



THE RHODENIZER REPORT

MARCH 2008

www.rhodenizer.com

INSIDE THIS ISSUE:

FUNDAMENTAL CONCEPTS OF SECURITY	1
PART 3 OF 4: DATA SECURITY	2
SECURITY FLAWS FOUND IN OVER 80% OF ALL PC'S	2
QUESTIONS FROM THE INBOX	3
ENCRYPTION MAY NOT BE ENOUGH	4
ABOUT RHODENIZER IT	4

THE TAKE-AWAY POINTS:

- Information security is a strategy.
- Strategy dictates policy, then measures.
- Always keep installed programs updated.
- Make sure laptops are completely turned off when not in use.

FUNDAMENTAL CONCEPTS OF SECURITY

Information security is not a service or a product you can buy. It is a **strategy**. Formulating a successful strategy begins with understanding these fundamental concepts.

#1). There is no such thing as "secure information". The term is an oxymoron. Merriam-Webster defines information as: "The communication or reception of knowledge or intelligence." It cannot be information if no one has access to it. And, "secure" in the ultimate sense equals complete inaccessibility. Therefore, security is never an absolute when it comes to information.

#2). Security is a balance between isolation and access. Whether it's land, people, or information, maximum security equals total isolation and zero accessibility. Likewise, a com-

plete lack of security equals unlimited access and zero isolation. This explains why freedom, in everything, is the antithesis of security. The best we will ever achieve is an acceptable balance between the two.

#3). Achieving an acceptable balance of security for the information you manage requires:

A). Knowing what to allow, and what **not to allow.** Establish who is authorized to view information, who is authorized to view and modify, and under what conditions may they do so.

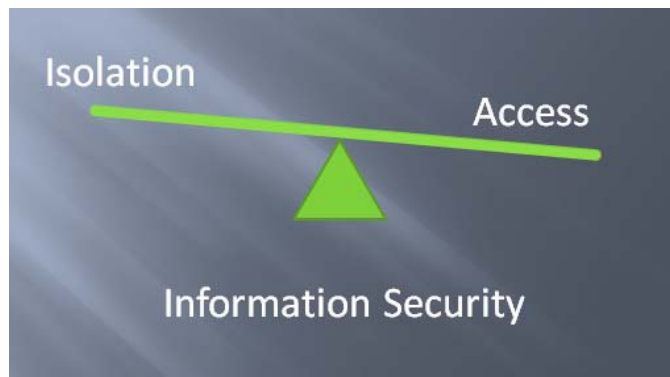
B). A means of authentication by which to prove identity. Keys, biometric scanners, and passwords are among the methods that can be used to authenticate users. Multiple methods may even be appropriate depending upon the nature of the information at risk.



C). Having complete control over all points of access. We cannot enforce "A" without "B" and "C".

One of the biggest challenges to controlling access is the problem of portability. It's one thing to grant access to information under your control, yet another to allow users to make copies of their own that you can't control. **Security measures become useless once you allow restricted information outside your realm of control.**

Ultimately, all data security measures are just means and methods by which we use technology to enforce your policy mandates. Those mandates, in turn, will come from the strategic planning sessions between you and your professional IT consultant. - C. R.



PART 3 OF 4: DATA SECURITY

In the last issue, we covered backing up and recovering your data. In this issue, we focus on data security - (the terms "information" and "data" are often used interchangeably. However, "information" actually refers to intangible knowledge while "data" refers to tangible bits and bytes being used as the source of the information).

There are 3 distinct dangers to all stored data:

- #1. Loss
- #2. Corruption
- #3. Unauthorized access.

Here are some proactive and reactive measures you can take to protect your business.

PROACTIVE: Avoiding the three dangers requires having complete control over all access to company data and company computers. Then,

users must be instructed on policy concerning the proper handling of sensitive information and acceptable use of company owned assets.

Technology gives us tools for monitoring compliance, but these alone are not enough.

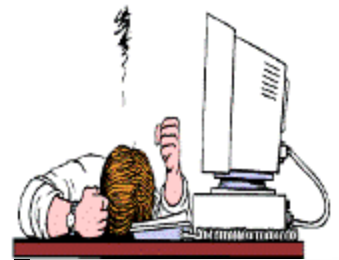
If you centralize all critical data into one location, it is much easier, and more economical to manage security. If stored on a server, we can configure appropriate access permissions and require strong passwords. We can further strengthen security by limiting physical access to it. Locked doors and security alarms serve as a deterrent, but are not fool-proof.

REACTIVE: We can restore backed-up data in response to damage caused (either intentionally or inadvertently) by the first two dangers. But, early detection is key to mini-

mizing your loss. Lost or corrupted data is usually obvious. But, if left undetected for a long time, corrupted data is also backed up and eventually replaces the corresponding "good" data on all subsequent backups in the rotation. This is why periodic archives are so important.

Unauthorized access can be difficult, if not impossible, to detect. And, reactive measures can only be thought of as damage control at best. Change passwords and account numbers quickly. Notify all who will be affected. Seek legal counsel as needed. No business owner ever wants to go through that. That's why it's vital to consult with an IT pro and prepare a comprehensive security strategy for your business.

Next time, we'll look at some methods for remote access.



"...early detection is key to minimizing your loss."

SECURITY FLAWS FOUND IN OVER 80% OF ALL PC'S

Internet security firm Secunia estimates that 81% of all PC's connected to the Internet urgently need to have one or more programs updated.

Security vulnerabilities were recently discovered in 229,023 out of 282,726 computers tested, and attributed to flaws in four particular programs that can be exploited and used to plant malicious code on the PC's of unsuspecting users.

Until updated, users of PC's running these programs risk falling victim to hackers simply by visiting certain websites, opening PDF files, or viewing videos online.

If you have any of these four programs installed on your PC, I recommend completely uninstalling them. Restart, then download the latest version from each company's website if you want to continue using them. - C. R.

81% failed security tests due to flaws discovered in one or more of these programs:

PROGRAM	VERSION	OF ALL PC'S AFFECTED
Adobe Reader	8.0	61%
Apple Quicktime	7.0	47%
Sun Java	1.5.0	35%
Skype	3.0	20%

Source: <http://www.secunia.com/blog/20>

QUESTIONS FROM THE INBOX

Q- “Will I eventually have to upgrade to Windows Vista?”

A- Absolutely not. You can continue to use Windows XP as long as you like. However, Microsoft will discontinue all support and security updates sometime in 2014.

One alternative I’ve been exploring is the free, open source version of Linux called **Ubuntu**. It takes a little tweaking to get everything setup the way you want it, but it’s easy to use and I can do just about everything on it except run QuickBooks. I don’t need antivirus or anti-spyware protection and... did I mention it’s free?

We have already seen greatly increased interest in Linux since Windows Vista was released. I predict there will soon be even more support from application vendors as Linux gets better, and easier to use. I think it will soon emerge as a viable alternative to Microsoft Windows for many small businesses.

Q- “How can I check the security of my firewall to find out if it’s adequate?”

A- There are some free tools on the web for that purpose. Check out www.grc.com and run the “Shields Up” tests. Then, go to www.pcflank.com and step through all of their tests **except for the DoS (denial of service) simulated**

attack. Unless your router has a DoS prevention feature, that test would probably cause it to lock-up.

If the test results show all your ports in “**stealth**” mode, you are invisible to those on the Internet looking for a random target. If some ports show “**closed**”, you’re still OK though you may get picked on and probed. If ports are “**open**”, you should have it immediately checked and possibly even replaced by a qualified IT professional.

When looking for an inexpensive home/office router with firewall, the most important features I look for are **SPI** (Stateful Packet Inspection), **NAT** (Network Address Translation), and the ability to disable **UPnP** (Universal Plug and Play). These can usually be found for less than \$100.

For the best prices on these and other computer items, go to the “**Cliff’s Pick’s**” page of my website and click on “NewEgg”.

Q- “Why do I need a security “strategy” when I can just install a firewall that blocks out everything bad?”

A- Everything bad is not on the outside. Some of the worst threats to the security of your business actually work for you. Employees unknowingly do more each year to cause damage and cost

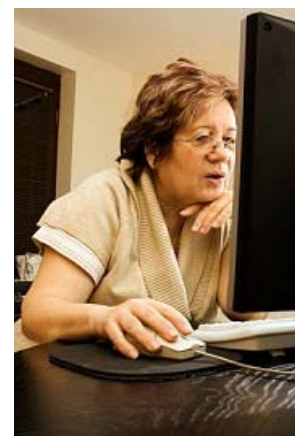
companies unnecessary IT expense than all attacks initiated from the outside.

Employees (and their kids) sometimes bring all kinds of entertainment software from home, or download it from the Internet, and install it on office computers inside your network, effectively bypassing your firewall security.

These programs slow computers to a crawl, or worse - unleash malware and expose company servers to dangerous exploits. These personal liberties taken with company computers can cost employers many thousands of dollars in unnecessary expenses, and even expose them to liability lawsuits.

Most users mean no harm. They just don’t know any better. But, some actually don’t care. If their personal use of a company computer creates problems, it doesn’t really cost them anything. And, if there’s no company policy against it, what’s to stop them?

That’s why every business needs a strategy for asset protection, and policies that establish rules of conduct for employees. Don’t let the business you’ve worked so hard for fall victim to the careless behavior of others. - C. R.



“Some of the worst threats to the security of your business actually work for you.”

Send your questions to:
questions@rhodenizer.com

ENCRYPTION MAY NOT BE ENOUGH

An experiment by Princeton University has revealed that modern encryption used to protect data on laptops is not as secure as we thought.

A video demonstration found on YouTube shows how a memory module from a stolen laptop can be frozen by mist from a spray can, removed, then inserted into another laptop and examined by a program students have created. This program looks for the encryption key that was resident in memory while the laptop was last being used. Once extracted, the key can be used to unlock the

contents of the stolen laptop's hard drive without requiring any password.

Microsoft Vista's Bit Locker, and even the open source TrueCrypt, are defeated by this technique if the stolen laptop is taken while still in "sleep" mode.

The best protection against this method of stealing data is to **completely shut down and turn off your laptop when you are not using it**. And, turn off the "hibernation" feature.

Encryption is still a security measure necessary for all laptops that contain private

information. However, as we have seen with all security measures, there are always flaws that can be exploited.

The important lesson to learn here is to not rely upon any one method to keep you safe. Information security is a strategy that combines various methods and measures to achieve an acceptable level of overall security.

To watch this fascinating video clip, just go to the "Video Tips" page of my website (www.rhodenizer.com) and scroll down to the last video. It's definitely worth watching. - C. R.



"... key can be used to unlock the contents of the stolen laptop's hard drive without requiring any password."

ABOUT RHODENIZER IT

We are a different kind of IT service provider. We don't sell any hardware or software. There are no sales incentives for steering you toward a particular product. We provide IT consulting services that include finding the best deals on what you really need and passing the savings along to you.

Our mission is to do more than fix computer problems.

Our mission is to help small companies save money, increase productivity, and safeguard private information.

We work with clients to prepare disaster recovery plans that ensure their critical data remains safe, yet easily accessible. The benefits of such strategic planning also includes money-saving ideas for managing resources and reducing IT expenses.

We have the training, experience, and know-how to provide the right solutions for your needs, and your budget.

Just call to schedule your **free initial consultation with no risk, and no obligation.**

Tell me about your computer needs or IT issues. I'll recommend a course of action that makes sense for your situation at no cost to you. What have you got to lose?

Rhodenizer IT
Information Technology Services

P. O. Box 768122
Roswell, Georgia 30076

(404) 202-8657

www.rhodenizer.com

The Rhodenizer Report is published and distributed by Rhodenizer IT, Inc. © Copyright 2007. All Rights Reserved.

DISCLAIMER: The information, opinions, and recommendations expressed within are for general knowledge and are not intended to be a substitute for personal consultation. Furthermore, some information may be based upon other information provided by third parties. Unless specifically stated, no form of independent verification is undertaken. The author is not responsible for any errors, omissions, or inaccuracies. This information is provided free of charge and is without warranty, neither explicit nor implied. The reader assumes all risk when performing any computer modifications without the direct supervision of a qualified IT professional.