

AUTOMATED PENETRATION TESTING PRODUCTS

Justification and Return on Investment (ROI)

EXECUTIVE SUMMARY

This paper will help you justify the need for automated penetration testing software and demonstrate the positive Return on Investment (ROI) that can be achieved by acquiring a product such as CORE IMPACT Pro. It reviews the latest trends in cybercrime, outlines the cost of security breaches, and demonstrates how penetration testing can help manage vulnerabilities to defend against these threats. It further provides examples of how to calculate an ROI to help justify acquiring an automated penetration testing product. As you will see, each case study reveals a significantly positive ROI, making the purchase decision easily justified.

THE COST OF SECURITY BREACHES

A critical problem for public and private institutions is the increasing threat of attack. This is due to a combination of increasingly sophisticated and automated attack tools, the rapid increase in the number of vulnerabilities being discovered, and the increasing connectivity of users. As systems are opened to employees, customers and trading partners, networks becomes more complex and are more susceptible to a security breach. That is why information security is one of the most challenging issues facing companies today

It's difficult to put a dollar figure on the cost of a security breach. Companies that experience breaches often don't report them, fearing negative consequences to their reputation and exploitation by their competitors. Even if they do report them, victims of a breach seldom know how to quantify their loss. But there are industry statistics available that can give you a rough idea of what it will cost your organization if a breach does occur.

One of the best sources for computer crime information in the United States is the "CSI/FBI Computer Crime and Security Survey."¹ According to the report, cybercrime includes the following categories: viruses, unauthorized access, theft of proprietary information, denial of service, insider net abuse, laptop theft, financial fraud, system penetration, sabotage, spear phishing, instant messaging misuse, internal bots, theft of customer/employee data, abuse of wireless network, password sniffing, website defacement, misuse of public Web application, exploit of DNS server, and telecom fraud.

The 2008 edition of this survey reports the average cost of addressing a security breach to be roughly \$289,000. Note that the cost of a single serious breach can potentially be far worse than this figure discloses. For example, the theft of at least 45.7 million customer records in 2006 cost TJX \$40.9 in one legal settlement alone.

Industry statistics are a valuable starting point when calculating the cost of a breach, but clearly they don't reflect the unique characteristics of your business. For example, what is your organization's reputation worth? How much will it cost your organization if your critical services go down for a day? When it comes to your business, only you can provide accurate answers to these questions.

EFFECTIVELY MANAGING VULNERABILITIES WITH PENETRATION TESTING

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. Your 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?
- ▶ Are there any sensitive systems or data exposed by the vulnerability?

Clearly, the answers to these questions will allow you to prioritize your vulnerabilities and structure your security strategy as effectively and efficiently as possible, instead of simply identifying your 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 ongoing basis, is to perform a penetration test on your network.

A penetration test is an authorized, local attempt to "hack" into a system, to identify exploitable weaknesses, and to reveal what systems and data are at risk. The tester may use several methods to gain entry to the target network, often initially breaking into one relatively low priority section and then leveraging it to attack more sensitive areas. Your organization is probably already running (or

¹ "2008 CSI Computer Crime and Security Survey," Computer Security Institute Publications:
http://www.gocsi.com/forms/csi_survey.jhtml

considering running) vulnerability scans on your network and/or web applications, and you may wonder what penetration testing offers you that vulnerability scanning does not. It's simple: A vulnerability assessment tells you only what an attacker can *potentially* do to your environment. A penetration test tells you what an attacker *can definitely* do to your environment.

That's because penetration tests *exploit* identified vulnerabilities, just as an attacker would. Unlike vulnerability scans, penetration tests leave little doubt as to what an attacker can or cannot do. Penetration tests eliminate the guesswork involved in protecting your network by providing you with the information you need to effectively prioritize your vulnerabilities.

CALCULATING RETURN ON INVESTMENT (ROI) FOR CORE IMPACT

Since IT and security budgets are tight, many organizations undertake an ROI analysis for new software purchases to justify product acquisitions. Let's see what this would look like for penetration testing software.

To calculate ROI we need to know both the investment for the software as well as the returns generated. Clearly, the investment is the cost of the software, \$30,000 per year for a license of CORE IMPACT Pro to test up to 512 IP addresses from a single machine (talk to your account executive for pricing specific to your testing needs). Typically, returns are realized in the form of increased revenue or reduced or avoided costs – either direct out-of-pocket cost savings or indirect savings, such as employee productivity gains. Additional cost savings are realized from intangible benefits that are hard to quantify, but are often significant. Examples of these include avoiding negative publicity or maintaining a trustworthy public image. Since the intangible benefits vary greatly from company to company, in this analysis we'll simply use a factor of the direct costs to estimate their value. We'll conservatively estimate this to be 20%.

Let's now look at the types of savings users of penetration testing products typically report:

Direct Savings:

1. Prioritized remediation efforts

An automated penetration testing product will help you safely understand which vulnerabilities are actual paths of attack that must be eliminated, thereby enabling you to focus your staff appropriately. To calculate what cost savings this represents, estimate what percent of your staff's time is spent working on vulnerabilities that don't represent real threats to your organization. For example, if you have 2 network administrators that cost on average \$70,000, and each spends 10% of his time in these activities, this cost is \$14,000 annually.

2. Increased staff productivity

If you are implementing manual penetration tests and creating exploits internally, then using an automated product will allow you to conserve valuable staff time. To calculate the savings this represents, you need to determine the following:

- ▶ How many hours are your security managers and team members devoting annually to building and running manual pen tests?
- ▶ How much is this time worth?

For example, if you assume a single security professional makes \$100,000 per year and is spending 25% of his time on creating exploits and running manual pen tests, this represents an annual cost - and potential savings - of \$25,000.

3. Avoid cost from network outages/downtime from security breach

Once a security breach occurs, there is a direct cost to recovering from it. Industry estimates of this cost range from \$100,000 to tens of millions. The estimates include IT staff time spent remediating the problem (e.g., bringing servers back up, installing patches on servers and PCs, etc.), lost productivity of employees due to network downtime and, in some cases, lost revenue. If you can't estimate this cost for your organization, you may want to use the average cost of \$289,000 noted earlier from the CSI study.

4. Ability to meet regulatory/audit requirements and avoid fines

An automated testing product will help you meet the auditing/compliance aspects of regulations such as PCI, GLBA, HIPAA, and Sarbanes-Oxley. Violators of these regulations are subject to criminal penalties with fines up to \$5 million and 20 years in prison (Sarbanes-Oxley). Automated penetration testing products provide you with a detailed record of every testing action performed, and can help avoid these penalties. In our case studies below, none of these companies has been assessed a fine, so we have omitted this cost.

Intangible Benefits:

1. Improved security and associated peace of mind

Using an automated product allows you to consistently test your network and easily integrate the practice with your overall security program. This means you'll have more confidence in the overall security of your network.

2. Ability to preserve corporate image and customer loyalty

A single incident of compromised customer data that becomes public can cost a company significant amounts of customer goodwill and market reputation. The nature of your business determines how important this is to your organization. This could be a fraction of the direct savings, or a significant multiple.

3. Ability to justify existing security investments

You can use an automated penetration testing product to evaluate and test the effectiveness of deployed (or proposed) security products, such as IDS and IPS, to see if they are actually detecting and preventing attacks. This will help you determine if you are getting, or will get, the promised return on your security investments.

As mentioned earlier, we conservatively estimate Intangible Benefits as 20% of Direct Savings in the case studies below.

CASE STUDIES

The following are customer case studies demonstrating the ROI for CORE IMPACT Pro, the leading automated, commercial-grade penetration testing software solution from Core Security Technologies.

Financial Services Case Study

This case study involves one of America's largest specialty mortgage companies. The Information Security Officer (ISO) and his group determined that they needed to more effectively audit and validate their vulnerability findings. The ISO felt that while his current security tools did a good job of detecting potential vulnerabilities, they did not help him determine if the vulnerabilities they had discovered were real or if they posed an actual risk to their network resources. This lack of reliable

information also made it challenging for him to prioritize his team's remediation efforts: "I didn't know if my engineers were spending time working on the most mission-critical projects."

Ultimately, this corporation turned to CORE IMPACT Pro as their solution. IMPACT Pro made it possible for them to determine whether a vulnerability was real and its actual impact on network resources.

Annual Return on Investment for Automated Penetration Testing

Direct Savings:

- ▶ Increased staff productivity: The major return on investment in this case is increased productivity. By acquiring IMPACT Pro, this company freed a significant amount of their security manager's time as well as significant time for every member of his staff. Assuming this company has a staff of four security specialists, each making approximately \$100,000 annually. The manager makes \$150,000 annually. If IMPACT Pro saved the manager and his staff even 20% of their time on an annual basis, the cost savings would be \$110,000:

$$0.2 * [(4 * \$100,000) + \$150,000] = \$110,000.$$

Intangible Benefits

- ▶ In this case, the company avoided the costs of loss to reputation, and loss of service to customers had the company suffered a major security breach.

Annual ROI

Direct Savings	\$110,000
Intangible Benefits @ 20% of direct	<u>+\$22,000</u>
Total Savings	\$132,000
Cost of CORE IMPACT Pro	<u>-\$30,000</u>
ROI Savings	\$102,000 per year

Healthcare Case Study

This case study involves a group of five leading healthcare providers. The challenge at this organization was to comply with HIPPA legislation, which designates the way healthcare institutions must implement, monitor and audit the security that is employed to protect information stored on their networks.

The security manager decided the only way the group would meet HIPPA requirements would be to perform regular network penetration testing. He had previously attempted manual penetration testing and found it to be time-consuming and a strain on his limited budget and resources. Upon deploying CORE IMPACT Pro the security manager realized several immediate and significant returns, including immediately increasing the productivity of his staff. The security manager was also able to use IMPACT to evaluate and test the effectiveness of his IDS and IPS solutions by safely launching real-world intrusion events. He was therefore able to prioritize his team's remediation work by determining which vulnerabilities posed real threats to corporate information assets and eliminating wasted efforts on false positives.

In addition, IMPACT Pro helped him avoid a major loss. "By proactively testing our network with CORE IMPACT, we discovered and fixed a potential help desk and IP telephony problem that could have been very detrimental to how we service our customers. If we didn't have CORE IMPACT, it would have been a significant amount of time before the problem was identified." The security manager estimated that had this threat been exploited, his systems would have been down for 24-48 hours.

Annual Return on Investment for Automated Penetration testing

Direct Savings

- ▶ Increased staff productivity: One security staff member would have to put in three months of work annually to penetration test as thoroughly as IMPACT Pro. As the average staff member at this company makes \$100,000 annually, the annual cost savings in this area is \$25,000.
- ▶ Avoided network outage: What would it have cost the organization if their critical services had gone down for a day? One way to estimate this is to use the \$289,000 figure provided by the CSI/FBI Survey representing the average cost of a security breach. Another way is to estimate this would have cost them 5% of their daily operating expenses. Total operating expenses from their annual report were \$509,171,375. Divide this by 365 and we get \$1,394,990. Then multiply this by .10 to estimate the cost of an outage in lost productivity and poor customer service and we get \$139,500. Since this is less than \$289,000, we'll use the more conservative number.

Annual ROI

Direct Savings	\$164,500 (\$25,000 + \$139,500)
Intangible Benefits @ 20% of direct	<u>+\$32,900</u>
Total Savings	\$197,400
Cost of CORE IMPACT Pro	<u>- \$30,000</u>
ROI Savings	\$167,400 per year

CONCLUSION

By now, you probably have a general idea of CORE IMPACT Pro can do for your organization. Whether your return on investment from the product will ultimately be generated by direct savings such as increased team productivity, intangible benefits related to preserving corporate image and customer loyalty, or some combination of the two, the end result you will achieve by acquiring CORE IMPACT Pro will be the same: a strong return on your investment and a more secure IT environment.