SYSTEM SECURITY & SYSTEM ADMINISTRATOR TERMINATION POLICIES, PROCEDURES

Marcé DE Jeffries
February 12, 2003

Examples of Security Policies at Work

Academia

The University of Texas at Austin
The University of Oklahoma
The University of Oklahoma College of Geosciences
The University of Northern Arizona
The University of Arizona Tucson
The University of Indiana
The Virginia Commonwealth University
The University of Florida State

State

The Virginia Department of Technology Planning (DTP)
The Great State of Arizona
The State of Florida
The State of Mississippi
The State of Maine (The most Detailed of states researched)

Federal (many sites were restricted)

National Institute of Standards and Technology
Federal Bureau of Investigations (Declassified Brief)
Department of Defense

Introduction

Today we face another risk, a silent threat, a well known vulnerability, the possible unforeseen loss or termination of a system or network administrator. This vulnerability can sometimes be very crippling, and yet most of us accept it as an everyday "doing business as usual" concept. Yet no one seems to account for its very exisistance! How can this be? Well for one, we as CIO's, Network and system administrators, department heads and supervisors do not factor in this known vulnerability as a risk to our entity. Nor do we consider it in our defense in depth strategy!

There seems to be no simple reason for this omission other than the fact that we do not account for our own mortality or job security and how the loss could be related to the Risk, Threat and Vulnerability Assessment. How do we address this? The answer is quite simple. A company awareness program would be a start and secondly, an effective policy for voluntary and hostile loss of key system administrators would add a comfortable layer of protection. In this paper I will explore what are some common system security policy practices at some university and corporate sites as well as the mandated differences federal organizations have to adhere to and the non existence of such policies at local and state levels. Also I will define and evaluate a security policy that will address system administrator terminations and the procedures to handle such terminations.

Common Practice & Impractical Business Standards

In my research I have found out that many organizations find themselves trying to write a comprehensive policy that follows or meets industry or mandated guidelines. These regulations or industry standards range from HIPAA, GLBA, GISRA, and ISO17799. Some organizations have taken the "cookie cutter" or template approach to system security when writing their standardized guideline security policies or acceptable use guidelines for all users. The reason for this approach could be for several reasons i.e. lack of funding, technical resource availability, enterprise or corporate wide template use, and even the possibility of non-IT educated personnel doing the writing. Many of these templates can be acquired form various websites and Books that have a system to step you through the process such as a web based Command Center from Meta Security Group or downloading a sample template from a security website like IT Security Policies & Network Group or SANS. As we will discover most all of them addressed the expected elements of purpose, scope, related documents, and a policy statement.

The most basic blanketed policies, which were not to my surprise since I worked at one, were the State University Systems, the most open of all organizations. These organizations were at one point IT centralized and had one blanket policy that covered the common users of the computing systems and very little

clarification of separation of responsibilities for their administrators. An example of a centralized blanket policy would be one published by the Arizona State University. As these Universities grew larger and states grew poorer during economic stress, there became a need to decentralize IT operations as more technology became abundant to defray cost to the university. This decentralization put the burden on the academic departments to carry the cost of their IT infrastructure needs. This included a very expensive staffing requirement which many departments could not adequately fund and many reorganized by promoting current staff with the most pc knowledge to administrator positions and technicians.
In the corporate world however, impractical business standards became the norm in order to find a "Technological Silver Bullet" by focusing all of their energies into implementing security technology without policy guidance, says security firm Meta Security Group. The Meta Security Group goes on to say:

> Volatility and immaturity in security technology will continue to make enterprise wide technology architectures impractical through 2003. However, the need for agility and auditability will drive development of adaptive, top-down security architectures encompassing consistent policy frameworks, strong process orientation, service definitions, formal roles/responsibilities, and domain specific technology standards (2002/03). Scalable technology architectures for security will evolve as a result of broader standards (2004-06).

Centralized Responsibility

In order to buy into a heavy decentralized IT burden of the university system, central IT would become the sole entity responsible for the corporate network infrastructure, university business systems, infrastructure security, and centralized help desk for supported software and systems. Central IT would also have direct oversight over all technologies encompassed at all satellite locations as well. This could be easily gleaned from the stated policies written by these organizations as in the ASU IT example.

The business sector was operating in a different dilemma of migration from mainframe to client server and large support staffing to being able to meet and respond to customer's needs, thus minimizing the cost of processing transactions. 'A centralized approach was also decisive. It promoted a "we/they" attitude." States Stuart Lieberman at computerworld. Yet some larger corporations were consolidating data centers and taking on multiple trends where help desk support is concerned. A majority of security policies still remain the same and in force during these consolidations and decentralizations. One company, Experian, who specializes in information, saw this becoming as a significant problem and decided to adopt BS 7799 and implement a company information security policy. Further investigation revealed when there are policy rewrites, it is often a scaled down version or modified template that is put in place of the old.

Policies and Procedures

First off let's define what a policies and procedures are for those individuals who have some obscurity to the difference of the two. A "policy", by definition of The Heritage Dictionary, "is a plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, procedures, guiding principle and other matters". In the case of information security policies we will need to expound on this definition to include realistic and achievable security goals. We now have the gist of the general policy definition and now let's look at what a procedure entails. Generally defined, it is a set of established forms or methods for conducting the affairs of an organized body such as a business, club, or government. And when applied to computer science it is defined as a set of instructions that performs a specific task; a subroutine or function. By these definitions a security policy must state the "who, what and why" and a procedure must represent the "how, where and the when". With this in mind we can now proceed forward and look at examples presented in the next section and understand much clearer what is going on.

Generalized or Non-existent Policies

Business sectors consist of local, state, federal and civilian. All of which have their own priorities when it comes to security policy objectives. Anyone who has been fortunate enough to work in each sector at one point in time would corroborate the existence of extreme differences in corporate policy as well as its non-existence. Here's perfect example of a real life story I found to this effect presented by the National Center for Education Statistics:

> It Really Happens!
>
> Like many people, Fred Jones thought he had a difficult job. As the Information Systems Manager in a small school district, he was responsible for operating a district-wide computer network--everything from installation and maintenance to user support and training. While it was clearly not a one-man job, he was his own one-man staff. Fred had tried to explain to his superintendent that the district's network was vulnerable to a range of threats because his small budget and non-existent staff prevented him from handling system security effectively, but his warnings had always been ignored.
>
> One morning at a staff meeting, and much to Fred's surprise, the superintendent announced that he had read a newspaper article about a student breaking into a neighboring school district's computer system and changing report card records. The boss proceeded to declare that Fred

> was now being charged with developing and instituting a computer security policy for the school district.
>
> As soon as the meeting was over, Fred approached the superintendent to request an appointment for them to discuss a shared vision for development of the security policy. "Effective security policy requires input and commitment from the whole organization, so I think we should sit down and map out a plan for developing our security policy," Fred asserted.
>
> But the superintendent declined the invitation to participate in the policy-development process. "Fred, I'm just too busy to get involved in this project. I trust you to do a job that will make us all proud." When Fred asked about expanding his staff and budget to meet the increased workload, the superintendent again dismissed the issue. "Fred, times are tough and the budget is lean. Maybe next year we'll be able to work something out. In the meantime, you get cracking on securing our system as if your job depends on it... in fact; I guess your job does depend on it."
>
> Fred watched his unrealistic, if well-intentioned, boss walk away, realizing that his job was no longer difficult, but truly impossible. He was now expected to develop, institute, manage, and monitor an organization-wide security policy without assistance, consent, or buy-in from a single employee, much less empowered high-level administrators. He knew that the organizational support he failed to receive meant that there was little chance of his being able to effectively secure the system--and that it was just a matter of time before a significant breach in system security would take place. Fred found himself in the terrible position of being responsible for stopping the inevitable, yet powerless to do so.

When I had read this I felt an overwhelming sense of deja vous! I myself had been in this very same situation at one point in my career. Keep this scenario in the back of your mind because it will soon hit home.

Many IT professionals take their security experiences with them and the acquiring entity reaps the benefits and the losing entity suffers because they are lacking a secure infrastructure and educated security conscious IT staff. Several companies that I have worked for had no security policy at all and one just happened to be a well known ISP in Arizona. At the state level I have learned that a division-wide policy exists and is augmented by local policy in diversified areas. As in some of the University systems, which use the Decentralized IT model, adopts the enterprise-wide security model with the expectation that governing departments will dictate local, issue Specific and Standard Operating Procedures (SOPs).

Federal and Government Contractor Security Policies

The Federal organizations follow the strict adherence of enterprise-wide guidelines set by the National Security Agency and the Chief Information Officer Council. This enterprise-wide guideline governs corporate businesses that contract in defense and information products for the government. These policies are not generalized and are uniquely customized and modified frequently to counter evolving threats.

The National Institute for Standards and Technology has a Security Computer Division that maintains a web site that contains agency policies, procedures and practices; the CIO pilot BSPs; and, a Frequently-Asked-Questions (FAQ) section. Many agencies submit and share their security information practices on the FASB site. This web site is used to effectively guide and to inform federal employees.

Security Policy Amendment

With a few keystrokes applied to the faithful google search engine we can find a security policy for hundreds of entities all of which fail to address one thing. What does an organization do if they lose a senior level system administrator? Most all follow the steps of defining a sound security policy.

- Purpose
- Related Documents
- Cancellation
- Background
- Scope
- Policy Statement
- Action
- Responsibility

Deeper interrogation finds termination policies within the Human Resource domain. These policies are standard and some consist of procedures for different types of employee terminations for probationary and regular employment types and are pretty straight forward.

Evaluating the Basic Security Model

In today's economy gainful employment trends have fallen to the wayside. There's corruption in the executive bubble, poor corporate profitability, and business reorganization has caused many long unemployment lines. These poor economic times has taken a great toll on information technology careers. Not only are the front line technicians at risk but the once highly praised and valuable system/network administrators. What do we do if we lose our administrator? I know many had asked themselves that very same question when I was abruptly mishandled and had to immediately resign. The risk of losing a system administrator is virtually unthought-of when evaluating a security policy. We tend to look at internal and external attacks, malicious code that attacks known vulnerabilities, current patches and updates to see if we've got all your bases covered. In the back of our minds it seems too unrealistic and it never makes it to the pages of our evaluation checklist.

But where do we look at this eventuality? As I look back to the Sans Security Essentials course chapter on Basic Security I can recall that a key question was posed in the evaluation slides. "Is your policy forward looking?" ours sure wasn't now that I look back in hind sight. I thought, was a "bad" policy written nine years ago when the university department was formed? Most would think not. At the time when the policy was written, it was clear, concise, realistic, consistent, and readily available and provided sufficient guidance for a period of time in the departments' life cycle.

Have you stopped and looked up your current policy? Have you stopped to think what will be done if this happens in your organization? If not! You should be!

The loss of a critical system/network administrator should put a new unrealized spin on risk assessment. So far there are two ways to look at this risk and I will break it down from each level. The first is a "normal termination" and the second is a "hostile termination". I'll use the acronyms of (nT), (hT) and system administrator Termination (saT) in our break down for simplicity sake.

Under the auspices of a normal (saT), one would have to assume that there has been some fore warning to the event. Typically two weeks or more, preferably on the "more" side, and proper actions have been taken to make a smooth transition. What would constitute a hostile (saT)? examples would be an administrative termination for various reasons analogous of what company HR policy dictates, a sudden abandonment of the post for any reason and an undocumented security architecture of a normal (hT) to name a few.

Risk Assessment

Let's look at the afore mentioned examples and follow the road map taught in the Security Essentials coursework and analyze these risks to come up with a working security policy model. Now we're in the territory of risk management and we need to determine if any type of (saT) is a Threat, what are the threat vectors and what could possibly be routes of attack if any.

Let's assume that there is a good viable security policy already in place, we've done our evaluation and now we must look at our risk choices. Losing a critical administrator is an unacceptable risk so we have to make changes to our policy and all of our processes that come to bare. We must also minimize the risk because it has the potential to harm the business entity. And since this type of threat is not insurable, it is safe to deduce that we cannot transfer the risk to protect the business entity.

Now that it has been determined that there could be potential harm done to the business by this loss, let's determine what could or can happen and the impact of the threat.

Normal (saT)

- Critical passwords/pass phrases not relinquished can cause work stoppage and administration of critical infrastructure
- Undocumented backdoors not disclosed leaves the network vulnerable to attack and can be exploited
- Undocumented administrative and auditing tool processes have the potential to cause problems if they stop functioning causing down time of workstations or critical systems
- A disrupted transfer of power to the incoming administrator can have an IT department backlogged for months until the new administrator can be up to speed
- Sole working knowledge of some critical system can cause a company to reinvest training or scrap that system and take the hit if it is not cost effective

Hostile (saT)

- Any combination or all of the above plus the fear of retaliation and the extent of any type of damage that could be inflicted
- Undocumented vulnerabilities designed and implemented can cause a myriad attacks to occur on business systems
- Undocumented trusts between servers and workstations will allow entrance to critical systems by attackers sniffing the network and leaves the system open to attacks from the inside and outside of the network, malicious code and the internet
- Some cases will cause the company to rebuild the network for a one-man shop
- Subordinate technicians are left without leadership and guidance and will cause unsatisfactory business practices
- Loss may take up to six months to fill the position which can be an expensive process
- Business will have to outsource to a consulting firm to audit and secure the infrastructure – A VERY COSTLY SOLUTION!

As you can see this risk involves a lot of uncertainty and all of it is unacceptable. In any event it will be very expensive if any of the above were to happen in a small or large company. The Single Loss Expectancy (SLE) for the larger company could be ten-fold if across the board losses were to be realized in an annual accountability cycle.

A Case for Policy Amendment

There are a vast number of documented and undocumented network/system administrator's out in the work force and they all have their way of doing things within their job scope. Common practice and work habits of system administrators are almost never documented. You can stereo-type this phenomenon with poor programmers who don't self document.

Many administrators are poorly educated in the realm of system security as evident in the growing number of cases concerning prosecution of administrators doing so-called "testing security" audits that were highly unauthorized and inappropriate as seen in the Princeton University case in august of last year. In this case an admissions director was caught perusing files on the Yale University web server without authorization.

When the need to automate or simplify a task, an administrator whether in an understaffed environment or an adequately staffed institution will knowingly create vulnerabilities for ease of passage or convenience and they almost always go undocumented. Linux varieties include but not limited to rhost, heartbeat, and PAM. Whereas in the windows environment we see the likes of overly applied domain trust, RAS and FTP servers, and public shares with everyone permissions.

Some product packages provide personalized vendor support accounts like the infamous Compaq Insight Manager and its many open and obscured port usages. Unless you are completely familiar with this product you can rest assured that it will cause a multitude of headaches should the software malfunction.

All-in-All most networks have become the personal playground for most administrators especially if they designed and built the systems from the ground up. Over time a system could accumulate many passwords and passphrases known only by the system administrator.

Minimize the Threat

As you can plainly see, there are a myriad of threats posed to a system when there is a loss of a network/system administrator. Therefore we must investigate by audit and eliminate any vulnerability ASAP!

Establishing policies and procedures specifically to deal with this type of risk would fall under the Issue-specific policy type. This is where the password policies will be readdressed if needed, documentation guidelines are laid out and event documentation procedures instituted. Once this action has been defined in the broadest terms and it passes another evaluation checklist the policy can be put into action.

The Mechanics

Let's take this a bit further and walk through it step-by-step keeping in mind this process can be easily amended. First we'll start off with a policy worksheet. A good place to start off is with a template that I discovered at sans.org.

POLICY WORKSHEET

Procedures are derived from policies. A procedure can be used to identify and define the parent policy, even if the policy is not written and signed.

Action: List procedures for which you need to document the policy. Make notes on who, what, when, where and why.

Step1: Who does the procedure?

The network security analyst or senior IT supervisor performs the system administrator termination audit and business section notifications based on the type of termination.

Why?

Business section (HR) requires notification of termination. Central IT to needs terminate applicable accounts. The depth of the system administrators' responsibilities during tenure are identified. Determine any vulnerability that may be present from common and uncommon administration of the network. Full administrative rights are required in order to use the special auditing tools and backups on the network.

Step 2: What is the procedure?

Administrator: Submit written notice. Return issued items i.e. company property, security access devices/badges, clear corporate debts, complete (HR) exit interview.

Supervisor: Determine termination type as normal or hostile. Notify HR of termination. Sign-off on administrator procedure. Notify Central IT to terminate applicable accounts. Notify appropriate business sections to delete authorizations to parallel business systems. Transfer recovered issued items to appropriate business sections. Audit network systems and system documentation. Review vulnerabilities and secure networks and systems. Document and report findings.

IT: Remove applicable authorizations. Backup and audit the affected network. File interim reports. Submit reports to Senior VP or CIO.

Corporate: Review reports. Determine termination action. Determine law enforcement action. Issuance of personnel action to (HR*)*

Why?

Define areas of responsibility and identifies additional detailed guidance

Step 3: When is the procedure done?
The procedure is performed at the onset or first knowledge of a normal or hostile senior system administrator termination.
Why?
To minimize the danger of anything that would negatively affect the confidentiality, integrity, or availability of any or all business systems and services.

Step 4: Where is the procedure done?
The procedures are performed at the affected locations of responsibility and the affected network and systems.
Why?
Network and system audits can be performed remotely if needed but not recommended. It is preferable to be at the console when performing audits whenever possible. Other procedures are performed in the primary office of responsibility or if necessary in other secure designated areas.

Step 5: The notes in this worksheet helps give the policy a clear and concise meaning and defines the need to protect the organization from a viable potential threat.

Sample policy derived from procedures outlined in the worksheet above:
To insure the confidentiality, integrity, and availability of the business network and its systems, the senior IT supervisor or appointed network security analyst will perform the appropriate system/network administrator termination procedures at first knowledge of such event and appropriately notify (HR) and Central IT administration. Each incident shall be reported, reviewed and submitted to the corporate area of responsibility.

With further examination one should be able to deduce that this policy has action because it specifies what is necessary and what is to be accomplished within a defined time frame. Secondly, the policy is clear because it identifies the individuals being responsible for carrying out various tasks. Since this can be construed as a concise issue-specific policy. The policy sample passes the forward looking criteria because it was designed with “subject to change” in mind because of the ever changing influx of next generation risks and vulnerabilities when such incidents occur an organization.

Conclusion

As I noted in the beginning that we are faced with an unrealized risk that seems to escape our policy evaluations and risk assessments. My intention was to identify and bring attention to a known vulnerability into our layered defense. This topic has a great potential to be expounded upon and revised to meet specific organizational needs. I myself had no idea of the affect such an incident could exist until I was an unwilling factor. The SANS Security course work was a dynamic aid to my realization to actually how much of a threat to the organization this risk posed. There was so much more room to expand on this topic and I look forward to see different spins on this topic in the reading room.

References:

1. Brownlee, N. (2000). Computer and Network Security. Retrieved January 10, 2003, from University of Auckland Information Technology Systems & Services website: http://www2.auckland.ac.nz/itss/Policy/security.html

2. Adverse Termination Procedures –or- “How to Fire a System Administrator. Retrieved January 12, 2003, from the Lumeta research website: http://research.lumeta.com/tal/papers/LISA1999/adverse.html

3. Stryker, Laurey T. (1998). Using and Protecting Microcomputing Resources. Retrieved January 10, 2003, from University of South Florida Policies and Procedures Manual website: http://usfweb.usf.edu/usfgc/gc_pp/genadm/gc501.htm

4. Policies, Governance. (1999). Administrative Applications and Data Security Policy. Retrieved January 10, 2003, from UC Berkeley Computing & Communications website: http://ist-socrates.berkeley.edu:7015/admsecpol.html

5. Arizona Board of Regents. (2000). ACD 125: Computer, Internet, and Electronic Communications. Retrieved January 10, 2003, from Arizona State University manuals website: http://www.asu.edu/aad/manuals/acd/acd125.html

6. Alter, Allen E. (1996, February). Change in the weather. *COMPUTERWORLD*. Retrieved January 10, 2003, from http://www.computerworld.com/news/1996/story/0,11280,17020,00.html

7. Lieberman, Stuart. (1995, November). Should IS be Centralized or Decentralized. Computerworld Vendor Technology Solutions. Retrieved January 11, 2003, from http://www.computerworld.com/news/1995/story/0,11280,16798,00.html

8. SANS Institute. (1999). the SANS Security Policy Research Project. Retrieved February 9, 2003, from Web site: http://www.sans.org/y2k/sec_policy.htm

9. HRnext. Termination and Severance Pay Policy (standard). (n.d.). Human resource policies. Retrieved January 13, 2003, from http://www.hrnext.com/tools/view.cfm?articles_id=157&tools_id=5

10. Meta Security Group. (2002) Information Security: Best Practices. Retrieved January 14, 2003 from http://www.metasecuritygroup.com/library/deltas/InformationSecurityPolicy.pdf

11. Desmond, Paul. (2002). The Need for Security -- And Ethics – Education. eSecurity Planet. Retrieved January 15, 2003 from http://www.esecurityplanet.com/views/article.php/1454591

12. The American Heritage® Dictionary of the English Language, Fourth Edition. (2000) Houghton Mifflin Company.

13. Centers for Medicare & Medicaid Services. The Health Insurance Portability and Accountability Act of 1996 (HIPAA). Retrieved February 9, 2003, from Web site: http://www.cms.hhs.gov/hipaa/

14. Netforensics. (2001). Government Information Security Reform Act – GISRA. Retrieved February 9, 2003, from Web site: http://www.netforensics.com/gisra.html

15. Electronic Privacy Information Center. (1999). The Gramm-Leach-Bliley Act (GLBA). Retrieved February 9, 2003, from Web site: http://www.epic.org/privacy/glba/#introduction

16. Beeb (2001). ISO 17799 - What is iso17799 (the ISO Security Standard)? Retrieved February 9, 2003, from Web site: http://matrix0.members.beeb.net/iso-17799

17. DTI. Data Security: MANAGING INFORMATION SECURITY. Retrieved February 7,2003, from Website: http://www.dti.gov.uk/cii/datasecurity/managinginformationsecurity/experian.shtml

18. National Center for Education Statistics. Safeguarding your technology. Retrieved February 8, 2003, from Web site: http://nces.ed.gov/pubs98/safetech/

19. National Institute of Standards and Technology. Federal Agency Security Practices. Retrieved February 7, 2003, from Web site: http://www.csrc.nist.gov/fasp/