WHITE PAPER

WHY SECURITY POLICIES FAIL

CONTENTS

INTRODUCTION

No asset can be 100% protected against theft, tampering, or accidental damage. This is especially true of information assets. If a hacker is sufficiently determined, patient, and skilled, no system is impenetrable, and no solution will last long.

Most attention to network security has traditionally centered on tactical preventive or reactive procedures, or on gadgetry. Less emphasis is given to examining the security policy itself and maintaining its operational health.

Objective analysis reveals that many breaches are linked to common weaknesses in the security policy…accidents waiting to happen.

Even the most reliable, state-of-the-art technologies can be undermined—or rendered ineffective—by poor policy decisions, or by weak operational practices. The human element of security is often the weakest part of the process, and therefore should be accorded more scrutiny when designing policies and procedures.

This article does not address the tactical "point solutions" typically used to thwart specific direct attacks; it instead focuses on strategic and systematic weaknesses that can slowly degrade security operations, attract thieves, or make a disaster more likely to happen. Its intent is to stimulate further analysis of the security infrastructure, and to suggest mechanisms to combat the "natural weaknesses" of the security process.

Most of the concepts discussed are not unique to information security; they apply to security policies and practices in general.

This document is organized as follows:

- Examination of "natural weaknesses" of security policy, why they exist, and how overlooking them can degrade the effectiveness of a security policy.
- Commonly overlooked "real" threats and their potential impact.
- Hypothetical scenarios that illustrate these natural weaknesses.
- Considerations for the security life cycle that are presented in the context of these natural weaknesses.

THE "NATURAL WEAKNESSES" OF SECURITY POLICY

Before attempting to develop a security policy that will not fall under its own weight, one must acknowledge certain weaknesses in the process of securing any asset.

Failure to respect these weaknesses and develop compensating maintenance processes will subject the policy to the inevitable decay of time and entropy.

1 – Security is a Barrier to Progress

Protective measures for security or disaster planning are (by definition) either obstacles or impediments to commerce. Other than mitigating specific threats, they typically add zero benefit, and always hamper on some level the ability to freely share information.

Human nature begets desire—for more information, for greater access, for faster response. Imagine waiting for a traffic light. Obviously, the light exists for safety, but if the intersection is vacant, the light's "protection" is annoying and wastes time. Our patience has a limit, and we at some point proceed through the red light, under the assumption that the light is broken, or the guise that the wait time was unacceptable.

Even friendly, common-sense security measures reduce productivity. The balance between security and disruption differs for each company.

Every network user reaches a "red light" limit with compliance as well. At some level of annoyance, we conclude that compliance is ultimately not in our own self-interest.

Policy plans, rarely measured by impact on users and the business process, can lead—at least—to a false sense of security. Worse, disparate compliance can result in a security breach. If you give up on the red light just as another car approaches on the green…

2 – Security is a Learned Behavior

Self-preservation is instinctual behavior; securing assets is not. It is a higher-level function that must be learned and occasionally reinforced.

Information security procedures are often not intuitive. Without proper education, users may not recognize the value of assets, risks, and costs of compromise. A user who is unaware of the value of an asset (or the reasons for protecting it) is more likely to think, "that's a stupid policy."

Teach and preach your policy. Tailor the training for each audience.

Even some self-preservation practices must be learned: children do not just *know* to look both ways before crossing the street, or to wait an hour after eating before swimming; these are learned behavior.

It is also imperative that management is taught the value of information assets, the risks associated with these assets, and the appropriate protection policies. If management is unaware of the security policy and its justification, it is unlikely that proper funding or commitment will be secured either. Managers need not know the technical minutiae; educating managers on security policy should merely focus on the potential impact of lax security on information assets.

3 – Expect the Unexpected

Any process designed for a global enterprise will involve many users making many transactions at all hours. The more complex a policy or process is to accommodate these users, the more likely it is to fail.

Preparation, planning and practice keep your skills up. They also weed out faults and loopholes before they cause breaches.

A good security officer expects failures and disasters, and constantly checks the radar for signs of "bad weather."

4 – There Is No Perfect Mousetrap

You can never be finished. Securing assets is a continuous process. Technology is rapidly changing; systems become outdated, and systems either fail or lose effectiveness over time. Threats will always exist, and policy and procedures must also grow and change to remain effective.

Don't expect to perfect your policy and go home. Security is a 24-hour job…it's never finished.

Every process and policy should undergo regular health checkups in good weather and in bad.

THE "REAL" THREATS

Despite recent media attention, penetration of your network by a highly skilled hacker is an unlikely threat. In fact, protecting your environment from cover to cover may be a waste of the security budget. The real threat is often from within.

Extreme protective measures are usually only warranted for highly sensitive information and assets. Also, the more extreme the measures, the greater the costs associated with the "natural weaknesses."

What information is most valuable? Who are your greatest threats? Is there any danger from within?

The real threat to information assets is non-malicious damage resulting from human error, denial of service, and inappropriate disclosure. These compromises often inflict more damage than a Hollywood-style hack.

The vast majority of overt policy violations, and their resulting damage, typically come from "borderline" hackers who only consider intentionally violating policy because they are tempted by unsecured assets, or complacent monitoring and enforcement.

If the security policy (and enforcement) projects the image that you do not value your assets, it will attract petty thieves and casual curiosity seekers. These non-malicious breaches may become more severe if the perpetrators are used to averting policy and getting away with it.

More likely, intentional violations will assume the form of exploiting weaknesses in existing policies and procedures, rather than any elegant technology attack. Retail stores lose more cash from petty theft and cashiers pocketing unrung sales than from someone cracking the vault.

POLICY BREAKDOWN

Example 1 – Key Under the Doormat

*An electronics manufacturer owns some very expensive testing equipment that is used in production. Because the equipment is valuable, the security department decides that these assets will be **most** secured if access is limited to a few people.*

Smart cards and costly locks are used to protect the equipment room. Only one person per shift, a senior manager, is given a key.

Ten other people on each shift need access to the room to perform their daily duties. They are not issued keys and must be escorted to the equipment room by a key holder.

Initially policy is followed, but managers soon tire of escort duties. Productivity suffers when managers are unavailable to open the door. The security department resisted manager requests for more keys, so managers arranged with the people needing access to leave the key in an unmarked desk drawer.

One day, while a manager and her employees are in a meeting, equipment was stolen from the room. The key was also taken.

The security department investigated, but failed to find the thief. There was debate over whether to discipline the manager, who was the only person issued the key.

The managers recoiled because they felt the policy negatively impacted productivity, and because they had followed the key-sharing practice.

Final Outcome

- *Expensive equipment was lost*
- *Employees, managers and the security morale were negatively affected*
- *A thief is at large*
- *The costly measures provided no security value*
- *The security policy caused the loss because it was inconvenient and easily circumvented*

Analysis

The policy's authors did not consider the impact of the policy on workflow. Had they involved users in policymaking, perhaps this problem would have been avoided.

The security department was also unable (or unwilling) to note that the policy was thwarted. Proper auditing and follow-up would have raised the issue and given a chance to develop a workable policy. Instead, the technology was made ineffective by a policy that had decayed.

Example 2 – The Fault of John Q. Public

Network managers decided their company had too many unassigned or inactive e-mail accounts. They enacted an e-mail policy requiring the signatures of three vice presidents to create a user.

New requests were issued daily, but it was difficult to obtain signatures in a timely manner. The VPs typically did not even know who the users were. To help expedite processing, some VPs simply signed stacks of blank forms and distributed them to managers.

Confidential company files were stolen and posted on the Internet by an anonymous user. The company suffered negative publicity.

An audit of the logs and account records revealed that a user named JQPUBLIC had accessed the files that were later compromised. Further investigation showed that an account request form was approved for JQPUBLIC some months earlier. No one had any direct knowledge of this person, or who might have made the account request.

Analysis

The policy implemented in this scenario also did not evaluate its viability or effectiveness in the business cycle. Further, the signatures required to establish an account appear to have been somewhat arbitrary, and they did not represent a practical model for identifying users.

Final Outcome

- *Proprietary information was compromised*
- *Loss of reputation from public disclosure*
- *A hacker is at large*

The risks associated with granting computer accounts were not properly communicated to the VP's. It is the responsibility of any security service to effectively communicate the value, risks, and protective measures to management. Had the vice-presidents understood the risks associated with granting a computer account, they probably would not have been so casual in their practices.

In this instance, the security department should also have been aware that copies of the forms were circulating with signatures already on the form. Had some routine assurance procedures been in place to spot check new user accounts, it would have been uncovered that the VP's were not aware of to whom, or when, new accounts were being issued. This could have lead to the design of a new process, or to the education and buy-in of management to follow the existing model.

Example 3 – Burned by the Backlog

All Web server equipment was located in a central computer room at the company's headquarters. This policy provided strong security and system support, but as the service grew, expansion requests were denied.

The process for requesting computer room space and billing individual departments was complex. Although the computer department maintained the machines and conducted regular backups, some departments found it easier to keep their servers in their own areas. One business unit, which ran a subscription-based Web service, kept a server in a closet filled with office supplies and toilet paper.

The closet server, suffocated by cleaning supplies, caught fire. The server, its wiring, and part of the building were destroyed

The company was fined for safety code violations. Since it was not maintained by the computer department, the burned server had not been backed up in a year. The computer department's disaster recovery procedures were useless in helping to restore service, identify paying customers, and determine their account balances.

Analysis

Management did not understand the importance of these production servers and also did not have a proper understanding of the business ramifications of their loss. It is the responsibility of the security organization to effectively communicate this information to management.

Final Outcome

- *Customers demand refunds and/or go to competition*
- *Proprietary information was compromised*
- *Building and property were damaged*
- *Business was lost due to fire and cleanup*
- *Company was fined by Fire Commissioner*

Because the space allocation and departmental billing procedures were so complex, the computer room staff was unaware that there were unprotected assets. It is the responsibility of the security organization to be aware of the users and systems that they must protect. Had it been known that production servers were in unsecure or unsafe environments, they could have escalated the issue to the proper levels of management. The also probably would have picked up on the fact that this orphan production system was not being backed up.

Over a period of two years, it was also not discovered that some systems were not on the backup schedule. Had an audit been performed to verify all systems on the network, it may have caught the fact that this server was a production server, and that it was not being backed up.

Placing the server in a closet with office supplies and toilet paper sends the impression that this piece of equipment is of little value to the company. Those who come in contact with it will also not treat it with much more respect than the toilet paper that it shares the closet with.

Another point in this scenario is that all backup procedures should take into account that the backup program or its media may no longer be available. Annual audits of backup processes should verify that all stored tapes are on a media and format that will continue be recoverable. If a backup program or hardware vendor should go out of business, procedures should be investigated to transfer necessary old media into a recoverable state.

HOW DO YOU WIN?

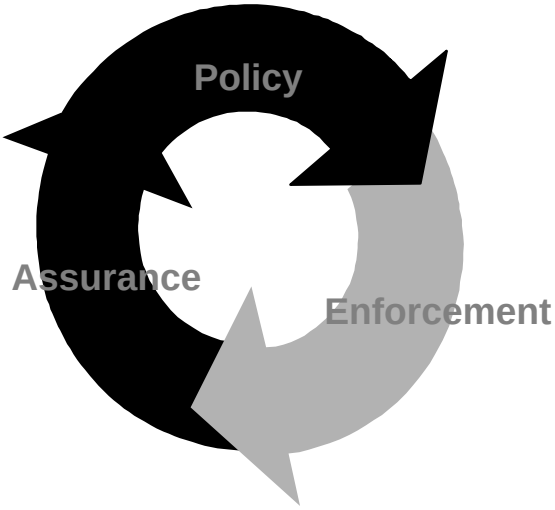
Remember that there is no perfect mousetrap, and you can never be finished with security procedures and policies.

1. Plan for the natural weaknesses of security policy.
2. Educate users in policy, enforcement, and the value of assets.
3. Perform regular health checks on the enforcement operations.
4. Make corrections when needed.

THE SECURITY LIFECYCLE

Staying ahead and maintaining a healthy, robust policy program requires diligence throughout the security lifecycle.

The security lifecycle is an ongoing process of *policy*, *enforcement*, and *assurance*, where each phase in the lifecycle feeds into the next.



Policy

This is the *discovery* phase of the security lifecycle, the identification of possible threats and risks, and the determination of assets to be protected. An enforcement strategy is developed to safeguard those assets against the predicted threats. The strategy dictates the technologies, resources, tactics, and training required for enforcement.

The method developed to collect information will later be needed to test the policy and its enforcement assumptions.

Enforcement

This is the *action* phase of the security lifecycle, where everything happens. Policy design, data collection, assumptions, the education of users and enforcers, tactics, enforcement, and prosecution methodologies are tested. Operational life and execution of the security policy are part of the enforcement phase of the security lifecycle. Herein, all the security assumptions are tested, and either survive or decay.

Assurance

This is the *proof* phase, where the policy, the strategy, and their effectiveness are tested. Failures are analyzed for future incorporation into the policy. Plan to rely on data and tactics defined by the policy; that information was collected through execution of the enforcement strategy. Additional indicators of the policy's success or failure will arise as part of the assessment.

Lifecycle Considerations

Here are some suggestions for keeping a security policy healthy throughout the lifecycle.

Policy: Determine Your Policy's Impact

Security is Inconvenient – Recognize and respect security's disruptions of the business process and daily life. You need not make the process transparent, but each extra step, each extra disruption, makes noncompliance more likely. Build a "user impact" phase into the design methodology. Invite discussion; it may identify problems waiting to happen, and may lead to increased understanding on both sides.

Avoid Excessive Complexity – Strive for common security tools that have already been tested and proven. This controls costs and lessens the chance of hackers slipping through cracks.

To Prosecute or Not to Prosecute? – Decide in advance how far to go, and get management buy-in. If you decide against prosecution in favor of reprimand, it is less important to build evidence once a hack is discovered. If you decide to prosecute, know what evidence the burden of proof requires and train the security staff to collect it.

Make the Punishment Fit the Crime – You may merely reprimand employees for sending personal email on the company network, but you want to prosecute someone who hacks the payroll. Decide in advance how far you will go.

Enforcement: Be Visible

Make Security Overt – Consider uniforms or badges, even in small firms. The psychological effects may include increased sensitivity to threats, teamwork in reporting suspicious activity, and acknowledgement that you value your information.

Remind Constantly – Give security briefings through newsletters, Web pages, or network logon notices. Explain that your information assets are of value to all employees.

Painless Policy In Practice

While on rounds, a bank's security staff enforced a policy that unattended workstations must be secured with password-protected screen savers. They placed yellow notes reading, "Security needs your help—please lock your workstation" over unprotected monitors. This non-disruptive reminder helped change the user community. Bankers would leave their desks for lunch, then return saying, "I better lock my screen so I don't get one of those yellow notes."

911 Service – Coordinate with your physical security staff and establish an emergency line backed up by people and policy. Make it important.

Drill the Troops – Attempt to identify the location of legitimate online users so that you will know how to locate a real hacker. Perform occasional "fire drills" to test backup and restore processes.

Empower the Enforcers – Get executive support. Train, drill, and patrol. Keep enforcers' skills sharp, and increase their visibility. Consider penalties that are more symbolic than punitive.

Training, Training, Training – Make training and awareness an integral part of the plan, and of company policy. Everyone can do a little bit for security with a little training and motivation. Use frequent sessions with light content rather than long, detailed seminars. Budget continuing education for your security personnel to keep them informed of the latest threats and protective practices.

Know Your Environment – The more you know about what the "normal" routine is for your business and network, the more likely you are to notice when things are not right.

Painless Policy In Practice

Security staff at a consulting firm checked cubicles nightly for unsecured laptops used by the mobile workforce To prevent theft, any laptops (even guests') left in view or in unlocked desks were collected. In their place were left notes: "Watching out for you; protect your laptop." Users could present their ID at the security office to retrieve their laptops without reprimand. The inconvenience made employees and visitors remember to protect and value their assets.

- Know your users and their job functions
- Know your business routine
- Know the sounds and rhythm of your normal business practices:
  - How many users are normally on your servers
  - How many hits your Web server typically has per day
  - Normal message traffic per day internally/externally
  - Who normally connects remotely to your network
  - Which people normally work late
- Investigate Everything

If you see anything out of the ordinary or abnormal, investigate and understand it. Play cautious, play curious, seek education (rather than inquisition). Your curiosity may be enough to scare off a hacker.

Walk in Your User's Shoes – Use the same hardware, software and OS as your mainstream users, and use as few security privileges as possible. This will help you to identify barriers to the business process and annoyances, which can push users into sneaking around policies or security features. If possible, utilize separate hardware and user accounts for your heavy security work, and keep your work brief. The longer you stay in a privileged state, the more likely you are to accidentally delete files, introduce a virus, or cause some other similar damage.

Assurance

Expect Failure – Audit your operational practices to detect leaks and design flaws. Ensure that regular audits are part of your security policy and have *prior* management approval (managers may fear that audits bring bad news, and postpone them). Audit at a level representative of the risks you face. Audit user logon IDs and ensure that they are still required and active. When in doubt, disable suspect userIDs, but have a fast process to reconfirm and reinstate users who call in.

Break Into Your House – Try to thwart your own policies. Find out if users and security staff understand the system and if they can gain unauthorized access by pretending to forget their password or saying, "my manager told me…" Solicit suggestions; let users opine. They may offer helpful recommendations or identify overlooked threats.

Learn From Your Mistakes – Empower your auditors with the authority or the processes needed to affect change. Improve the next generation of policy. Good luck!

ABOUT CONTROL DATA

Control Data helps global organizations design, apply, and monitor distributed information-sharing technology. Control Data offers consulting, application development, integration and outsourcing services worldwide.

For more information, contact your local Control Data office, or:

Control Data Systems, Inc.
Electronic Commerce Solutions
4201 Lexington Avenue North
Arden Hills, MN 55126 U.S.A.

+1-888-742-5864 (Toll-free in U.S. and Canada)
+1-651-415-3001 (International)
<http://www.cdc.com>