The Security Virtues

1. Daily Consideration
2. Community Effort
3. Higher Focus
4. Education

More on the Four Virtues

Daily Consideration: security MUST be a daily consideration in every area.

Community Effort: security MUST be a community effort.

Higher Focus: security practices MUST maintain a generalized, higher focus.

Education: security practices MUST include some measure of training for everyone.

Virtue 1: Daily Consideration

Security must be practiced on a daily basis if it is to be effective.

Adopting a **reactive philosophy to security** is never a good idea and often leads to problems.

Daily consideration often results in the adoption of a **proactive security posture**.

Security issues can then be dealt with *automatically* and with *minimal effort*.

The Seven Steps of Doom

Organizations that fail to follow the virtue of Daily Consideration are often attacked. An identifiable pattern emerges:

1. Do something without thinking about security.
2. Get attacked.
3. Realize that step 1 introduced a flaw that resulted in step 2.
4. Secure the organization against the attack from step 2.
5. Wait (go off and work on something ``more important'').
6. Get attacked again.
7. Discover that another new attack was introduced by step 1.

The Three Steps to Success

Step 1: Think about security.

Step 2: Do something (while still thinking about security).

Step 3: Continue to think about security.

Simply ask yourself: *Will what I'm about to do have security implications?*

Considering Security in Everything

The most devastating security vulnerabilities are the ones that have no obvious relationship to security at all.

Until they happen, that is.

The Virtue of Daily Consideration needs to be drummed into our minds and the minds of those around us.

Practicing Daily Consideration

1: Make security a continual thought.

2: Encourage others to be continually mindful of security.

3: Formally include security considerations in all new projects.

4: Formally include security considerations in all new implementations and purchases.

Virtue 2: Community Effort

There are two communities:

1. The **inner community**: us, our end-users, executives and public.
2. The **outer community**: the IT world outside our inner community boundary.

Both communities need to participate in ensuring the security of our organization.

More on Inner Community

Never rely solely on the *security professional*.

Also, don't believe that security can be accomplished by working independently from those ``*troublesome end-users*''.

Think of end-users as **security gate-keepers**.

It is important to *integrate the end-users into the local security practices*.

More on Outer Community

Keep yourself safe so that others will be safe from you.

Through the process of being conscious and aware of the security around us, we are much better equipped to handle the security issues within the local environment.

Don't adopt a *not invented here* attitude.

Practicing Community Effort

1: Keep informed, and stay up-to-date.

2: Inform others, and report all incidents.

3: Keep your systems patched and up-to-date.

4: Inform end-users of their responsibilities.

5: Make group-based decisions about your organization's IT security policy.

Case Study: 1999 Meltdown

- In 1999, *Yahoo*, *CNN* and *eBay* (and others) fell foul to an attack, resulting in their web-sites being shut down.
- This was a *Distributed Denial of Service Attack (DDoS)*, which are about as bad as Internet attacks get.
- **How can we protect ourselves if the ``big guys'' can't?**
- It wasn't the ``big guys'' fault they were attacked. A large number of poorly defended servers throughout the Internet were compromised, then used to launch a co-ordinated and joint attack against specific targets ... it is all but impossible to secure against a DDoS.
- If those other organizations had practiced the **Virtue of Community Effort**, the attack would not have happened.

Virtue 3: Higher Focus

Too many organizations concentrate on specific details of security exploits/attacks.

In the world of IT security, there are thousands of vulnerabilities exploitable by tens of thousands of attacks with virtually millions of possible permutations.

Do not lose sight of the bigger picture. Think at a Higher Level about Security.

More on Higher Focus

By keeping an eye on the bigger picture, the details of security are easier to deal with.

Do not allow *exceptions* to established security policies (unless cleared by a **formal change management process**).

Getting bogged down in the details makes us more vulnerable to attack, not less so.

Practicing Higher Focus

1: Learn and share the concepts behind the virtues and rules of security (we will study these soon).

2: Think in terms of the bigger picture.

3: Follow the practice of higher security (more on this later). Learn to pro-actively deal with security.

4: Follow the practice of the written policy (more on this later, too). Use the policy to help make difficult decisions, as well as resolve arguments over details.

Virtue 4: Education

Security is not (nor should be) a lonely task performed by a single individual.

It is a daily effort, a community effort, and it must be considered in *everything*.

It follows that *everyone* needs to be involved.

So, everyone needs to be **educated regarding security**.

Think About It!

The security of your organisation is in the hands of your end-users.

Without secuity training, end-users are a ***huge security risk*** and IT Security is very hard to achieve.

Take the time to train IT staff members, managers, executives and end-users on good security **practice** and **awareness**.

The Great Psychological Obstacle

Do not let a ``them and us'' relationship develop between IT and its end-users. Work hard to build good two-way relationships with your end-users.

Take the time to teach end-users a little-bit-at-a-time.

Do not allow end-users to view security policies as restrictions on what they do.

An untrained, uninformed and uncoorperative end-user is often more deadly than a highly-skilled outside attacker.

Practicing Education, 1 of 2

1: Develop and encourage good software installation practices.

2: Develop and encourage good awareness practices.

3: Develop and encourage good web-browsing practices.

4: Develop and encourage good confidentiality practices.

Practicing Education, 2 of 2

5: Continually present security concepts to employees.

6: Provide in-house education for all staff.

7: Provide regular security reminders: be brief.

8: Learn from the mistakes of others: be creative.

9: Enforce the organisations IT security policy without making end-users feel like criminals.

Summary

- The Four Virtues of Security are:
  - Daily Consideration
  - Community Effort
  - Higher Focus
  - Education
- By keeping the virtues in mind, you can vastly simplify the process of securing your organization. The cost of security lessens, too.