



INTERNET
SECURITY
SYSTEMS™

Outsourced Information Security Management

A Business Case For Shareholder Value

Updated June 2002

Executive Summary: The Relationship between Shareholder Value and Information Security Management

All year long, you're the hot company to watch. Your employees have never worked harder, or more efficiently. Employee morale and retention has never been higher. Sales are up significantly, both year-to-year and quarter-to-quarter. You exceed analyst expectations. The conference call goes brilliantly. Then, the next day, your stock loses 20% of its value. At the end of the day, it's still falling.

This could easily happen if your mission-critical systems are successfully attacked. And it could happen in spite of what seems like a reasonable, in-house information security program. The result: key information – about your products, your finances, your employees and most importantly, your customers – is compromised. Even if you've enjoyed outstanding customer relationships for years, such a breach could cause you to instantly lose that trust. Your great relationships with the media won't stop them telling the world how a company thought to be infallible can lose it all. Employee morale falls. Your shareholders watch their investment lose value. And no one hesitates to show exactly how they feel about it.

The scenario isn't hypothetical. It has happened. It continues to happen. It will happen again. The question is: how can you make sure it doesn't happen to you?

Chances are, you already do many of the right things. You select the right people to implement your strategies. You insist that they lower expenses to improve efficiency, productivity and profitability. You give them the information and autonomy they need to make good decisions. You define strategic differentiators – those key products, services and qualities that make the difference between you and your competition. And that's where you concentrate your resources.

Think about it from the perspective of your key team members. They take your directive to be efficient very seriously. So, they devote existing in-house staff to core business issues, not "low-priority" functions like security.

And yet: 20% down and still falling.

The Benefits of an Outsourced Information Security Solution

The right outsourced information security provider can help you:

- Focus staff and resources on your key strategic differentiators
- Manage costs and save money
- Improve information protection
- Attract and retain excellent personnel
- Protect your organization's stakeholders

Focus on Your Strategic Differentiators

The fact is, like your physical security systems – alarms, guards, etc. – information security management is neither a key skill nor a key strategic differentiator in your organization. It's unlikely that your customers, the press or your investors will like you any better because you have a good information protection program. People don't notice security – except in its absence.

Analysts like Forrester Research recommend that organizations of all types and sizes consider outsourcing the management of their security infrastructure.ⁱ Your IT staff is most effectively deployed on tasks you know best – information management, systems support, establishment of business functions that make a strategic difference. In other words, information security – like physical security – is more efficiently applied as an outsourced function than an in-sourced one.

Meanwhile, you can enjoy the benefits of an outsourced information systems security approach: You free up both staff and money to focus on your core business issues. Your systems are better protected. You attract and retain technology professionals whose focus is your business. And protect the trust of employees, customers and shareholders.

Manage Costs and Save Money

The decision to adopt a managed network security solution can deliver considerable cost savings – especially when you consider the costs associated with keeping your staff completely up to date on the latest tools, technologies and strategies for both network destruction and information protection. To truly protect your systems on a 24/7/365 basis, you would need to hire multiple security experts, each specializing in different types of security issues, to work around the clock, just keeping an eye on your systems. Especially at today's salaries, that's expensive.

Consider the expenses associated with comparable in-house and outsourced information security management strategies over the first two years of a protection program for a representative small-midsize business:ⁱⁱ

<i>Year One Information Security Management Investment</i>		
Component	In-house	Outsourced solution
Hardware/Software ⁱⁱⁱ	\$60,000	\$60,000
Setup/Installation (one time)	N/A	\$18,000
Management ^{iv}	N/A	\$75,000
Employee salaries ^v	\$180,000	N/A
Employee training ^{vi}	\$24,000	N/A
Totals	\$264,000	\$153,000
Estimated Year One Savings		\$110,000

Year Two Information Security Management Investment		
Component	In-house	Outsourced solution
Hardware/Software	\$8,000	\$8,000
Management	N/A	\$75,000
Employee salaries	\$180,000	N/A
Employee training	\$24,000	N/A
Totals	\$212,000	\$83,000
Estimated Year Two Savings		\$129,000

It's easy to see how the cost of building and training a 24/7/365 staff can spiral out of control. Not to mention the costs associated with employee attraction and retention over time. In just the first two years, you could spend close to a half million dollars on an in-house security plan. Now, project those savings over time. The numbers speak for themselves.

Improve Information Protection

Today's information systems and networks are far more complex than those of even a few years ago. Likewise, the tactics and technologies of today's hackers are growing increasingly sophisticated. As a direct result, information protection strategies must also grow in complexity and sophistication. Yesterday's reasonable due diligence could easily become today's negligence.

If security is not your organization's primary focus, you do not have the research, development, training and personnel resources necessary to keep your security practices up to date. Of course, security is the primary focus of an information security management company. Such a business must extend significant resources toward attracting the most experienced, qualified network security professionals, and toward the development of sophisticated protection strategies for the benefit of their clients. When you outsource information security to a security management expert, the advantages of those resources become yours.

Attract and Retain Excellent Personnel

Nobody has to tell you that as your networks and information systems become increasingly sophisticated, your need for experienced IT personnel grows. At the same time, qualified, experienced computer professionals continue to become increasingly expensive. Those professionals want to focus on the core business areas for which they are hired. They do not want to be taken off task to address "extraneous" tasks such as computer security.

More importantly, as your business continues to evolve, your enterprise-wide information affects everything from the responsiveness of your sales and customer service teams to the quality of your products and services. The security of that information plays a direct role in your employees' ability to focus on your business, and thus, in their overall job satisfaction.

Summary – Protect Your Stakeholders

Many organizations have come to realize that security management in a networked systems environment is a business necessity, especially given the connected and public nature of today's global business environment. A scenario like the one in the opening section of this paper is a very real possibility, even for companies with seemingly well-planned, in-house security practices. It bears repeating: Yesterday's reasonable due diligence could be today's negligence, and tomorrow's disaster.

Fortunately, the decision to select a managed services provider and outsource information security management can create a much more attractive scenario: You attract and retain technology professionals whose focus is your business. You free up both staff and money to focus on core business issues. Productivity soars more than ever. Your systems and information are well protected. You regain and protect the trust of your employees, customers and shareholders. The next quarter is a stunning success. The day after the conference call, the media can't say enough good things about you. Stock value goes up – and continues to gain momentum, quarter after quarter.

About Internet Security Systems (ISS)

Founded in 1994, Internet Security Systems (ISS) (Nasdaq: ISSX) is a pioneer and world leader in software and services that protect corporate and personal information from an ever-changing spectrum of online threats and misuse. Internet Security Systems is headquartered in Atlanta, GA, with additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. For more information, visit the Internet Security Systems Web site at www.iss.net or call 888-901-7477.

Copyright © 2001-2002 Internet Security Systems, Inc. All rights reserved worldwide.

Internet Security Systems, and the Internet Security Systems logo are trademarks of Internet Security Systems, Inc.. Other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.

ⁱ Prince, Frank and Carl D. Howe: "exSourced Security Arrives," *The Forrester Brief* (November 29, 1999).

ⁱⁱ Cost assumptions are based on current market value for security specialists at non-security companies; typical hardware and software needs of most small-medium sized companies, and current hardware, software and services pricing. Figures are approximate and subject to change without notice.

ⁱⁱⁱ Based on a 250-user network using a single T1 Internet gateway. Security elements include single Check Point FireWall-1™ 250-user license running on a Nokia IP330 device, and two Sun Netra T1 servers running Internet Security Systems' Real Secure™ Intrusion Detection and Response software.

^{iv} Annual maintenance costs based on 15% of equipment cost.

^v Employee salaries are based on three salaried employees, each working an 8-hour shift daily and earning \$60,000 per year, while devoting 100% of their on-duty time to managing/monitoring security devices.

^{vi} Employee training includes two courses per year for each employee mentioned above, plus travel expenses.