



Not to be Ignored: IT Security Policies and Procedures

Introduction

Companies approach network security in a multi-layered fashion that can include Virtual Private Networks, firewalls, intrusion detection, and multiple encryption methods. Today's threats render many current strategies inadequate; therefore, companies must continually find new ways to address and defend against evolving dangers. One component that is often ignored has quietly always been at the core of a secure IT infrastructure. Companies need to maintain a comprehensive set of up-to-date security policies and procedures. This is easier said than done when taking into account the real world stresses on IT departments -- which is why Zequel Technologies developed *DynamicPolicy*®.

Risks

While risks, threats, and new technologies have grown, most security policies and procedures have become outdated. They often fail simply because they cannot deal with today's threats. Furthermore, new technologies are becoming more ubiquitous, and thus present added security issues.

As hackers become more sophisticated, the risks also become greater. The greater the risk, the more robust and complete the defense that a company must develop, deploy, and continually modify. This can result in increased costs of doing business to defend the corporate network and restore and repair it after an attack. Losses may be incurred from stolen information, lost productivity, and downtime. Other less quantifiable concerns are corporate image and confidential company and customer information. Stagnant policies and procedures are insufficient for dealing with evolving threats. Current and dynamic policies and procedures must be implemented, communicated, and understood.

Problems

According to the FBI, 85% of networks have been hacked at least once. Just recently, over eight million credit card numbers were stolen and had to be re-issued. Social Security numbers were stolen from a University of Texas network. There have been countless denial of service attacks affecting millions of internet users. Banks in the United States, Japan, and Australia have recently been hacked. Attacks today can come from outside or from within an organization. There are many more ways today to breach a network, and the potential losses from such breaches continue to grow.

IT Security policies are critical, but have often been ignored.

Hackers become more sophisticated, resulting in greater risks, more losses, and drive the need to have policies updated regularly.

The risks become more apparent as new products and technologies are deployed and used. According to the Gartner Group, 50% of companies today plan to install wireless equipment. Internet messaging is pervasive, and millions of files, pictures and text are sent every day. Meanwhile, hackers simply listen, probe, and wait for their opportunity to strike.

In addition to maintaining current policies and procedures that can deal with new risks, attacks, and technologies, companies today must be more diligent than ever in demonstrating compliance with internal and external controls, lest they run afoul of auditors. Federal government regulations such as Gramm-Leach-Bliley and HIPAA require adherence to certain levels of confidentiality.

Real World Dynamics

Traditionally, IT security policies and procedures have not been the focus of most companies. In the real world, budgets have been tightened or drastically cut, resulting in fewer projects and a loss of key personnel. IT departments are typically focused on technology, keeping the network running on a daily basis, evolving the network to lower the cost of business, and trying to prevent attacks. As one MIS manager stated, "I would like to take someone off the front lines to focus on policies and procedures, but we are so strapped that I cannot."

How can a company continue to upgrade its network, keep it up and running, manage daily issues, while at the same time attempt to deal with evolving risks (internal as well as external), and adhere to governmental regulations with fewer people, constrained budgets, and minimal knowledge? These are the real-world dynamics faced by many chief executive, financial, information, and security officers.

IT projects that receive the highest priority tend to be those related to security. IDC reported in July 2002 that 40% of IT executives stated their number one priority was network security. According to CIO Magazine, 56% of IT executives surveyed in November 2002 said they will be increasing spending on IT security over the next year. The Gartner Group further supported these findings when it reported recently that these same companies are currently looking at integrated approaches to defend their networks.

The problems and risks are well understood. A November 2002 CompTIA study revealed that 83% of security breaches are attributable at least partly to human error. This critical dynamic has not been adequately addressed, and is the one issue on which many companies need to focus to better secure their IT infrastructure. To do so, an IT department must have as much control as possible over its network, its use and by whom, what runs on it, what gets installed, and how. To exercise even greater control over a network, IT departments must manage not only technology, but also people and policies.

Corporations have cut budgets drastically and IT Directors need to make stark choices about priorities and how to handle policies and procedures.

Research has shown that human error due to not knowing and understanding security policies can be linked to over 80% of breaches.

Some IT directors are beginning to recognize that employing greater control over processes and people via a comprehensive set of policies and procedures is the crucial building block upon which secure networks are built. A recent survey by Aladdin Knowledge Systems indicates that 30% of IT managers are evaluating ways to improve their policy management. However, this means 70% have not yet come to the conclusion that 83% of security breaches have a direct link to human error.

Research in the United Kingdom has shown that executives in almost 80% of companies do not know if their policies have been read and understood by their employees. Companies that realize the direct correlation between comprehensive and up-to-date IT security policies and procedures, coupled with employee understanding of them, are inherently safer. But how does one get there given the real world stresses that IT departments face?

Policy and Procedure Cycle

In order to overcome obstacles to the creation, deployment and enforcement of comprehensive IT security policies and procedures, five essential areas must be considered.

There are five critical steps to developing and deploying IT Security Policies, among them – educating employees and reporting.

Content

A company must first examine how it develops policy content. Given the constraints in most IT departments, two viable solutions exist: hiring a consultant, or drawing upon existing standards and best practices for IT security. Once the content is established, there must next be an easy way to customize it. Policies need to address the particular requirements, revenue sources, and strategies of different businesses. The ability to tailor generic policies to fit the unique needs of each company is essential. Like hardware that is constantly updated with the latest firmware, policies and procedures also have to be easily amended over time to reflect new needs, dynamics, and risks. These things go hand in hand.

Collaboration

The next logical step in the process is for a company to enable collaboration by specific groups to review draft policies. It is typical for one person to own a policy, but s/he includes others in the policy review. A policy is normally approved by the CIO after the review process has been completed. The ability to collaborate and do so easily is essential in addressing time and cost constraints within IT departments.

Distribution

Once a policy or procedure is approved, there must be an easy way to distribute it to the policy's target audience. However, in large companies, managing that distribution can be a challenge because of the proliferation of policies across many departments and business units. The sales department does not necessarily need to see the finance department's policies and procedures, and the company's operations group has its own policies. Business continuity and disaster planning policies and procedures are often reviewed and approved only by the officers of a company. And the IT department has different policies that are specific to its operations. Finally, some policies apply across the entire company. Managing this vast array of policies so that each department has access to only what it needs can be extremely labor intensive. The right solution must facilitate the creation and selection of groups, assign policies and procedures to them, and maintain a logically organized and accessible policy library.

Education

Distributing policies and procedures, whether on an Intranet, CD-ROM, or in a booklet, is only half the battle; it does not ensure that they will be read, much less understood. As the study in England found, the overwhelming majority of companies cannot say with any certainty that their employees have read or understood their policies and procedures. Then take into account the fact that 80% of security breaches can be linked in some way to human error. This is further evidence that a true solution for policy management must provide a means to evaluate employees' knowledge and understanding of corporate policies.

Reporting

For policy management to be truly effective, management needs the capability to monitor which policies have been read and accepted by the intended audiences. Corporate management should have access to on-demand reports that can identify specific groups or individuals who have demonstrated their understanding of critical policies. Likewise, they need to know which employees may need assistance in understanding policies. Management must be able to provide such reports to auditors to prove due diligence.

The Solution

Addressing both the increasing need for more secure networks and the overwhelming task of managing the policies and procedure life cycle can be a major project. Zequel Technologies has developed a web-based application called *DynamicPolicy*® that is a logical and intuitive program that automates the entire policy management process. With *DynamicPolicy*®, Zequel Technologies addresses the real world issues that IT departments face -- time, monetary, and knowledge constraints. In one easy to install and use web-based application, companies can create, collaborate, distribute, educate, and report on their policies and procedures. Periodic updates or amendments can be

The right solution is the one that is least taxing to IT department resources, while at the same time providing the greatest functionality.

quickly and easily distributed, so that policies and procedures stay current. In collaboration with our certified partners, we offer not only the tool, but also the ability to help companies create content that meets their unique business needs and addresses regulatory compliance. Even companies with limited resources can reduce the risks created by outdated policies and procedures, and can easily keep their employees properly informed and educated.

Conclusion

Companies are seeking new ways to protect their valuable IT infrastructure. The one area that has frequently been overlooked is the management of policies and procedures. There is a direct relationship between new risks, outdated policies, the lack of knowledge on the part of employees, and security breaches. More than ever, the success of a company's overall IT security strategy depends upon having a comprehensive set of updated IT security policies and procedures that can be easily created, distributed, and understood by the employees. *DynamicPolicy*® from Zequel Technologies can help companies achieve that goal, because real security begins with total control over technology, policies, and procedures.

Robert Freeman
Director of Sales
www.zequel.com
April 2003