

By Michael Kassner

I recently attended a seminar on how to prevent security breaches. As the meeting progressed, I realized something: People have been infringing on others' security for a long time. Is it too bold to think that we can finally do something about it? Maybe if we use the direct approach -- but how about working with human nature?

More specifically, security has been and always will be about effort. If I want to steal a car, I'm certainly not going to walk past a car with the doors unlocked and engine running to the next one that's locked and has the alarm activated. I think we can agree that under most conditions, the car requiring more effort to compromise is assumed to be more secure.

With that premise in mind, I created a list of 10 practices that will significantly increase the effort required to breach the security of your network and computers.

## Definition

Before we get started, let's define what we're talking about. The term *security breach* can conjure up all sorts of meanings, but I'd like to focus on how it relates to information technology. See what you think about this definition:

**Security breach:** A situation where an individual intentionally exceeds or misuses network, system, or data access in a manner that negatively affects the security of the organization's data, systems, or operations.

I like that definition because it implies that any breach of security has real-world implications, be it stolen personal financial information or business trade secrets getting into the wrong hands.

## 1: Change default passwords

It's surprising how many devices and applications are protected by default usernames and passwords. Attackers are also well aware of this phenomenon. Not convinced? Run a [Web search](#) for default passwords, and you will see why they need to be changed. Using [good password policy](#) is the best way to go; but any character string other than the default offering is a huge step in the right direction.

## 2: Don't reuse passwords

On more than one occasion, I've run into situations where the same username/password combination was used over and over. I realize it's easier. But if I know this, I'm pretty sure the bad guys do as well. If they get their hands on a username/password combination, they're going to try it elsewhere. Don't make it that easy for them.

There are many helpful password vaults that require you to only remember the master password to gain access to the vault. After that, it's usually a matter of selecting the proper entry.

For instance, **Figure A** shows [Password Safe](#), the password vault I use. It's open source and recommended by [Bruce Schneier](#).

## 3: Disable user accounts when an employee leaves

Security breaches are easier to pull off when the attacker has insider information. That makes it essential to disable all IT accounts of a user who has terminated employment. It doesn't matter whether the employee is leaving under amicable terms or not.

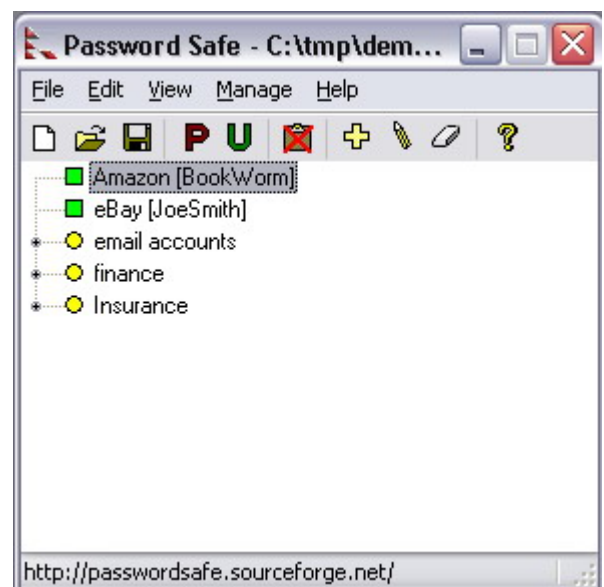


Figure A

## Determine baseline characteristics

In the past, when I've called my mentor with a problem I couldn't solve, his first words would always be, "What's changed?" After a few times, what he was trying to teach me finally sank in and I started paying attention to [baseline characteristics](#). Baselineing has two purposes:

- To understand what it means to be operating normally
- To simplify finding what's not operating normally

I may be stating the obvious with regards to baselining, but defining it may help everyone realize how big a role it plays in the next three topics.

## 4: Examine security logs

Good administrators know about baselining and try to review system logs on a daily basis. Since this article deals with security breaches, I'd like to place special emphasis on security logs, as they're the first line of defense.

For example, when reviewing a Windows server security log, the administrator comes across multiple 529 events (Logon Failure - Unknown user name or bad password). That should immediately raise an alert, with the administrator trying to determine whether a valid user has forgotten a password or an attacker is attempting to gain access.

Windows security logs are cryptic, to say the least, so having some kind of reference guide is beneficial. That's where Randy Franklin Smith helps out; he has a [Web page](#) that defines most every Windows security log event. Randy also has a free [reference chart](#) that can be invaluable in explaining security log events.

## 5: Do regular network scans

Comparing regular network scans to an operational baseline inventory is invaluable. It allows the administrator to know at a glance if and when any rogue equipment has been installed on the network.

One method of scanning the network is to use the built-in Microsoft command [net view](#). Another option, and the one I prefer, is to use freeware programs like [NetView](#). They're typically in a GUI format and tend to be more informative.

## 6: Monitor outbound network traffic

Malware is becoming sophisticated enough to avoid detection. One method of exposing it is monitoring outbound network traffic. Suspicions should be raised when the number of outbound connections or the amount of traffic deviates from normal baseline operation. To tell the truth, it may be the only indication that sensitive information is being stolen or that an email engine is actively spamming.

Most firewall applications can monitor outbound traffic. Advanced firewalls can even create scheduled reports similar to the one in **Figure B**.

## 7: Patch and update regularly

Keeping operating system and application software up to date is the best way to foil breach attempts originating from outside the network's perimeter (Internet). It's that simple. If the operating system and applications aren't vulnerable, the exploit will not work.

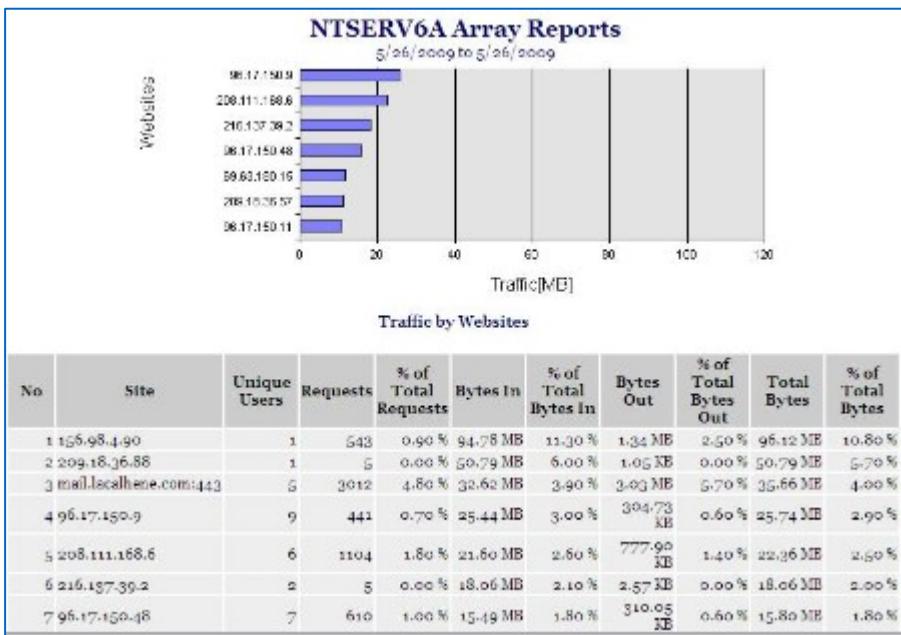


Figure B

*Title goes here*

Using a product like [Microsoft Baseline Security Analyzer](#) or one of the [products from Secunia](#) is the most effective way to ensure that computers under your care are indeed up to date and have all of the necessary patches.

## Now the hard topics

Up until now, each improvement was in the realm of the IT department. That's about to change, as the last three topics require input from other departments in the organization. It's going to be tough, but it's worth the effort.

### 8: Implement a security plan

No matter what size the organization, having a security plan in place is invaluable for the following reasons:

- Everyone is working off of the same playbook, which provides continuity.
- When the organization is in panic mode, the security plan will provide solid solutions developed at a time when everyone was less anxious.

Security plans should be individually sculpted to fit the needs of each organization. To get an idea of what's required, I've linked to two guides, a rather generic one by [Microsoft](#) and an all-encompassing guide by [NIST](#).

### 9: Raise user awareness about information security

Some of my clients are bullish on user training -- and others aren't. The difference is night and day, with the proof being evident in my billable hours. The Web is littered with [papers](#) that explain the benefits of user training, but they're typically geared toward increasing user efficiency in the work environment.

The user education I'm referring to is focused on creating well-informed users who can function on the Internet securely. Kathleen Coe of Symantec has written a paper titled [Employee Awareness - The Missing Link](#), which does a good job of explaining what's required to set up a computer security training program.

### 10: Get upper management to buy in

I saved the hardest for last. Getting upper management buy-in for security policies and for purchasing the required technology is typically a tough sell. Another problem is when people in upper management give the go-ahead to implement security practices but feel the rules don't apply to them.

One thing I've found that usually changes upper management's position is to perform a security breach personally (get permission) or have a TPV do a security audit. It's been my experience that the results are a real wake-up call for everyone involved.

## Final thoughts

Completely eliminating security breaches may indeed be an impossible task. But I get concerned when that conclusion drives the attitude of "Why even try, then?" The 10 methods above are simple to implement and will go a long way toward making it more difficult for a security breach to occur.

## Additional resources

- TechRepublic's [Downloads RSS Feed](#) **XML**
- Sign up for the [Downloads at TechRepublic](#) newsletter
- Sign up for our [IT Leadership Newsletter](#)
- Check out all of TechRepublic's [free newsletters](#)
- [10+ answers to your questions about IPv6](#)
- [10 Faces of Computer Malware](#)
- [10 answers to your questions about botnets](#)

## Version history

**Version:** 1.0

**Published:** June 3, 2009

## Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Content Team