

# *“Counties and IT Security*

-----

## *Homeland and More“*



June 18, 2009

# Security is Everyone's Responsibility



There was a story about four people named Everybody, Somebody, Anybody and Nobody. There was an important job to be done and Everybody was sure Somebody would do it. Anybody could have done it, but Nobody did it. Somebody got angry because it was Everybody's job. Everybody thought Anybody could do it but Nobody realized that Everybody wouldn't do it. It ended up that Everybody blamed Somebody when Nobody did what Anybody could have done!



# Why Start With Security?



- Everybody's Responsibility
- Complex Challenge
  - ❖ Employ Best Practices
    - Firewall
    - Virus Protection
- I.T. Reliance - Everywhere
- Convergence
- Risk Assessment



# Risk Management Approach



Many organizations have approached security risk management by adopting the following:

Reactive approach

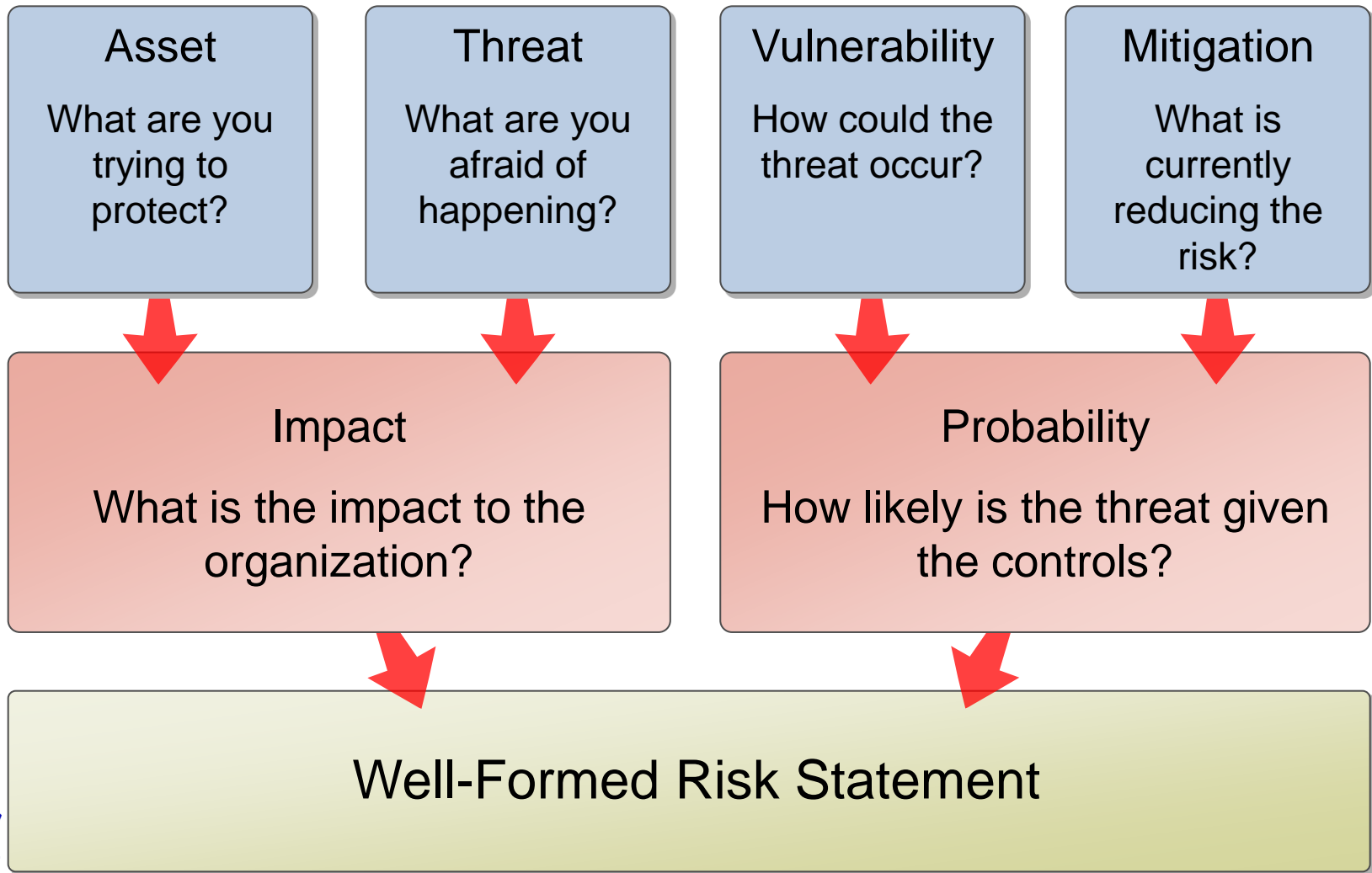
A process that responds to security events as they occur

Proactive approach

The adoption of a process that reduces the risk of new vulnerabilities in your organization



# Security Risk Assessment



# Positioning End User Security Awareness



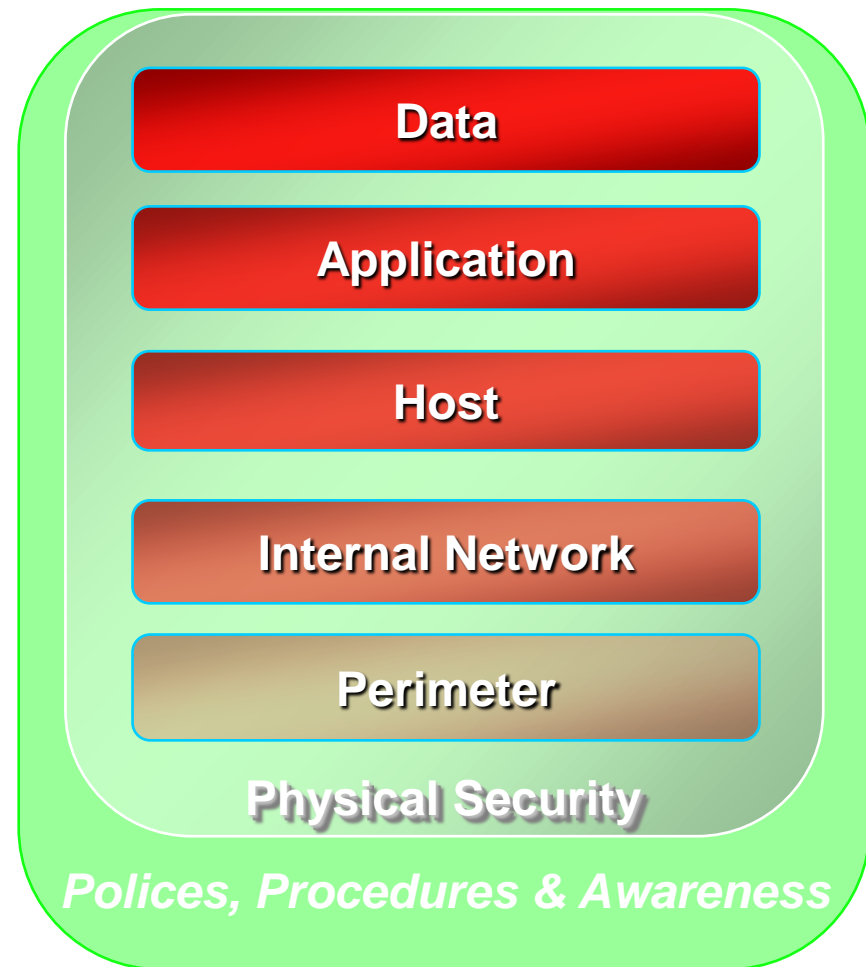
End User Security and Awareness programs reside in the Policies, Procedures, and Awareness layer of the Defense in Depth security model.

User security awareness can affect every aspect of an organization's security profile.

User awareness is a significant part of a comprehensive security profile because many attack types rely on human intervention to succeed.



## Defense In Depth



# Good News and Bad News



- You are doing a very good job at keeping the the networks save at the edge. Your I.T. Departments have done a great job under the hood with your firewall and virus detection systems.
- You have Hackers, Crackers and Attackers knocking at your network doors every day.

We have to get it right every time.

They only have to get it right once.



# What do we do?



# Types of Threats (Without Boundaries)



- Virus
- Worms
- Trojan
- Spyware
- Loggers
- Dialers
- Botnet
- Thumb Drives



# Social Engineering



**From:** security [mailto:service@bankofamerica.com]  
**Sent:** Monday, June 11, 2007 10:54 AM  
**Subject:** Bank Of America



## Your Bank Of America account is Blocked !

**Dear Bank of America customer,** we recently reviewed your account, and suspect that your Bank of America account may have been accessed by an unauthorized third party. Protecting the security of your account is our primary concern. Therefore, as a preventative measure, we have temporarily limited access to sensitive account features.

**Please login into your account to reset your passcode and resolve the problem .**

**Log in :** <https://www.bankofamerica.com>

Tank you for your patience as we work together to protect your account.

Sincerely,  
Bank of America Customer Service



Bank of America, N.A. Member FDIC.  
2007 Bank of America Corporation. All rights reserved.



# Why Do the Evil Doers Do This?



- Vendetta/Revenge
- Joke/Hoax/Prank
- The Hacker's Ethics - This is a collection of motives that make up the hacker character
- Terrorism
- Political and Military Espionage
- Hate (national origin, gender, and race)
- Fame/Fun/Notoriety
- Personal Gain



# Summary



**Deliver security information that users will view as being valuable to them personally and professionally**



**Communicate with users, let them know why policies exist and why they are enforced for everyone**



**Be mindful of security solutions that can impact usability and communicate the need to users whenever such solutions are implemented**



**Remember that security awareness isn't a one shot fix but a long term process designed to educate AND to change user behavior**



# Questions

