

Strategies for Supporting Advancement and Development

Thoughts *for* Advancement

Democracy and Responsibility

The Lives of Technical Staff and Security.



www.SupportingAdvancement.com
services@supportingadvancement.com

© SupportingAdvancement.com. All rights reserved.
Permission to use this information granted, provided that the SupportingAdvancement.com copyright notice and permission appears in all copies and use of information is for informational and non-commercial or personal use only and that no modification of the information is made.

Democracy and Responsibility

What's On!



Democracy and Responsibility 3
Security Considerations for Desktops 3
Lives of Programmers, Analysts and other Technical Specialists..... 4
 Server Backups..... 4
 Server Logs..... 4
 Staff Roles and Responsibilities 5
Our Stock in Trade - Working with our Data..... 5
 Data Update Statements, DDL, and Other Destructive Statements..... 5
The Headlines..... 6





Democracy and Responsibility

Democracy and Responsibility

Change management is all about politics.
Politics are all about visibility.
Visibility can be good or bad.

Recent changes in our technical environment and the way technical staff work continue to necessitate the need for radical improvements in the way we manage our data and keep it secure.

To get to where we are, where we have much greater control over our databases, has been a political and an organizational struggle.

In the past, most systems were maintained centrally but many of us are now running departmental systems, our own custom software, custom vendor software all in a complex environment using web enabled tools and technologies that were never really designed for security in the first place.

It used to be so simple. You put a terminal on someone's desk and there was only one choice. We now face many more challenges and the future continues to crash in upon us.

And we can't just blame the vendors. No software is perfect. We need to shoulder most of the responsibility for protecting our data.

Other changes in technology such as increases in hard drive space have greatly facilitated our ability to download and work with large amounts data. It's not uncommon to download the whole donor file and work with it locally.

So also hath the enemy observed all of this.

There have been a number of very public breaches of systems recently in higher education and as such, our industry will now become a much larger, broader and more visible target. We will not be spared the ravages of theft and criminal intent.

Security Considerations for Desktops

At least once a week, you need to run all of the following programs (or equivalents):

- Spybot search and destroy.
- Ad-aware.
- Norton anti virus alternative threats.
- Windows beta ad-aware and spyware software.

There are so many spyware and ad programs, that no single piece of software can scan, discover and eliminate all of the threats. You need to run them all.

Do not visit Internet sites with "questionable" purposes not related to work, turn off all music streaming and any other software that opens and exposes your workstation.



Democracy and Responsibility

Windows Security and Automatic Updates

- Automatic updates should be enabled.
- Once a week, go to the Microsoft site and check for updates, both for the operating system and for Office since automatic updates do not always work flawlessly.
- Check regularly for other updates on database, reporting, analysis software and any other tools you're using on your desktop.
- Subscribe to Microsoft's and other security bulletins for all software you use and pay close attention and make sure you implement recommendations.
- Firewalls should always be turned on.
- Passwords should be a password phrase with numbers, characters, spaces, etc. i.e. P@ss W0rD (Don't actually use this.)

All other standard security procedures should be in place such as turning off services you don't need, etc.

The baseline security analyzer from Microsoft can help you review and correct any vulnerabilities in the Windows operating system and is a free download. Make sure you're on update lists for all the software you use on your desktop. Other vendors are a much smaller target than Microsoft, but may also have enemies.

"The good of the many outweighs the needs of the few." Vulcan Philosophy

Desktops that are compromised because of lack of basic security procedures and repeated failures of staff to adhere to them should be converted to a managed system and locked down.

Many hundreds of additional pages could easily be written on security server, security audits, policies and procedures, changing job descriptions and a myriad of other security topics.

Lives of Programmers, Analysts and other Technical Specialists

Routine is good.

Routine hardens the infrastructure.

Good habits are hard to develop, but once developed they are hard to break.

Server Backups

Server backups are the most important first activity of the day. Nothing else in your daily routine needs to take place until you've verified that backups have run correctly. If they haven't, you need to work until any problem is resolved, and then re-run the backups so they are current.

The importance of this can be emphasized if you ask any user in the office to tell you exactly what they've done in the last two hours. Unless they've been out for lunch, they won't be able to tell you exactly what they did, what data they modified, etc.

Server Logs

The next most important task is to review the server logs and resolve any questionable items.



Democracy and Responsibility

Staff Roles and Responsibilities

Responsibilities need to be clear, and whenever someone with primary responsibility for a server is out of the office, they will need to ensure they have staff trained and available to review the daily backups and the logs, and resolve any errors or questionable items.

Our Stock in Trade - Working with our Data

No data that has any identifying characteristics such as a social security or social insurance number, name, email address or similar information that could expose donor or prospect information should be stored on a local hard drive.

Any data worked with on the local drive should be worked with in a local copy of the database software (secured with a password), as opposed to spreadsheets or other desktop tools with weak security.

Final exports of data with any identifying characteristics sent via email or other medium to users should be sent in a password protected format. The receiver of the data should be required to phone to get the password to open it. The passwords (pass phrases) should be strong.

All data with any identifying characteristics should be stored, manipulated and worked with on the server since it is much more secure than workstations.

Data Update Statements, DDL, and Other Destructive Statements

It's unfortunately just as easy to destroy data as it is to lose it to a thief. According to an FBI study, approximately 80% or higher of all security problems are caused by internal staff, whether through mistakes, willful negligence or malfeasance.

Whenever you need to do an update statement, drop a table, delete or insert data or any similar function with a live table, always make a copy of the original table first. Ideally you should code this into these scripts so it happens automatically.

Give it a name such as `zzz_backup_entity_` and concatenate the time stamp.

It's easy to write a program, think you've covered all the bases and 4 hours later get a phone call from a user who just happened to look at data from 2 years back and realized that something was wrong. You will obviously lose some data, but with a backup you'll at least be able to restore it to a point.

Client server systems are also funny in that if you accidentally type in the wrong server name, you can do deeds like upgrade the production server with a new release without even realizing it until the phone starts ringing.

Always look before you leap, and make sure you understand how deep the water is before diving. If you're not careful, you can hit your head.



Democracy and Responsibility

The Headlines

Simple habits, routines, precautions and a philosophical outlook focusing on trying to make sure we're all following proper procedures 100% of the time will go a long ways to keep us out of the headlines.

We are in a situation where global information system terrorist activities are going to proliferate and escalate as more and more data systems with high value data are attacked. This is only a very short discussion of what is a very large, broad and complicated topic. We can't all become security experts, but just as we lock our doors at home, we need to be more conscious of actions that increase our vulnerability.

Stories on compromised systems are currently "top of the hour". As a hot press commodity, if your system is compromised, you can rest assured that the information will become public. In any case, at a minimum, you will need to inform the public which will be picked up on by the press anyway. It's a no win scenario.

Be wary, and be vigilant.
The battle is engaged.
If you haven't been attacked, you've had good luck.
Luck is spelled work.