THE CENTER FOR INTERNET SECURITY

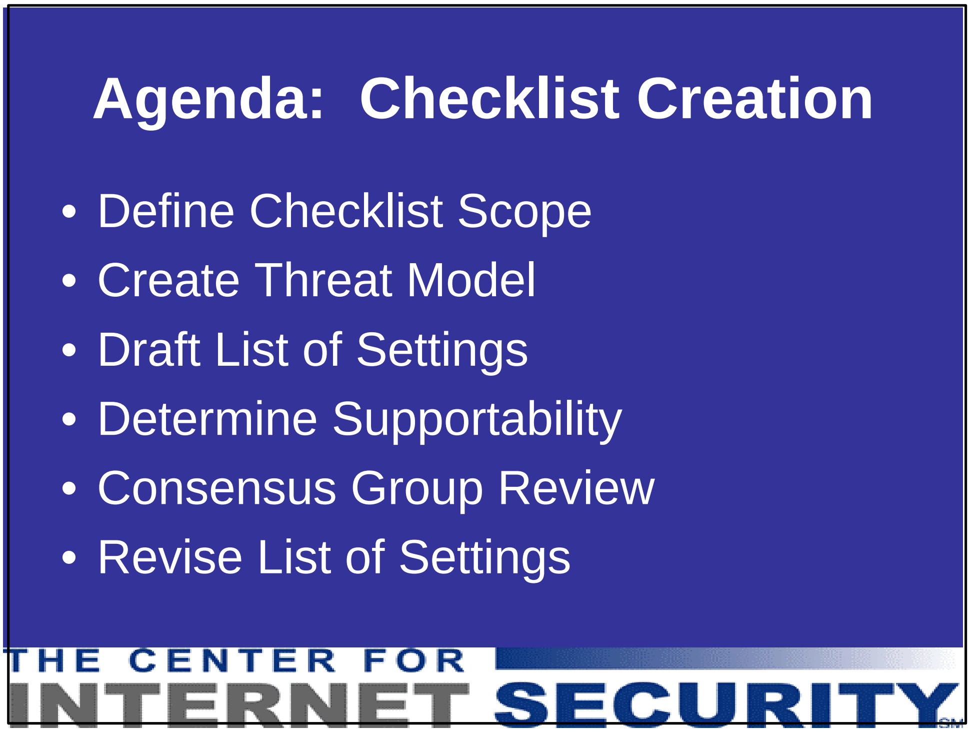
Security Checklists: Creation and Obstacles

Jeff Shawgo

The “Who Am I?” Slide:

- **Benchmark Editor for CIS since 2001.**
- **Author: SANS Securing Windows 2000 Step-by-Step.**
- **1991-1997 United States Marine Corps.**
  - Cryptologic Linguist
  - Signals Intelligence Intercept
  - Help Desk/LAN Administrator

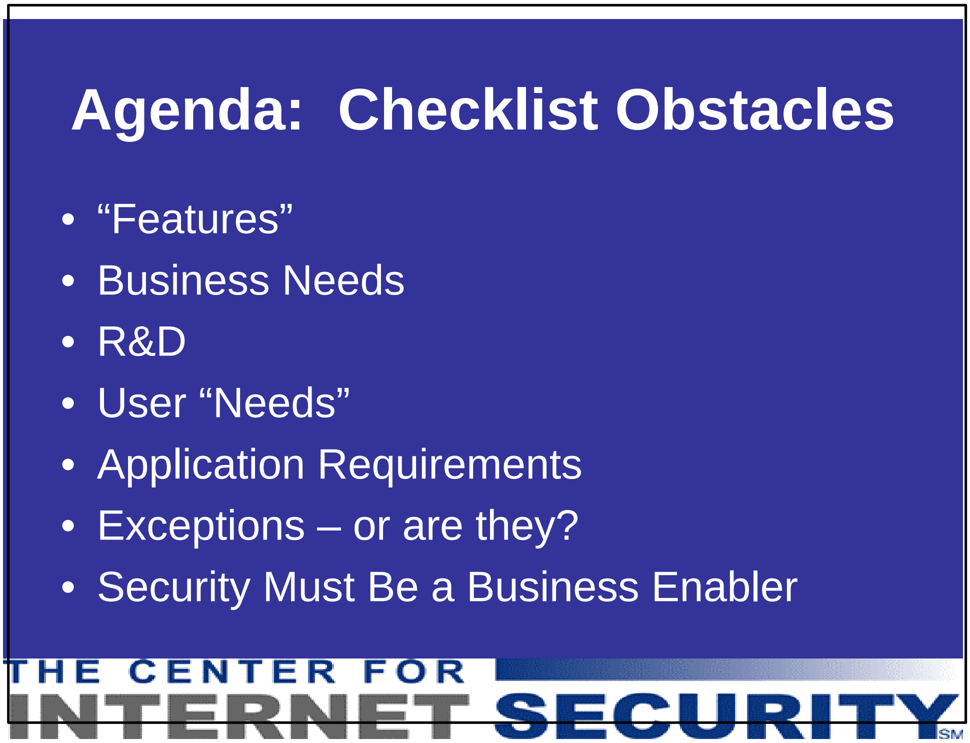
THE CENTER FOR INTERNET SECURITY



Agenda: Checklist Creation

- Define Checklist Scope
- Create Threat Model
- Draft List of Settings
- Determine Supportability
- Consensus Group Review
- Revise List of Settings

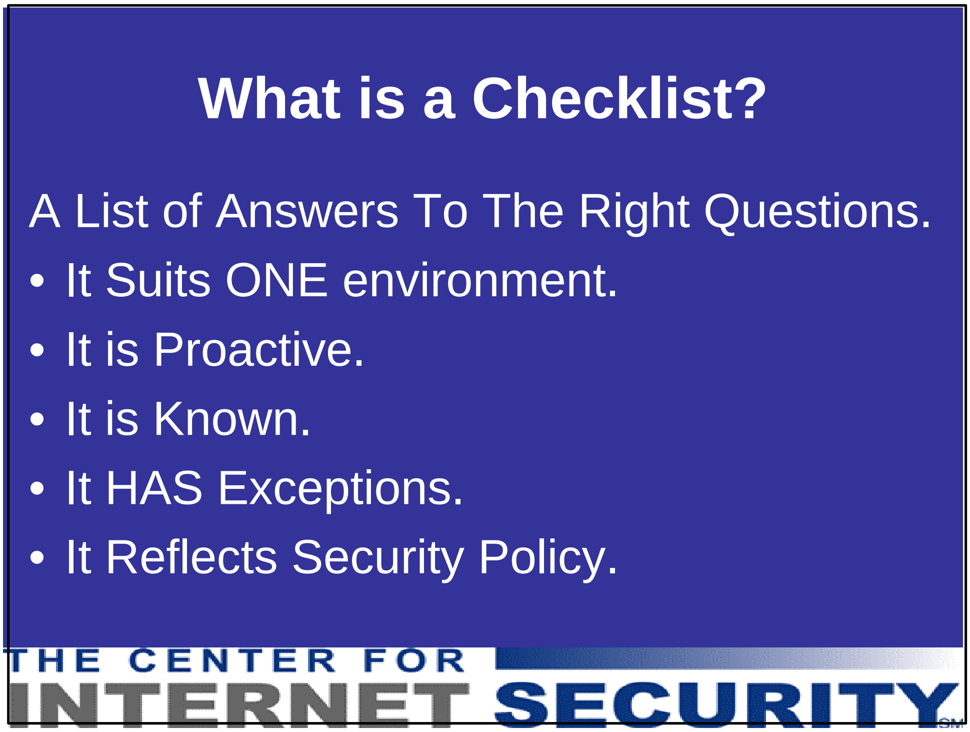
THE CENTER FOR INTERNET SECURITY



Agenda: Checklist Obstacles

- “Features”
- Business Needs
- R&D
- User “Needs”
- Application Requirements
- Exceptions – or are they?
- Security Must Be a Business Enabler

THE CENTER FOR INTERNET SECURITY

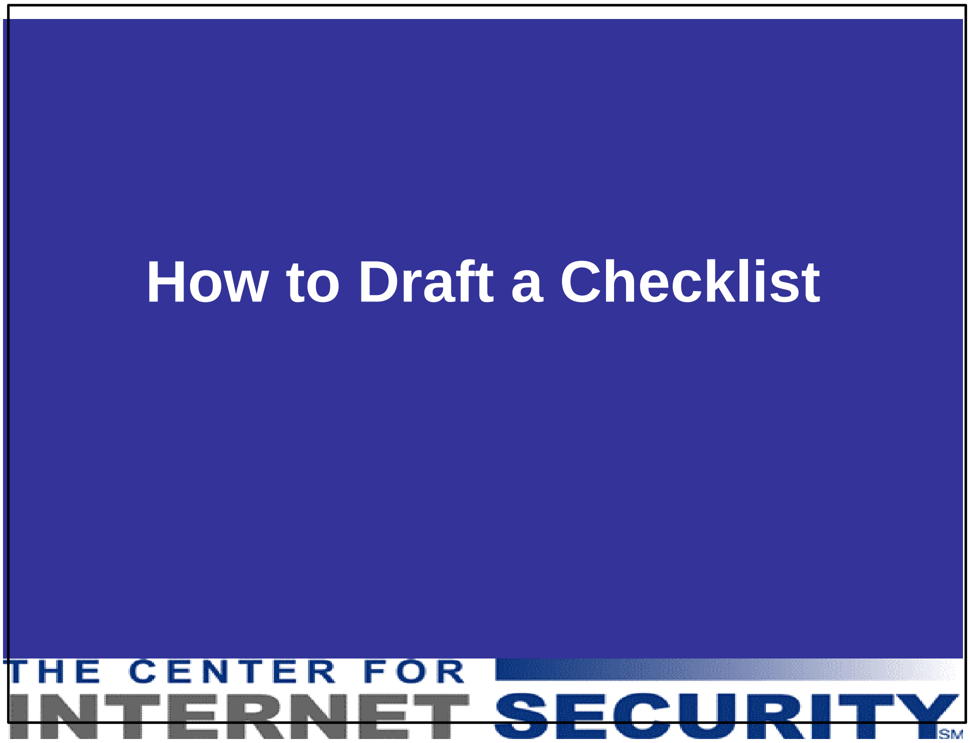


What is a Checklist?

A List of Answers To The Right Questions.

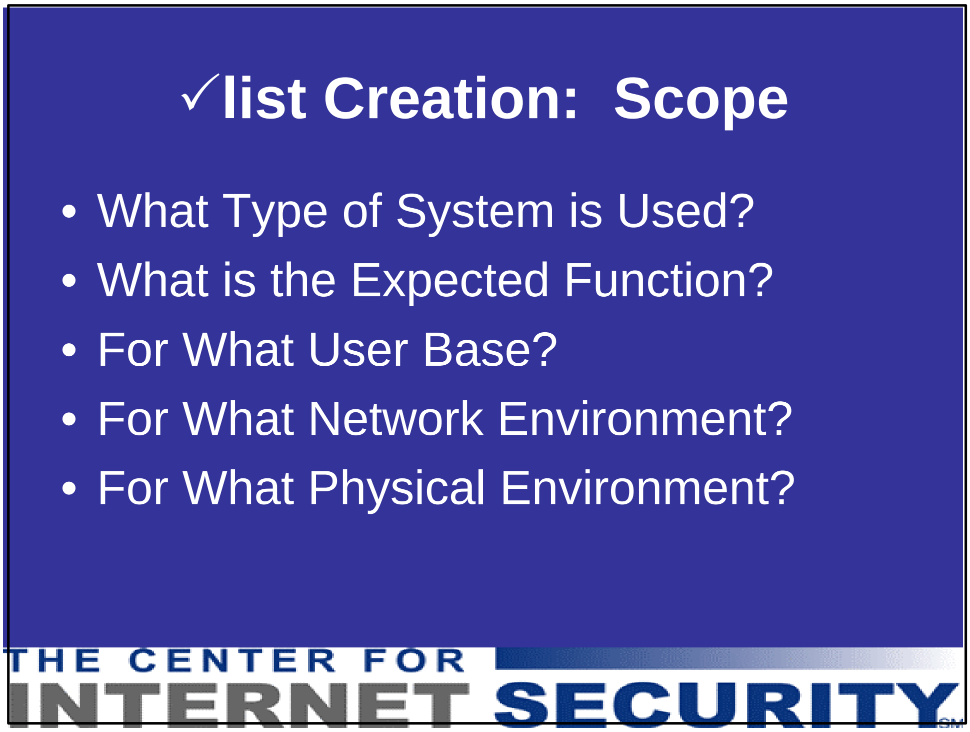
- It Suits ONE environment.
- It is Proactive.
- It is Known.
- It HAS Exceptions.
- It Reflects Security Policy.

THE CENTER FOR INTERNET SECURITY



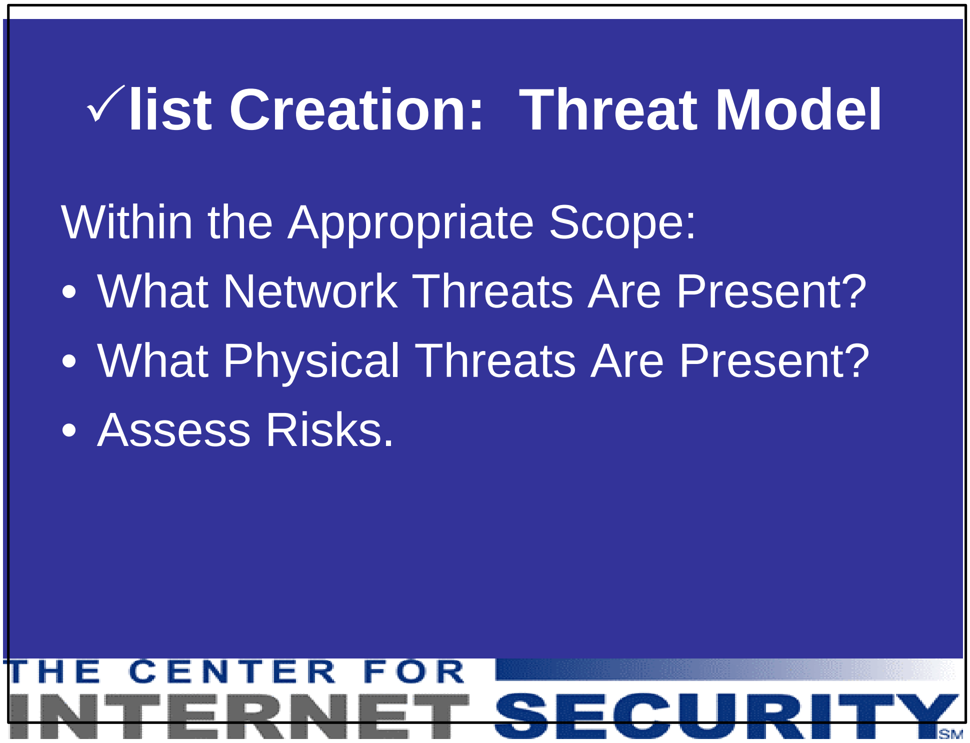
How to Draft a Checklist

THE CENTER FOR INTERNET SECURITY



✓list Creation: Scope

- What Type of System is Used?
- What is the Expected Function?
- For What User Base?
- For What Network Environment?
- For What Physical Environment?



✓list Creation: Threat Model

Within the Appropriate Scope:

- What Network Threats Are Present?
- What Physical Threats Are Present?
- Assess Risks.

✓list Creation: Draft List

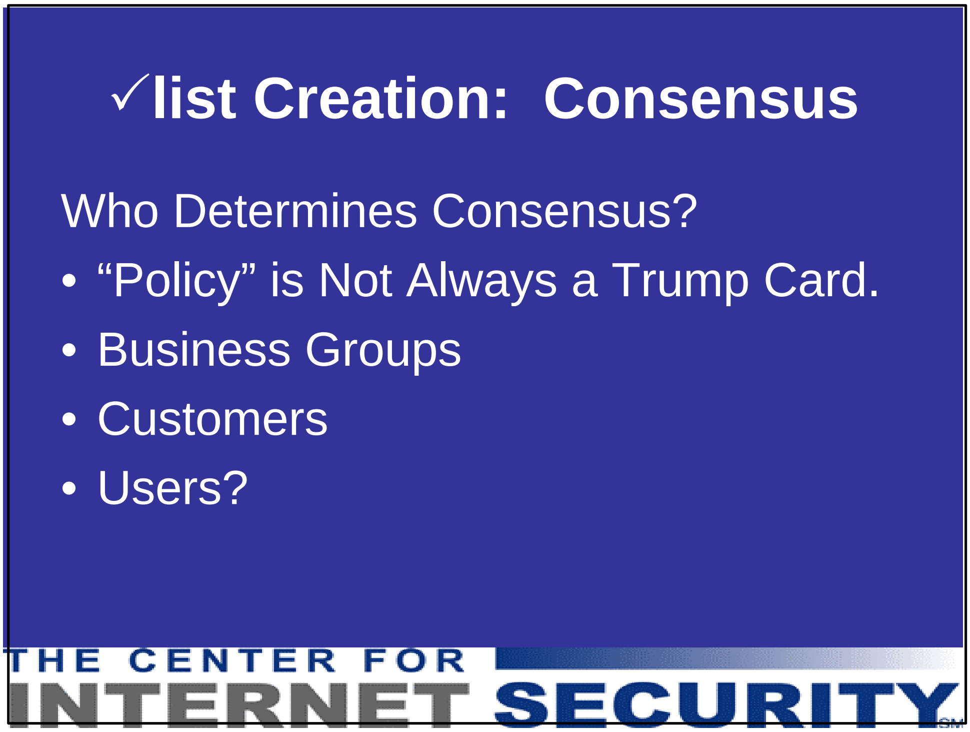
Define Settings to Support Policy:

- Defend Against Threats.
- Mitigate or Eliminate Risks.
- Accepting Risk is a Business Decision!
- Provide Defense in Depth.
  - Where possible, construct multiple defenses for each risk!

✓list Creation: Support

An Unsupported Checklist Doesn’t Work.

- Seek Operating System Support.
- Seek Application Vendor Support.
- Accept In-House Support.
- Test Applications in a “Hardened” OS.
- Be Prepared to Compromise.

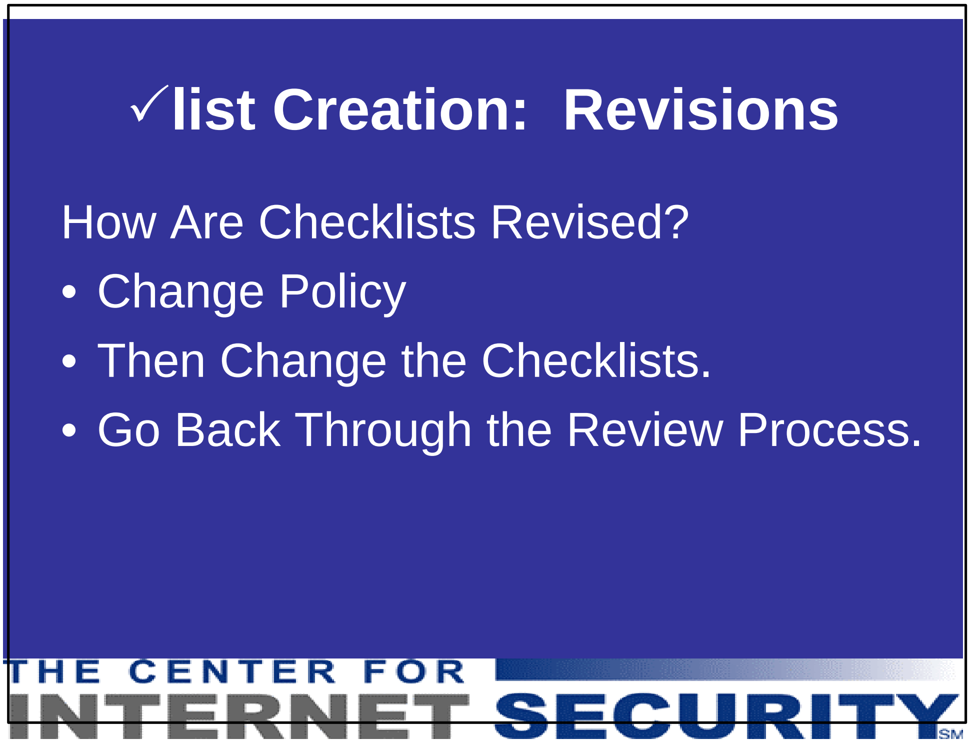


✓list Creation: Consensus

Who Determines Consensus?

- “Policy” is Not Always a Trump Card.
- Business Groups
- Customers
- Users?

THE CENTER FOR INTERNET SECURITY SM

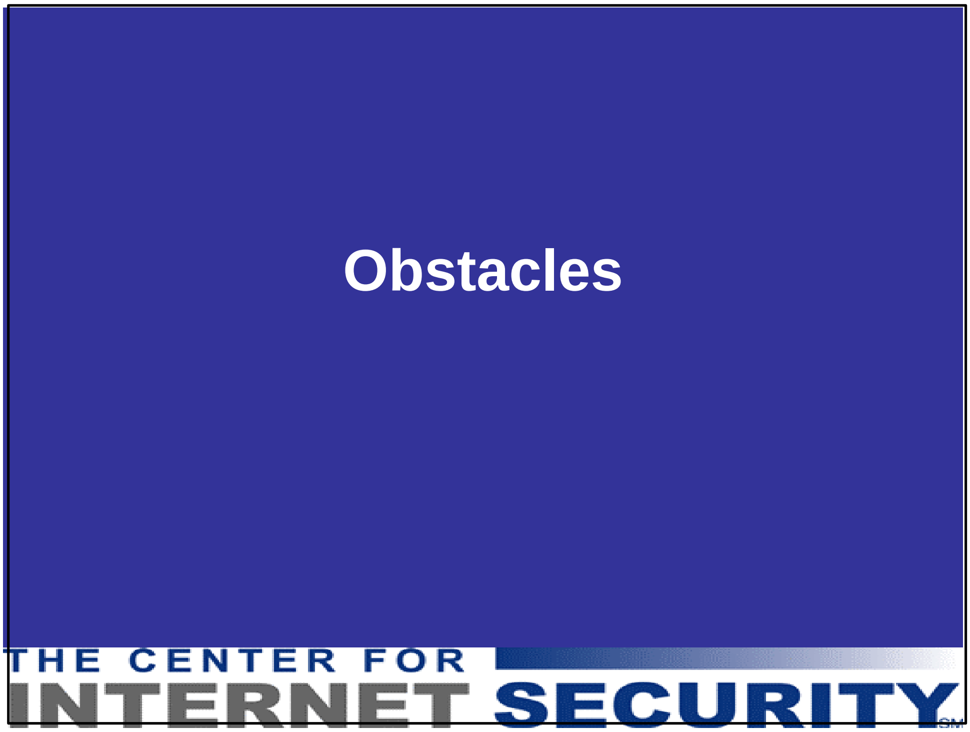


✓list Creation: Revisions

How Are Checklists Revised?

- Change Policy
- Then Change the Checklists.
- Go Back Through the Review Process.

THE CENTER FOR INTERNET SECURITY SM

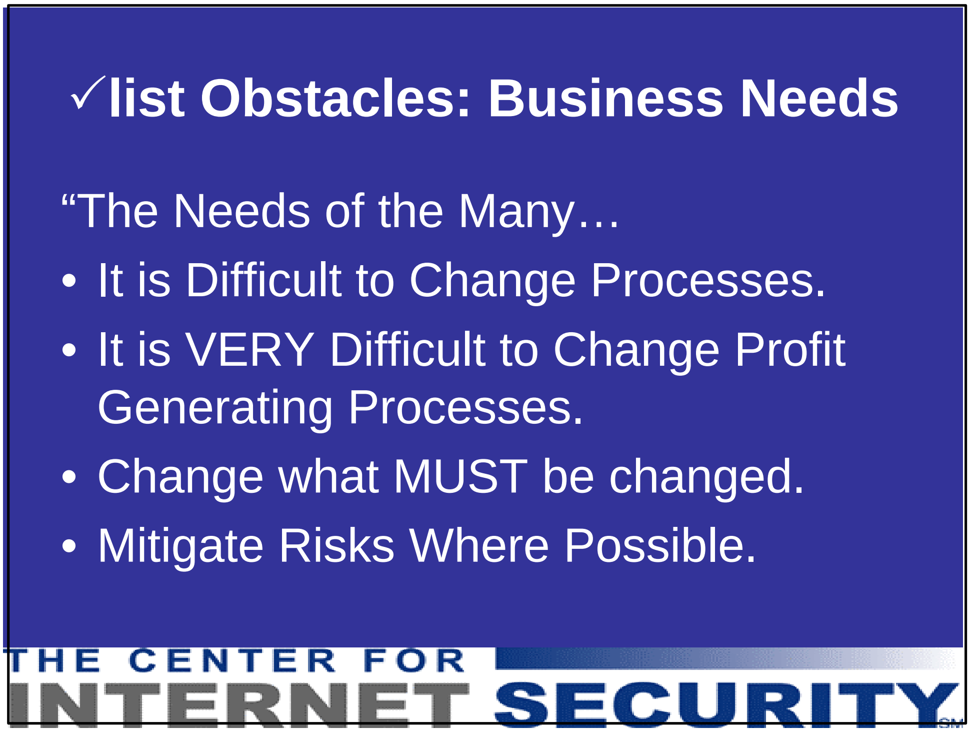


Obstacles

✓list Obstacles: Features

Does the Feature Outweigh the Risk?

- Unused Gadgets Are Easy to Disable.
- Useful Features Need to be Secure.
- Sometimes Usefulness Wins.
- Look for Creative Ways to Lock Down Insecure “Features”.

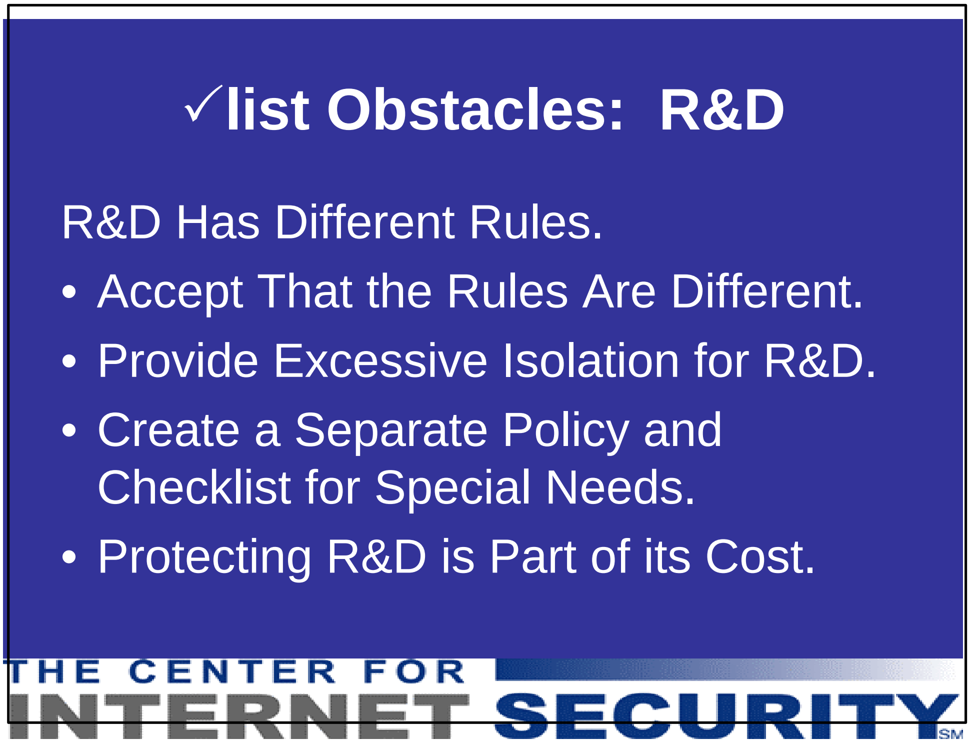


✓list Obstacles: Business Needs

“The Needs of the Many…

- It is Difficult to Change Processes.
- It is VERY Difficult to Change Profit Generating Processes.
- Change what MUST be changed.
- Mitigate Risks Where Possible.

THE CENTER FOR INTERNET SECURITY SM

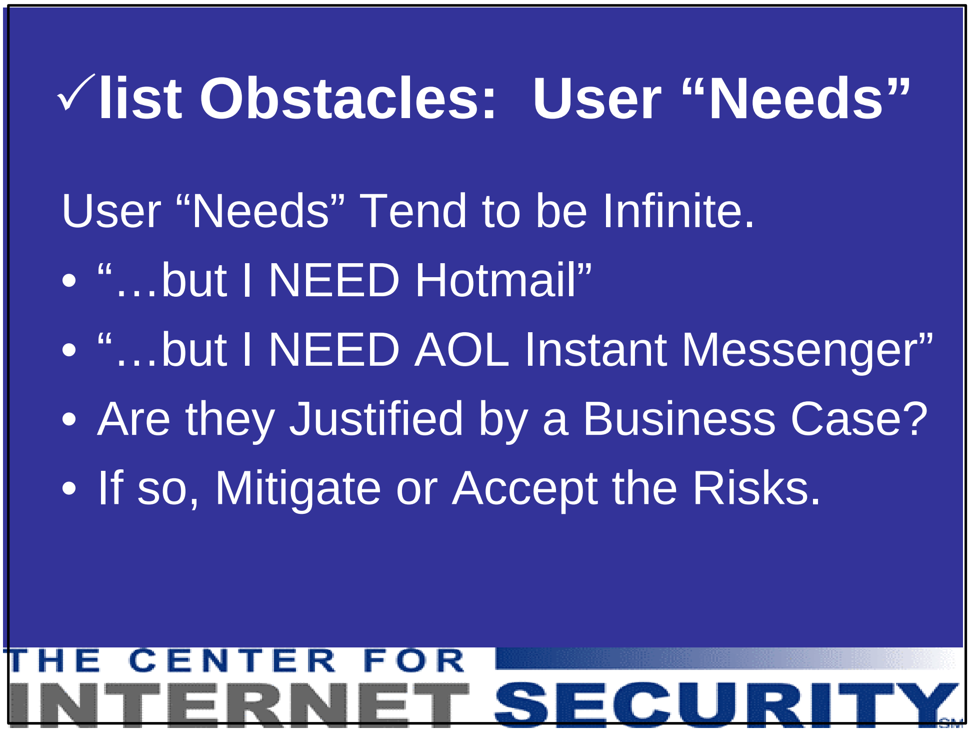


✓list Obstacles: R&D

R&D Has Different Rules.

- Accept That the Rules Are Different.
- Provide Excessive Isolation for R&D.
- Create a Separate Policy and Checklist for Special Needs.
- Protecting R&D is Part of its Cost.

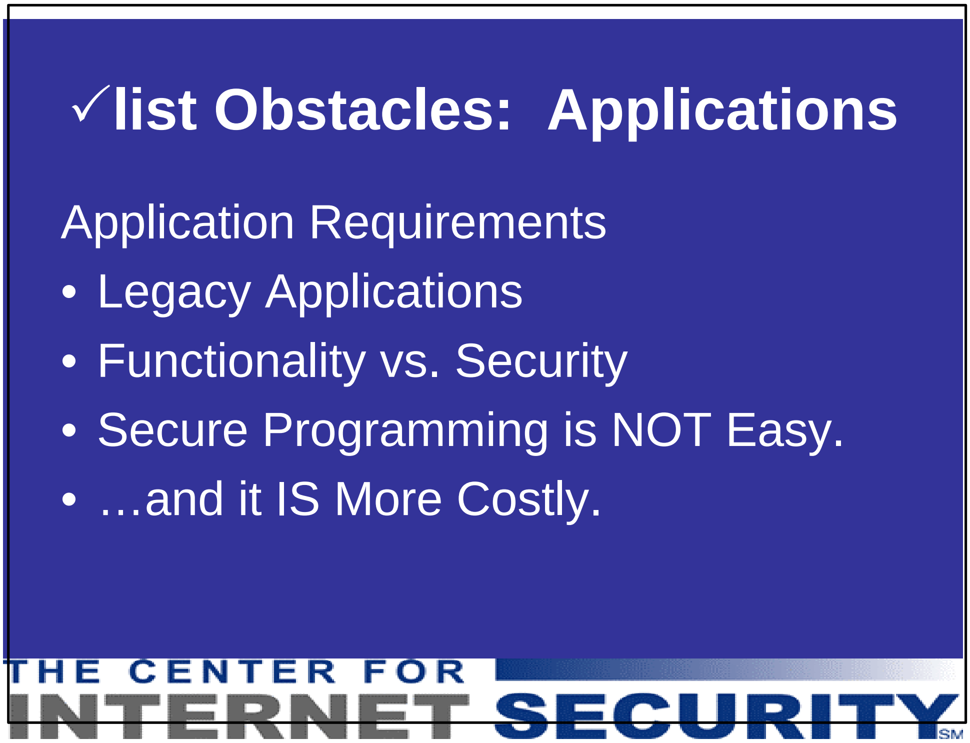
THE CENTER FOR INTERNET SECURITY SM



✓list Obstacles: User “Needs”

User “Needs” Tend to be Infinite.

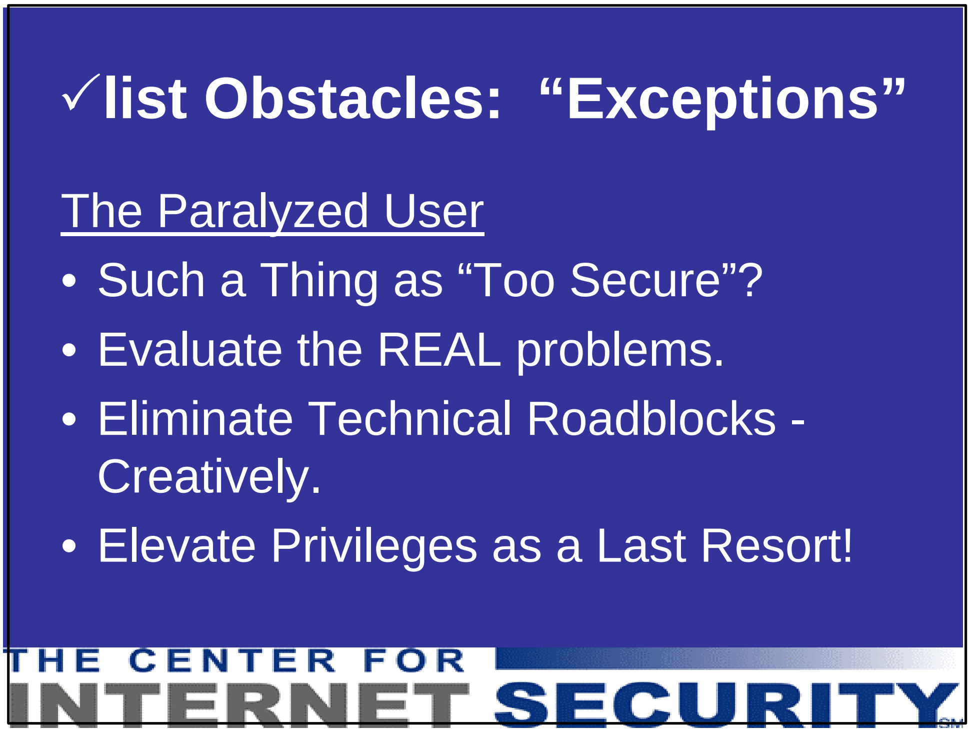
- “…but I NEED Hotmail”
- “…but I NEED AOL Instant Messenger”
- Are they Justified by a Business Case?
- If so, Mitigate or Accept the Risks.



✓list Obstacles: Applications

Application Requirements

- Legacy Applications
- Functionality vs. Security
- Secure Programming is NOT Easy.
- …and it IS More Costly.

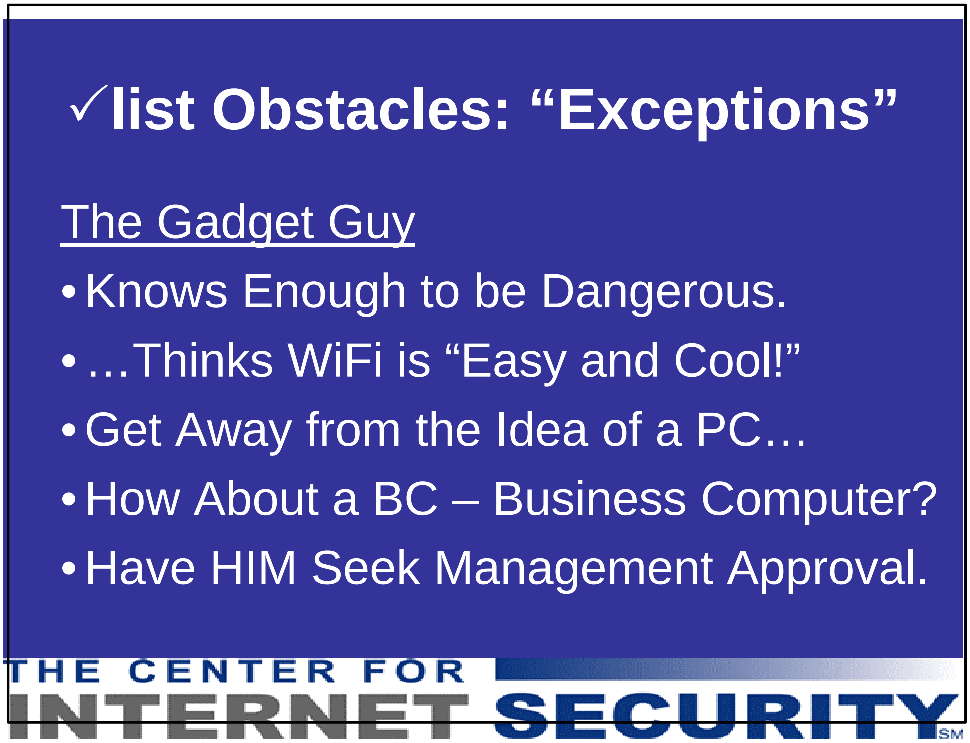


✓list Obstacles: “Exceptions”

The Paralyzed User

- Such a Thing as “Too Secure”?
- Evaluate the REAL problems.
- Eliminate Technical Roadblocks - Creatively.
- Elevate Privileges as a Last Resort!

THE CENTER FOR INTERNET SECURITY℠

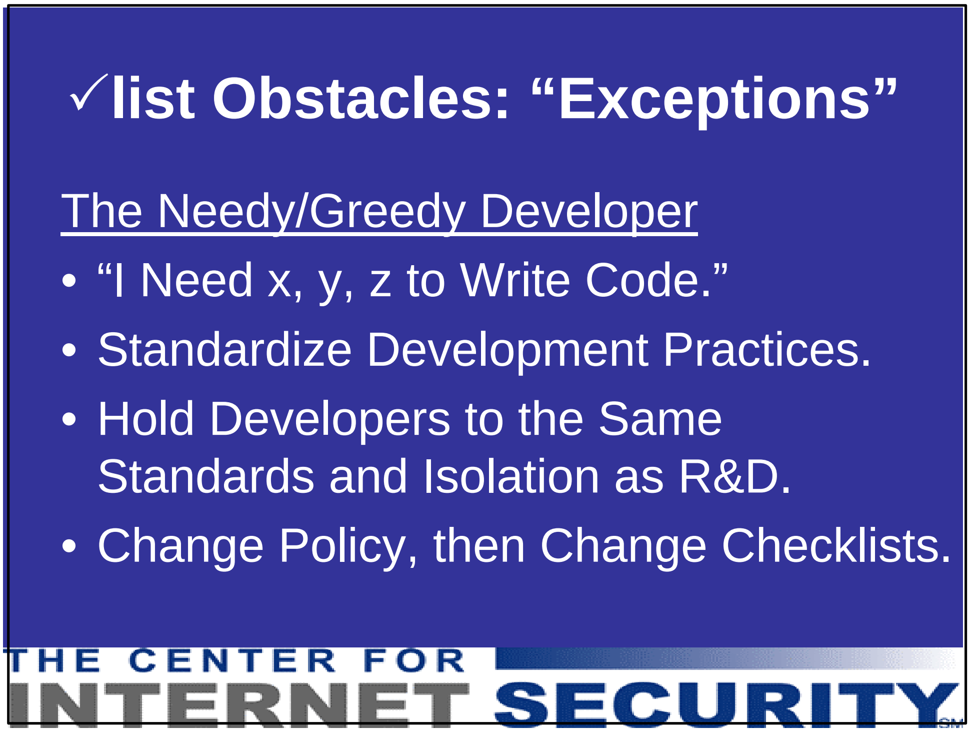


✓list Obstacles: “Exceptions”

The Gadget Guy

- Knows Enough to be Dangerous.
- …Thinks WiFi is “Easy and Cool!”
- Get Away from the Idea of a PC…
- How About a BC – Business Computer?
- Have HIM Seek Management Approval.

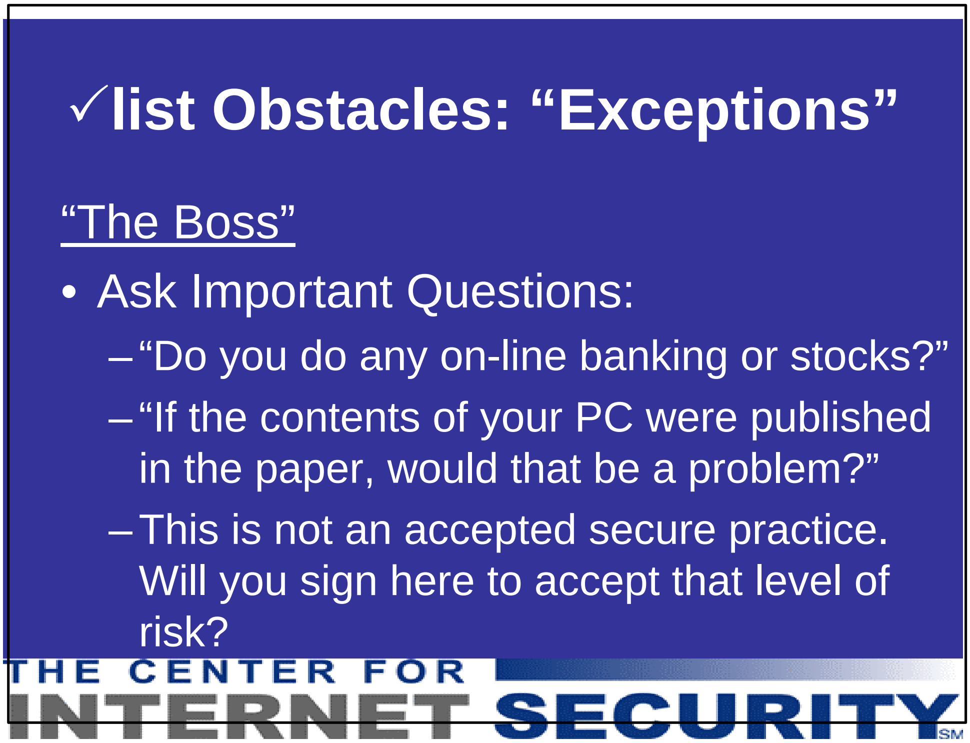
THE CENTER FOR INTERNET SECURITY℠



✓list Obstacles: “Exceptions”

The Needy/Greedy Developer

- “I Need x, y, z to Write Code.”
- Standardize Development Practices.
- Hold Developers to the Same Standards and Isolation as R&D.
- Change Policy, then Change Checklists.



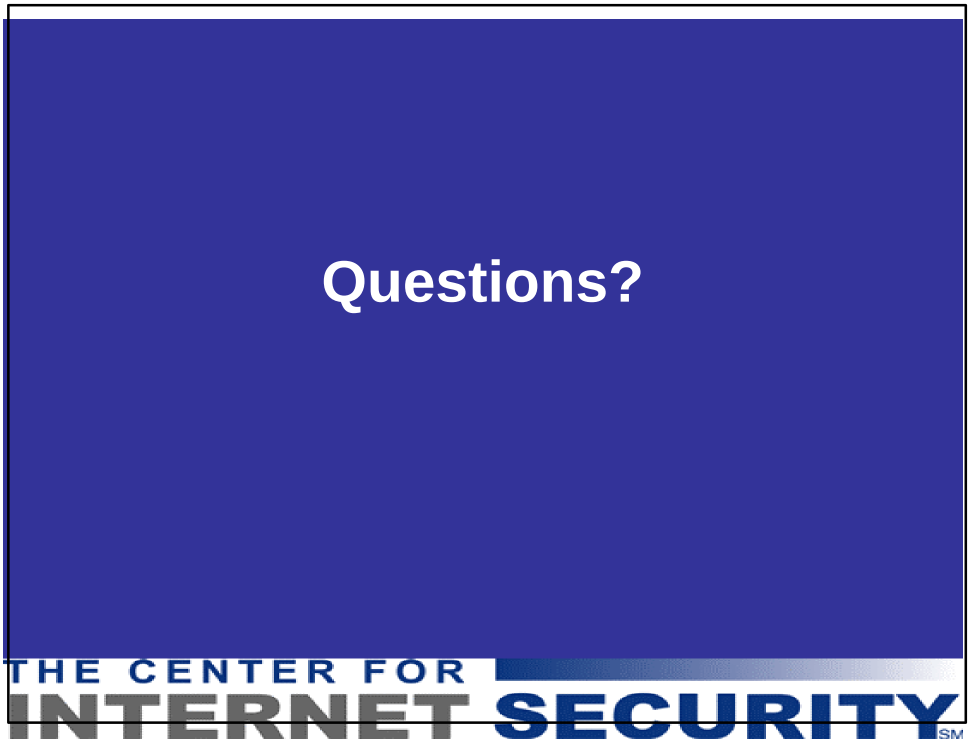
✓list Obstacles: “Exceptions”

“The Boss”

- Ask Important Questions:
  - “Do you do any on-line banking or stocks?”
  - “If the contents of your PC were published in the paper, would that be a problem?”
  - This is not an accepted secure practice. Will you sign here to accept that level of risk?

Conclusion:

- Security Must Be a Business Enabler!
- Look for Creative Ways to Secure.
- Practice Defense-In-Depth.
- Favor Applications that Favor Security.
- Chastise all the Others.
- Promote Security Awareness for ALL.



Questions?