Computer Network Defense Simulators Advance Cyberspace Protection

EADS North America Defense S3 Inc.
1476 N. Greenmount Rd.
O'Fallon IL 62269
Phone: 618-632-9878
chet.ratcliffe@eads-na-security.com

Chet Ratcliffe
EVP / CTO
EADS North America Defense

The Threat

- **In today's global environment, relying on security devices alone to protect computer networks is not enough**
- **Computer networks face a constantly evolving menace from cyber attacks, viruses, unauthorized probes, scans and intrusions**
- **Foreign Governments, Terrorists, Criminals, and Network Hackers are more determined than ever to steal information, cause disruption and destroy networks**
- **Inconsistent or no training of system operators in identifying and mitigating Cyber Attacks currently poses one of the biggest threats to critical computer networks.**

Mitigate through People + Processes + Technology

"***FAA's Air-Traffic Networks Breached by Hackers***" **(May 7, 2009, Wall Street Journal)**

"***Sophisticated Botnet Causing a Surge in Click Fraud***" **(Sep 17, 2009,** IDG News Service)

"***Swedish Hacker Indicted in Cisco, NASA Attacks***" **(May 6, 2009, Wall Street Journal)**

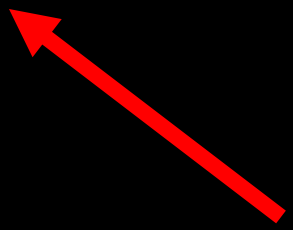
Conficker→10 million PCs, $10 Billion

“One in 10 people clicking through to receive the malware is a pretty sobering number“

- Stefan Savage, professor at UCSD and lead researcher on a recent spam study

FSLJDSLFFSFU.17.23.server29.akamae.com

FSLJDSLFFSFU.17.23.server29.akamae.com

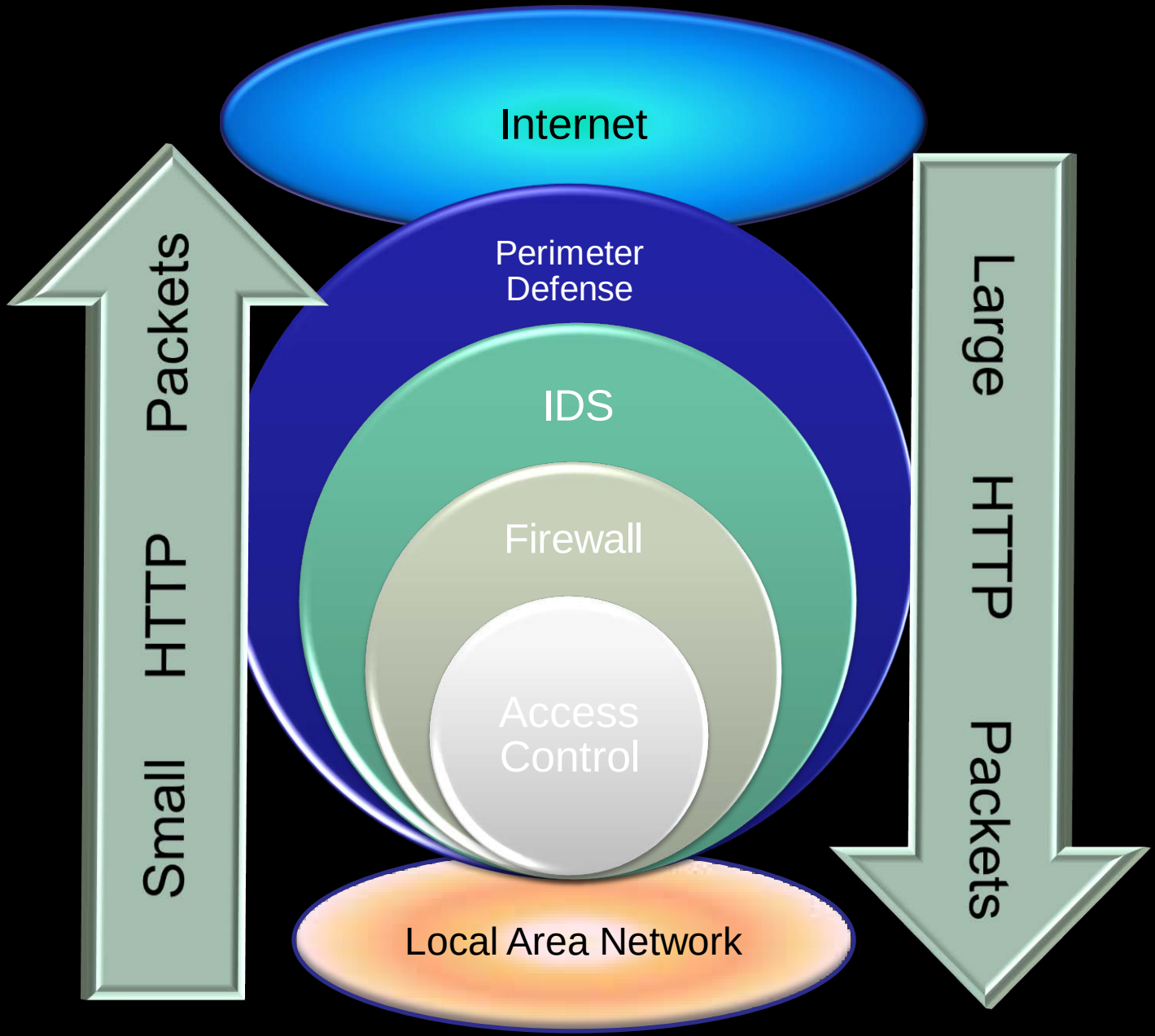


Exfiltrated Data


FSLJDSLFFSFU 17.23.server29.akamae.com
Sequence Number

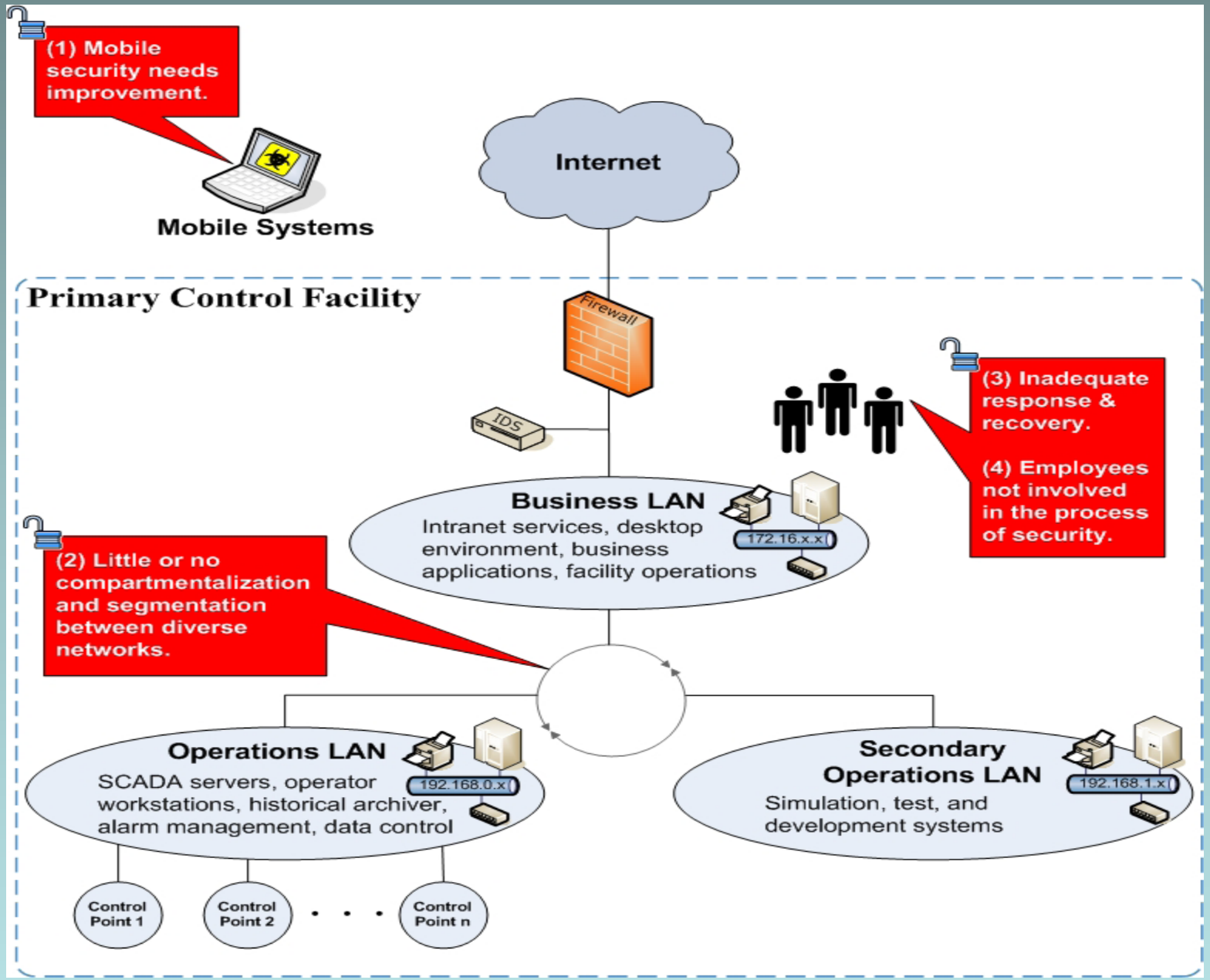

FSLJDSLFFSFU.17.23.server29.akamae.com
Bot ID

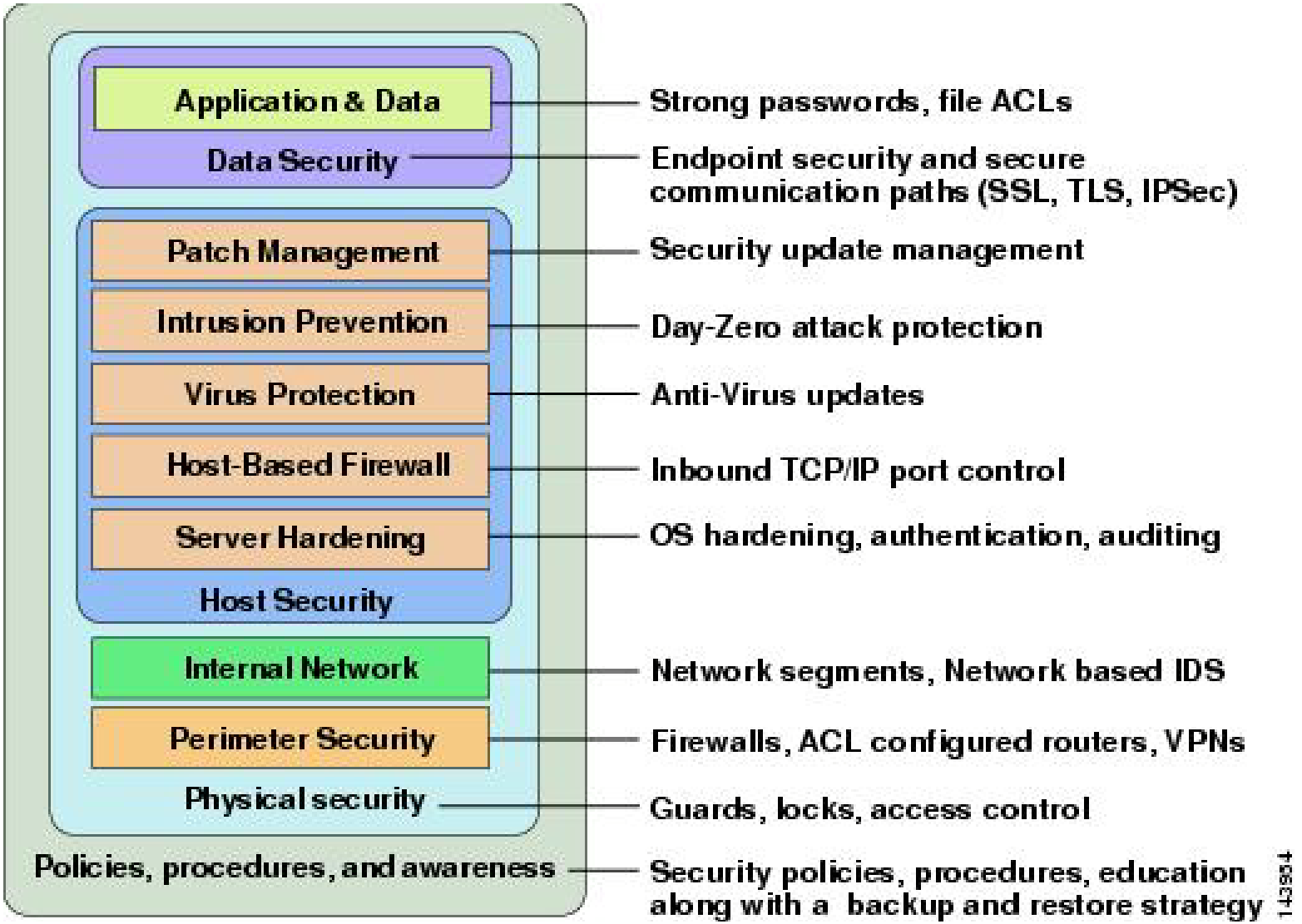
What is wrong with this picture?



- **Cyber attack on Alberta Health Services network**

  On July 8, the Government of Alberta issued a bulletin to notify the public of a cyber attack on the Alberta Health Services (AHS) network in Edmonton. AHS indicated that a computer virus briefly infected the network on May 14-15 and may have captured patient health information. AHS is notifying 11,582 individuals whose information may have been copied by the virus. AHS removed the virus, reinforced anti-virus protection and started a comprehensive review of its information technology security measures to ensure continued alignment with best practice standards.


(1) Mobile security needs improvement.
Mobile Systems
Internet
Primary Control Facility
Firewall
IDS
(3) Inadequate response & recovery.
(4) Employees not involved in the process of security.
Business LAN
Intranet services, desktop environment, business applications, facility operations
172.16.x.x
(2) Little or no compartmentalization and segmentation between diverse networks.
Operations LAN
SCADA servers, operator workstations, historical archiver, alarm management, data control
192.168.0.x
Secondary Operations LAN
Simulation, test, and development systems
192.168.1.x
Control Point 1
Control Point 2
Control Point n


Application & Data
Data Security
Patch Management
Intrusion Prevention
Virus Protection
Host-Based Firewall
Server Hardening
Host Security
Internal Network
Perimeter Security
Physical security
Policies, procedures, and awareness
Strong passwords, file ACLs
Endpoint security and secure communication paths (SSL, TLS, IPSec)
Security update management
Day-Zero attack protection
Anti-Virus updates
Inbound TCP/IP port control
OS hardening, authentication, auditing
Network segments, Network based IDS
Firewalls, ACL configured routers, VPNs
Guards, locks, access control
Security policies, procedures, education along with a backup and restore strategy
143954

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL

CISSP®

C|EH™

Certified Ethical Hacker

CCSP CISCO CERTIFIED SECURITY PROFESSIONAL


Malware
Worms
Hackers
Phishing
Spyware
Viruses
Adware
Rootkits
Spam
Trojans

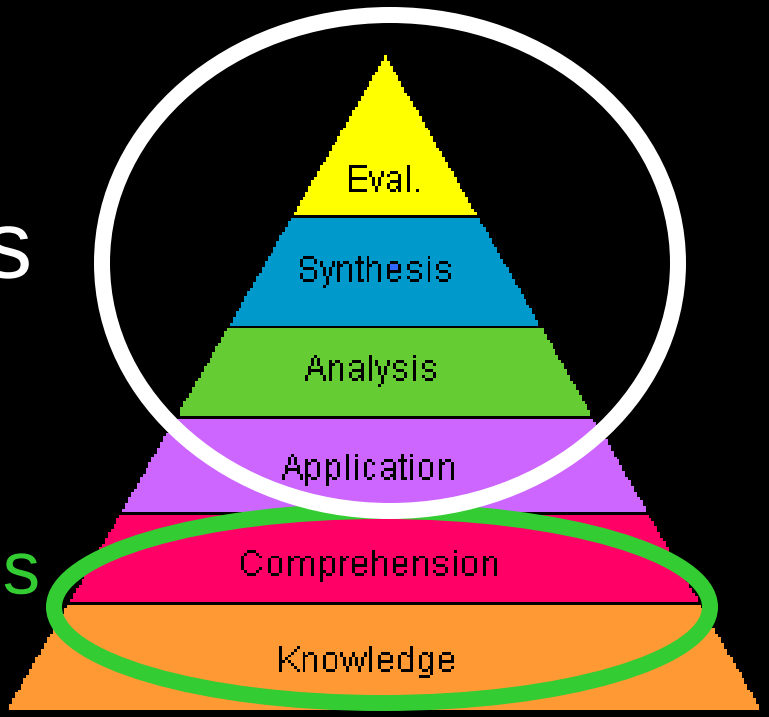
Adult Learning

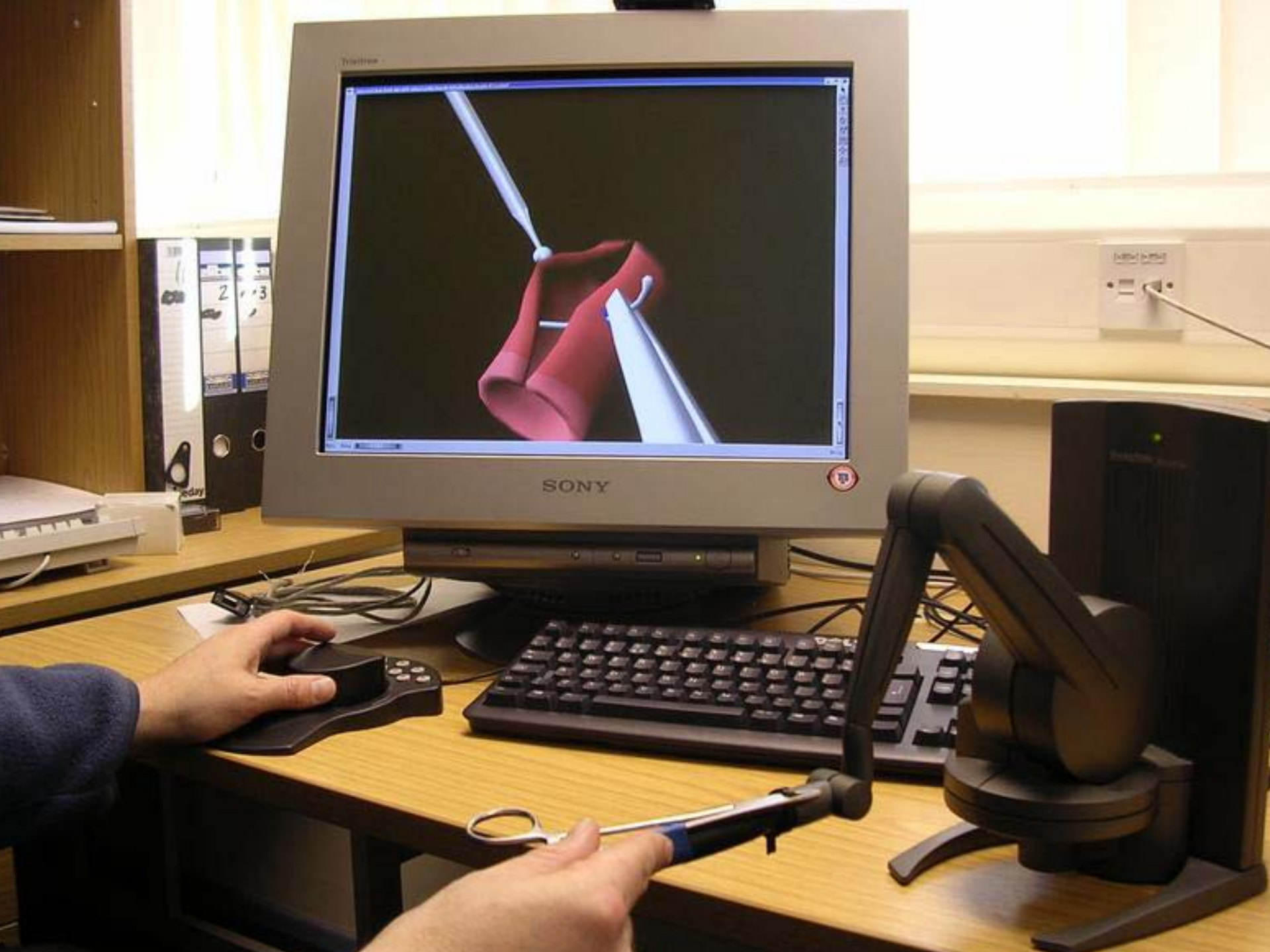
Adult Learning

Simulators

Certifications

Books




SONY

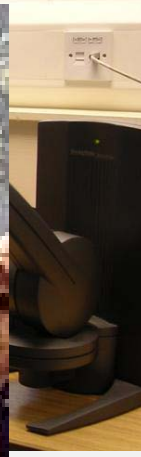

DANGER
DO NOT PULL
HANDLE

Crashed Planes = Loss $$$

Crashed Planes = Loss of Life

“One way of looking at this might be that for 42 years, I've been making small, regular deposits in this bank of experience: education and training. And on January 15 the balance was sufficient so that I could make a very large withdrawal."

- Chesley Sullenberger

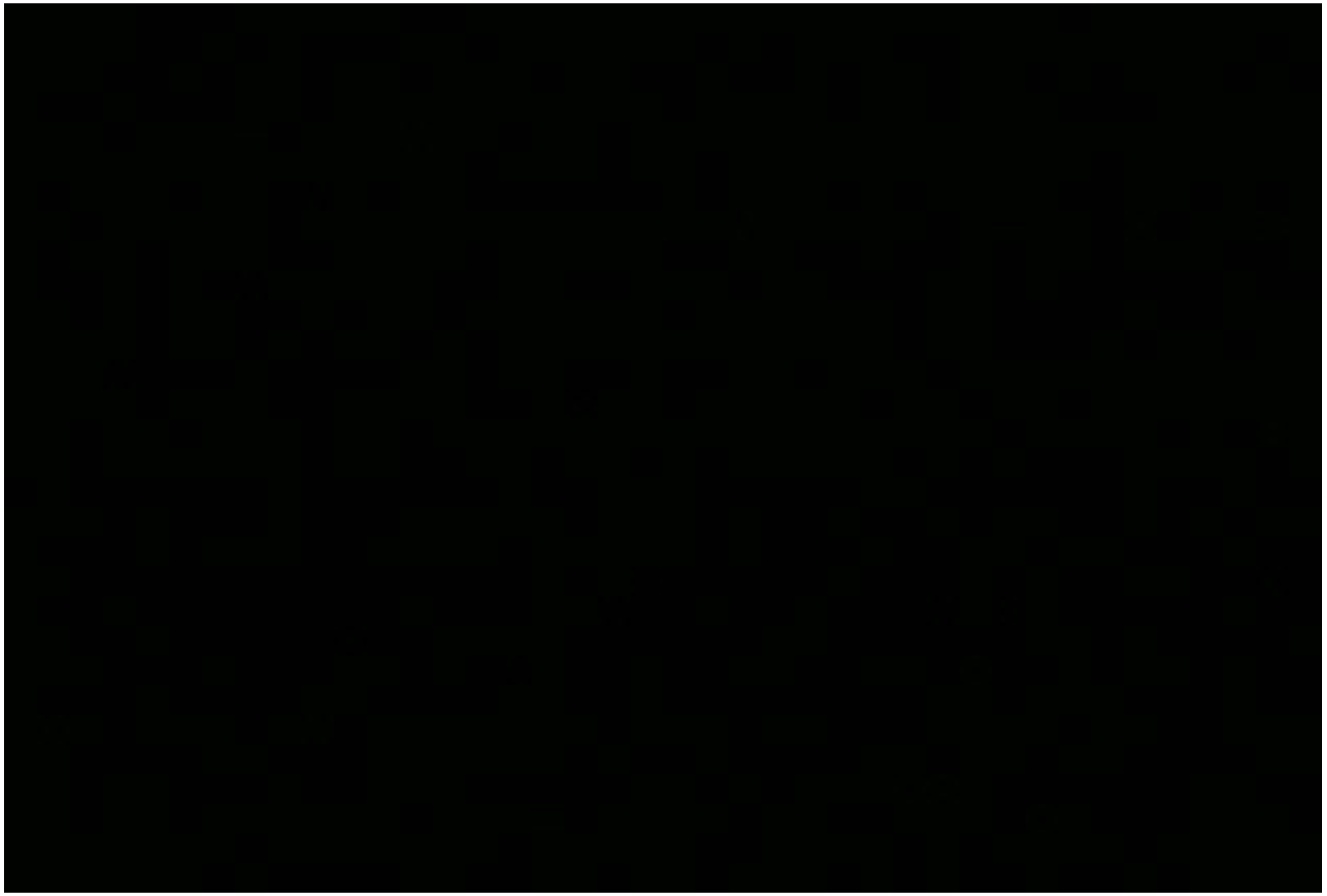





Crippled or Exploited Networks
• Loss of data and comm
• Loss of critical infrastructures
• Loss of customer confidence
• Loss of revenue
Total economic meltdown

Why are we willing to trust our networks to IT Professionals?

We just assume they know what they're doing…



…but all it takes is one stupid mistake!

How much damage can be done with a keystroke?

Poorly Trained and Overworked Administrators

Ineffective Policies and Procedures

Ineffective Communications

NETWORK OPERATIONS CREWS CAN TRAIN AND CERTIFY TO:

Detect, Recognize, Research, Mitigate, and Report attacks and anomalies

Practice as a team or individually

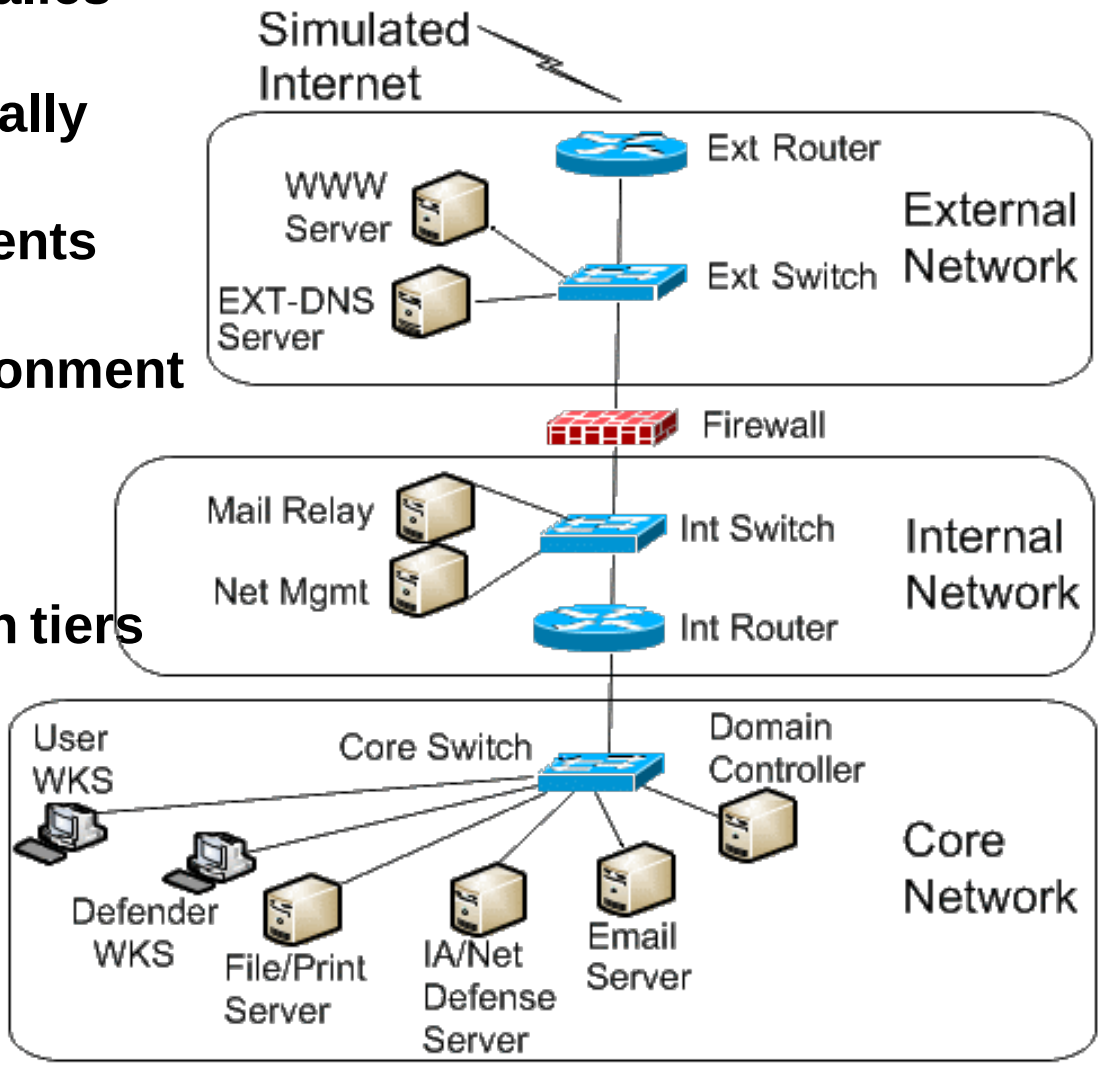
React quickly to malicious events

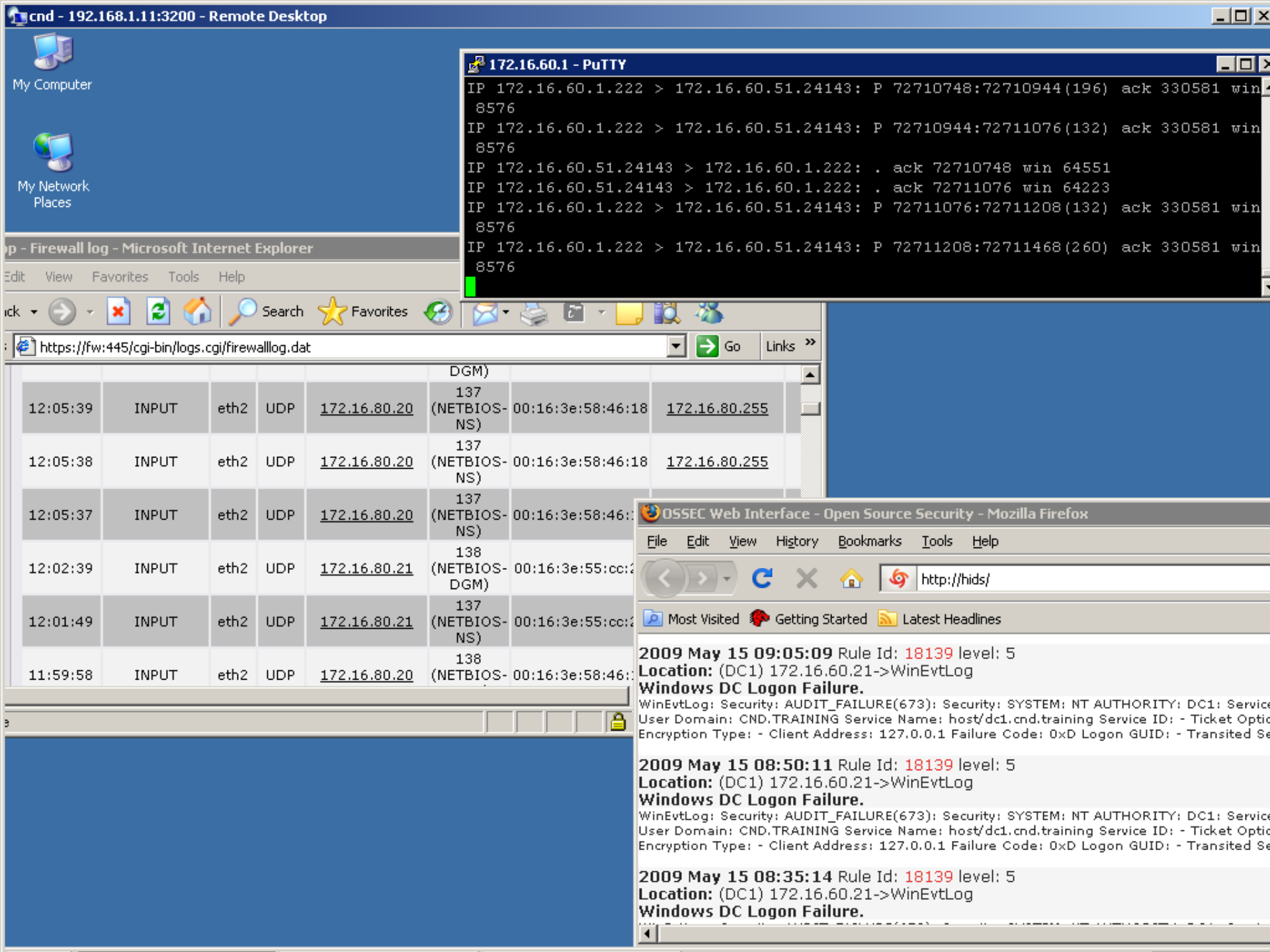
Make mistakes in a safe environment

Review checklists and tactics

Test communications between tiers

Test/evaluate new products




cnd - 192.168.1.11:3200 - Remote Desktop
My Computer
My Network Places
172.16.60.1 - PuTTY
IP 172.16.60.1.222 > 172.16.60.51.24143: P 72710748:72710944(196) ack 330581 win 8576
IP 172.16.60.1.222 > 172.16.60.51.24143: P 72710944:72711076(132) ack 330581 win 8576
IP 172.16.60.51.24143 > 172.16.60.1.222: . ack 72710748 win 64551
IP 172.16.60.51.24143 > 172.16.60.1.222: . ack 72711076 win 64223
IP 172.16.60.1.222 > 172.16.60.51.24143: P 72711076:72711208(132) ack 330581 win 8576
IP 172.16.60.1.222 > 172.16.60.51.24143: P 72711208:72711468(260) ack 330581 win 8576
p - Firewall log - Microsoft Internet Explorer
Edit View Favorites Tools Help
Search Favorites
https://fw:445/cgi-bin/logs.cgi/firewalllog.dat
Go Links
DGM)
12:05:39 INPUT eth2 UDP 172.16.80.20 137 (NETBIOS-NS) 00:16:3e:58:46:18 172.16.80.255
12:05:38 INPUT eth2 UDP 172.16.80.20 137 (NETBIOS-NS) 00:16:3e:58:46:18 172.16.80.255
12:05:37 INPUT eth2 UDP 172.16.80.20 137 (NETBIOS-NS) 00:16:3e:58:46:
12:02:39 INPUT eth2 UDP 172.16.80.21 138 (NETBIOS-DGM) 00:16:3e:55:cc:
12:01:49 INPUT eth2 UDP 172.16.80.21 137 (NETBIOS-NS) 00:16:3e:55:cc:
11:59:58 INPUT eth2 UDP 172.16.80.20 138 (NETBIOS- 00:16:3e:58:46:
OSSEC Web Interface - Open Source Security - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://hids/
Most Visited Getting Started Latest Headlines
2009 May 15 09:05:09 Rule Id: 18139 level: 5
Location: (DC1) 172.16.60.21->WinEvtLog
Windows DC Logon Failure.
WinEvtLog: Security: AUDIT_FAILURE(673): Security: SYSTEM: NT AUTHORITY: DC1: Service
User Domain: CND.TRAINING Service Name: host/dc1.cnd.training Service ID: - Ticket Optio
Encryption Type: - Client Address: 127.0.0.1 Failure Code: 0xD Logon GUID: - Transited Se
2009 May 15 08:50:11 Rule Id: 18139 level: 5
Location: (DC1) 172.16.60.21->WinEvtLog
Windows DC Logon Failure.
WinEvtLog: Security: AUDIT_FAILURE(673): Security: SYSTEM: NT AUTHORITY: DC1: Service
User Domain: CND.TRAINING Service Name: host/dc1.cnd.training Service ID: - Ticket Optio
Encryption Type: - Client Address: 127.0.0.1 Failure Code: 0xD Logon GUID: - Transited Se
2009 May 15 08:35:14 Rule Id: 18139 level: 5
Location: (DC1) 172.16.60.21->WinEvtLog
Windows DC Logon Failure.

Planning

- Size of network and number of employees
- Cost vs. budget
- Virtualization vs. actual hardware
- Management and support
- Ownership vs. timeshare
- Level of expertise

Functionality

- Familiar Environment (similar look and feel)
  - Architecture and Tools
- Realistic Traffic and Services
  - Simulated Internet with thousands of nodes
- Easy to use and configure (point and click)
- Reconstitution
- Automated attack engine
- Data collection (Metrics)
- Secure access (remote and local)
- Event builder with pre-built scenarios

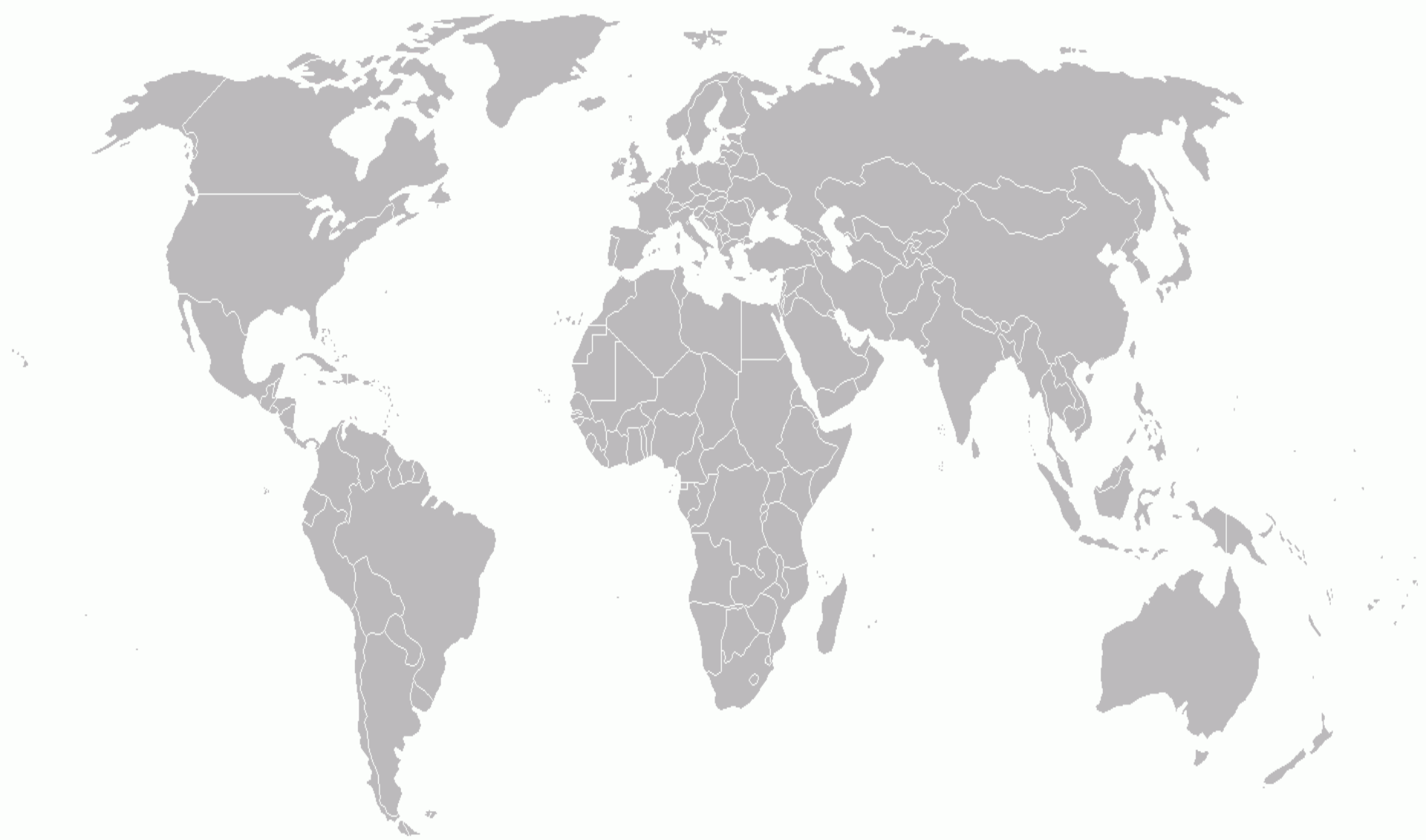
Implementation

- Training program
- Certification and “check-rides”
- Quarterly training
- Annual exercises
- Metrics to gauge improvement
- Keep management involved

“*Criminals find cyberspace too secure and return to conventional crime*” (TBD, Wall Street Journal)

“*Hackers thwarted in attempt to steal medical data and have been sentenced to 20 years in prison*” (TBD, Associated Press)

Conficker – 0 PCs, $0



A day in the life of an IT guy

- US CERT
  - http://www.us-cert.gov/
- Control Systems Security Program (CSSP)
  - http://www.uscert.gov/control_systems/csvuls.html