

# White Paper

## The Business Case for a Network Security Assessment

# Introduction

Why does any business need a Network Security Assessment?

Try answering that question with another question: how long could your organization afford to shut down its revenue stream?

When an organization suffers a security breach, the effects are felt immediately across the organization, not just in the IT department. It doesn't matter if the breach occurred through vulnerable web applications, leaked passwords, a poorly-configured firewall, an un-patched operating system or a misplaced zip drive; when the exploit is discovered, the common response for any company is to take the systems off-line to diagnose the source.

Typically, that means revenue-generating platforms like websites or web applications, or the backup systems that support them, will be off-line until the issue is fixed and the vulnerabilities are remediated.

Even for a small-to-medium organization with as few as ten people and as little as \$500,000 in revenue, an NSA is an essential process for ensuring operational continuity where:

- Their applications must be available to conduct business
- Their customer data needs to be protected
- Consumer confidence and trust is critical to their business
- Industry and security compliance applies to their industry
- It is necessary to protect brand and reputation

Just as companies take out insurance to protect their property and assets, an NSA is a risk-mitigation tool to help ensure that data disasters don't disrupt or permanently cripple existing business operations.

Network security is more critical than ever for three simple and interrelated reasons:

- Any disruption of revenue stream during today's tough market conditions can potentially bankrupt an organization.
- Given the pervasive nature of cyber-crime today in the form of SQL injection, cross site scripting, phishing and other types of attacks which can be deployed simultaneously to thousands of targets, it is not a question of whether your network will be attacked, but when. Companies that have not locked down their network will suffer consequences.

- A disruption to business operations from a security breach made inevitable by deferring security measures costs significantly more than an NSA for the vast majority of businesses.

# Protecting Your Cash Flow

In the current recessionary economic climate, companies are looking to cut back on all budgets. Layoffs are practically epidemic and capital investments have been mothballed. During this time, there is the need for organization to focus on maintaining current operations and keeping revenue generating IT infrastructure and applications up and running. Organizations not looking at security during uncertain times are placing their business at risk.

The average reported losses from data breach incidents were \$288,618, according to the CSI Computer Crime and Security Survey. The financial consequences for some specific attacks such as from botnets (\$345,600 average per respondent) were significantly higher.

Meanwhile, Darwin Underwriters suggests with their Identity Theft Data Loss Calculator that the full extent of an average-sized security breach can reach much higher costs (including brand damage control and civil litigation settlements) in the \$9 million to \$14 million range. This could cripple even large and very established organizations. The Ponemon Institute suggests that such a breach might cost around \$6.5 million ("Costs of a Data Breach" New York Times).

These studies vary in the numbers of their respondents and their methodology, so of course the numbers do not exactly match. The fact remains clear that industry analysts agree that the cost of a data security breach is significant.

But even before a company deals with longer-term liabilities suggested by those experts, businesses will have to deal with unique losses depending on the scale of their business and their daily revenue stream.

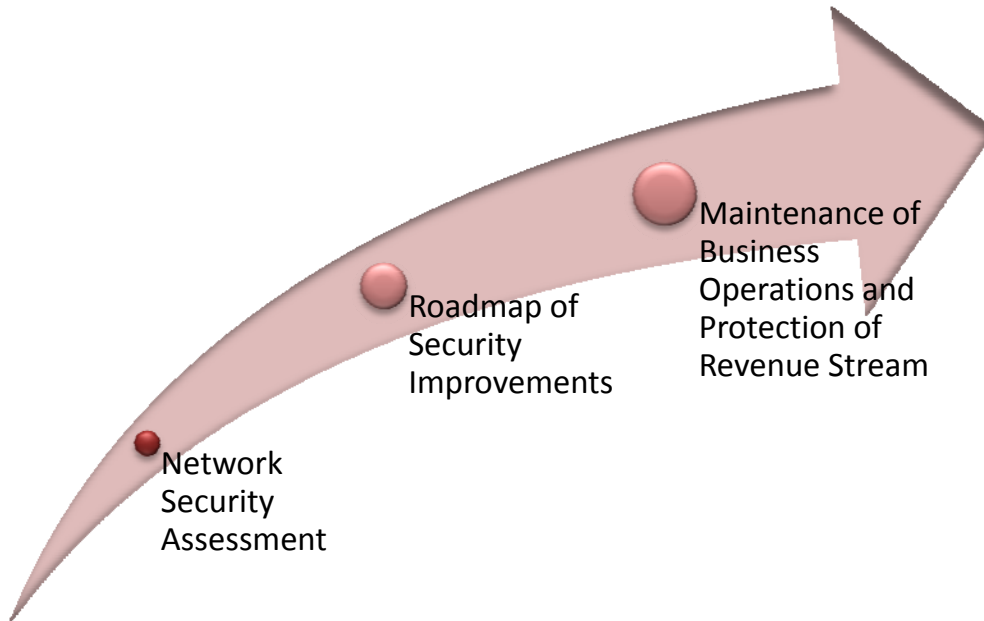
As a company's network allows access to databases across departments from multiple points of entry, when a data breach occurs the damage is not limited to the resources that the IT department must devote to fixing the issue. IT systems and applications are closely linked and integrated. Forensic investigation may require review and analysis of several components of your IT operations to diagnosis the source of the breach, fix any issues and close off vulnerabilities.

During our experience helping our customers to maintain continued IT and business operations for 15 years, including recovery from security breaches, we've found that to bring systems back on line can take an average of at least a day and a full diagnosis and remediation for prevention of future disruptions can range as long as several weeks. As more IT assets across the network are typically discovered later, to also be affected, this results in greater downtime for revenue facilitating applications.

For PCIS' business, non-profit and government clients, loss of revenue during unscheduled downtime hurt revenue streams from sales or donation campaigns in the range of tens of

thousands of dollars. For some organizations, a shut-down of a single day can disrupt a revenue stream that could pay for recommended security improvements many times over.

Obviously, the precise cost to revenue stream from a disruption will vary from organization to organization. But when an NSA can be had for as little as \$8,000, the question is not whether such a solution is affordable, but whether organizations can afford not to take action.



# The Real Need for Protection

While most organizations will be aware in general terms of the threat to data security through their networks, some may still require convincing that it truly is a matter of when, not if, the cyber attack will come.

Evidence suggests that there are literally millions of cyber attacks occurring every week, affecting companies, large and small, established and new. Security defenses based on obscurity won't work against attackers that use automated SQL injection attacks or a combination of phishing and spamming tactics. As one indication of this phenomenon, an automated scan conducted in early 2009 of the top one million websites found on Alexa.com found an average of more than 4,000 of every 50,000 sites were infected with malware.

Even worse, as the economy goes into rougher waters, industry analysts expect more disgruntled laid-off employees will attempt to get back at their former employers, many of whom will not have taken away account access in time to thwart their efforts. Moreover, cyber criminals have an even greater incentive to step up their efforts as they are getting proven return on investment from schemes that can rake in the private financial information of tens of thousands, or even tens of millions of vulnerable victims.

What does a security breach look like for these companies? The website, A Chronology of Data Breaches ([www.privacyrights.org/ar/ChronDataBreaches.htm](http://www.privacyrights.org/ar/ChronDataBreaches.htm)) systematically records these kinds of events. Here are some examples of recent breaches:

□

## **CheckFree Corp., Atlanta, GA (Jan. 6, 2009)**

*"CheckFree Corp. and some of the banks that use its electronic bill payment service say that criminals took control of several of the company's Internet domains and redirected customer traffic to a malicious Web site hosted in the Ukraine. The company believes that about 160,000 consumers were exposed to the Ukrainian attack site. However, because the company lost control of its Web domains, it doesn't know exactly who was hit. And so it must warn a much larger number of customers."*

□

## **Heartland Payment Systems, Princeton, NJ (Jan. 20, 2009)**

*"After being alerted by Visa and MasterCard of suspicious activity surrounding processed card transactions, the company last week found evidence of malicious software that compromised card data that crossed Heartland's network. This incident may be the result of a global cyberfraud operation."*

*UPDATE (1/26/09):*

*Heartland Payment Systems has been sued. The lawsuit seeks damages and relief for the "inexplicable delay, questionable timing, and inaccuracies concerning the disclosures" with regard to the data breach, which is believed to be the largest in U.S. history.*

*UPDATE (2/12/09):*

*According to BankInfoSecurity.com, the number of financial institutions that have come forward to say they have been contacted by their credit card companies Visa and MasterCard in relation to the breach has jumped from fewer than 50 to more than 200."*

□

**Wyndham Hotels & Resorts, Parsippany, NJ (Feb. 16, 2009)**

*"In mid-September, 2008, the company discovered that a sophisticated hacker penetrated the computer systems of one of the hotels. By going through the centralized network connection, the hacker was then able to access and download information from several, but not all, of the other WHR properties and create a unique file containing payment card information of a small percentage of our WHR customers. Potentially exposed through this breach are guest and/or cardholder names and card numbers, expiration dates and other data from the card's magnetic stripe."*

□

**University of Florida, Gainesville, FL (Feb. 19, 2009)**

*"A foreign hacker gained access to a University of Florida computer system containing the personal information of students, faculty and staff. The files included the names and Social Security numbers of individuals who used UF's Grove computer system since 1996."*

As mentioned before, companies that have not locked down their networks with effective security measures and processes will eventually pay the price. As such, an NSA is an essential part of many companies' security strategy.

## Businesses That Need NSA

Businesses need protection from constant attacks on their network. NSA provides a roadmap of security improvements an organization can take to protect their systems and provide better privacy and security compliance for customers.

Many types of organizations have these business needs. More specifically, here are some of the attributes of the kind of company might require the combined components of tools, methodology and expertise that comes with Network Security Assessment.

- Recognizes the need to maintain network security in order to maintain operational continuity
- Uses IP-based physical hardware (servers, workstations laptops), ports, networked printers, firewalls, and manages operating systems
- Requires assistance with Remote Access, Access Control, Password Policy, Segmentation, Encryption, Data Classification, User Account Management, Patch Management, Disaster Recovery and Business Resumption Planning, or Security Awareness and Training
- Needs a third-party expert assessment of IT policies, procedures and quality systems such as an organization's help desk.

Should an organization fit any of these requirements, it should seriously consider using an NSA to ensure operational continuity and to avoid the long-term costs associated with a security breach.



# Works Cited

Darwin Professional Underwriters. "Tech//404: Data Loss Cost Calculator". <http://www.tech-404.com/calculator.html>

Richardson, Robert. Computer Security Institute. "2008 CSI Computer Crime and Security Survey".

Ponemon, Larry. "Costs of a Data Breach – Can You Afford \$6.65 Million?". New York Times. February 4, 2009

"Network Security Assessment Approach Document". Pacific Coast Information Systems Ltd. Feb. 9. 2009.

A Chronology of Data Breaches. [www.privacyrights.org/ar/ChronDataBreaches.htm](http://www.privacyrights.org/ar/ChronDataBreaches.htm)

# About

## Pacific Coast Information Systems Ltd.

Pacific Coast Information Systems (PCIS) Ltd. is a full-service technology and consulting firm based in Vancouver. Founded in 1995, PCIS offers packaged infrastructure and network solutions that enable organizations to address security and compliance issues within today's complex IT environment.

PCIS combines the specific tools, expertise and proven processes to accelerate the problem identification and resolution of security compliance thereby lowering costs for customers.

More information about PCIS can be found at [www.pcis.com](http://www.pcis.com)

## Boonbox

Boonbox, a division of PCIS, was created in 2007. Boonbox provides solutions for identity management, data backup and recovery, and managed network services.

More information about Boonbox can be found at [www.boonbox.net](http://www.boonbox.net)