“The Human Firewall”
Creating a security aware workforce

Is your data protected by Human firewall?

Stephen Ndonga Kariuki  CISM,CISA,CGEIT, PMP
Principal Consultant

Harmony Solutions Ltd
info@harmony.co.ke
Cell: (0726)609145
Office: (020 )2473145/6
Is your data protected by Human firewall

1. What is the current security scenario
2. Why a human firewall?
3. What is a Human firewall?
4. How to implement a human firewall
5. Benefits of effective Human firewall
Data Vs Information

1. Information is often defined as data with context.
2. Observations and recordings are done to obtain data, while analysis is done to obtain information.
3. Data is the lowest level of knowledge and information is the second level.
4. Data by itself alone is not significant. Information is significant by itself.

’Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected’

ISO 27002:2005
ISO 27002:2005 defines Information Security as the preservation of:

- **Confidentiality**
  - Ensuring that information is accessible only to those authorized to have access

- **Integrity**
  - Safeguarding the accuracy and completeness of information and processing methods

- **Availability**
  - Ensuring that authorized users have access to information and associated assets when required
1.3 What is the current security scenario

INFORMATION SECURITY

1. Protects information from a range of threats
2. Ensures business continuity
3. Minimizes financial loss
4. Optimizes return on investments
5. Increases business opportunities

Business survival depends on information security.
Protection of information and information systems to meet business and legal requirements by

- Provision and demonstration of secure environment to clients
- Preventing loss of product knowledge to external
- Preventing leak of confidential information
- Ease of access to large mobile work force
- Introduction of new technologies and tools
- Disaster recovery & Business continuity
- Managing legal compliance
- Managing costs v/s risk
Common Myths About Information Security

- **Myth 1:** Information Security is the concern and responsibility of the MIS/IT manager
- **Myth 2:** Security Threats from outsiders are the greatest source of risks
- **Myth 3:** Information Security is assured by safeguarding networks and the IT infrastructure
- **Myth 4:** Managing People issues is not as important
- **Myth 5:** Adopting latest technological solutions will increase security
• 2011 Set to Be Worst Year Ever for Security Breaches

• Sony, the data-security firm RSA, Lockheed Martin, the email wholesaler Epsilon, the Fox broadcast network, NASA, PBS, the European Space Agency, the FBI, the British and French treasuries — and, just this morning, the banking and insurance giant Citigroup.

• What do all these organizations have in common?
The Human Element of Information Security

Information Flow Is The Lifeblood Of Your Business.

Information is arguably your most important asset

- Confidentiality requirements
- Protection of Brand and reputation
- Financial Costs of dealing with the aftermath of a breach
- Loss of productivity

“Most security breaches occur at ground floor level, through employees making errors or inadvertently revealing information.

The Human Element of Information Security
Agenda

Is your data protected by Human firewall

1. What is the current security scenario

2. Why a human firewall?

3. What is a Human firewall?

4. How to implement a human firewall

5. Benefits of effective Human firewall
2. Why a human firewall?

90/10 Rule

90\% 

People

Process

Technology

10\%
2.1 Why a human firewall?

– Employees are responsible for most security breaches – up to 80%

– Kevin Mitnick in The Art of Deception: “The employees are the target!”
2.2 Why a human firewall

Achieving Information Security

**FIGURE 6-16** Spheres of Security
2.3 Why a human firewall?

Sphere of Protection overlays each of the levels of the “sphere of use” with a layer of security.

protecting that layer from direct or indirect use through the next layer

The people must become a layer of security :-) a human firewall that protects the information from unauthorized access and use
Agenda

Is your data protected by Human firewall

1. What is the current security scenario

2. Why a human firewall?

3. **What is a Human firewall?**

4. How to implement a human firewall

5. Benefits of effective Human firewall
3. What is human firewall?

- What is Firewall?
- **firewall** as a system designed to prevent unauthorized access to or from a private network/systems. [Webopedia.com](http://www.webopedia.com)

Human Firewall

- An individual who is employed with the task of defending against human based attacks which targets employees within the organization, using variety of methods.
3. 1 What is human firewall?

Direct Internet connection: modem, DSL or cable modem

Install firewall on this computer
3.2 What is human firewall?

1. Proper policies, procedures, rules, regulations (a framework of acceptable behavior) +

2. Awareness of above by employees (knowledge of acceptable behavior) +

3. Total commitment of ALL employees to above (desire towards acceptable behavior) =

Desired Employee Behavior / Human Firewall
3.3 What is human firewall?
3.4 What is human firewall?

What is Security Awareness?

**Security awareness** is the knowledge, skill and attitude an individual possesses regarding the protection of information assets.

Being Security Aware means you understand that there is the potential for some people to deliberately or accidentally steal, damage, or misuse your account, computer or the data stored on your computer.

Awareness of the risks and available safeguards is the first line of defense for the security of information, systems and networks.
Security Awareness

Includes:

• Information about how to
  ✓ Protect
  ✓ Detect
  ✓ React

• Knowledge, Skill and Attitude
  ✓ The What
  ✓ The How
  ✓ The Why

What’s in it for me?
The change management approach is based on understanding the various phases in the commitment curve and the related activities during the course of the change lifecycle.

**Awareness**
- Stakeholders know that change is imminent. They do not know yet what will be the benefits coming from the change.

**Understanding**
- Stakeholders can explain the impact of the change on them and on their organization.

**Acceptance**
- Stakeholders have a positive attitude toward the change and what will personally affect them. They are prepared and willing “to give it a try.”

**Commitment**
- Stakeholders will champion the changes associated with the change to their peers and will do everything in their power to make it work and deliver the expected benefits in their organization.

3.6 What is human firewall?
Is your data protected by Human firewall

1. What is the current security scenario

2. Why a human firewall?

3. What is a Human firewall?

4. How to implement a human firewall

5. Benefits of effective Human firewall

©2011 Harmony Solutions Ltd
info@harmony.co.ke
4 How to Implement a human firewall?

- Design Awareness and Training Program
  - Conduct Needs Assessment
  - Develop Strategy
  - Develop Awareness and Training Program Plan

- Implement Program
- Develop Awareness and Training Material
- Post-Implementation
Agenda

Is your data protected by Human firewall

1. What is the current security scenario

2. Why a human firewall?

3. What is a Human firewall?

4. How to implement a human firewall

5. Benefits of effective Human firewall
5. Benefits of an Effective Human firewall

1. Provide better protection for assets
2. Save money
3. Give your organization a competitive advantage, protect and enhance your organization's reputation and brand
4. Improve morale
5. Protect customer information and corporate information
6. Reduce the potential for lawsuits against your organization
7. Reduce C-level executives' exposure to prosecution
8. Reduce the potential for fines and mandatory audits
9. Facilitate disciplinary or legal action against those who don't comply with information security rules
6. Summary

- Regardless of a company’s current resources and commitments, it should:
  - investigate the potential costs and potential benefits of a human Firewall initiative.
  - The value of information is too high and the resourcefulness of the information criminal too well-proven to ignore the issue entirely.
  - find a rational basis on which to proceed with the implementation of the best practices described.

- And the result of that implementation will be vastly improved security for its customers, its business partners and itself.
Human Wall Is Always Better Than A Firewall
Thank you!

Stephen N. Kariuki, CISM, CISA, CGEIT, PMP
Harmony Solutions Ltd

training@harmony.co.ke
Cell: (0726) 609145
Office: (020) 2473145/6