack poses a critical problem for public and private institutions. This growing threat is caused by a combination of increasingly sophisticated and automated attack tools, the rapid rise in the number of vulnerabilities being discovered and the increasing connectivity of users. As systems are opened to employees, customers and trading partners, networks become more complex—and more susceptible to security breaches. That is why information security is one of the most challenging and complex issues facing companies today.

One of the best sources for cybercrime information in the United States is the "CSI/FBI Computer Crime and Security Survey." This annual survey found that financial losses related



# THE COMPUTERWORLD HONORS PROGRAM

## CASE STUDY

**ORGANIZATION:**  
*Core Security Technologies*

**PROJECT NAME:**  
*CORE IMPACT*

**LOCATION:**  
*Boston, Massachusetts, United States*

**YEAR:**  
*2006*

**STATUS:**  
*Laureate*

**CATEGORY:**  
*Business and Related Services*

**NOMINATING COMPANY:**  
*Morgan Stanley*

to unauthorized access to information and theft of proprietary information are rapidly increasing. Together, they now account for close to one-half of the total annual explicit financial loss experienced by the survey respondents. And, if implicit costs (e.g., loss of sales due to negative corporate image) were included, these categories alone would account well over half the financial losses.

These recent trends in cybercrime make it more critical than ever that organizations acquire a true assessment of their security vulnerabilities so they can identify and address those vulnerabilities associated with their most valuable information assets. A recent edition of the survey estimated the average cost of a security breach to be \$203,000. Note that the cost of a single serious breach can potentially be far worse than this figure discloses. For example, the average remediation cost to companies breached by the MS Blaster worm was \$475,000. Larger companies reported losses up to \$4,228,000.

An organization's true vulnerability to threats can be determined only by answering the following questions in regards to each of your identified vulnerabilities:

- \* Is the vulnerability real, or is it a false positive?
- \* Can the vulnerability be exploited?
- \*What is the value of the information exposed by the exploited vulnerability?

Clearly, the answers to these questions will allow organizations to prioritize their vulnerabilities and structure their security strategies as effectively and efficiently as possible. This is in contrast to simply identifying vulnerabilities and then attempting to address them based only on assumptions about risk. One of the easiest and fastest ways to obtain these answers, both initially, and on an on-going basis, is to perform a penetration test on their network with CORE IMPACT.

### Originality

Securing network infrastructures is about managing security risks. And to assess those security risks, organizations have historically turned to vulnerability scanning. Vulnerability scanning surveys a network and identifies all the potential vulnerabilities that exist. However, it does not address the implications of a successful intrusion. Vulnerability assessment only lists what the potential vulnerabilities are, and does not probe deeper to reveal the true threat to assets when a vulnerability is exploited. Organizations need to understand the actual risk to their business posed by vulnerabilities, and performing a penetration test with CORE IMPACT is the best option.

CORE IMPACT is the first, most comprehensive and most intuitive product that goes beyond the data yielded by vulnerability scanners to enable safe, real-world attacks on IT assets. Using its patent-pending technology, users actually exploit vulnerabilities in their networks and try to replicate the kinds of access an intruder or worm could achieve. With CORE IMPACT companies can identify what resources are exposed and determine if their current security investments are detecting and preventing attacks. Network administrators are better able to prioritize and verify the volumes of information received from a vulnerability scanner, saving days and weeks of time otherwise spent on finding a network's true weak points. So, if it is necessary for an organization to understand the actual risk to its business posed by a vulnerability, then CORE



# THE COMPUTERWORLD HONORS PROGRAM

## CASE STUDY

**ORGANIZATION:**  
*Core Security Technologies*

**PROJECT NAME:**  
*CORE IMPACT*

**LOCATION:**  
*Boston, Massachusetts, United States*

**YEAR:**  
*2006*

**STATUS:**  
*Laureate*

**CATEGORY:**  
*Business and Related Services*

**NOMINATING COMPANY:**  
*Morgan Stanley*

IMPACT is its best and only option.

### Success

CORE IMPACT User Scottish Re exemplifies many of the common benefits experienced by Core's customers. Mark Odiorne is the Senior Network Systems Manager at Scottish Re, a publicly-traded (NYSE:SCT) global life reinsurance specialist and issuer of customized life-insurance based wealth management products for high net worth individuals and families.

To protect the network and meet regulatory demands, Odiorne and Scottish Re had hired a security consultancy to perform monthly and quarterly vulnerability scans. During its monthly security scans, the consultants often revealed potential vulnerabilities in Odiorne's network, but did not probe deeper to evaluate the extent of the threats posed by the individual vulnerabilities or the implications of successful intrusions. Furthermore, if Scottish Re made any changes to network security following the scans, Odiorne had to wait until the next scheduled visit by the consultants to determine if those changes created new vulnerabilities, or if any previously identified vulnerabilities remained. Additionally, after the consultancy revealed vulnerabilities to Odiorne, he needed to test each vulnerability to assess the potential risk it posed to Scottish Re's network—a process that typically took him several hours a month to complete.

Odiorne was able to completely eliminate the use of outside consultants. He uses CORE IMPACT continuously throughout the month to test the overall security of Scottish Re's network. If a change to his network occurs, Odiorne has the ability to run CORE IMPACT immediately, rather than wait for the next scheduled appointment with the consultants he previously used. "We get immediate, on-going results with Core," Odiorne said. "IMPACT validates the risk each vulnerability poses, saving us the time and money we spent each month remediating false positives. Also, I now have the added benefit of being able to test my patches to be sure they are deployed correctly."

CORE IMPACT also helps Scottish Re meet its various compliance requirements. To maintain its license as an insurer, the company undergoes frequent standard insurance audits of its security measures. In the past, these audits also revealed potential vulnerabilities that Odiorne had to examine to ensure his company was not in violation of insurance regulations. Now, using CORE IMPACT, Odiorne is able to instantly prove to auditors that his network is as secure as he says. As Odiorne puts it, "Core is the final stamp of approval."

IMPACT has allowed Odiorne to accomplish his goal of internally validating the security of Scottish Re's network. "With IMPACT we don't have to overextend our staff and budget in order to achieve the peace of mind of knowing that our network is protected," he said. "I now sleep better at night."

CORE IMPACT was immediately embraced by security-conscious organizations that recognized the shortcomings in the way penetration testing had been done in the past. Illustrating the growing demand for comprehensive penetration testing products at security-conscious organizations, Core's customer base has more than doubled each of the past three years and CORE IMPACT is now used by more than 300 organizations worldwide. Core's customer base now includes leading organizations in a broad variety of industries—spanning all branches of the US armed forces, government agencies, and regulated industries such as healthcare and financial services, to major corporations in the technology, telecommunications, manufacturing, retail



# THE COMPUTERWORLD HONORS PROGRAM

## CASE STUDY

**ORGANIZATION:**  
*Core Security Technologies*

**PROJECT NAME:**  
*CORE IMPACT*

**LOCATION:**  
*Boston, Massachusetts, United States*

**YEAR:**  
*2006*

**STATUS:**  
*Laureate*

**CATEGORY:**  
*Business and Related Services*

**NOMINATING COMPANY:**  
*Morgan Stanley*

and media, entertainment and travel companies.

The broad adoption of Core's penetration technology reflects a major shift that is taking place in security technology as companies awaken to the need for more proactive measures to strengthen their security postures. In fact, industry analyst firm IDC predicts that penetration testing, will take a larger share of the security software market over time compared with passive security, as represented by vulnerability scanning. In addition, Core has just received further validation of the importance of its technology by the leading technology analyst firm Gartner, which named Core a "Cool Vendor in Security and Privacy" for 2006.

### Difficulty

Because Core Security entered a technology space with no established commercial software vendors, its primary challenge has been to educate the market on the utility, availability and safety of its penetration testing software, while continuing to build a market-changing product. Since the company's primary challenge lies in the fact that most organizations are unaware that comprehensive penetration testing product is commercially available, Core has invested considerable effort in educating businesses on the proactive measures they can take to secure their networks. These efforts have resulted in a change in the buying habits, security budget allocations and use frequency of a large number of organizations toward a more proactive approach to network security.

The company's CORE IMPACT product was designed specifically to overcome the stigma that all penetration tests are disruptive in nature. Core devotes significant ongoing research to staying abreast of current threats and assuring that its products enable organizations to exploit those threats safely on their network as part of the penetration testing process. CORE IMPACT offers a complete suite for penetration testing in one package designed to minimize the possibility of system damage, while offering capabilities significantly beyond those available to the common hacker.

And finally, to be effective, a penetration testing product needs to remain up-to-date on the latest attacks. To ensure IMPACT has regular updates 1-2 times a week, Core Security has established a team that is completely devoted to creating new, safe exploits and maintaining and improving the product's existing exploits. This is not a trivial effort. Writing safe exploits requires significant programming skills and technical expertise. Furthermore, the exploits also have unique capabilities (e.g., support for additional attack vectors, support across the life-cycle of each exploit). Core's strength in developing exploits has earned it great respect in the world of security researchers, and has put the company's exploit developers in demand for teaching others how to write exploits.