Building Your Government Security Culture

COL Curtis A. Carver Jr.
Associate Dean, Information and Educational Technology

Quotes from Educause last week

New technology is like a new puppy. It is lovely until you buy it.

Toilets will go paperless before the federal government does.

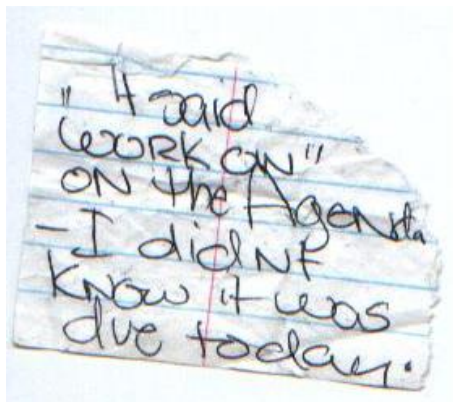
Every-time I think I have met the perfect idiot, God creates a better one. Geeky variant: Worms live on ignorance.

Culture eats strategy every day of the week.

Leadership reshapes culture every month of the year.

What to Take from this Presentation

- What is organizational culture?
- Why should I build a security culture?
- How do I build an organizational security culture?
- What did West Point do to shape organizational culture?



What is Organizational Culture?

Organizational culture is the personality of the organization.

Culture is comprised of the assumptions, values, norms, and tangible signs (artifacts) of organizational members and their behaviors.

"How do things get done around here?"

http://managementhelp.org/org_thry/culture/culture.htm

Types of Organizational Cultures

- **Academy Culture**: Employees are highly skilled and tend to stay in the organization, while working their way up the ranks. The organization provides a stable environment in which employees can development and exercise their skills. Examples are universities, hospitals, large corporations, etc.

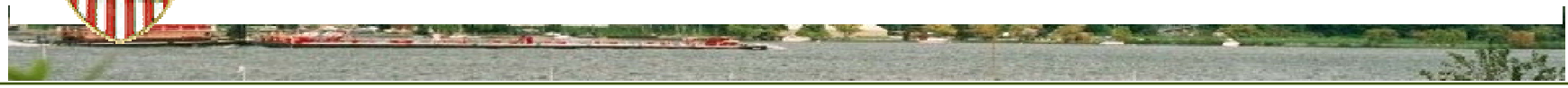
- **Baseball Team Culture**: Employees are "free agents" who have highly prized skills. They are in high demand and can rather easily get jobs elsewhere. This type of culture exists in fast-paced, high-risk organizations, such as investment banking, advertising, etc.

- **Club Culture**: The most important requirement for employees in this culture is to fit into the group. Usually employees start at the bottom and stay with the organization. The organization promotes from within and highly values seniority. Examples are the military, some law firms, etc.

- **Fortress Culture**: Employees don't know if they'll be laid off or not. These organizations often undergo massive reorganization. There are many opportunities for those with timely, specialized skills. Examples are savings and loans, large car companies, etc.

http://managementhelp.org/org_thry/culture/culture.htm

Types of Organizational Cultures



- **The Tough-Guy Macho Culture**. Feedback is quick and the rewards are high. This often applies to fast moving financial activities such as brokerage, but could also apply to policemen or women, or athletes competing in team sports. This can be a very stressful culture in which to operate.

- **The Work Hard/Play Hard Culture** is characterized by few risks being taken, all with rapid feedback. This is typical in large organizations, which strive for high quality customer service. It is often characterized by team meetings, jargon and buzzwords.

- **The Bet your Company Culture**, where big stakes decisions are taken, but it may be years before the results are known. Typically, these might involve development or exploration projects, which take years to come to fruition, such as oil prospecting or military aviation.

- **The Process Culture** occurs in organizations where there is little or no feedback. People become bogged down with how things are done not with what is to be achieved. This is often associated with bureaucracies. Whilst it is easy to criticize these cultures for being over cautious or bogged down in red tape, they do produce consistent results, which is ideal in, for example, public services.

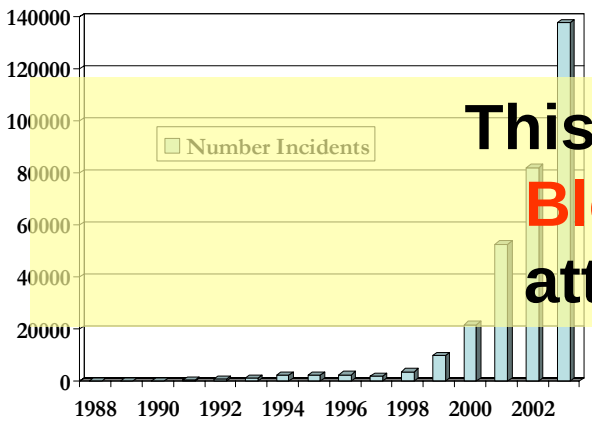
Why Should I Build a Security Culture?

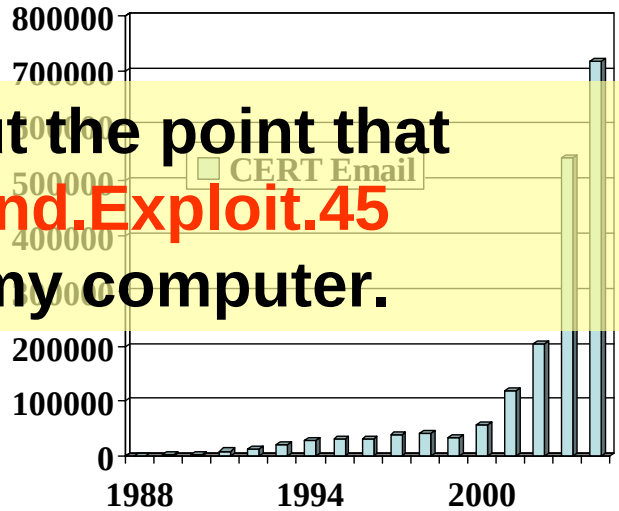
- The situation is getting worst.
- Perimeter defenses and centralized management are not working.
- Passive approaches to awareness and training are not working.

The Situation is Getting Worst

- Increasing number of attacks
- Increasing complexity of attacks
- Decreasing interval between patch release and attack exploitation

Increasing Attacks





This is about the point that
Bloodhound.Exploit.45
attacked my computer.

Date	Filename	Threat	Original Location	Status
10/11/2005 8:37:15 PM	3B67DD5E.emf	Bloodhound.Exploit.45	C:\Documents and Setti...	Infected
10/11/2005 8:37:15 PM	62655091.emf	Bloodhound.Exploit.45	C:\Documents and Setti...	Infected
10/11/2005 8:37:10 PM	366DCE75.emf	Bloodhound.Exploit.45	C:\Documents and Setti...	Infected
10/11/2005 8:37:04 PM	1305368F.emf	Bloodhound.Exploit.45	C:\Documents and Setti...	Infected
10/11/2005 8:37:04 PM	E03CB46.emf	Bloodhound.Exploit.45	C:\Documents and Setti...	Infected

How could I be Attacked!

- Antivirus on perimeter.
- Antivirus updates 14 times a day.
- Anti-spam updated automatically.
- Windows patches update automatically.
- Firewalls on computer and on perimeter.
- Was working over an encrypted VPN channel.

Attacked occurred at 8:37PM.
Patches released 6:00 PM.

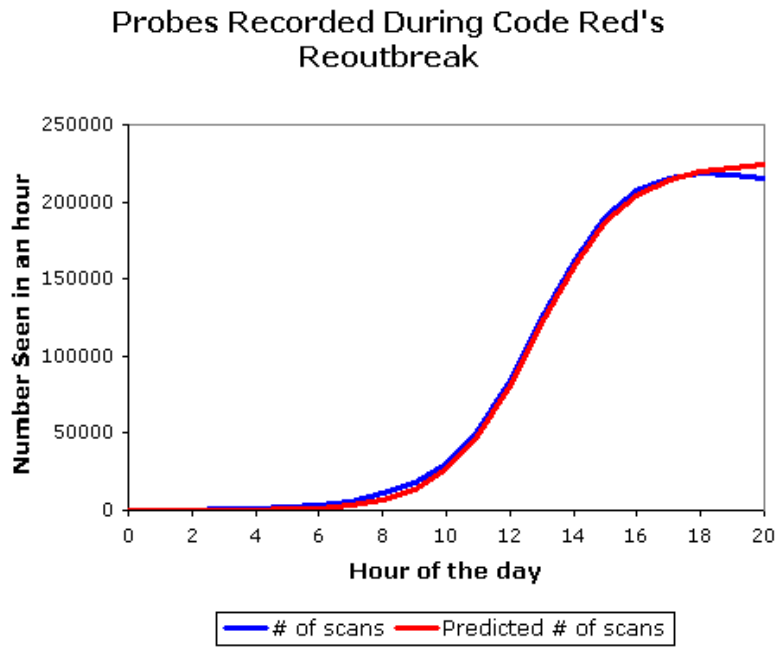
Remedial Action

- Check for updates to anti-virus and anti-spam (didn't work).
- Ran anti-virus (didn't work), ran anti-spam (didn't work), ran windows update (worked!)
- Set anti-virus to run at reboot. Reboot (worked!).

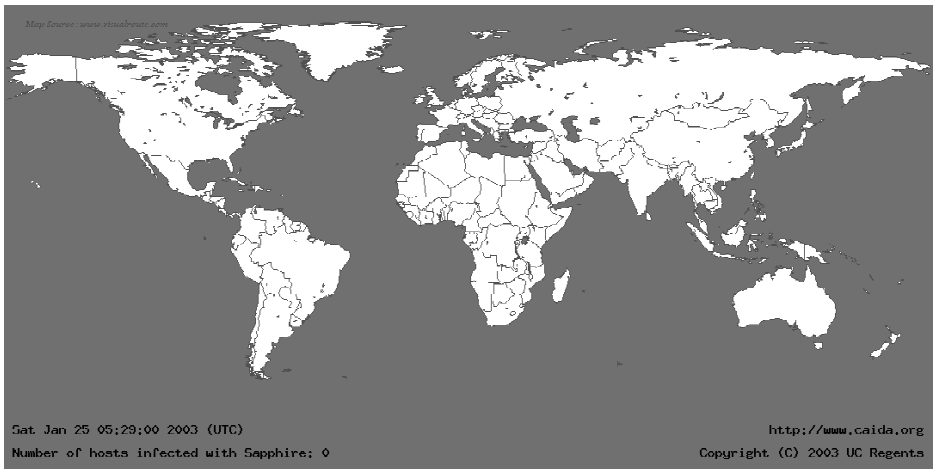
Changing Environment

(Speed of Attack)

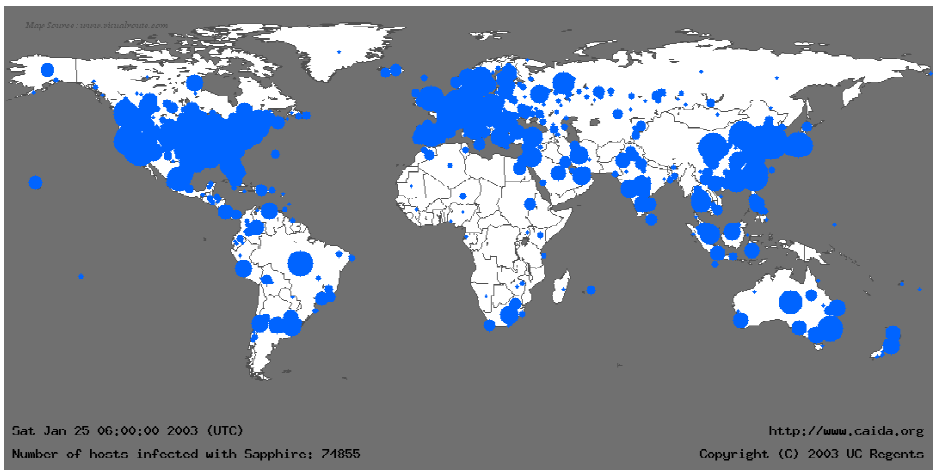
- **Morris Internet Worm** (1988 - Over 72 hours affected 6,000 computers taking 90 minutes to bring a system down).
- **Melissa Virus** (May 1999 – Over 72 hours affected 100,000 computers. One site received 32,000 Melissa email messages in 45 minutes.)
- **Code Red** (July 2001 approx. 250,000 computers in 20 hours)



Slammer



The World
January 25, 2003



Slammer penetration 30 minutes after release.

http://www.cs.berkeley.edu/~nweaver/sapphire/

Increasing Complexity

Slammer

- Sapphire contains a simple, fast scanner in a small worm with a total size of only 376 bytes.
- In the first minute, the infected population doubled every 8.5 seconds.
- Achieved full scanning rate in less than 3 minutes. Full scanning rate was 55 million scans per second.
- The scanning rate was limited because significant portions of the internet ran out of bandwidth.
- Sapphire spread nearly two orders of magnitude faster than Code Red.

http://www.cs.berkeley.edu/~nweaver/sapphire/

Perimeter Defenses are not Working

(Necessary but not Sufficient)

- Anti-virus, anti-spam, firewall, intrusion detection, and intrusion prevention systems are all necessary but not sufficient.
- Why?
  - Mobile worker population is out there working hard to pick up new and exotic attacks.
  - Insider threat much greater than outside threat.
  - New computing devices are coming in all shapes and sizes.

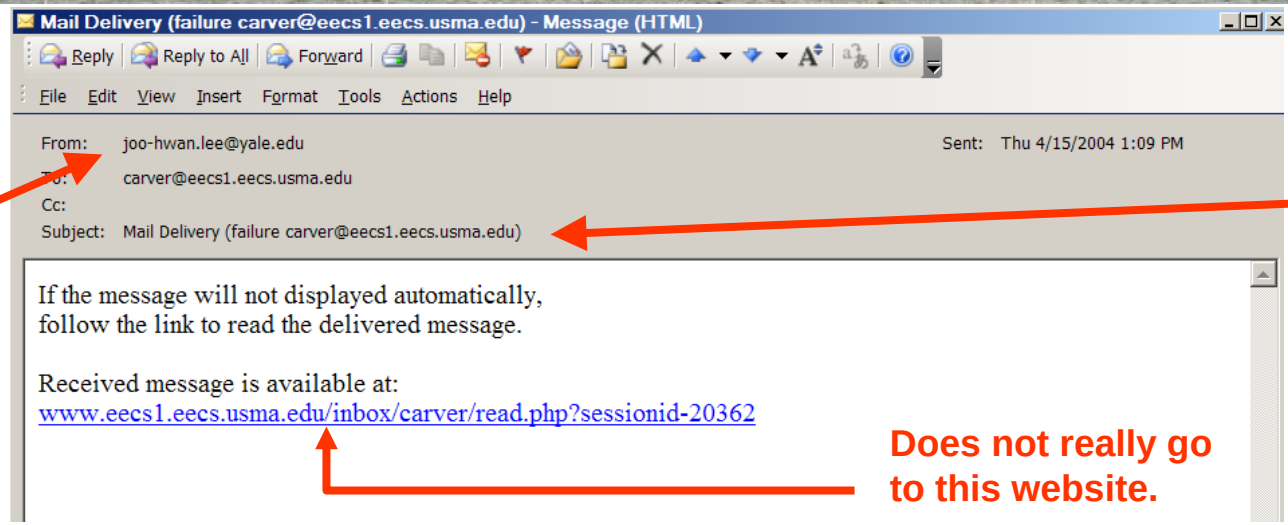
My Projector is attacking my network!

Centralized Management is not Working
(Necessary but not Sufficient)

- Anti-virus and software update servers are necessary but not sufficient. Active directory helps with authentication and authorization but is not enough.
- Why?
  - Mobile work force
  - Time between release of patch and release of an attack tool, “flash to bang”, is rapidly shrinking.
  - As you hardened the perimeter and central management, attackers attempt to bypass these defenses through social engineering attacks.

Social Engineering

(Hidden Attack)



Who is Joo-hwan Lee is and why is he sending you email?

How can someone at Yale post email messages in EECS and you cannot?

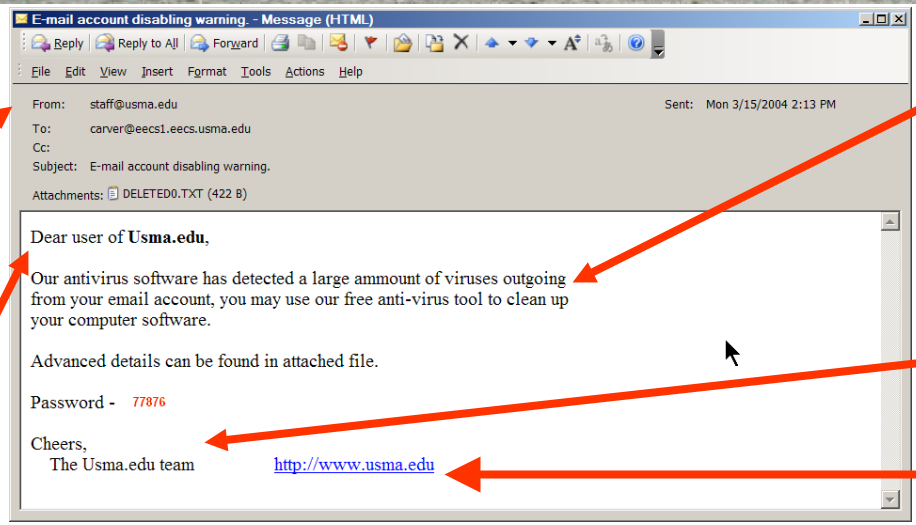
Does not really go to this website.

In this case, the attacker is trying to trick you into clicking on the embedded link. The link does not go to an webserver in the Electrical Engineering and Computer Science (EECS) department but instead opens an invisible frame and launches a program embedded in another part of the email message.

Social Engineering (Hidden Encrypted Attack)

The Military Academy does not use non-personal accounts such as staff@usma.edu to send security announcements.

The Military Academy will not refer to you as "Dear member of usma.edu" – it will refer to you by name.



Military Academy can automatically update software – no need to ask permission.

An email from the "usma.edu team" sounds suspicious

Does not really go there.

As you might imagine, the virus creators were not thrilled about their viruses being deleted by the corporate virus checkers so they tried another approach. They encrypted the virus to disguise it, gave the user the password to decrypt it and install it, and hide it behind a familiar looking web address that did not go to the website but launched the virus.

Social Engineering
(Hidden Zipped File)

From: Gaskins, F. MS DOIM
Sent: Wednesday, September 07, 2005 09:36 AM
To: allusers
Subject: Required Password Change

In order for West Point \ USMA to comply with DA policies in regards to computer passwords, **ALL** users of the West Point \ USMA network will be required to change their domain password. Passwords must be changed no later than 1700 19 Sep 2005 in order to comply with the new password guidelines.

When choosing your new password please keep the following in mind:

- Password must contain no less than **10** characters.
- Password must contain **2 characters of each of the 4 types of characters listed**: uppercase letters, lower case letters, numeric characters (0 – 9), Nonalphanumeric characters, (!, @, #, $, etc.).
- Password can **NOT** contain three or more characters from the user's account name, social security numbers, birthdays, names, and dictionary words.
- The password can **NOT** be the same as any of your previous **10** passwords.

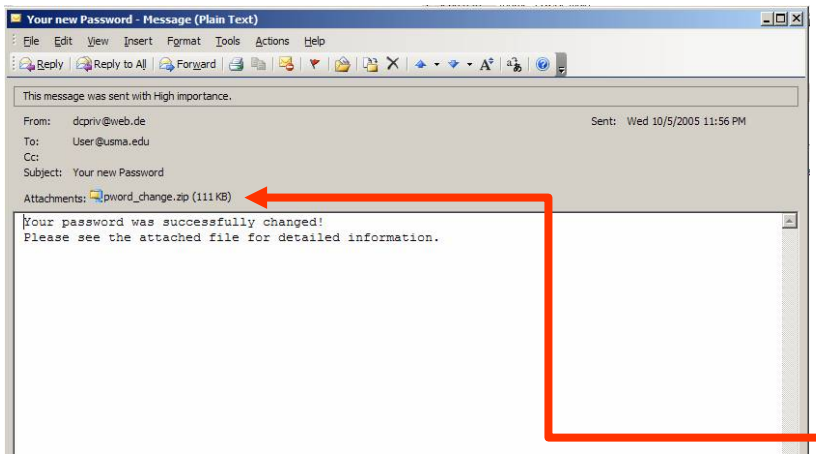
Please be sure to pass this note along to any personnel who may be currently located outside of West Point \ USMA (i.e. TDY, leave, sabbatical) and using resources remotely (i.e. Webmail, VPN).

Users inside USMA can press CTRL+ALT+DEL while logged onto their machines and choose the "Change Password" option.

From outside USMA passwords can be changed by logging on to Webmail and choosing "options" in the lower left hand corner, scroll down the options page and click the "Change Password" button.

For additional information please contact your Department Computer Officer, Information Management Officer or Information Assurance Manager.

Legitimate email to all users.



Illegitimate email to all users 28 days later.

The attack contained in the zipped file is new and host anti-virus software cannot protect the computer. The computer must be reimaged.

Passive Approaches to Awareness and Training are not working

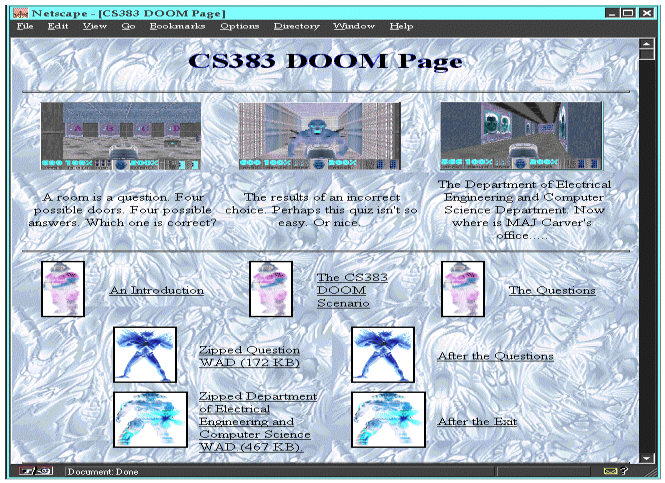
- Attacks are bypassing perimeter defenses.
- Sophistication of attacks is increasing.
- Every user is an attack point.
- Every user is a vulnerability.
- Even one user fails, insider attack occurs and it will spread very rapidly.

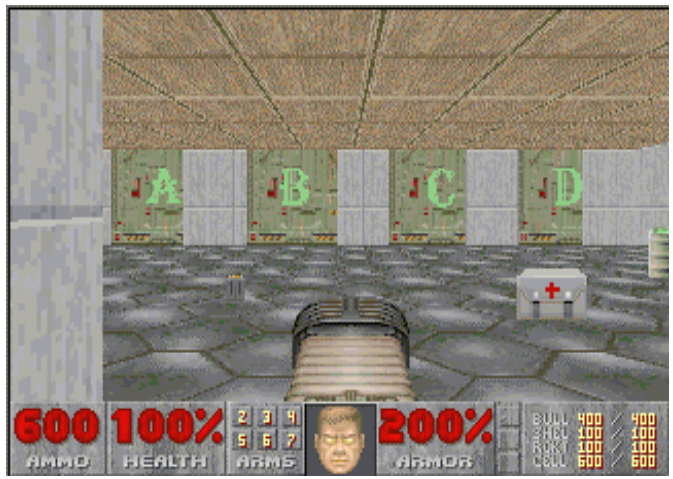
Passive to Active

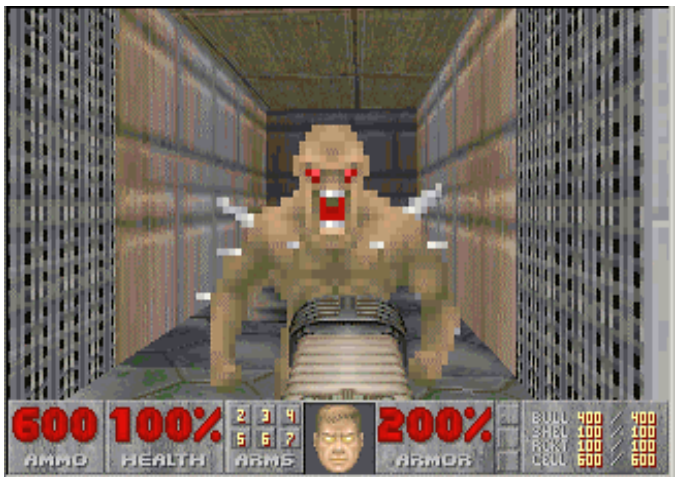
- Users remember:
  - 30% of what they hear
  - 40% of what they see and hear
  - 70% of what they do.

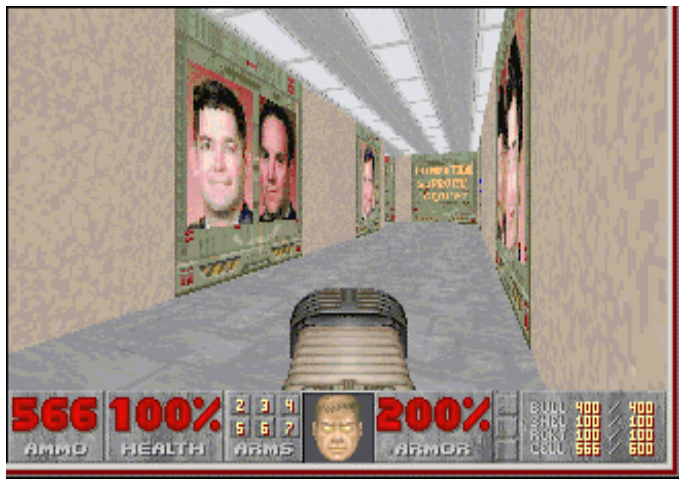
- We have to get the users actively involved in learning. We have to change culture.

The New Face of Assessment









3 Waves of Information Security

- Technical Wave
  - Authentication and access control
- Management Wave
  - Policies, procedures
  - CISO and separate security staff
- Institutionalization Wave
  - Information Security Awareness
  - Information Security Culture
    - Norms
    - Community
    - Leadership

Von Solms (2000)