
DR. KAMI VANIEA
First, the news...

- First 5 minutes we talk about something interesting and recent
- You will not be tested on the news part of lecture
- You may use news as an example on tests
- Why do this?
  1. Some students show up late
  2. Reward students who show up on time
  3. Important to see real world examples
Security properties
Defining Security

• Confidentiality
  ◦ Ensures that computer-related assets are accessed only by authorized parties.

• Integrity
  ◦ Assets can be modified only by authorized parties or only in authorized ways.

• Availability
  ◦ Assets are accessible to authorized parties at appropriate times.
Security is a whole system issue

- Software
- Hardware
- Physical environment
- Personnel
- Corporate and legal structures

<table>
<thead>
<tr>
<th>Security properties to ensure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidentiality</strong></td>
<td>No improper information gathering</td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td>Data has not been (maliciously) altered</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>Data/services can be accessed as desired</td>
</tr>
<tr>
<td><strong>Accountability</strong></td>
<td>Actions are traceable to those responsible</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>User or data origin accurately identifiable</td>
</tr>
</tbody>
</table>
BRUCE WAYNE/BATMAN’S THREAT MODEL

ASSETS
- BAT CAVE
- ALFRED
- EMAILS
- TEXTS

PROTECTION
- SECURITY SYSTEM
- HIDE LOCATION
- ENCRYPTION

THREATS
- POLICE
- THE JOKER
- JOURNALISTS

Think-pair-share

• **Think** quietly to yourself for 1 minute
• **Pair** and discuss with your neighbor for 3 minutes
• **Share** with the class – group discussion
A classic data breach

1. Employee is sent a phishing email with a link to a realistic looking internal site.

2. Employee opens the email, clicks the link, and types in her user name and password.

3. Malicious site collects the password and shows the user that everything is actually fine so they are not suspicious.

4. Malicious actor uses user name and password to download sensitive files.
10 Steps To Cyber Security

Defining and communicating your Board’s Information Risk Management Regime is central to your organisation’s overall cyber security strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.

- **Network Security**: Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

- **Malware Protection**: Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

- **Establish an effective governance structure and determine your risk appetite.**

- **Home and Mobile Working**: Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

- **Secure Configuration**: Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

- **Removable Media Controls**: Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing it to the corporate system.

- **Monitoring**: Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.

- **Produce supporting information risk management policies.**

- **Managing User Privileges**: Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

- **Incident Management**: Establish an incident response and disaster recovery capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

- **User Education and Awareness**: Produce user security policies covering acceptable and secure use of the organisation’s systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

**Information Risk Management Regime**
10 large steps are too complex for small companies....
10 Steps To Cyber Security

Defining and communicating your Board’s Information Risk Management Regime is central to your organisation’s overall cyber security strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.

- **Network Security**: Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

- **Malware Protection**: Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

- **User Education and Awareness**: Produce user security policies covering acceptable and secure use of the organisation’s systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

- **Home and Mobile Working**: Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

- **Secure Configuration**: Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

- **Removable Media Controls**: Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing on to the corporate system.

- **Information Risk Management Regime**: Establish an effective governance structure and determine your risk appetite. Maintain the Board’s engagement with the cyber risk.

- **Incident Management**: Establish an incident response and disaster recovery capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

- **Producing Information Risk Management Policies**: Produce supporting information risk management policies.

- **Managing User Privileges**: Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.
Cyber Security Essentials

It requires...

**FIVE MANDATORY CONTROLS:**

- Secure configuration
- Boundary firewalls and internet gateways
- Access control and administrative privilege management
- Patch management
- Malware protection
Cyber Essentials Certification

- Self-assessment
- External vulnerability scan by an approved tester
- Internal vulnerability scan by an approved tester

**How it works...**

1. **Self-Assessment Questionnaire**
2. **External vulnerability scan**
   - External full TCP port and top UDP service scan for stated IP range
   - Vulnerability scan for stated IP range
   - Basic web application scanning for common vulnerabilities
   
   * According to CREST-accredited Certification Bodies.
3. **Internal vulnerability scan and on-site assessment**
   - Inbound email binaries and payloads
   - Inbound emails containing URLs linking to binaries and browser exploitation payloads
   - Authenticated vulnerability and patch verification scan
Cyber Essentials provides a good summary of what basic level protection looks like.
Cyber Essentials Controls
Sample Network

- User
- User
- Mobile Devices
- Wireless Access Point
- Desktop PCs and laptops
- Card Readers
- Email, web and application servers
- Databases
- 3rd party server
- Personal Devices
- Home PC
- Home Router
- Internet
- Boundary Firewall
- Router
- Home Network Card
- Readers
More Secure Sample Network
“A system which is unspecified can never be wrong, it can only be surprising.”
Cyber Security Essentials

It requires...

FIVE MANDATORY CONTROLS:

- Secure configuration
- Boundary firewalls and internet gateways
- Access control and administrative privilege management
- Patch management
- Malware protection
Secure Configuration

Objectives: Computers and network devices should be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.

• Default settings are not necessarily secure.
• Predefined passwords can be widely known.
Secure Configuration

1. Unnecessary user accounts should be removed or disabled.
2. Any default password for a user account should be changed to an alternative, strong password.
3. Unnecessary software should be removed or disabled.
4. The auto-run feature should be disabled.
5. A personal firewall (or equivalent) should be enabled on desktop PCs and laptops, and configured to disable (block) unapproved connections by default.
Sample Network

Scope boundary

User

Mobile Devices

Wireless Access Point

Desktop PCs and laptops

Card Readers

Email, web and application servers

Databases

Boundary Firewall

3rd party server

Internet

Home PC

Personal Devices

Home Router

Desktop PC

laptops
Configuration is a real problem

- Misc Errors
- Crimeware
- Insider Misuse
- Physical Theft/Loss
- Web App Attacks
- Denial of Service
- Cyber-espionage
- POS Intrusions
- Payment Card Services

Verizon 2015 Data Breach Investigations Report
Cyber Security Essentials

It requires...

FIVE MANDATORY CONTROLS:

- Secure configuration
- Boundary firewalls and internet gateways
- Access control and administrative privilege management
- Patch management
- Malware protection
Boundary firewalls and internet gateways

Objectives: Information, applications and computers within the organization's internal networks should be protected against unauthorized access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices.

• Boundary devices are the first line of defense.
• Firewall rules can be used to stop basic attacks before they even reach the internal network.
Sample Network

- User
- Mobile Devices
  - Wireless Access Point
- Desktop PCs and laptops
- Boundary Firewall
- Personal Devices
  - Home PC
- Boundary devices
  - Home Router
- Internet
- Router
- Email, web and application servers
- Databases
- Card Readers
- 3rd party server
Boundary firewalls and internet gateways

1. Change default administrator passwords for all network devices and firewalls.

2. Each rule that allows network traffic to pass through the firewall should be subject to approval by an authorized individual and documented.

3. Unapproved services, or services that are typically vulnerable to attack, should be disabled (blocked) by the boundary firewall by default.

4. Firewall rules that are no longer required should be removed or disabled in a timely manner.

5. The administrative interface used to manage boundary firewall configuration should not be accessible from the internet.
Windows 8 Firewall rules
Cyber Security Essentials

It requires...

FIVE MANDATORY CONTROLS:

- Secure configuration
- Boundary firewalls and internet gateways
- Access control and administrative privilege management
- Patch management
- Malware protection
Access control and administrative privilege management

Objectives: User accounts, particularly those with special access privileges should be assigned only to authorized individuals, managed effectively and provide the minimum level of access to applications, computers and networks.

• Principle of least privilege – only give users access they need.
• Admin accounts have the most access, if one gets compromised it can lead to large scale loss of information.
Access control and administrative privilege management

1. All user account creation should be subject to a provisioning and approval process.
2. Special access privileges should be restricted to a limited number of authorized individuals.
3. Details about special access privileges should be documented, kept in a secure location and reviewed on a regular basis.
4. Admin accounts should only be used to perform legitimate admin activities, and should not be granted access to email or the internet.
5. Admin accounts should be configured to require a password change on a regular basis.
6. Each user should authenticate using a unique username and strong password before being granted access to applications, computers and network devices.
7. User accounts and special access privileges should be removed or disabled when no longer required or after a pre-defined period of inactivity.
One of the US companies that manages credit scores sold data to a person who ran an online ID Theft service.

Cyber Security Essentials

It requires...

FIVE MANDATORY CONTROLS:

- Secure configuration
- Boundary firewalls and internet gateways
- Access control and administrative privilege management
- Patch management
- Malware protection
Patch management

Objectives: Software running on computers and network devices should be kept up-to-date and have the latest security patches installed.

- Vulnerabilities in software are patched through updates.
- If you don’t install the update, the vulnerability is not patched.
- However, patching can cause compatibility problems. So you should always test the patches.
Patch management

1. Software running on computers and network devices on the internet should be licensed and supported to ensure security patches for known vulnerabilities are made available.
2. Updates to software running on computers and network devices should be installed in a timely manner.
3. Out-of-date software should be removed.
4. All security patches for software should be installed in a timely manner.
Vulnerability survival

- The % of computers patched X days after disclosure.

Heartbleed

- 600,000 vulnerable serves initially
- 300,000 vulnerable one month later
- 300,000 vulnerable two months later
- 200,000 vulnerable one year later

Cyber Security Essentials

It requires...

FIVE MANDATORY CONTROLS:

- Secure configuration
- Boundary firewalls and internet gateways
- Access control and administrative privilege management
- Patch management
- Malware protection
Malware protection

Objectives: Computers exposed to the internet should be protected against malware infection through the use of malware protection software.

• Todays Firewalls are very good, most malicious software must be invited in by a user opening an email, browsing a compromised website, or connecting compromised media.

• Protection software continuously monitors the computer for known malicious programs.
Malware protection

• Install anti-malware software on all computers that are connected to or capable of connecting to the internet.
• Update anti-malware software on all computers.
• Configure anti-malware software to scan files automatically upon access and scan web pages when being accessed.
• Regularly scan all files.
• Anti-malware software should prevent connections to malicious websites on the internet.
“Malicious payloads were being delivered to around 300,000 users per hour. The company guesses that around 9 percent of those, or 27,000 users per hour, were being infected.”
“Clients visiting yahoo.com received advertisements served by ads.yahoo.com. Some of the advertisements are malicious ... Instead of serving ordinary ads, the Yahoo's servers reportedly sends users an ‘exploit kit.’”
Questions