SANS Institute
Information Security Reading Room

Endusers - A Critical Link in the Chain of Security

Dana Brigham

Dana Brigham
GIAC Security Essentials Certification (GSEC) Practical
Version 1.4b
05/13/03

End-users – A Critical Link in the Chain of Security

Abstract

Establishing the security of Information System (IS) resources is an important
and major undertaking in any organization. End-users have a very important role
in the chain of establishing and maintaining that security. No reliable security
policy or procedure can be implemented without taking end-users into
consideration.

Background

Every organization with IS resources has end-users. From the huge multi-
national corporations with tens of thousands of employees spread across the
globe, to the home-based business that rolls the CEO, system administrator and
end-user into one. Most IS-based businesses may service many customers, and
these customers are also end-users.

The process of securing IS resources can be compared to forging a chain, link by
link. Some organizations may require more links than others due to the
complexity of the organization and the variety of the resources being secured.
The most common links in this chain will be physical security (i.e. locked
computer room, smartcards), electronic access security (i.e. secure protocols,
password requirement for access, firewalls), data security (i.e. encryption, access
control lists), account security (i.e. allow no guest access, password
requirements and expiration), archival security (i.e. tape backups, optical
archiving systems, offsite secure storage of backup media), operating-system
maintenance, operating-system patch management, and acceptable-use policies.

Establishing these primary elements of IS resource security will also require an
overall security policy, security staff and security procedures.

The creation of the policies and procedures will almost always take place at the
"back end" of the IS management structure. The personnel responsible for
creating and implementing these policies and procedures will typically not be
involved directly with end-users. But in order for these policies and procedures
to be as effective as possible, end-users must be taken into account.

End-users and Policy

A common piece of the security policy is the end-user acceptable-use agreement that end-users are generally required to acknowledge or sign. This is extremely useful as a fallback after a security incident has happened, but this agreement is often ignored or misunderstood by end-users. Just signing or acknowledging the agreement does not mean that end-users understand it. Additional methods need to be used to make the essence of this agreement understandable to end-users.

End-users need to understand, first and foremost, that they not only have a responsibility to maintain the security of the IS resources that they use, but also that they have a vested interest in doing so. Much like the "carrot and stick" approach, end-users must realize that there are benefits to their adhering to, and consequences of not adhering to, the security policies and procedures.

> When there is no vision, the people are unrestrained. But happy is he who keeps the law (Prov. 29:18, NASB).

It is important to note that while IS staff may be key in creating the IS resource security policies and procedures, they should not be the staff to handle breaches of security or non-adherence to the policies by end-users. These are jobs for the legal and human-resources departments of the organization.

The Benefits and the Risks

Employees in for-profit corporations need to realize that their adherence to the security policies has a positive effect on the health and profitability of their company. They must understand that the failure to do simple things (like protect their workstations from viruses) has the potential of damaging major IS resources. Downtime and costs associated with security incidents can easily affect the revenue and profits of a company, and the company's reputation, which can have a detrimental affect on the salaries, raises, bonuses, and even jobs of the employees.

David M. Smith, PhD., of Pepperdine University, estimated that in 1998, out of 72 million PCs in use, 305,700 suffered data loss due to computer viruses. Dr. Smith estimated that the average data loss costs $2,557.00. These computer-virus incidents alone accounted for $781,674,900.00 in costs to the owners/businesses where these incidents occurred.

End-users must be conscious of the sensitivity of the data to which they have access, and follow the policies that dictate who can have access to that data and what can be done with that data. The release of personal, sensitive or classified data can not only cost the company or individual money, but it can even cost lives, in the case of government or military data.

The current director of the United States Central Intelligence Agency (CIA), George J. Tenet, in a speech in 1998, described the growing dependence of the United States, including the United States military, on its information infrastructure:

> Unfortunately, our heavy and growing societal and strategic dependence on information technologies and information systems has created vulnerabilities -- vulnerabilities to our economic institutions, to the systems that support public needs, to our privacy, and to our military capabilities. I know that the extent of our vulnerabilities is still to be studied and debated (Tenet).

Personal Use

In many organizations, there is a certain amount of personal use allowed for end-users while using IS resources. Management may often consider this a benefit provided for end-users, while end-users may often consider this a right. The acceptable-use policy must make it clear what types of personal use are, and are not, allowed, as well as how much of end-users' time can be devoted to personal use. Personal use by end-users may often be the primary "back door" where security breaches take place (i.e. malicious code attached to personal email or transmitted over messenger applications, suspect or compromised external web sites that download malicious code to end-users' workstations).

The amount and type of personal use allowed for end-users must be carefully balanced with the additional security risks that it creates.

These examples show that IS resource security is not only critical, but that end-users play an important part in maintaining that security.

As stated before, end-users need to be thought of as a link in the chain of components of IS resource security. If that link is weak, the chain is easily broken; and if that link is broken, then there is no chain.

Big Brother

It may be difficult for some IS managers and system administrators to believe that end-users must be thought of as equals when it comes to security responsibilities. It may be easy to develop a strong set of rules and regulations that end-users are required to follow, but it may not be so easy for end-users to follow those rules and regulations.

In many organizations, the IS staff tends to take a "Big Brother" approach to handling end-users. The staff often believes that end-users do not have the knowledge, skills or experience necessary to handle responsibility for the proper

configuration and maintenance of their hardware and software. So the IS staff often invests a large amount of time and money in tools that control these items for end-users. This is not only an additional burden on an often overworked staff, but it also takes end-users out of the loop of being aware of what is really happening on their workstations.

This management approach and these management tools can go a long way toward making the organization's IS structure heterogeneous and consistent, but they should be combined with the participation of end-users, for a more successful outcome. End-users should know what management software and enforced configuration policies are on their workstations. They should be aware that, for example, they have antivirus software running, or that their workstations are periodically scanned for vulnerabilities. This knowledge should be a comfort for end-users and should give them a positive view of IS management, when they are presented with the fact that such systems are in use to make their jobs easier and to increase their productivity.

These tools are a key part of IS security procedures, even if they have not been thought of that way in the past. Certainly a properly and consistently configured and managed end-user workstation is much less of a security vulnerability than one that is not.

The more involved that end-users feel in the process of creating the rules and regulations, and participating in the security of IS resources; and the more ownership that end-users feel over the IS resources, the more end-users are likely to be a strong link in the IS-resource security chain.

Strengthen the End-user Link

End-users should be involved in the development and refinement of IS-resource security policies and procedures. End-users should also be involved in periodic review of existing policies and procedures in order to keep them up to date and relevant. Below are some examples of end-users-oriented activities that can be used to help strengthen end-users as a security resource:

- Security-policy introduction as part of new-employee orientation.
- Required end-user acknowledgement of security policies through signing the policy or a statement of understanding, or having to acknowledge a pop-up window before being allowed access to secured IS resources.
- Stronger end-user acknowledgement requirements for more highly secured IS resources, or for end-users taking parts of the organization's IS resources (i.e. laptops) outside of the protection of the secured IS infrastructure.
- Regular end-user training sessions on established security policies and procedures.

- Implement security-awareness reminders (i.e. sidebars on intranet web pages, pop-up windows in corporate applications, posters in the hallway).
- Implement postings on intranet websites, application help files, and other internal IS resources, of the complete security policy, how-to guides, tips and FAQs.
- Periodic seminars/presentations on the importance of security (having security representatives of other organizations/companies present true-to-life stories of security incidents would be a plus).
- Periodic round-table discussions with small groups of end-users to get feedback on how well they perceive that the current security policies and procedures are working.
- A working group of selected employees should be involved in the actual revision process for security policies and procedures, especially after any security incidents have occurred.
- Implement a performance-recognition system (i.e. naming end-users in company newsletters, giving employee-of-the-month awards) for exceptional end-users who are the first to spot security incidents.
- Implement a penalty system (i.e. employee performance/salary reviews may be adversely affected) for failure to follow existing security policies.
- Periodically post internal reports of security incidents that have occurred within the organization, and the impact on the finances and reputation of the organization.
- Don't reinvent the wheel; research what is being done at other similar organizations and government agencies.

All of these possibilities are designed to reinforce that proper security, and end-users' adherence to security policy, is a positive thing. The idea is not to scare end-users about all of the terrible things that can happen with inadequate security, or their failure to adhere to security policies, but to show them that security is taken seriously in the organization, and that they are an important part of the organization.

At the same time, the IS staff should use the tools at its disposal to determine exactly what end-users are doing with the IS resources to which they have access – and maybe some to which they should not have access.

Collecting statistics on the use of the corporate infrastructure and IS resources, down to the per-end-user level, will help any organization realize exactly how end-users "use." From this information, the security policies and procedures can be honed to fit the true actions of end-users much more appropriately, and save unnecessary expenses and staff hours. This information should be used to enhance the security policies and procedures, the goal being to enhance the health and strength of the organization.

Are There Different Classifications of End-users?

Usually there are not generic end-users in any organization. Any employees of the organization that have access to IS resources are end-users, but they can be in quite a range of positions, with quite a range of job titles, descriptions and responsibilities.

Security policies and procedures should apply to all end-users. There should be no exceptions for CEOs, mid-level management, IS staff, customers or anyone else. But there may be specific classes of end-users who require additional security policies and procedures. Telecommuters, contractors and consultants are just a few examples where additional security policies may be in order. These end-users may have not only more restrictions on their access to IS resources, but there may be a need to have stricter policies enforced with them due to the nature of the methods of their access to IS resources, or their not being direct employees of the organization.

When employees leave the office with corporate laptop computers for use at home or while on travel, those employees are taking pieces of the corporate IS resources with them. They must maintain the highest level of control over those pieces at all times, not just when they might use them to access the main corporate IS resources. Those pieces may be accessible to persons without any connection to the corporation at all, as well as be accessible to the wider world of data communications from which the main corporate IS resources are sheltered. These employees should be made to understand the high level of responsibility that they are assuming.

Regardless of these classifications, all end-users should be made aware of their role in IS resource security, and their responsibilities. Careless contractors who accidentally allow a virus to enter the corporate network may find that their contract is not renewed. System administrators could be embarrassed by the results of the quarterly security audit when their systems are found to be a year behind in security patches.

What about Customers?

IS management must remember that customers of any data resources are also end-users. Organizations with a Web presence, especially Internet retailers, should consider anyone who uses their sites as an end-user.

It may seem that these end-users would not have as much investment in the security of the IS resources that they use as would the employees of the organization, but often the security of the sites that they access can be just as critical to them. Retailers and large corporations with an online-customer base usually hold a good amount of their customers' personal data within their IS resources. Addresses, phone numbers, Social Security numbers, and even credit-card numbers may be stored at these sites.

These sites need to be highly protected from adverse actions, but also from unintentional mistakes made by customers. It may make a customer's experience seem less user-friendly to implement the following security procedures, but here are some examples of actions that can be taken to strengthen the weak points of customer access:

- Include a security/user-agreement dialog box that must be acknowledged before customers are allowed access to, or input of, any sensitive information.
- Use only secure protocols and encryption.
- Encourage end-user familiarity with the process of using the data/site through pop-up windows, help screens and online manuals.

What about Management?

Most organizations have at least one level of management that exists above end-users, but the IS staff is not part of that level of management. These managers are end-users, but they often feel that they are not necessarily governed by the same policies and regulations that end-users who work for them are. But in order for security policies to work, these managers must be treated just like every other end-user. And since they have a direct influence on end-users who work for them, they need to take responsibility for encouraging their end-users to adhere to security policies.

They not only need to understand the importance of the policies but the reasoning behind those policies. They need to understand that the productivity of end-users who work for them can be drastically reduced by security incidents, and that this reflects poorly on their management record.

Management should directly and publicly exemplify the security-conscious end-user by adhering to security policies, attending security forums, and preaching the positive aspects of what these policies do for the organization.

And Don't Forget the Support Staff

Any staff of the organization that handles end-users support issues or training and general support of end-users (i.e. Help Desk, IS staff, human resources) should be more highly trained and more cognizant of the security policies and procedures than end-users. These support personnel are the people who will be most often directly interfacing with end-users and influencing end-users' view of security policies.

The support staff should take every opportunity to encourage end-users to not only adhere to the security policy, but also to reinforce the benefits and consequences for end-users.

Provide Resources that Enable End-users to Help

Just having well educated end-users who feel a stake in the security of IS resources is not enough to ensure that these end-users will help maintain that security. End-users must have the ability to report any possible security issues as easily as possible.

Organizational support staff, help desks, and system administrators can all be possible contact points for the reporting of possible security issues. For organizations with IS resources available 24/7 there should be a 24-hour phone number/email contact for end-users to report possible security incidents. The staff manning this contact point should not only be knowledgeable in determining whether or not the report is a possible security incident, but also in providing positive reinforcement to end-users.

There should be a suggestion box (i.e. email, webpage form) available at all times, where end-users can provide feedback and suggestions on security policies and procedures.

IS staff can provide end-users with feedback and tools to measure how well end-users are adhering to security policies. Some examples are:

- Password-change programs that check for/do not allow passwords that do not meet IS security policies.
- Tools that show and explain to end-users their access permissions.
- Tools that end-users can choose to run, and IS staff can remind end-users to run, that check their systems for proper access, network and permission settings, and then give the user feedback on what needs correction and how it can be corrected.

The IS staff should be continually conscious of how end-users see and interface with the organizational IS resources. It is only in this way that they can be aware of what tools and provisions they can provide to enhance the ability of end-users to adhere to security policies and procedures.

Conclusion

Any organization with any amount of IS resources should be concerned with protecting those resources. Protecting those resources requires planning and the implementation of security policies and procedures. The more comprehensive those procedures are, the better; but incomprehensible procedures and policies will be very difficult to implement.

End-users are a key component of any organization, so they must be a key component of the security policies and procedures. And in order for end-users --

often personnel who are very far removed from the IS management and staff -- to comprehend and follow those policies and procedures, they must be taken into consideration throughout the planning and implementation of those policies and procedures.

References

Bird, David. "Encouraging End-user Self Sufficiency." Intranet Journal. October 3, 2002. URL: http://www.intranetjournal.com/articles/200210/ij_10_03_02a.html (May 7, 2003)

Gartner Group. "Security and Privacy." Gartner Group Events Best Practices Whitepapers. May, 2002. URL: http://www.gartner.com/2_events/best_practices/securpriv.pdf (May 4, 2003)

Heckman, John. "Internet Security: What You Need to Know to Protect Your Firm." Microlaw Columnists. Uknown origination date. URL: http://www.microlaw.com/columns/guest/heckman1.html (May 7, 2003)

Hicks, Matt. "Security: How Do You Rate?" eWeek. December 17, 2001. URL: http://www.eweek.com/print_article/0,3668,a=20185,00.asp (May 5, 2003)

Information and Technology Division (ITD), Brookhaven National Laboratory. "Personal User Agreement." Brookhaven National Laboratory Cyber Security. October 4, 2002. URL: http://www.bnl.gov/cybersecurity/files/pdf/UserAgreement.pdf (May 4, 2003)

Liebmann, Lenny. "Monitoring the End-user." Network Magazine. June 5, 2002. URL: http://www.networkmagazine.com/article/NMG20020602S0002 (May 7, 2003)

NASB -- New American Standard Bible. 1995. The Lockman Foundation.

Onley, Dawn S.. "DISA Official: Users should be accountable for security." Government Computer News. April 25, 2001. URL: http://www.gcn.com/vol1_no1/daily-updates/4028-1.html (May 8, 2003)

Rudolph, K. and John Tressler. "Getting the Word Out." Native Intelligence Security Article 2. June 1997. URL: http://nativeintelligence.com/trnart.asp (May 12, 2003)

Smith, David M., PhD.. "The Cost of Lost Data." Legato White Papers. September, 1999. URL: http://portal1.legato.com/resources/whitepapers/W052.pdf (May 13, 2003)

Tenet, George J.. "Information Security Risks, Opportunities, and the Bottom Line." Central Intelligence Agency – Speeches and Testimony. April 6,1998. URL:
http://www.cia.gov/cia/public_affairs/speeches/archives/1998/dci_speech_04069 8.html (May 13, 2003)

van der Walt, Charl. "Introduction to Security Policies, Part Two: Creating a Supportive Environment." SecurityFocus InFocus Library. September 24, 2001. URL: http://www.securityfocus.com/infocus/1473 (May 12, 2003)

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS New York City Winter 2020	**New York City, NYUS**	**Feb 10, 2020 - Feb 15, 2020**	**Live Event**
SANS Northern VA - Fairfax 2020	**Fairfax, VAUS**	**Feb 10, 2020 - Feb 15, 2020**	**Live Event**
SANS London February 2020	**London, GB**	**Feb 10, 2020 - Feb 15, 2020**	**Live Event**
SANS Cairo February 2020	**Cairo, EG**	**Feb 15, 2020 - Feb 20, 2020**	**Live Event**
SANS Dubai February 2020	**Dubai, AE**	**Feb 15, 2020 - Feb 20, 2020**	**Live Event**
SANS Brussels February 2020	**Brussels, BE**	**Feb 17, 2020 - Feb 22, 2020**	**Live Event**
SANS Scottsdale 2020	**Scottsdale, AZUS**	**Feb 17, 2020 - Feb 22, 2020**	**Live Event**
SANS San Diego 2020	**San Diego, CAUS**	**Feb 17, 2020 - Feb 22, 2020**	**Live Event**
Open-Source Intelligence Summit & Training 2020	**Alexandria, VAUS**	**Feb 18, 2020 - Feb 24, 2020**	**Live Event**
SANS Training at RSA Conference 2020	**San Francisco, CAUS**	**Feb 23, 2020 - Feb 24, 2020**	**Live Event**
SANS Manchester February 2020	**Manchester, GB**	**Feb 24, 2020 - Feb 29, 2020**	**Live Event**
SANS Secure India 2020	**Bangalore, IN**	**Feb 24, 2020 - Feb 29, 2020**	**Live Event**
SANS Jacksonville 2020	**Jacksonville, FLUS**	**Feb 24, 2020 - Feb 29, 2020**	**Live Event**
SANS Zurich February 2020	**Zurich, CH**	**Feb 24, 2020 - Feb 29, 2020**	**Live Event**
Blue Team Summit & Training 2020	**Louisville, KYUS**	**Mar 02, 2020 - Mar 09, 2020**	**Live Event**
SANS Northern VA - Reston Spring 2020	**Reston, VAUS**	**Mar 02, 2020 - Mar 07, 2020**	**Live Event**
SANS Munich March 2020	**Munich, DE**	**Mar 02, 2020 - Mar 07, 2020**	**Live Event**
SANS Secure Japan 2020	**Tokyo, JP**	**Mar 02, 2020 - Mar 14, 2020**	**Live Event**
ICS Security Summit & Training 2020	**Orlando, FLUS**	**Mar 02, 2020 - Mar 09, 2020**	**Live Event**
SANS Jeddah March 2020	**Jeddah, SA**	**Mar 07, 2020 - Mar 12, 2020**	**Live Event**
SANS St. Louis 2020	**St. Louis, MOUS**	**Mar 08, 2020 - Mar 13, 2020**	**Live Event**
SANS Prague March 2020	**Prague, CZ**	**Mar 09, 2020 - Mar 14, 2020**	**Live Event**
SANS Paris March 2020	**Paris, FR**	**Mar 09, 2020 - Mar 14, 2020**	**Live Event**
SANS Dallas 2020	**Dallas, TXUS**	**Mar 09, 2020 - Mar 14, 2020**	**Live Event**
Wild West Hackin Fest 2020	**San Diego, CAUS**	**Mar 10, 2020 - Mar 11, 2020**	**Live Event**
SANS Doha March 2020	**Doha, QA**	**Mar 14, 2020 - Mar 19, 2020**	**Live Event**
SANS London March 2020	**London, GB**	**Mar 16, 2020 - Mar 21, 2020**	**Live Event**
SANS Norfolk 2020	**Norfolk, VAUS**	**Mar 16, 2020 - Mar 21, 2020**	**Live Event**
SANS SEC504 Nantes March 2020 (in French)	**Nantes, FR**	**Mar 16, 2020 - Mar 21, 2020**	**Live Event**
SANS San Francisco Spring 2020	**San Francisco, CAUS**	**Mar 16, 2020 - Mar 27, 2020**	**Live Event**
SANS SEC401 Lille March 2020 (in French)	**Lille, FR**	**Mar 16, 2020 - Mar 21, 2020**	**Live Event**
SANS Secure Singapore 2020	**Singapore, SG**	**Mar 16, 2020 - Mar 28, 2020**	**Live Event**
SANS Security East 2020	**OnlineLAUS**	**Feb 01, 2020 - Feb 08, 2020**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**