Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Organizational IT Security Theory and Practice: And Never the Twain Shall Meet?

In our effort to increase productivity and enhance communications we have created a modern interconnected business environment that provides opportunities for criminals and vandals to disrupt normal operations. For some, it's a revenue-generating exercise but for others it's a place to vent adolescent frustrations. A multibillion dollar industry has grown out of the need to both prevent and recover from resulting service disruptions, yet these disruptions continue to grow in frequency, impact, and cost 1. To properly a...

Copyright SANS Institute

Author Retains Full Rights

AD

SANS Security Essentials
GSEC Practical Assignment
Version 1.2e

Submitted By: John Jenkins
August 2001

Organizational IT Security Theory and Practice: And Never the Twain Shall Meet?

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Table of Contents

Introduction **1**

1 The Requirement **2**

2 The Practice **3**

2.1 Concept 3
2.2 Architecture 3
2.3 Implementation 3
2.4 Execution 4

3 The Perception **5**

4 The Reality **6**

4.1 Common Incidents 6
4.2 Common Causes 7

5 Solutions **9**

5.1 Limitation of User Freedom 9
5.2 Security Infrastructure Resourcing 9
5.3 The Software Industry 10

6 Summary **12**

References **13**

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Introduction

In our effort to increase productivity and enhance communications we have created a modern interconnected business environment that provides opportunities for criminals and vandals to disrupt normal operations. For some, it's a revenue-generating exercise but for others it's a place to vent adolescent frustrations. A multibillion dollar industry has grown out of the need to both prevent and recover from resulting service disruptions, yet these disruptions continue to grow in frequency, impact, and cost [1].

To properly address typical organizational security requirements we must first recognize that commonly-accepted mitigation methods can be inadequate, and we must then develop new methods based on an industry-wide paradigm shift in the way we approach technology in the workplace.

This paper presents an overview of common information technology security practices, demonstrates how and why they can frequently be ineffective, and finishes with suggestions on how we might better equip ourselves to prevent, and recover from unnecessary disruptions in the future.

© SANS Institute 2001, Author retains full rights.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

1 The Requirement

Organizational assets include electronic information created and collected during the normal course of operation. These information assets are comprised of financial data, personal data, trade secrets, and much more. For various reasons most organizations are obliged to protect information assets.

Most modern offices house electronic information assets on network-attached storage, and the network itself is attached, both physically and logically, to the rest of the world via the Internet. With the physical connection comes a host of threats to asset integrity, forcing each organization to create a virtual and physical fortress. Those tasked to develop a suitable security infrastructure must strike a sometimes difficult balance between cost, functionality, and security.

To function effectively, organizations have two basic information security requirements:

- Embracing the concept of IT security: Organizations must be able to effectively *demonstrate*, both internally and externally, that sufficient policies, procedures, checks, and balances are in place to adequately protect information assets. This may be a legal, regulatory, or certification requirement, and is frequently needed to protect reputation and instill confidence in both employees and customers.

- The execution of IT security: The concept of information asset protection must be put into practice. Again, this may be a legal or regulatory requirement, and be needed to ensure confidentiality and maintain competitiveness.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

2 The Practice

In practice the majority of large organizations have well-defined security policies and procedures, as well as significant security infrastructures. A typical scenario involves response to an internal or publicized threat: Top management will decree that information technology security becomes a high priority within an organization. Steering committees are formed, roles are defined, and tasks are assigned.

2.1 Concept

The first step involves defining the concept via the creation of information security policies and procedures. These are usually based on best-practices which may be difficult, if not impossible for many organizations to implement because of cost considerations. Development of these policies and procedures is a lengthy undertaking, frequently involving risk assessments and changes to business processes. Care must be taken to ensure that the final product does not end up as shelfware: Ranked according to weight, read by few, and typically out of date due to a continual need to modify content in response to environmental or organizational changes.

2.2 Architecture

The next step involves the design of an IT infrastructure capable of protecting assets as described within the policies and procedures. This task is given to the IT department, where the abstract concepts defined within the policies mandated by the CEO are translated into network schematics and detailed configurations. Although resourcing considerations are very important during the architecture phase, many organizations assign related tasks to the staff members with, in order of priority:

- The most available cycles;
- the highest seniority;
- a demonstrated aptitude; and/or
- a demonstrated interest.

Participation by experienced staff or outside assistance will greatly improve the quality of the architecture deliverable.

2.3 Implementation

Implementation involves building the infrastructure defined within the architectural blueprint. Goals can be further blurred as the intent of the CEO is translated into a working model, constrained by the pervasive technical and budgetary limitations of IT. Vendors are contacted, pricing acquired, and purchase orders are written.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

As the hardware and software arrives, the IT team tackles the complex and sometimes impossible job of making the components function as advertised. Without the participation of experienced staff, this often involves placing new orders for additional options, completely replacing products, memorizing vendor support numbers, and dedicating a large amount of disk space to firmware updates, service packs, miscellaneous patches, and documentation updates.

2.4 Execution

Once all of the pieces are in place an organization can go live with the new security infrastructure. Technical and end user training and employee awareness programs are delivered, existing processes are modified, and new processes are developed to meet unforeseen operational requirements.

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

3 The Perception

Large organizations invest thousands, and sometimes millions, of dollars to create a secure infrastructure capable of protecting information assets, and according to the Gartner Group this amount is expected to increase significantly over the next ten years, from a current average of 0.4 percent of revenue to a full 4 percent of revenue in 2011 [2]. There is an expectation that a return on investment will be seen, manifested in one or more ways:

- Immunization from worldwide virus outbreaks
- Documented unsuccessful break-in attempts
- Protection of trade secrets
- No unscheduled downtime
- No lost data

Policies developed by management provide the perception that someone has thought about the issue and has instituted processes that preserve asset integrity. Infrastructure builds by IT staff give a measure of comfort that hackers and viruses are unable to penetrate organizational barriers. Training and awareness programs delivered to end users gives the impression that an armed camp has been created, with “perimeter defenses”, “demilitarized zones”, and “firewalls”.

The perception, internally and externally, is that an organizational safety net has been created, protecting data and keeping “the bad guys” out.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

4 The Reality

Despite significant IT security investments, large government agencies and Fortune 500 organizations are typically among the high profile victims of crimes related to IT security. Our methods of combating both internal and external threats are not as effective as they can be simply because we continue to create environments that are ideal targets for intruders. We use insecure software, give our users freedom to wander about the digital landscape, and underresource our protection efforts.

Most unfortunate is that many of the most prevalent vulnerabilities are easily rectified, such as those that are eliminated using a simple patch, or those resulting from default installations [3].

4.1 Common Incidents

Virus Infections
According to Computer Economics, the estimated financial impact caused by computer virus infections in 1999 was $12.1 billion. This rose in 2000 to $17.1 billion, an increase of over forty percent [4]. Indeed, during one notable virus attack, the health of the entire US population was potentially at risk: Had there been a biological crisis during the "I Love You" virus outbreak, the ability of the US Federal Government to react was significantly diminished [5].

Web Page Defacements
From the list of sites that have fallen prey to defacements and the sheer frequency of incidents one would assume that there is no method of prevention available [6]. The list includes top US Government agencies such as the FBI, CIA, and Pentagon, as well as major computer companies such as Network Associates, McAfee, Silicon Graphics, Dell, NEC, and IBM. Indeed, vendors of defacement recovery software discuss how quick recovery is simpler and less costly than prevention. Although web site defacement does not normally result in significant damage, public perception can be negative, loss of confidence can result, and reputation can suffer.

Information Theft: Trade Secrets and Customer Data
According to consulting firm PriceWaterhouseCoopers, losses by US companies due to theft of trade secrets amount to over $45 billion annually [7]. Trade secrets define the advantage one company has over its competitors, and in many cases make up much of a company's value; therefore trade secret theft can result in a significant negative impact on a company's financial health. Technology has exacerbated this problem by increasing ease of access to proprietary information and making theft detection more difficult. To be considered a trade secret, organizations must be able to demonstrate that proprietary information is adequately protected. In the past this was a simple affair: Locking secret documents in a safe, then limiting

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

access to the combination was once considered adequate protection. In the digital age it is a common occurrence to inadvertently release trade secrets in the normal course of business, such as disposing of obsolete equipment [8].

Theft of customer data involves identity theft, theft of personal information, and credit card theft. Again, technology through electronic commerce increases the ability of criminals to access and profit from personal information.

Denial of Service
Denial of service attacks prevent the proper operation of an organization's infrastructure by saturating capacity. These attacks are easy to carry out and when coordinated effectively can have a huge impact on the performance of the Internet worldwide. Some examples of high profile victims of DOS attacks include Amazon, eBay, CNN, and Yahoo!.

4.2 Common Causes

While the ultimate responsibility for causing the failure lies with the perpetrator of the crime, internal responsibility for allowing these security failures to negatively impact an organization can be determined as well. In most cases the failure lies with end users, the organizational IT support infrastructure, and/or specific software packages.

End Users
End users are not adequately trained to identify or handle potential IT security incidents. Many users place personal desires over organizational requirements. Despite the mass publication of previous worldwide macro virus infections, users continue to double-click on unknown attachments promising funny stories and untold riches. Despite corporate policies, users continue to download unsupported, non-standard software from the Internet for installation on corporate equipment.

IT Support Infrastructure
A wide range of infrastructure-related factors can contribute to a security incident. Most notably, lack of maintenance or misconfiguration results in vulnerable systems. This can be caused by a skill shortage, insufficient resources, and poorly developed and enforced procedures. In many cases IT security implementations are not adequately funded into the operational stage; time constraints result in less glamorous tasks, such as log reviews and patch updates, being given a low priority. Email notifications of security vulnerabilities become lost in the sea continually flowing into a system administrator's inbox.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Software

Quality control, and in some cases common sense, has given way to the quest for market dominance through "featuritis": Efforts to increase ease of use and enhance automation have resulted in new opportunities for criminals to exploit. One example of this is the scripting ability built into Microsoft's office productivity packages: Virus developers wreak havoc on a regular basis using functionality intended to increase productivity.

In addition to the billions of dollars in expenses caused by virus outbreaks, the cure can sometimes result performance issues or in extreme cases, unscheduled downtime such as McAfee's automatic update error early in the year 2000, which caused machines to lock on boot and required technician-level skills to repair [9].

Increasing the quality of software would reduce software maintenance costs, and also reduce the frequency and impact of software-related disruptions.

© SANS Institute 2001, Author retains full rights.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

5 Solutions

5.1 Limitation of User Freedom

Typical end users have far more freedom than is necessary to accomplish daily work-related tasks; the personal computer revolution coupled with the Internet gave each user the ability to disrupt the activities of the entire organization with a single mouse click.

Desktop Lockdown
Many information technology security policies stop short of locking down the desktops for fear of lessening the computing experience for end users. Unfortunately this extra flexibility results in additional costs from lost productivity and increased support requirements. Drastic measures are necessary when organizational data traffic is brought to a halt because end users think they've been the fortunate recipient of naked pictures of a famous tennis player [10]. Empowering users in this way transcends the boundaries of common sense.

End user machines should be configured with static, unchangeable local configurations, devoid of local storage, and able to execute standard work-related applications and nothing more. In a business environment the personal computer must revert back from the personal entertainment machine it has become to a task-specific appliance.

Proximity and Biometric Identification
Despite the best efforts of security personnel, users continue to leave machines exposed and use passwords that are easily compromised. Proximity and biometric devices provide simple and inexpensive solutions to combat this behaviour. According to representatives from the City of Oceanside, implementation of a fingerprint-based biometric identification system across 1,500 seats paid for itself in less than two months [11]. Inexpensive biometric systems are widely available and the technology is mature: Implementation should be considered a primary goal of the information security department in all large organizations.

Proximity systems can be configured to lock the desktop when the end user leaves his/her workstation. Coupling this technology with biometrics provides a highly secure, flexible and cost effective solution for desktop security.

5.2 Security Infrastructure Resourcing

Development of a security infrastructure should not be an in-house exercise. Experienced help should be hired, or retained as needed, from the concept phase through to the execution. Although security consultants can be expensive, the technology transfer to in-house staff is invaluable. Cost

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

savings also result from a successful implementation: No amount of research or training can replace the skills gained from using undocumented procedures to make multiple products, even those from the same vendor, interoperate. Experienced professionals have "been there and done that" and are aware of existing and potential pitfalls.

There must be in-house technical continuity throughout an organizational security infrastructure implementation. This ensures that management intent is communicated to, and understood by those responsible for execution, and tempers the desires of management with technical and budgetary realities.

Sufficient attention must be paid to the operational requirements of an organizational security infrastructure. In many cases only the architecture and build phases are adequately financed; operational tasks are informally incorporated into the ever-increasing workload of systems support staff. An organization serious about information security should ensure that staffing is sufficient to monitor and enforce adherence to policies and procedures.

5.3 The Software Industry

Liability

When you buy an automobile there is an expectation that the vehicle will operate as advertised. When you press on the accelerator the car will move, and when you press on the brake the car will stop. The software industry has a unique advantage over other industries: No warranty is expressed or implied. When you buy virus software, it might protect you from viruses, but then again, it might not. The cyclical pattern of updating virus software *after* the damage has been done would be unacceptable in any other industry.

To improve software quality we must tip the balance in the software industry: Costs of failure must be greater than those associated with prevention and appraisal [12]. Substantial penalties would ensure that adequate attention is paid to initial quality.

Complexity

We have been given excessive flexibility at the expense of manageability. Configuration tasks necessary to prevent intrusion should be much simpler: Web site administrators should be able to check a box that says: "Content in these directories shall not change" and it should actually work. Network administrators should be able to check a box that says "These operating system files are static and shall not be modified" and have some confidence that the files are indeed safe.

Layout

Much of the complexity stems from operating system layout: There is no legitimate reason to scatter dynamic operating system data amongst static

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

system files, as is typical of many default OS installations such as Windows NT/2000. All server operating systems should have a lockdown mode, allowing an administrator to completely protect groups of files from external or unapproved modification. Categories can include:

- Static, unchanging operating system files, unmodifiable externally when locked down;
- Dynamic operating system data such as configuration information, writeable by the operating system only;
- Dynamic logs, writeable by the operating system only; and
- User data.

To increase overall software security, the same techniques used by hackers to exploit software flaws should be employed by the software industry as an ongoing quality assurance process.

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

6 Summary

As the saying goes, “The road to hell is paved with good intentions”. We might also use this saying when describing information security: We want secure information, we define how we intend to secure it, then we pay to make it happen. Despite these efforts many organizations end up with crippling virus outbreaks, web site defacements, trade secrets lost to competitors, and lost data. Should we throw money at the problem with the expectation that we can buy security? Or should we change the way we do business, eliminating the reasons for our woes?

If we increase the quality of our software by holding the industry responsible for costly flaws, decrease the potential destructive capability of end users, and adequately resource our protection schemes, we just might see a return on our security investment dollars.

© SANS Institute 2001, Author retains full rights.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References

1. "Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar". Computer Security Institute. 12 Mar 2001. <http://www.gocsi.com/prelea_000321.htm>

2. Witty, Roberta and William Malik. "Security TCO Model Helps With More Than Cost Savings". GartnerGroup. 12 June 2001. <http://www3.gartner.com/resources/98700/98707/98707.pdf>

3. "How To Eliminate The Ten Most Critical Internet Security Threats". SANS Institute. 25 June 2001. <http://www.sans.org/topten.htm>

4. "Computer Economics Virus Impact Update". Computer Economics Inc.. 14 Aug 2001. <http://www.computereconomics.com/cei/news/codered.html>

5. "U.S. Govt. was disrupted by Computer Virus, GAO Says". Office of International Information Programs, U.S. Department of State. 8 Aug. 2001. <http://usinfo.state.gov/topical/global/ecom/00051902.htm>

6. Defacement Archive at alldas.de. <http://defaced.alldas.de/defaced.php?archives=complete>

7. "American Society for Industrial Security/PricewaterhouseCoopers Trends in Proprietary Information Loss Survey Report". PriceWaterhouseCoopers. <http://www.pwcglobal.com/extweb/ncsurvres.nsf/DocID/36951F0F6E3C1F9E852567FD006348C5>

8. Heuser, Peter. "Trade Secret Protection in the Computer Age". June 1997. <http://www.khdmh.com/tradesecret.html>

9. McCarthy, Kieran. "McAfee virus update freezes PCs". The Register. 11 Feb 2000. <http://www.theregister.co.uk/content/1/14437.html>

10. Sieberg, Daniel. "New e-mail virus preys on Anna Kournikova fans". CNN. 12 Feb 2001. <http://www.cnn.com/2001/TECH/internet/02/12/anna.worm/>

11. "City of Oceanside implements biometric security on network". Serverworld. May 2000. <http://www.serverworldmagazine.com/compagent/2000/05/oceanside.shtml>

12. Kaner, Cem. "Quality Cost Analysis: Benefits and Risks". Software QA, Volume 3, #1, 1996, p. 23. <http://www.badsoftware.com/qualcost.htm>

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced