Microsoft® Official Course

Module8

Implementing IT Security Layers

Microsoft®

Module Overview

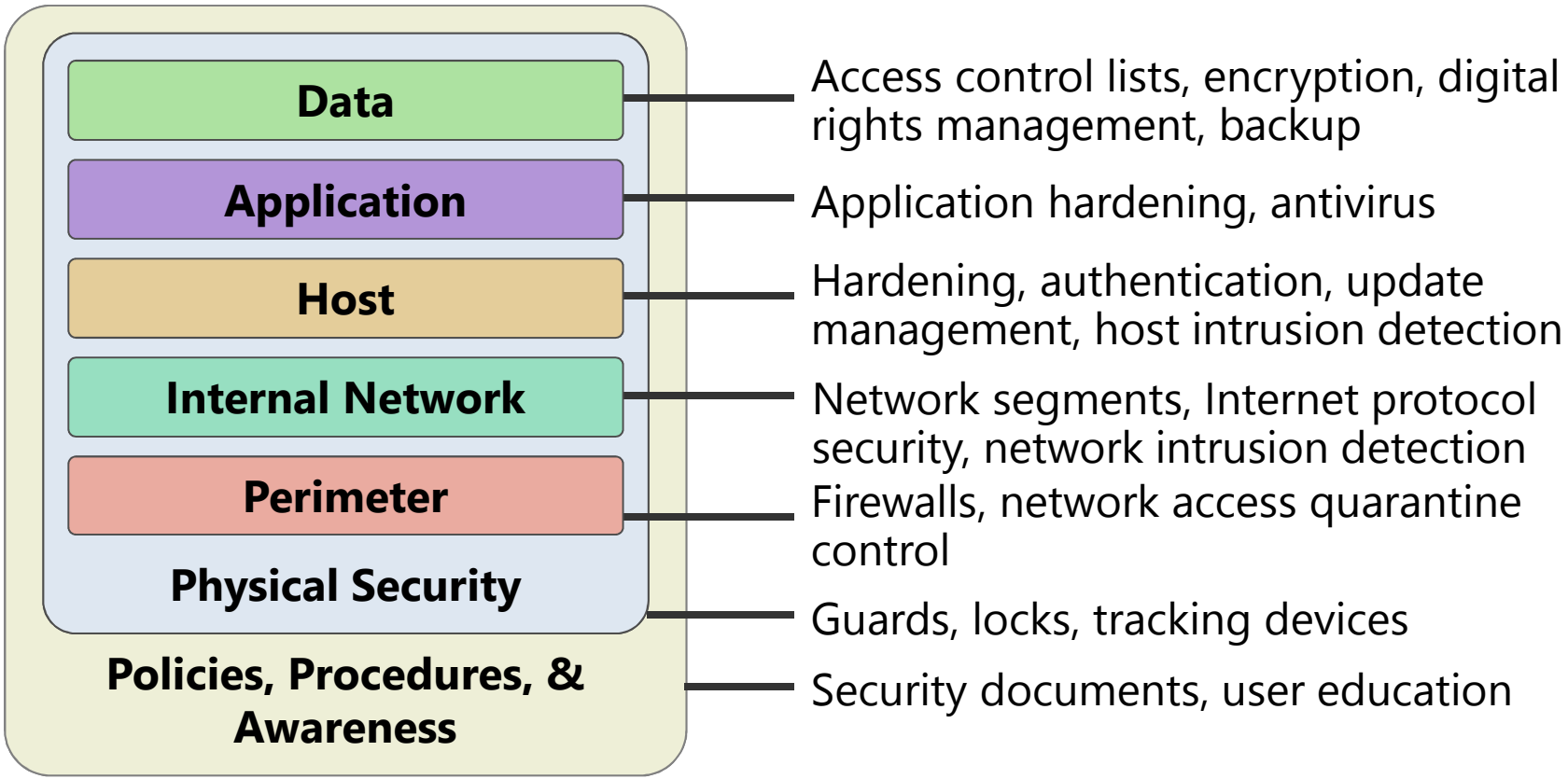
- Overview of Defense-in-Depth
- Physical Security
- Internet Security

Lesson 1: Overview of Defense-in-Depth

- What Is Defense-In-Depth?
- Policies, Procedures, and Awareness
- Physical Layer Security
- Perimeter Layer Security
- Internal Network Layer Security
- Host Layer Security
- Application Layer Security
- Data Layer Security

What Is Defense-In-Depth?

- Defense-in-depth uses a layered approach to reduce an attacker's chance of success and increase an attacker's risk of detection



Policies, Procedures, and Awareness

- Policies, procedures, and awareness refers to an organization's formalized, agreed upon commitment to help prevent security incidents from occurring, and to address security issues in the event of a security incident
- Sources of compromise include:
  - Users unaware of rules
  - Users viewing rules as unnecessary
  - Social engineering

Physical Layer Security

- Physical layer security refers to preventing unauthorized physical access to IT infrastructure
- Restricting physical access can prevent someone from:
  - Damaging systems
  - Installing unauthorized software
  - Modifying data
  - Stealing data
  - Stealing hardware

Perimeter Layer Security

- Perimeter layer security refers to connectivity between your network and other untrusted networks
- Perimeter layer compromise includes:
  - Attacks on resources in a perimeter network
  - Attacks on remote clients
  - Attacks on business partners

Internal Network Layer Security

- Internal network layer security refers to safeguarding the infrastructure that is directly managed and controlled by your organization, including WAN endpoints
- Internal network layer compromise includes:
  - Unauthorized network communication
  - Unauthorized network hosts
  - Unauthorized packet sniffing
  - Compromising default network device configurations

Host Layer Security

- The host layer refers to the individual infrastructure devices such as computers, switches, and routers on your network
- Host layer compromise can be:
  - Exploiting operating system flaws
  - Exploiting default operating system configurations
  - Accomplished by a virus

Application Layer Security

- The application layer refers to the specialized software running on the hosts
- Application layer compromise can be:
  - Exploiting application flaws
  - Exploiting application default configurations
  - Viruses introduced by a user
  - Programming vulnerabilities

Data Layer Security

- The data layer refers to the information stored on your computers
- Data layer compromise can be:
  - Unauthorized access to data files
  - Unauthorized access to AD DS
  - Modification of application files

Lesson 2: Physical Security

- What Are the Physical Security Risks?
- Implementing Physical Security with Windows Server Tools
- Physical Security Best Practices

What Are the Physical Security Risks?

The main physical security risks to your networked computers are data compromise resulting from:

- Loss or theft of your server computers or server storage devices
- Unmanaged computers connecting to your network
- Introduction of storage devices into your network that can contain malicious software

Implementing Physical Security with Windows Server Tools

- Windows Server provides a number of tools and features that can help you implement physical security
- Windows Server provides:
  - Encrypting File System
  - BitLocker Drive Encryption
  - Read-Only Domain Controllers
  - Group Policies
  - Network Access Protection
  - Access Control

Physical Security Best Practices

- To help to reduce the physical security risks, consider the following points:
  - Site security
  - Computer security
  - Disable Log On Locally
  - Mobile device security
  - Removable devices and drives

Lesson 3: Internet Security

- What Are the Risks?
- Mitigating Risks
- Implementing Internet Security with Windows
- Internet Explorer Security Settings
- Demonstration: How to Secure Internet Explorer

What Are the Risks?

- When you connect your computer to the Internet you expose it to numerous potential security risks
- The security risks depend upon the applications:
  - Email
  - Web browsing
  - Instant messaging
  - Social networking
  - File download
  - Computer updates

Mitigating Risks

- When you connect your computer to the Internet, observe the defense-in-depth approach to help protect your computer
- Consider the following to help mitigate security risks:
  - Implement antivirus, anti-spam, and attachment handling in email
  - Implement antivirus and anti-malware protection in your web browser
  - Enable virus protection in IM conversations
  - Only download files with digital signatures or from a trusted source
  - Obtain computer updates that are signed and from a trusted source
  - Use a host-based firewall
  - Ensure that your router connects securely to the Internet
  - Be cautious about divulging sensitive personal or financial information

Implementing Internet Security with Windows

Windows-based operating systems provide a number of security features that help ensure that connectivity to the Internet is more secure

- User Account Control
- Windows Firewall
- Windows Defender

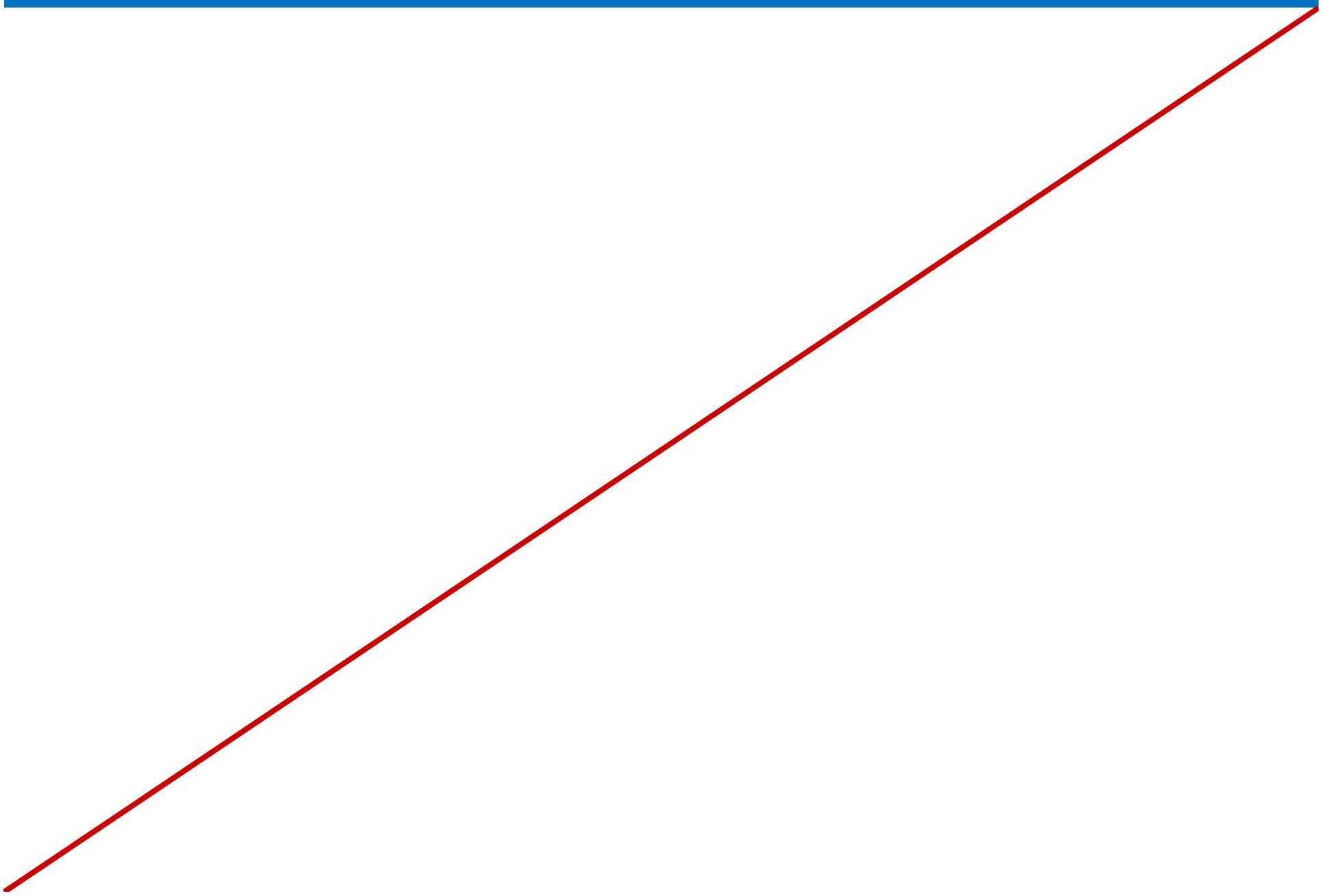
Internet Explorer Security Settings

- Internet Explorer security options help you secure your computer while providing a functional browsing environment
  - ActiveX Filtering
  - Protected Mode
  - Parental Controls
  - Manage Add-ons
  - SmartScreen Filter

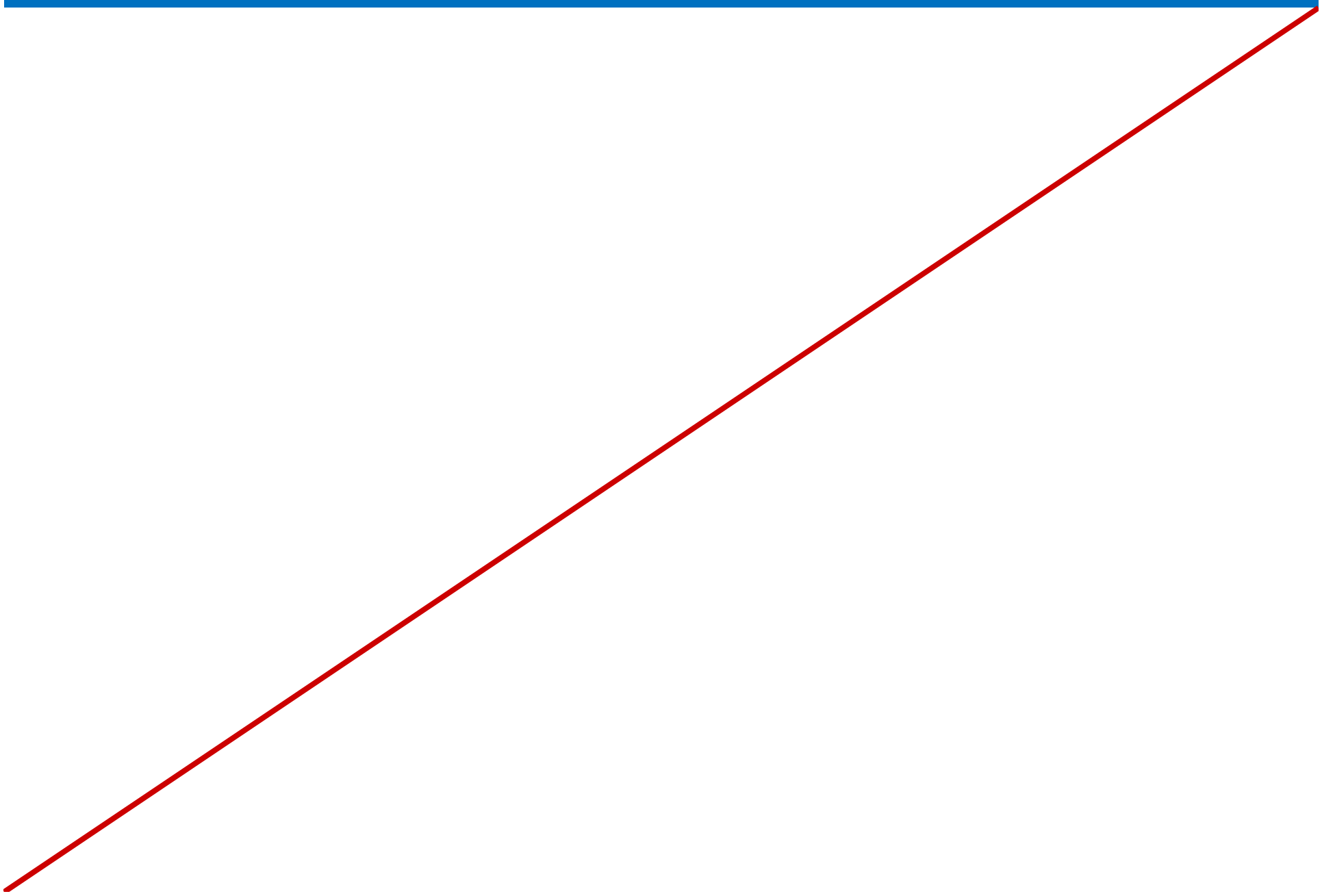
Demonstration: How to Secure Internet Explorer

- In this demonstration, you will see how to disable an Internet Explorer add-on

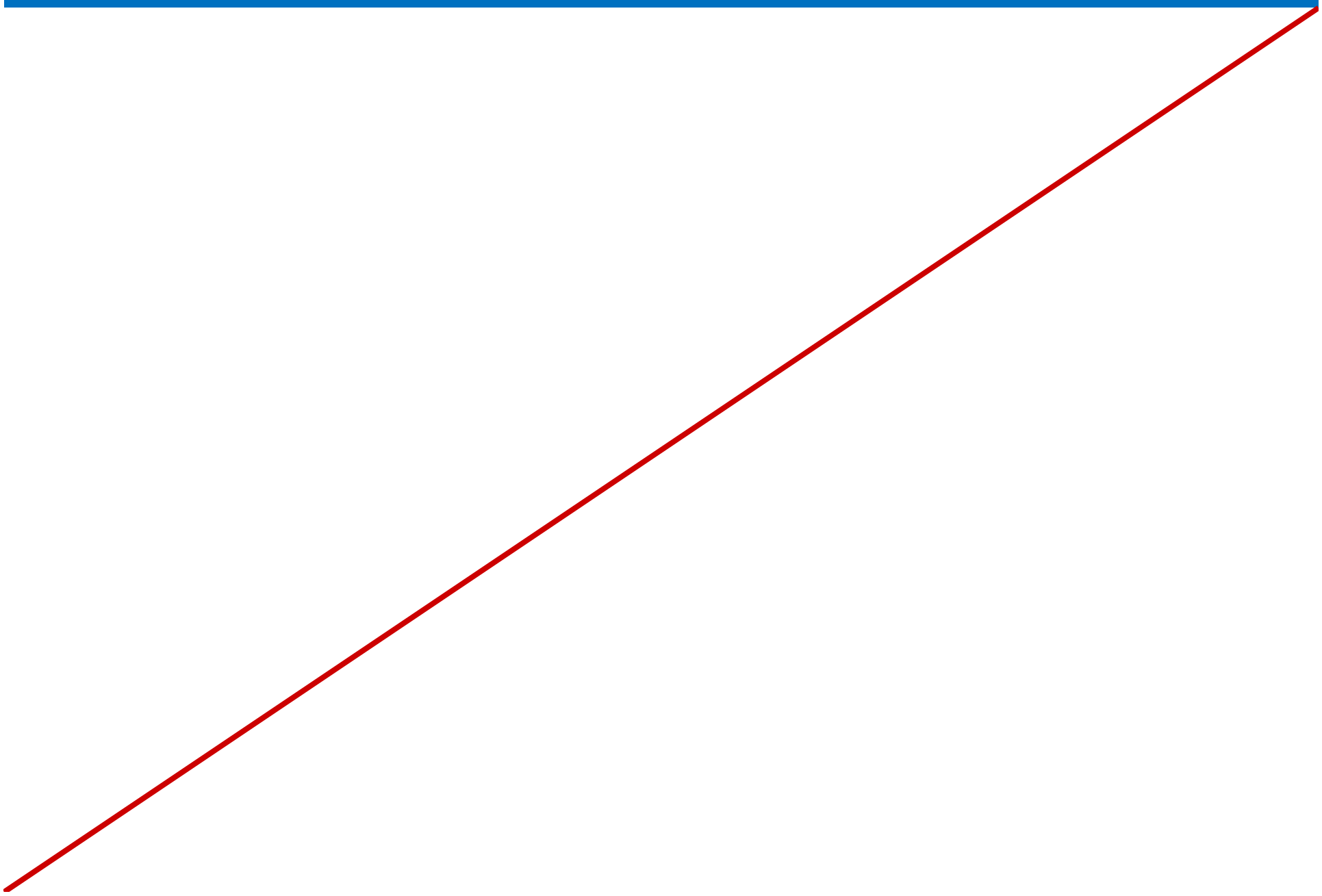
Notes Page Over-flow Slide. Do Not Print Slide.



Notes Page Over-flow Slide. Do Not Print Slide.



Notes Page Over-flow Slide. Do Not Print Slide.



Lab: Implementing IT Security Layers

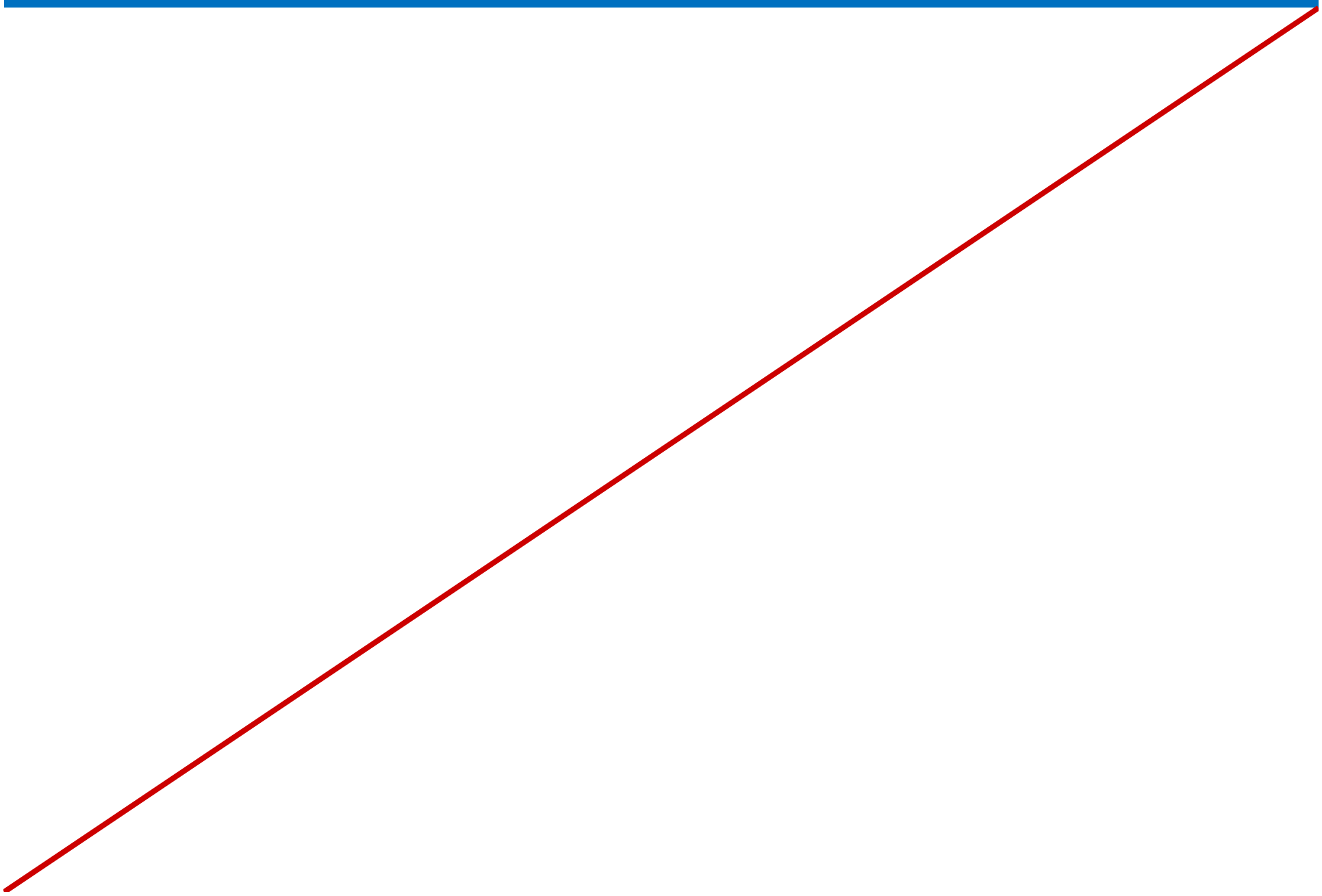
- Exercise 1: Implementing Physical Security
- Exercise 2: Configuring Security Settings in Windows® Internet Explorer®

Logon Information

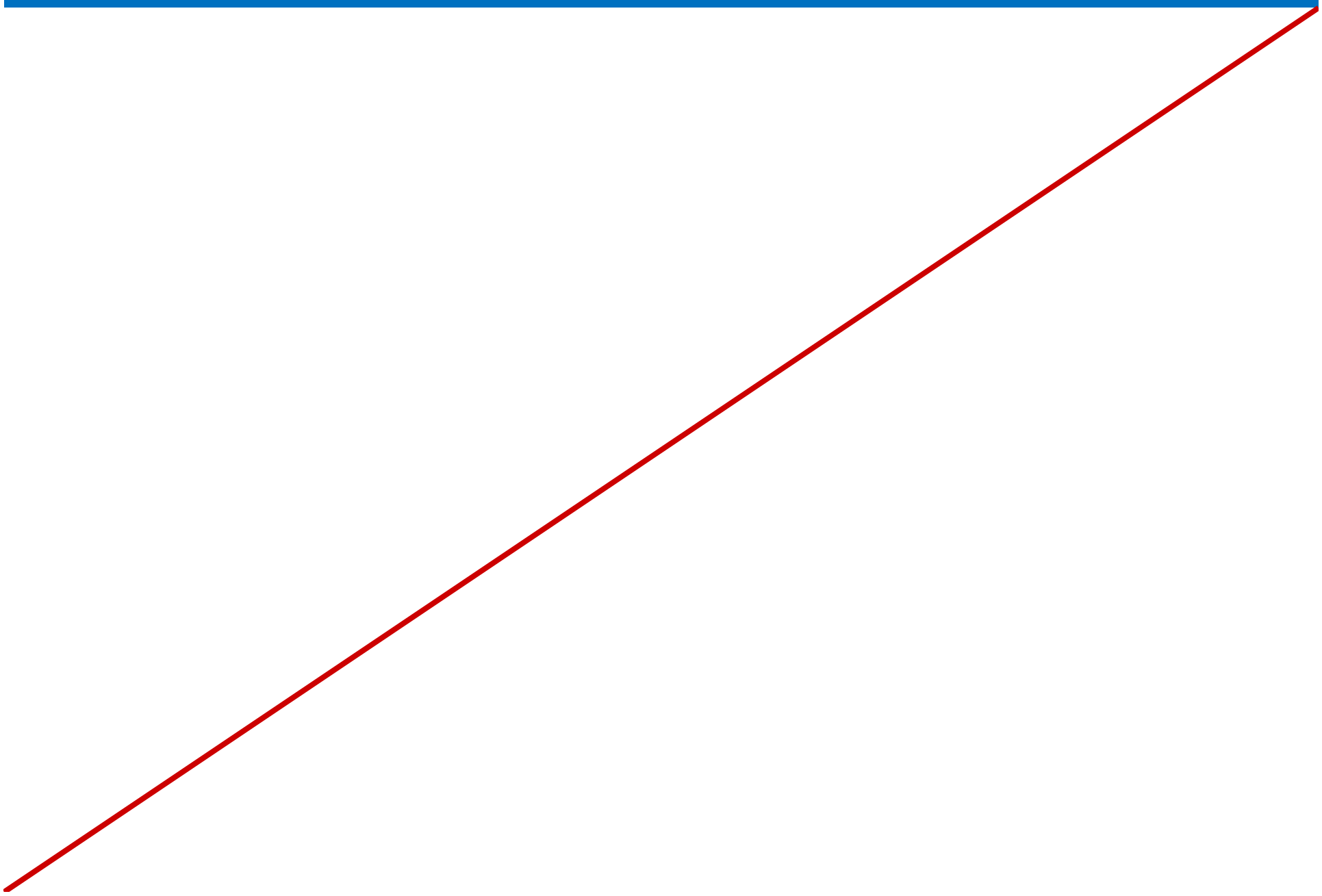
Virtual Machines: 10967A-LON-DC1
User Name : ADATUM\Administrator
Password : Pa$$w0rd

Estimated Time: 30 minutes

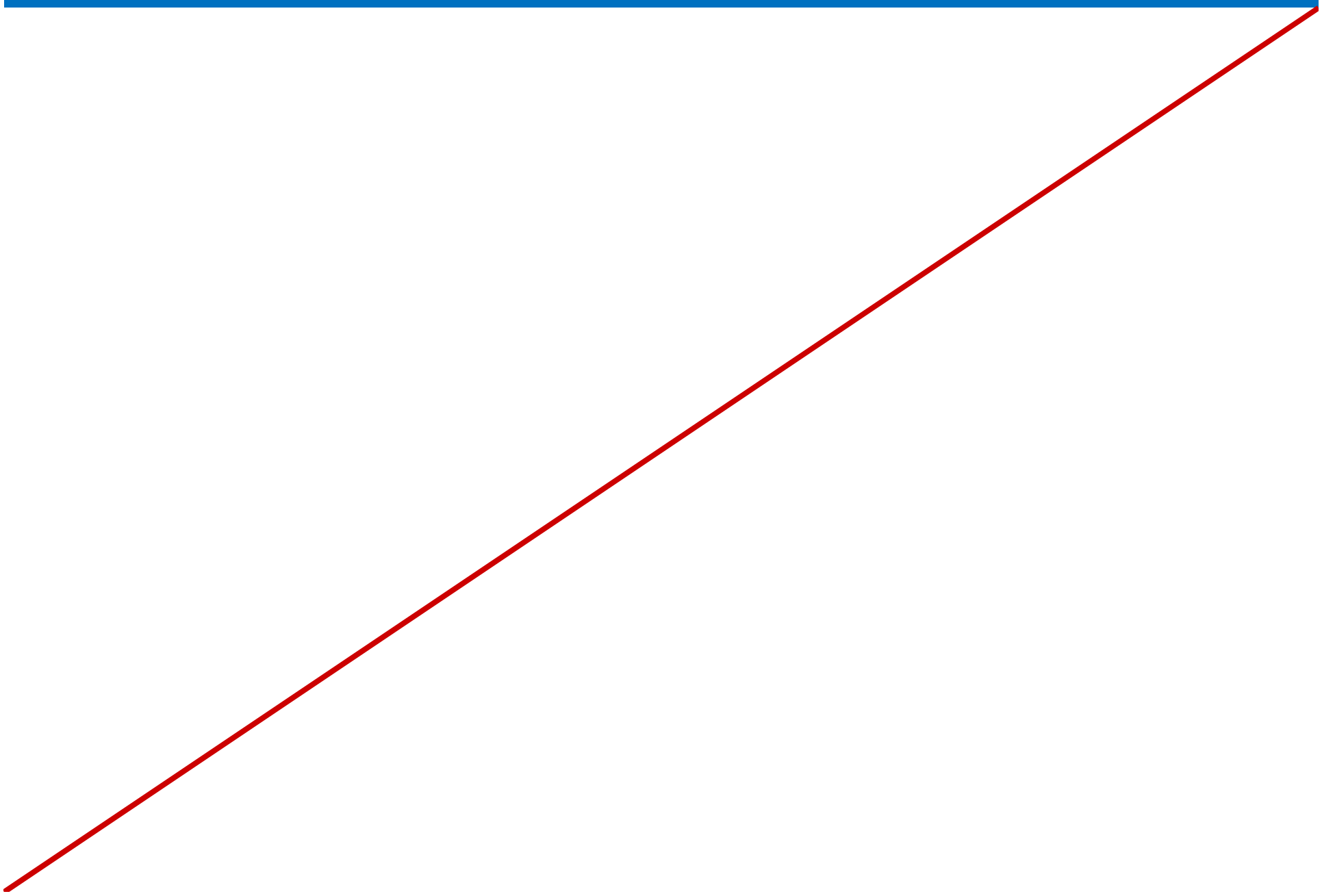
Notes Page Over-flow Slide. Do Not Print Slide.



Notes Page Over-flow Slide. Do Not Print Slide.



Notes Page Over-flow Slide. Do Not Print Slide.



Lab Scenario

Alan Brewer has visited various Research department branch offices. On his return to head office, he produced a list of security concerns and sent them by email to Ed Meadows, your boss. Ed has tasked you with the resolution of these issues.

Lab Review

- In the lab, you were concerned primarily with physical security concerns. What potential support issues might arise following implementation of your proposed changes? Specifically, what issues might arise surrounding the encryption of files and volumes and the prohibition of USB storage devices?

Module Review and Takeaways

- Review Questions
- Best Practice

Notes Page Over-flow Slide. Do Not Print Slide.