

The Cost of Non-Compliance – When Policies Fail

Elinor M. Madigan
Penn State University
200 University Dr.
Schuylkill Haven, PA 17972
001-570-385-6076
emm17@psu.edu

Corey Petrulich
Penn State University
200 University Dr.
Schuylkill Haven, PA 17972
001-570-385-6211
cme147@psu.edu

Kelly Motuk
Penn State University
200 University Dr.
Schuylkill Haven, PA 17972
001-570-385-6211
kjm264@psu.edu

ABSTRACT

Employees are the greatest threat to an organization's security. Their non-compliance with security policies not only threatens the integrity of the system, it also costs the organization a significant amount of money due to the loss of information or the man-hours spent fixing problems that the user causes. This paper looks at the man-hour cost due to non-compliance at a branch of a large university. We identified what constituted non-compliance and then had the IT staff track the number of hours they spent addressing these problems over a 13-month period. This paper also covers what actions and tools the IT department is using to combat the problem of user non-compliance.

Categories and Subject Descriptors

C.2.3 [Computer-Communication Networks]: Network Operations – *network management, network monitoring.*

General Terms

Management, Security

Keywords

Network Policy, Network Security, Malware, Viruses, Network, Tools, Administrative Staff, Backup

1. INTRODUCTION

We are all concerned with securing our computer systems from the outside intruder, whether it is a virus attack, a hacker attack or a denial of service. The statistics are impressive on quantity of these attacks. For the first three quarters of 2003, 114,855 incidents and 2,982 vulnerabilities were reported to CERT[®]/CC [3]. The 2003 CSI/FBI Computer Crime Survey indicated that an average of \$1.6 million in revenue was lost due to these intrusions [19]. And while this is a substantial amount for external abuse, internal abuse is far more costly. The same CSI/FBI report indicated that the average revenue loss due to theft of trade secrets was \$2,699,842. The average revenue loss due to insider abuse and unauthorized inside access was over \$370,000. The combined loss is over \$3 million due to internal abuse [19]. What is rarely reported is the cost of unintentional damage due to the failure of adhering to the day-to-

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

SIGUCCS'04, October 10–13, 2004, Baltimore, Maryland, USA.
Copyright 2004 ACM 1-58113-869-5/04/0010...\$5.00.

day procedures that are, or should be, in the organizations' information technology policy.

2. COSTS OF VIOLATIONS

The cost involved in resolving policy violations is staggering, involving not only the direct costs of salaries and fees paid to external support but also indirect costs such as the hours lost during down time or when the system's performance is reduced [13]. Consider a 1998 University of Michigan study that estimated that over \$1 million and over 9000 employee hours were spent on investigating and resolving 30 security-related incidents [14].

Viruses and worms are the most reported violations since they affect hundreds of thousands of computers globally. The direct cost of applying patches and software updates associated with the removal of the Code Red worm was approximately \$1 billion. The indirect costs of lost productivity, attributed to the worm, are estimated to be at least \$1.4 billion [1]. ICSA Labs, a division of TruSecure Corporation, estimated that an organization would spend an average of \$81,000 in both direct and indirect costs when cleaning up after a virus attack [4].

One way to help prevent malicious attacks is to apply software patches before the incident occurs. But this is easier said than done. The IT staff is not lazy or unaware of patches; they are wary of patches and understand the cost of patch management. New patches to systems are often untested and when installed can create conflicts within the system which could take the system off-line. Another consideration is the volume of patches available and the time it takes to install them. One estimate is that IT staff spends up to two hours per day managing patches [2]. Internet Security Systems in Atlanta estimated that if an organization has 1000 servers they could spend up to \$19 million per year just installing patches [10].

Another area of vulnerability is the effective administration of computers and at a university this can be a very daunting task. Faculty, staff and students are often free to install software, change the configuration of their computer and are responsible in keeping their system secure. However, most users do not update their software or install the required patches. For example, at Georgia State University an audit revealed that one in five users had no antivirus software installed and of those who had such software 60% of them were outdated. At the University of Texas, the MS-Slammer worm was able to attack the system since 40 of their hosts had not been patched. [5].

3. POLICY

The costs associated with violations are not always easy to calculate, especially at universities. Legal liability, intellectual property issues, delayed research, and damage to reputations are all areas of concern

for which a cost estimate is difficult to obtain. These are items that need to be protected from internal and external threats. [14]. Keeping the network secure is vital, and the security policy is the first line of defense. Without a well-designed policy, the security of the system becomes arbitrary, subject to the capriciousness of the network administrator [6].

Policies should be written so that they are clear, concise and easy to understand - follow what we call the SMARTER rule - Specific, Measurable, Achievable, Realistic, Traceable and **Enforceable**. As Charles Cresson Wood says, "if policies cannot be enforced they will be little more than window dressing" [21]. Vague policies will increase the occurrence of non-compliance.

The security policy should inform the end users of their roles and responsibilities in protecting the organizational assets. The end users at a university are not just employees; they are a diverse group made up of students, faculty, staff, alumni, outside vendors and a variety of other stakeholders. Each and every one of these stakeholders should be educated on the importance of security policies, but education does not guarantee that policies are followed.

People cannot always see what effects a policy might have on them directly. Risks to the system are not always visible or physical. For example, most policies have recommendations about email attachments – don't open them if you aren't sure of their legitimacy and scan them for viruses first. People are often so curious that they will open the attachment anyway, no matter who it's from. Training, intelligence and good intentions do not always lead to compliance.

Educating the end users on the contents of the policies is an essential component to compliance. When the behavior of the end user is such that it must be changed, we must help them conclude that their current behavior is no longer appropriate. People continue to act in the same way because that is the way they always have acted and because their actions have worked in the past. In general, people oppose change because they are comfortable with the way things are.

4. TRACKING VIOLATIONS

Tracking violations is the key to enforcing policies. From January 2002 to May 2004 we used work orders to research what violations occurred. The pool of work orders were from two campus locations that serve approximately 4,500 people. During this time period a total of 9,954 hours were spent fixing problems and 3,706 were identified as non-compliance with policies and standards.

The fewest violations were software and Internet incidents. The software incidents were mostly due to improper configuration of programs, which resulted in rebuilding or reconfiguring the computer. The Internet incidents were configuration issues; some resulting from poor patch management.

Virus and email problems together account for 16% of the total time spent correcting violations. Some incidents involved quarantined documents that were never cleaned, improperly configured programs, and failure to understand that doing a 'live-update' is not the same as scanning the system.

Table 1. Violation Summary

| Type of Violation | Number of Instances | Number of Hours to Correct | % Violation Time |
|---------------------------|---------------------|----------------------------|------------------|
| Software | 30 | 40 | 1% |
| Internet | 106 | 54 | 1% |
| Viruses | 213 | 231 | 6% |
| Email – non virus related | 266 | 362 | 10% |
| Network | 748 | 553 | 15% |
| Hardware | 266 | 582 | 16% |
| Miscellaneous | 709 | 1884 | 51% |
| Totals | 2338 | 3706 | 100% |

Hardware violations included power-on problems, crashes, freezes, stack overflows and total system failures. Many of these incidents were the result of computer overloads due to insufficient RAM. Others occurred because security patches were not updated. Most of the crashes can be attributed to lack of basic maintenance and management of the system.

The greatest number of violations were from network issues. They are also the most severe violations ranging from improper Internet protocol addressing to rogue access points. The majority were login problems and improper connections.

The most time consuming were reported as other or miscellaneous work orders which includes slow network connections. Slow connections have been good indicators that a violation has occurred with improper configurations, unauthorized software or viruses.

5. ENFORCEMENT

5.1 End User Awareness

Effective policy enforcement involves assuring that the policies are understood by all interested parties, regularly checking to see if the policies are being violated, and having well-defined procedure guidelines to deal with incidents of policy violation.

The ability of the end user of an institution to understand its policy is paramount to ensuring that the policies are followed. End users need to be properly educated about their responsibilities and the responsibilities of others, such as outside contractors, managers, directors, etc., as outlined in the policies.

While the initial instruction concerning the policies is important, policy education must not stop there. We must all be constantly updated and informed of the policies that impact our working environment. Information about the policies, and the policies themselves, should be available to the end users. It is better to provide the information proactively to the end user rather than spend time, and thus capital, recovering from a severe violation.

Even though you have trained and educated the end users, violations still occur. To deal with a policy violation, there needs to be a predefined set of procedures and best practices to ensure that the

goals of the institution are achieved. This will ensure that improper techniques have not been used.

A procedural model will allow you to define the precise steps that need to be taken during an investigation, as well as providing you with a basis for installing, configuring, and monitoring safeguards on your system(s) [9].

The effective enforcement of policies involves several key elements of a procedural model, such as:

- Constant monitoring of the working environment to ensure that violations have not occurred is a necessary and logical service. This regular checking of system and environment enables the administrative staff to detect subtle changes that have occurred throughout the working environment. From the gathered data it is then possible to generate reports and possible trends in violations. This aspect of monitoring can prove to be very useful, especially in a large institution.
- Analysis of the working environment, generated reports, and future trends can provide much needed insight into the working environment. Analysis of violations enables the administrative staff to discover the cause, the perpetrator of, and possibly the reason for any given violation.
- Properly documenting all incidents of policy violation, as well as the methods used to detect and deal with the violation is essential. Having suitable documentation can aid you if you should have to go to court or if you run into the same, or similar, situation. There is, however, a big difference between suitable documentation and over-documentation. Writing down everything you do and every step you take is a good idea, but making a checklist of what you should do and then neglecting to check off steps that you did, or omitting steps, can lead you down a slippery slope in court. This can appear, or be made to appear, as neglect or falsification on your part.

5.2 Monitoring the System

Monitoring, analyzing, and documenting every aspect, or even a great majority, can be overwhelming. It is nearly impossible for a small group of employees, such as an IT department, to physically check on the activities of all the employees and of their computers.

This is where automation comes into play. There are tools available both freely and for a fee that will enable an institution to enforce its policies without the need for constant intervention on the part of the administrative staff.

One free tool that enables the automation of system updating is Microsoft's Software Update Service (SUS) [12]. SUS allows administrative staff to configure a server that will contain and distribute system patches. The administrator chooses what updates will be provided to the users which will significantly lower the possibility of users downloading potentially unstable patches from Microsoft. On the "for a fee" side Microsoft also has the Systems Management Server (SMS) [11]. This has all the features of SUS and more. The interface uses the Microsoft Management Console (MMC) as opposed to the web interface of SUS. It also has robust administration features such as the ability to deploy custom installation packages to select computers or the entire network of computers.

Both of these tools are excellent for system management; however they cannot detect policy violations or audit machines for compliance with policy. Two tools that can do this are NESSUS [18], a Linux based tool, and GFI's LANguard Network Security Scanner, [7] for Microsoft platforms. Both tools allow an administrator to search the entire network, a single machine, or a range of machines for potential policy violating exploits.

NESSUS [18] is freely available with most Linux builds. Two excellent Linux builds for network administrators are PHLAK (Professional Hacker's Linux Assault Kit) [16] and KNOPPIX STD [8]. KNOPPIX [8] comes with a forensic based tool kit and network utilities while PHLAK [16] has more aggressive tools to deal with system vulnerabilities. PHLAK [16] also contains an excellent library of common exploits and their countermeasures.

LANguard on the other hand not only searches the network, but can also deploy patches to the machines that it scans [7]. Patch deployment only works on Microsoft based machines. There are also features such as the ability to schedule scans, generate reports, and even use a built-in scripting language for advanced tasks. Unlike NESSUS [18], LANguard [7] is not free, but you can download a full version fifteen day evaluation copy.

These tools will aid in the deployment of software updates and system patches, as well as give the administrative staff the ability to audit the working environment for violations in policy. This automation saves both time and money, as one person has the ability to monitor and administer several machines at once. In addition to the ability to monitor and analyze several machines at once, these tools generally will also allow an administrator to generate reports on any of the systems that have been monitored. Then a plan of action to deal with any violation that has occurred can be developed. Some of these tools even allow the administrator to send generalized reports and trends anonymously to a consortium of administrators. This allows the online community, like www.incidents.org, to analyze larger patterns of resource abuse and to interact with each other to discuss general issues as well as specific problems, such as worm and virus attacks.

When dealing with issues of policy violation there are two types of tools that will most aid you, *Enforcement* and *Analytical* tools. Enforcement tools are those tools that are used to detect violations and, either through automation or administrative intervention, properly deal with the violation in accordance with the defined rules set forth in the policy. Analytical tools are those tools that are used to monitor the working environment, generate reports, and, possibly, predict future trends in policy violation.

Now that you know what types of tools are needed, when do you use them? One of the most logical times to use a tool is when the policy violations are rampant and/or require too many man-hours to resolve manually. A good example of a violation that requires too many man-hours to resolve is that of disaster recovery. Suppose an employee has inadvertently overwritten data on a production server, causing months worth of research to be destroyed; what do you do? Do you try to repeat the research techniques and reconstruct the data from scratch? No! You would simply restore from your most recent backup, assuming that your organization backs up its sensitive data on a regular basis, using a hardware or software backup medium. Suppose that you don't back up, your backups are too old, or they just don't work, what then?

There are tools that will recover information that has been deleted, overwritten, or otherwise damaged. These tools are categorized as

Disaster / Data Recovery tools. They are not always one hundred percent effective and there are situations where data cannot be recovered. It is not a good idea to merely rely on data recovery tools in place of a system of weekly, or even nightly, system backups.

There are a myriad of freely available tools for data recovery. PC Inspector File Recovery [15] allows an administrator to search a disk for lost or damaged files and then attempt a recovery. A tool used to recover damaged or corrupt self-extracting archives (SEA), such as .zip files, is SEARecovery [17]. A more proactive solution to the free tools, which only allow you to recover data after it has been damaged, is Recovery Manager from Winternals Software [20]. This software takes snapshots of your Operating System at certain intervals and allows the administrator to remotely restore all or part of the damaged system.

Tools can also be used to boost the efficiency and effectiveness of enforcement. Using tools to recover from serious loss is not the only occasion for which a tool is required or necessary. Tools can be used when you are understaffed or require the assistance of automating certain processes, when there exists external violations of policy committed by someone other than an employee, and/or when you can no longer trust that an employee will follow policy if it is not strictly enforced and monitored.

Take caution in choosing your set of tools, however. The only tools that should be used on an operational environment are those tools that have been tested and verified on a simulated working environment. Using untrusted and untested tools on your operational environment is very dangerous and ill advised.

6. MANAGEMENT

After policies are in place and you have enforced them to the best of your ability, violations will still occur. The first response to a policy violation is to stop and assess the situation. Be sure not to jump to conclusions; crawl to them. Ask yourself the following questions:

- How severe is the violation?
- Does the policy violation also violate any laws?
- Can the violation be addressed without the need for human intervention?

The second step in dealing with a policy violation is to determine which policy has been violated and from there formulate a strategy that is appropriate, feasible, and falls within the bounds of all pertinent laws and regulations.

The strategy should be based on the type of offense, the rules of the policy, and the severity of the offense. Once an appropriate strategy on how to deal with the violation has been determined, both the policies and the procedural model must be followed to ensure that your institution deals with the situation in an appropriate manner.

The final step is recovery planning. Recovering from a violation may not require much time or effort; however, it can require a great deal of assets to correct the problem. To effectively develop a recovery plan, you must consider more than just the violation itself. Policy violations may have far-reaching implications into the personal and professional lives of the end user, since some violations could require the intervention of the criminal justice system. Using proper documentation and well written, officially stated policies and procedures can save you a great deal of time should the offense go to court.

Another option to consider when training no longer works is the provision of managed care. Managed care involves providing services to the end user either through remote administration or physical intervention. This enables the administrative staff to detect and eliminate policy violations or situations that lead to policy violations. Managed care services can range from remote virus scanning and software auditing to the physical intervention of administrative staff removing malware and spyware. The administrative staff with minimal effort and cost using a large gamut of software tools that are free or inexpensive can perform these tasks. The provision of managed care reduces the number of violations by making the end user aware of the presence of the administrative staff. This in turn should reduce costs of recovery.

7. CONCLUSION

At the university level, the end user is not just an employee. Students, outside contractors and friends of the university can all be end users. A critical error of network administrative staff is to omit the possibility that one of these end users will not be subject to the policies.

How these end users work within the system is the major cause of the problems that we have encountered. Their errors fall into two categories: errors of omission and errors of commission. Errors of omission occur when the end user is unaware of the infractions that they are committing. Errors of commission occur when end users blatantly abuse policy for whatever reason.

We found that most of our policy violations were errors of omission – the end user was ignoring the policies of the institution. In most cases after some additional instruction the end user would not repeat their violation; there were some who were repeat offenders. These end users had penalties imposed on them that ranged from being placed in managed care to denial of network services.

There were some errors of commission such as downloading inappropriate material and using network services for illegitimate or malicious purposes. The penalty imposed was immediate denial of network services.

It's the institution's responsibility to have solid policies in place, the IT professional's responsibility to enforce them, and it's **everyone's** responsibility to understand and follow them.

8. REFERENCES

- [1] Bott, E., and Siechert C., Microsoft Windows Security Inside Out for Windows XP and Windows 2000. Microsoft Press, Redmond, WA, 2002.
- [2] Burry, C., and McCune, R., Tips for speedy and safe patch deployment. Computerworld, (Nov. 5, 2003), <http://www.computerworld.com>.
- [3] CERT[®]/CC, http://www.cert.org/stats/cert_stats.html.
- [4] Cooley, A. Virus Protection Strategies to Combat Electronic Attacks. (Nov. 3, 2003), http://www.astaro.com/data/pdf/whitepapers/Whitepaper_VirusProtection_en.pdf
- [5] Cox, J., and Kistner, T., Security lesson. Network World, 20, 27 (Jul. 7, 2003), 35.

- [6] David, J., Policy enforcement in the workplace. *Computers & Security*, 21, 6 (Oct. 2002), 506-513.
- [7] GFI Software Ltd, <http://www.gfi.com/lannetscan/>.
- [8] Knoppix STD, <http://www.knoppix-std.org/>.
- [9] Kruse, W.G and Heiser, J.G., *Computer Forensics: Incident Response Essentials*, Addison-Wesley Professional, Boston, MA, 2002.
- [10] Meckbach, G., Patch management. *Computing Canada*, 29, 23 (Nov. 28, 2003), 20.
- [11] Microsoft Corporation, <http://www.microsoft.com/smsserver/>.
- [12] Microsoft Corporation, <http://www.microsoft.com/windowsserver/system/sus/>.
- [13] Nicholson, B.J., Slash your tech support bills—support yourself first. *Agency Sales*, 33,5 (May 2003), 32-33.
- [14] Oblinger, D., and Petersen, R. Cyber security: it takes a community, In *University Business* (April 2004), <http://www.universitybusiness.com>.
- [15] PC Inspector, <http://www.pcinspector.de/>.
- [16] PHLAK, <http://www.phlak.org/>.
- [17] SmartLine, Inc., <http://www.protect-me.com/>.
- [18] The NESSUS Project, <http://www.nessus.org/>.
- [19] 2003 CSI/FBI Computer Crime Survey, <http://www.gocsi.com>
- [20] Winternals Software LP, <http://www.winternals.com/>.
- [21] Wood, C.C., *Information Security Policies Made Easy Version 6*, Baseline Software, Sausalito, CA1997, 15.