Security ROI

The costs of network security failures

In a world where computer hacking has become a sport, cyber terrorism is on the rise, and government regulations are becoming more stringent, companies are increasingly concerned regarding the security of their networks. While technology for securing networks has increased, hackers, too, have improved technology and malicious purposes in mind: accessing your confidential information and interfering with your business operations. Hackers have unlimited time to attempt unauthorized entry into corporate networks, and only need to get it right once. Security professionals must defend all attacks, without the benefit of foresight, or risk potentially devastating economic consequences.

The 2004 Computer Crime and Security Survey, conducted by the Computer Security Institute and the FBI, shows that 53% of companies surveyed detected unauthorized use of their computer systems[1]. An additional 10% were unable to determine if they had been attacked or not, leaving only 37% of companies able to report no unauthorized use. Of the incidents, approximately 50% came from inside the corporate network, showing that firewall protection alone is not a complete solution.

The situation is likely far worse, as companies have no incentive to report intrusions or financial loss as a result of malicious attacks. Nothing positive comes from publicly reporting that your network was hacked. Due to this, only 264 respondents (54%) of companies surveyed reported the economic impact of attacks on their networks. They estimated the total loss to be $141,496,460[2]. This represents $535,931 per company. Considering the severe underreporting this information represents, the true losses are likely to be staggering. Indeed all companies recognize the financial risk they assume by not investing further in network security.

Financial views of network security

While corporations understand the importance of network security, IT managers often have difficulty justifying these expenses. Capital budgeting is based on the expected return on investment (ROI) for a project. With no positive cash flows being generated from these projects, many managers are left wondering how to calculate ROI for their security investment; however, if managers are able to prevent the hefty losses described above, the return on investment for security products can be enormous, often with payback periods as short as one month.

To understand ROI for security, we must first understand what comprises making a network secure. Network security is a multi-step process that encompasses assessing, planning, monitoring and enforcing security policies.

The first step of IT security management involves assessing and identifying the security requirements and risks of the business. Better tools allow a higher degree of accuracy in this assessment, which ultimately creates a much more accurate budget for investment. A company whose revenue is generated largely online (e-commerce) or through IT-intensive processes has a higher degree of risk than those who do not. When a company suffers a malicious attack, the economic consequences can be enormous, occurring over several spans of time (see Figure 1). Additional security may be necessary for compliance with government regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), or the Sarbanes-Oxley Act of 2002.

Identification of corporate requirements leads to establishing security policies that define, control and enforce the security arrangement between users and assets. These policies must address the means for identifying and authenticating trusted users and granting permission to use certain resources. They must also define the appropriate use of resources and establish mechanisms for enforcing and remedying violations.

Impacts of Malicious Network Attack	
Immediate	Downtime – idle workers IT must solve problems NOW!
Short-term	Loss of business Potential lost contracts
Long-term	Declining market capitalization Investor confidence drops Loss of brand equity

Figure 1 – The economic impact of malicious attacks is enormous and varies over time (Source: Computer Economics[3]).

After implementation of these security measures, IT must be able to monitor and audit network usage for compliance, keeping the following questions in mind:

- Who is really using the network?
- Are they the intended, trusted users and are they using resources appropriately?
- If network users (or usage) are non-compliant, what is the remedy to enforce the policies?

In terms of driving down cost, the ability to quickly answer these questions is paramount. Less labor is required as a company becomes more efficient at monitoring and remedying its network, allowing more time for proactively evaluating the network for vulnerabilities. The ability to detect any unusual network activity, or possible vulnerabilities, is essential to determining if the network is still secure. When (not if!) network security is compromised, IT must be able to take actions quickly to get at the cause of the violation, to close the breach and to enforce the security policies. Finally, the IT security team must be able to document the details of security breaches in the event that legal action may be taken and to put in place changes that can prevent future breaches.

Calculating ROI

One method for calculating ROI for network security suggested by research firm Computer Economics, as cited by Cisco Systems, recommends performing a break-even-cost analysis of the investment[4]. Determining the complete economic impact of a malicious attack, and dividing this amount by the number of nodes in the corporation provides the break-even analysis price per node. For example, as shown in Figure 2, break-even for a company with moderate dependence on its 5,000-node network would be achieved with an annual investment of approximately $1.68M.

Companies with business models requiring increased e-business operations are at risk of even higher financial impact as a result of malicious attacks. The ROI for security spending is much higher for these companies. Notice that a 5,000-node company with a medium intensity, or moderate, e-business, investing $337 per node will see an ROI of over $2.4M annually.

Number of Nodes	Break-even Spending per Node	Cost of Network Security	Economic Impact of Attacks	Estimated Return on Investment
100	$335	$33,450	$109684	$76234
500	$336	$168,200	$430,614	$262,414
1000	$336	$336,400	$812,897	$496,497
5000	$337	$1,684,900	$4,113,023	$2,428,123
10000	$335	$3,347,200	$6,878,684	$3,531,484
50000	$267	$13,334,000	$25,251,408	$11,917,408

Figure 2 – The complete economic impact of malicious attacks can be based on the number of nodes in the network. Research shows the break-even analysis and the return on investment for various size enterprises that are only moderately dependent on their network. (Source: Computer Economics[5]).

Impact of the Fluke Networks solution

The Fluke Networks solution is a significant asset in network security management and yields a fast return on investment. As pointed out above, network security is a multi-step process and Fluke Networks can play a role in each phase of network security management.

Security assessment and planning. At the outset, IT engineers need tools to assist in security planning. The first step in this effort is getting an up-to-date view of the network resources. This can be a time-consuming and error-prone exercise if done manually. Through the use of Active Discovery, Fluke Networks can automatically provide a fast and accurate inventory of network elements that includes routers, switches, servers, hosts and wireless access points. For example, the OptiView Integrated Network Analyzer begins the process of discovery as soon as it connects to the network. For enterprise-wide visibility, the OptiView Console operates in a centralized location accessing data from Analyzers in remote locations. OptiView Console integrates results from these remotely located network analyzers to provide a single, comprehensive view of the entire enterprise network that enables assessment of risks and documentation necessary for security planning. For monitoring critical gigabit Ethernet links the OptiView Link Analyzer achieves full line rate capture and gives detailed views of traffic to assess risks and document usage.

Security monitoring and policy enforcement. Since the foundation for network security is the knowledge the IT staff possesses about their network, Fluke Networks allows IT to gather and maintain this information on an ongoing basis. With this information IT can determine whether or not the network is secure by being able to answer the critical questions identified above. OptiView Analyzers identify the actual users on the network and allow IT to determine quickly and easily whether or not they belong there. In addition, intruder traffic and activity can be documented. This enables IT to identify traffic that threatens operations and pinpoints it to the source so that policies can be enforced.

Case 1: Eliminating denial-of-service attacks that interfere with application services avoids unnecessary investment of $25K and improves network uptime. In this case, network servers, as represented in Figure 3, are repeatedly overwhelmed by network traffic. IT mistakenly assumes there

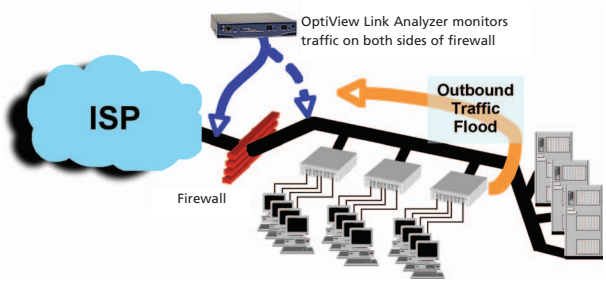

Figure 3 – By monitoring on both sides of the firewall, the source of a denial of service attack can be determined quickly and the firewall policies validated. If the attack was from an external source, firewall policies can be tuned as needed and tested to avoid future attacks from external sources.

is a problem with the firewall and that the problematic traffic is originating outside the network. By monitoring traffic on both sides of the firewall, IT quickly determined that traffic originating inside the firewall is the problem. With this information and the tools to quickly detect these situations, IT verified the firewall and avoided an unnecessary investment on the order of $25,000.

The network engineers used optical taps on the backbone to access traffic on the untrusted and trusted sides of the firewall to view the traffic. As shown in Figure 3, using the OptiView Link Analyzer to characterize the traffic on both sides, they were able to reveal the source of a denial-of-service (DoS) attack.

This quick and accurate visibility of activity on both sides allowed IT to verify the functionality of the firewall and tune the firewall policies. With this type of visibility, the security policies in use are based on the actual traffic. With this configuration, they are able to detect a wide range of intrusions and DoS attacks, locate their origin and mitigate external security threats from hackers caused by configuration problems.

Case 2: More productive monitoring and analysis avoid security incidents and saves $683K over five years. In this network, valuable bandwidth was used for peer-to-peer file sharing that was in violation of established security policies. In addition, denial-of-service attacks were sporadically interfering with application uptime. By reducing troubleshooting time and costs by using the OptiView Integrated Network Analyzer as shown in Figure 4 to quickly and easily pinpoint network problems, IT estimates a savings of more than $653K over five years. By allowing IT to easily find security problems such as intruders and viruses, the company will save

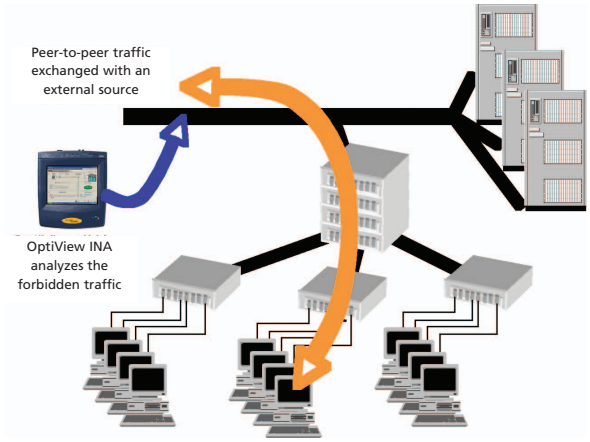

Figure 4 – Overall financial impact of network security is difficult to calculate but quickly pinpointing the type of network attack and its source avoids information losses and network downtime. In this case forbidden peer-to-peer traffic uses valuable bandwidth.

more than $48K in additional security costs over five years. In total, including costs associated with recapturing bandwidth lost to unauthorized use, productivity gains from increased network and application availability, and reduced expenses described above, IT estimates a cumulative net benefit of over $4.8M over the five-year period. For this particular company, these figures represent a annual ROI in excess of 3000% and a payback period of just one month.

Gordon, Lawrence A., Loeb, Martin P., Lucyshyn, William, Richardson, Robert. "2004 CSI/FBI Computer Crime and Security Survey." Computer Society Institute. Available at: http://www.gocsi.com/

[2] See id.

[3] "The Return on Investment for Network Security." Cisco Systems, Inc. Available at: www.cisco.com

[4] See id.

[5] See id.

NETWORKSUPERVISION

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to **www.flukenetworks.com/contact**.