

# Delaware's Cyber Brief

Rick Schandall CISSP,MCSE, CEH,etc  
Corporate Training Group



# Security Basics

- **Trusting Input from Untrusted Sources**
  - Phishing, Buffer Overflow, SQL Injection
- **Confidentiality (Secrets)**
- **Integrity (Lies)**
- **Availability**
  
- **Most Communication is Unauthenticated**
  - Authenticate the User, not the Packets.
- **Internet was built for a Trusted Infrastructure**

# Why Do I...

- Why Do I have to change my Password and why does it have to be complex?

# Why ...

- Why Can't I be a local Administrator?

# Why Do I...

- Why Do I have to keep Updating Windows and all of these other applications?

# Why Does...

- Why does Vista & Windows 7 keep bugging me?

# Why can't I...

- Why can't I have VPN access?

# Why can't I...

- Why can't I share or write down my credentials?

# Why shouldn't I...

- Why shouldn't I open unknown attachments?

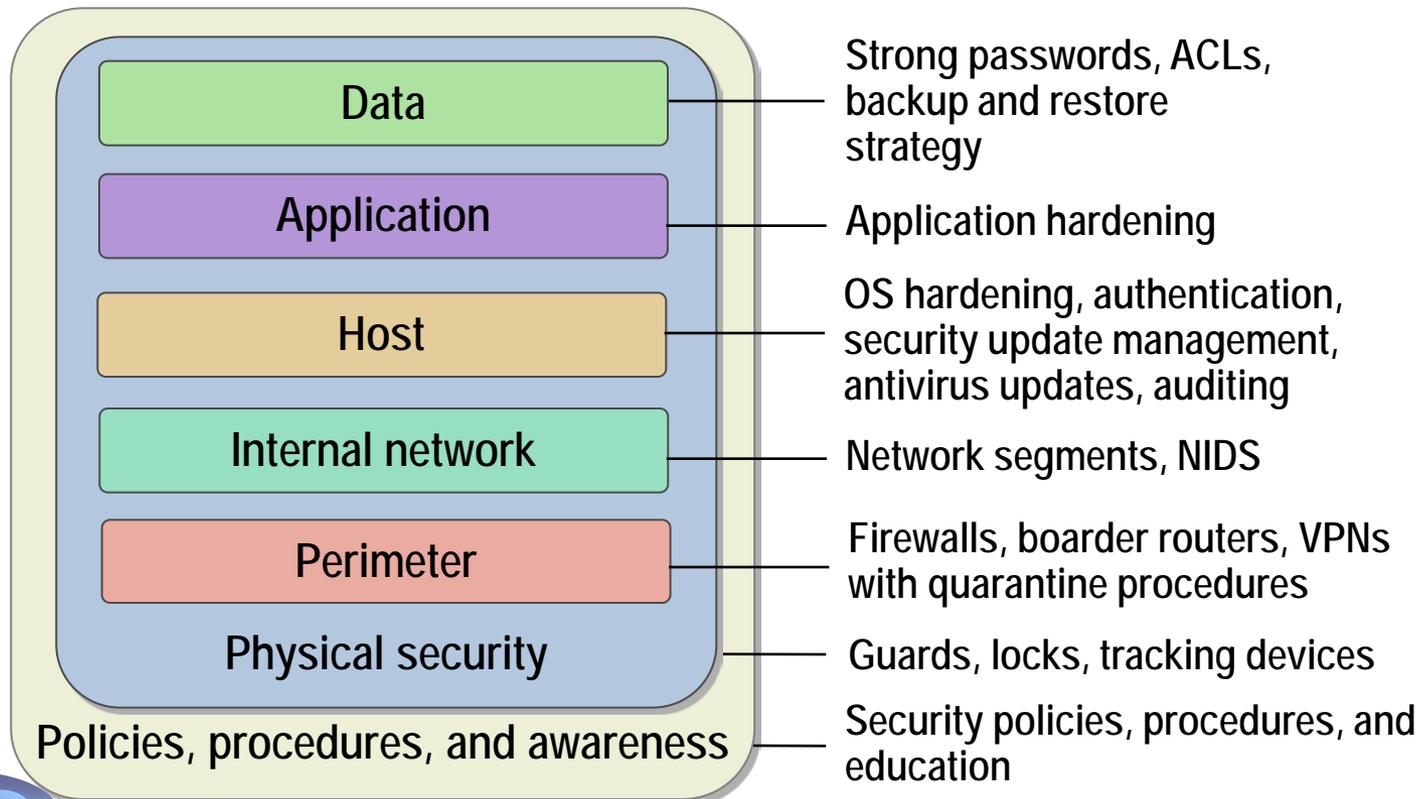
# Why should I...

- Why should I limit the personal information I put on the Internet?

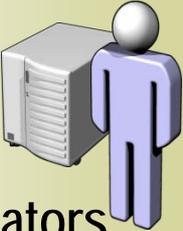
# Understanding Defense-in-Depth

Using a layered approach:

- Increases an attacker's risk of detection
- Reduces an attacker's chance of success



# Common Vulnerabilities

Source	Example vulnerabilities
<b>Users</b> 	<ul style="list-style-type: none"><li>• Sharing passwords or using weak passwords</li><li>• Not understanding or ignoring security policies</li><li>• Opening e-mail, visiting Web sites, or downloading software that contains malicious code</li><li>• Being manipulated into violating security policies</li></ul>
<b>Network administrators</b> 	<ul style="list-style-type: none"><li>• Misconfiguring services and not patching preinstalled software</li><li>• Not adequately securing network access accounts</li><li>• Not adequately securing physical access to hardware</li><li>• Ignoring security policies</li></ul>
<b>Software</b> 	<ul style="list-style-type: none"><li>• Using operating systems and applications that have design flaws that make them accessible to manipulation by attackers</li></ul>

# What Is a Denial-of-Service Attack?

**Denial-of-Service (DoS) attack:** Any attempt by an attacker to deny his victim's access to a resource

**DoS attacks can be divided into three categories:**

- Flooding attacks
- Resource starvation attacks
- Disruption of service

**Note: Denial-of-service attacks should not be launched against your own live production network**

Thank You

Corporate Training Group

Ctgtraining.com

rschandall@ctgtraining.com