Computer Security: Security Basics and Cyber Essentials

DR. KAMI VANIEA

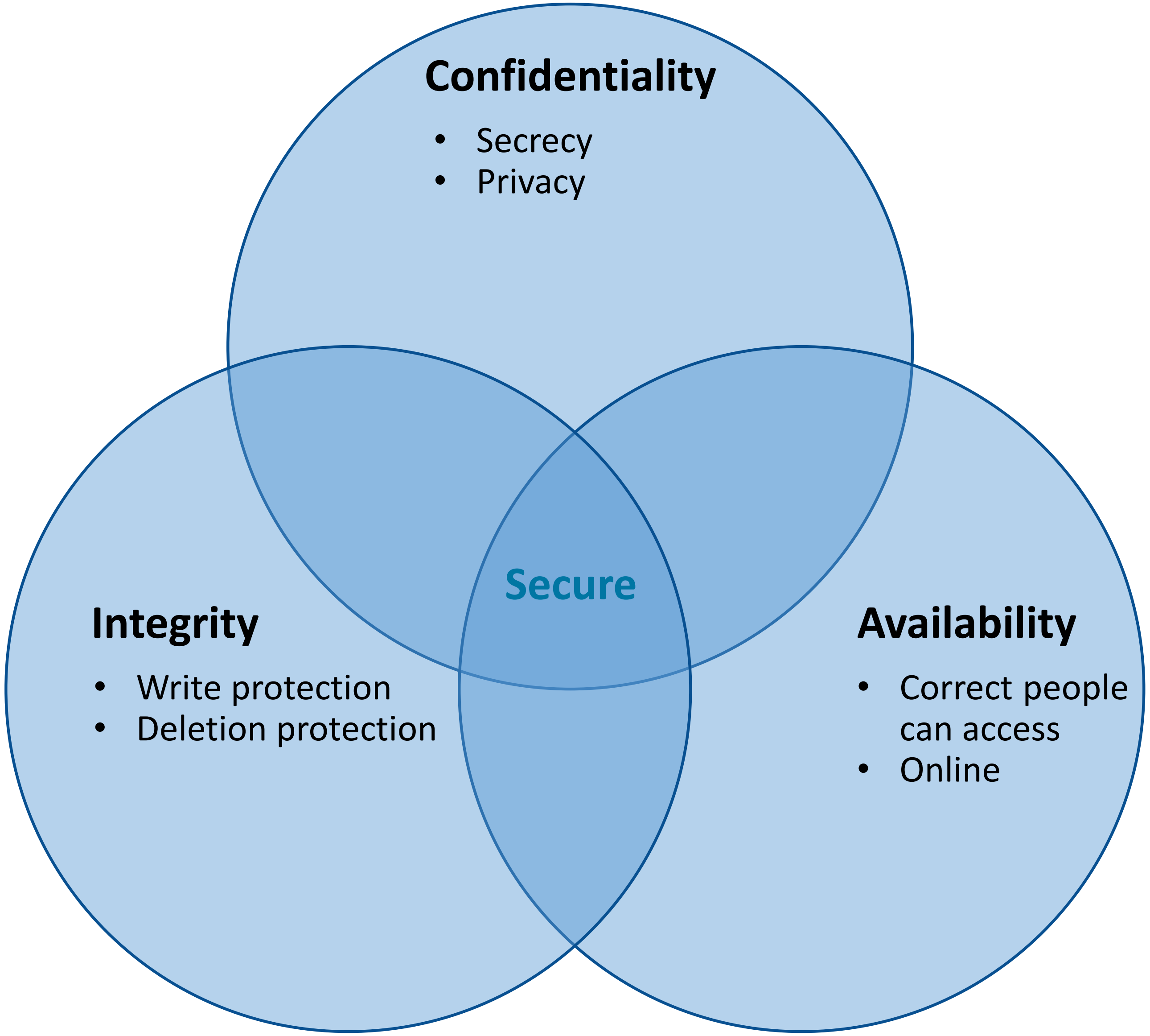
First, the news…

- 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.

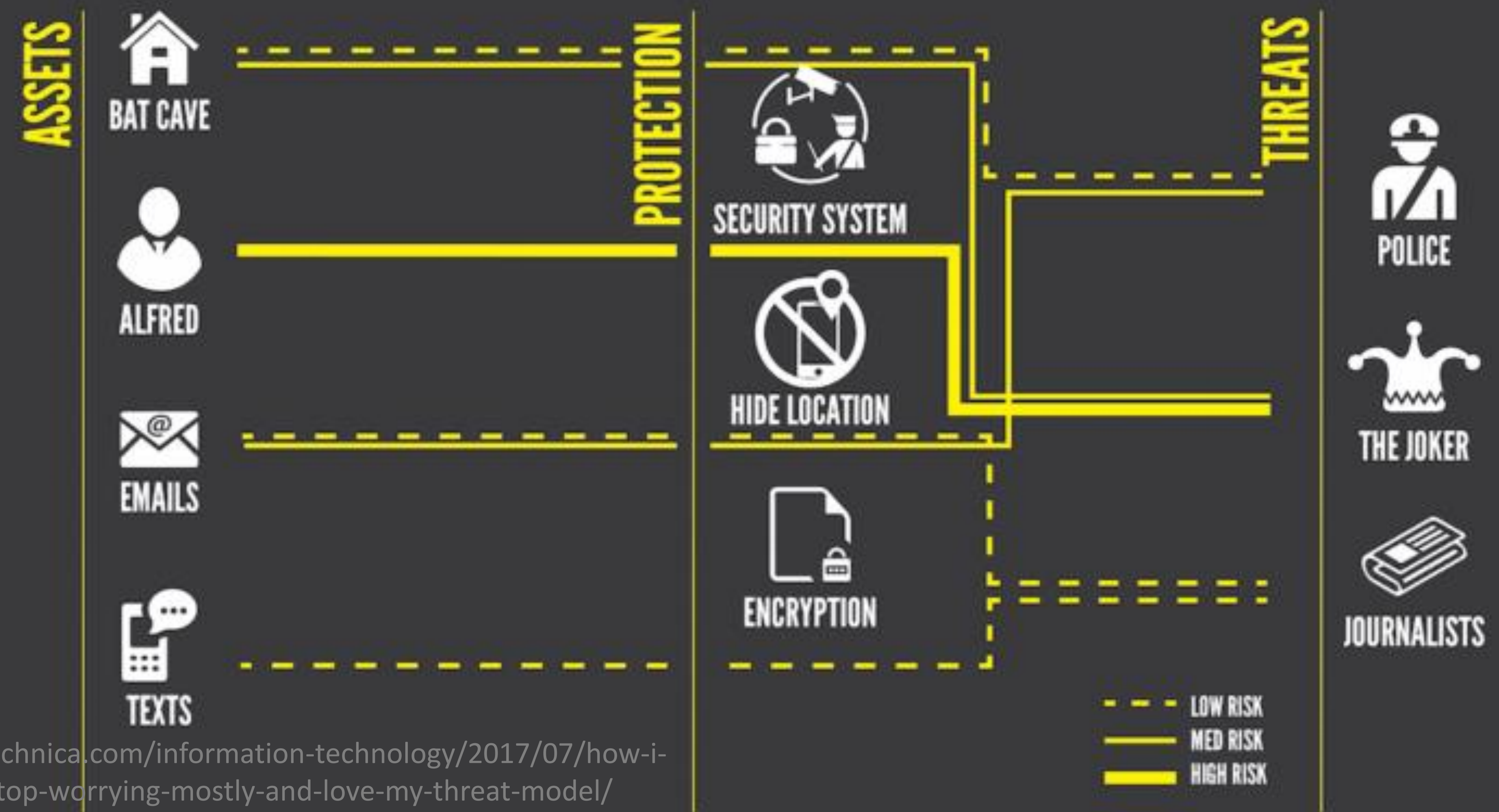


Security is a whole system issue

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

Security properties to ensure	
Confidentiality	No improper information gathering
Integrity	Data has not been (maliciously) altered
Availability	Data/services can be accessed as desired
Accountability	Actions are traceable to those responsible
Authentication	User or data origin accurately identifiable

BRUCE WAYNE/BATMAN’S THREAT MODEL



ASSETS

BAT CAVE

ALFRED

EMAILS

TEXTS

PROTECTION

SECURITY SYSTEM

HIDE LOCATION

ENCRYPTION

THREATS

POLICE

THE JOKER

JOURNALISTS

- - - LOW RISK

—— MED RISK

▬▬ HIGH RISK

https://arstechnica.com/information-technology/2017/07/how-i-learned-to-stop-worrying-mostly-and-love-my-threat-model/

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

CESG

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.

Information Risk Management Regime

Establish an effective governance structure and determine your risk appetite.

Produce supporting information risk management policies.

Maintain the Board's engagement with the cyber risk.

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.

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 recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

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.

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.

Network Security

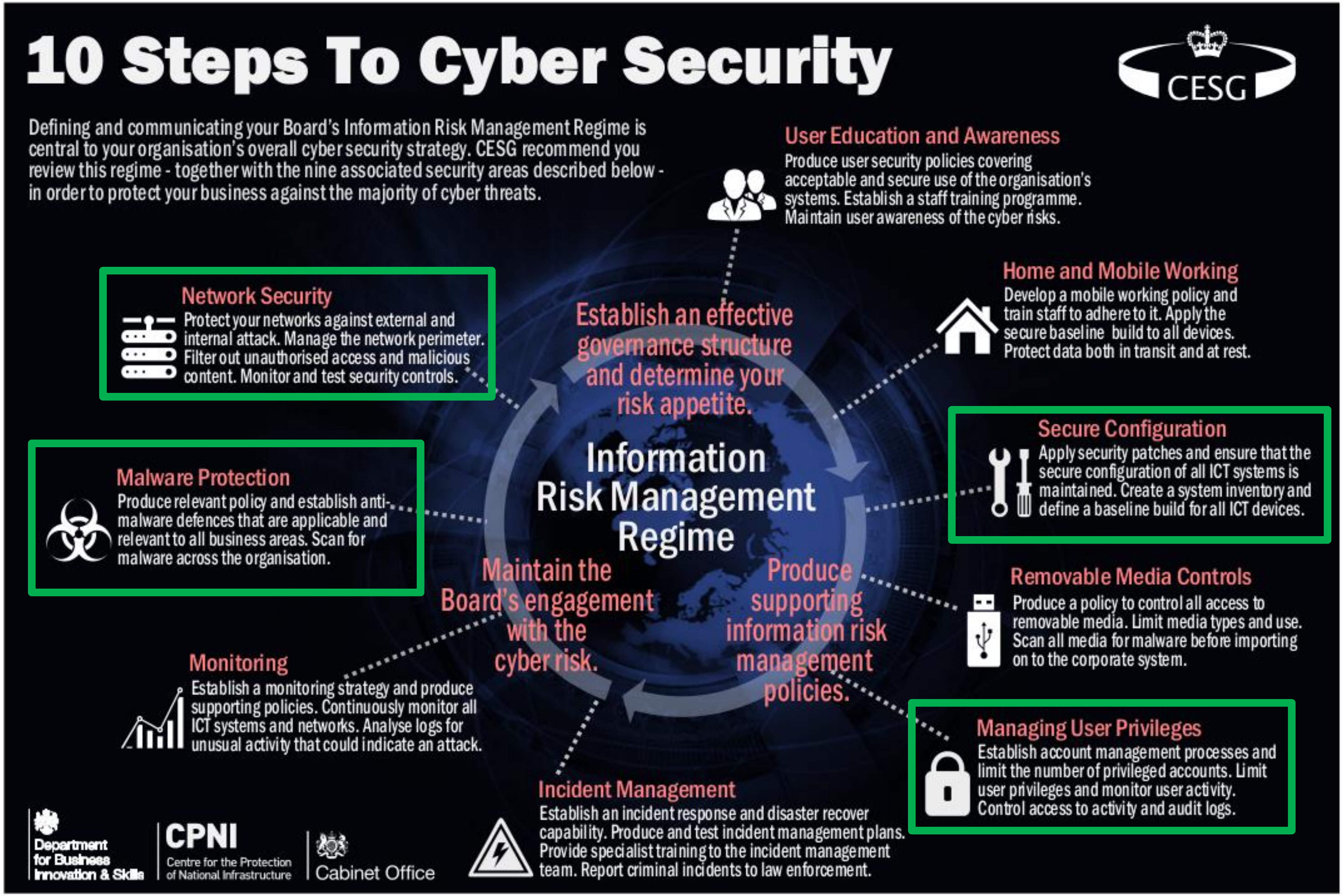
Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

Department for Business Innovation & Skills

CPNI Centre for the Protection of National Infrastructure

Cabinet Office

10 large steps are too complex for small companies….



10 Steps To Cyber Security

CESG

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.

Information Risk Management Regime

Establish an effective governance structure and determine your risk appetite.

Produce supporting information risk management policies.

Maintain the Board's engagement with the cyber risk.

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.

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 recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

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.

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.

Network Security

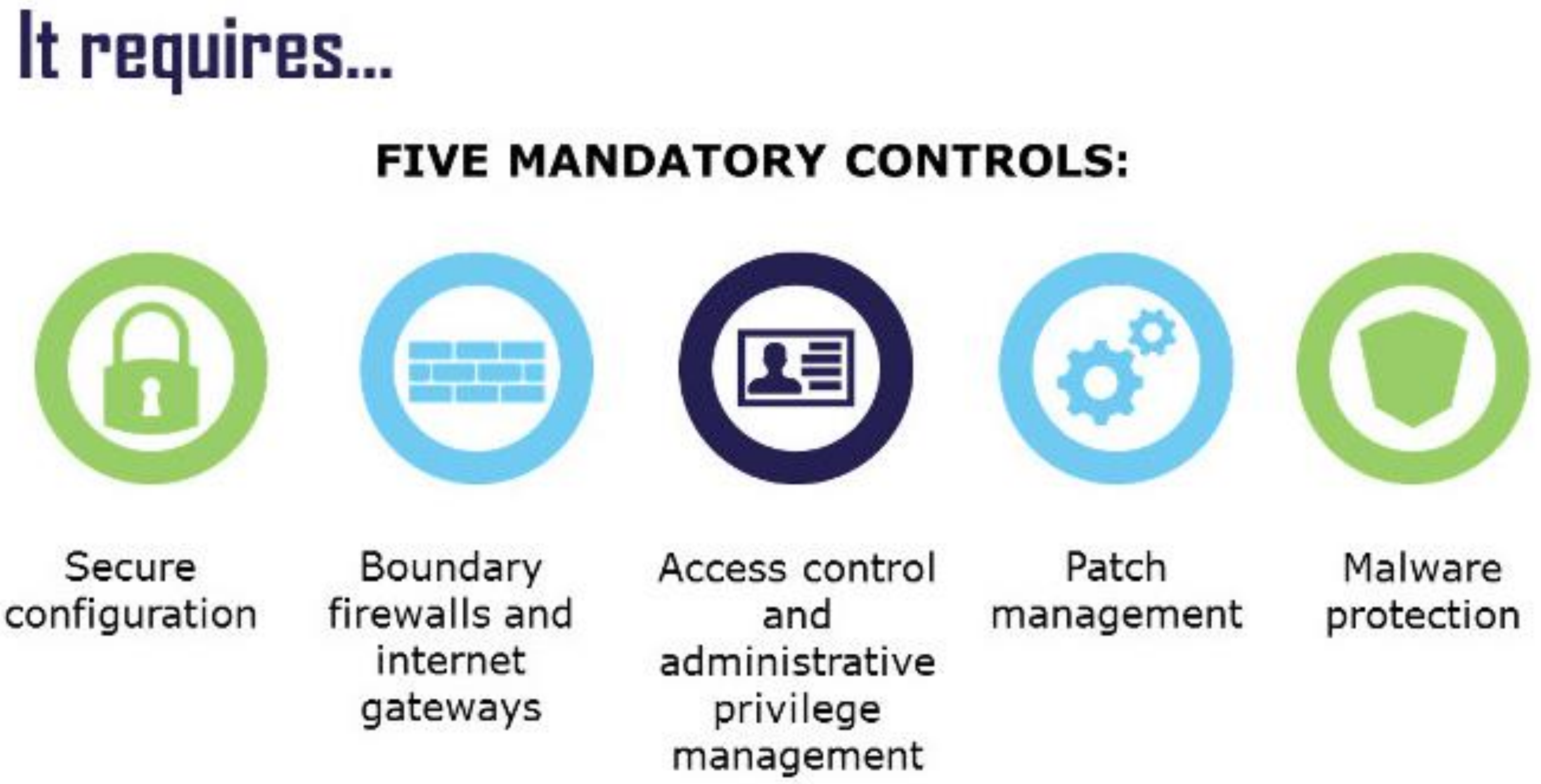
Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

Department for Business Innovation & Skills

CPNI
Centre for the Protection of National Infrastructure

Cabinet Office

Cyber Security Essentials



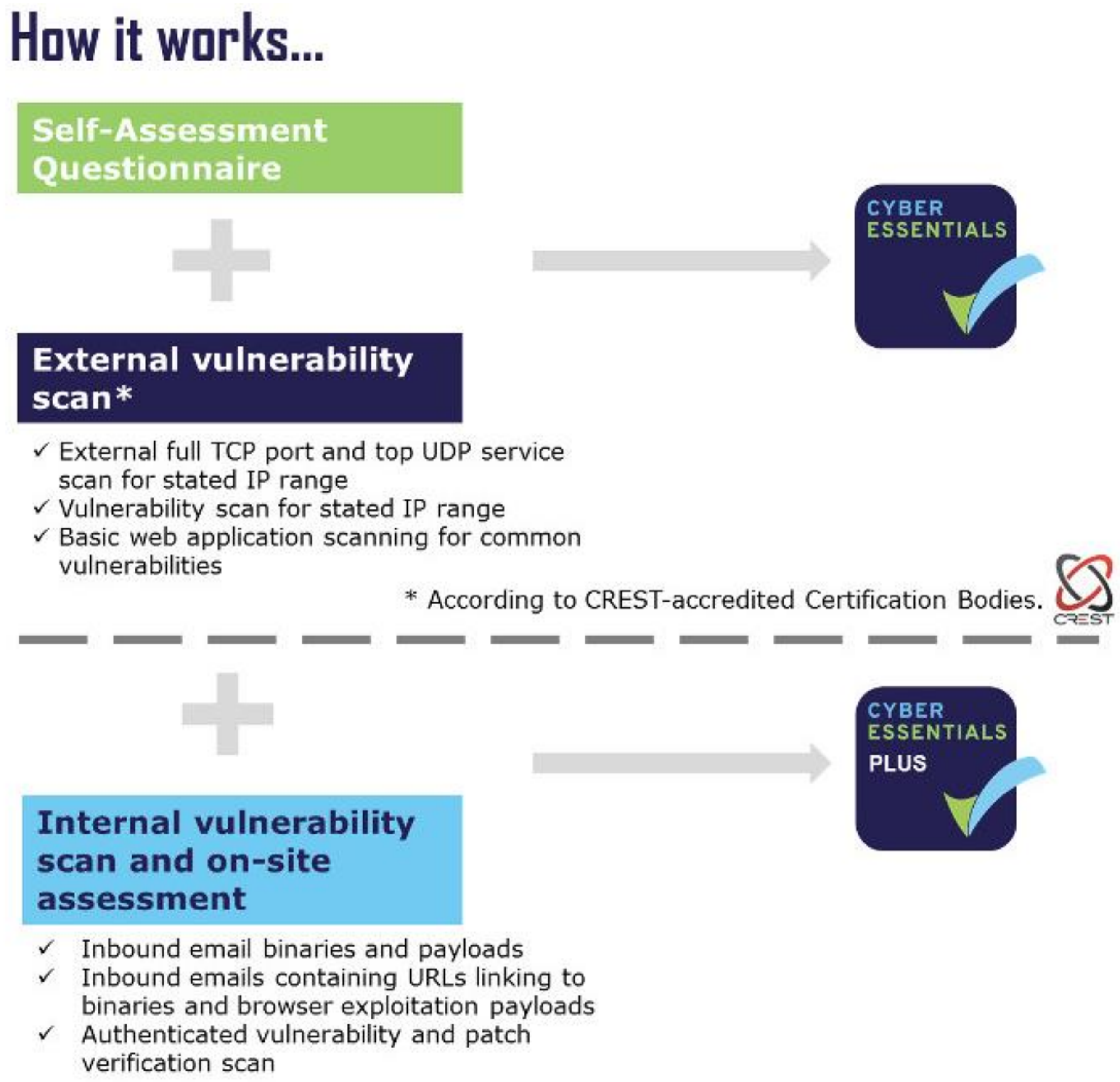
It requires...

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...

Self-Assessment Questionnaire

+

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.

+

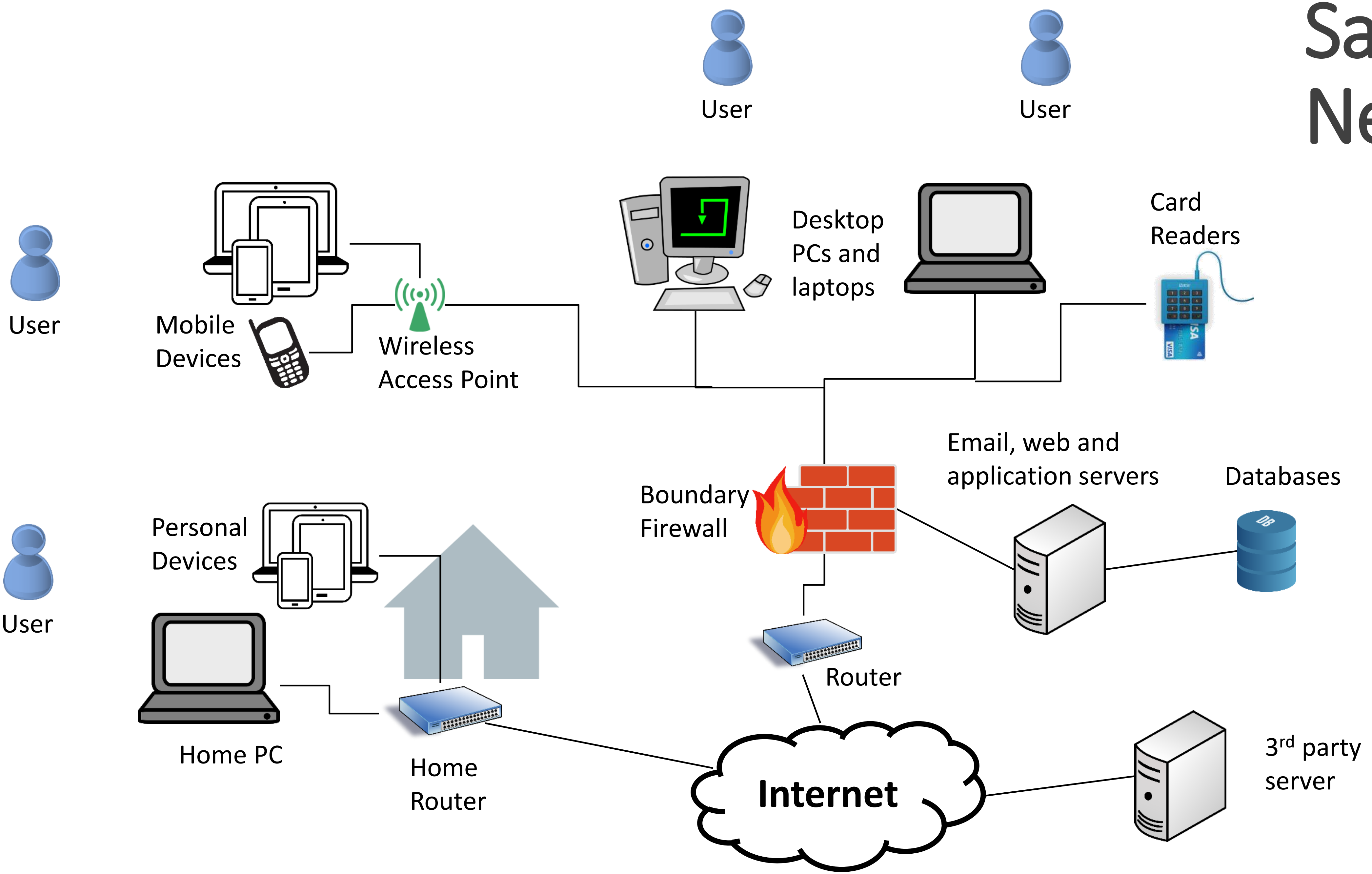
Internal vulnerability scan and on-site assessment

- ✓ Inbound email binaries and payloads
- ✓ Inbound emails containing URLs linking to binaries and browser exploitation payloads
- ✓ Authenticated vulnerability and patch verification scan

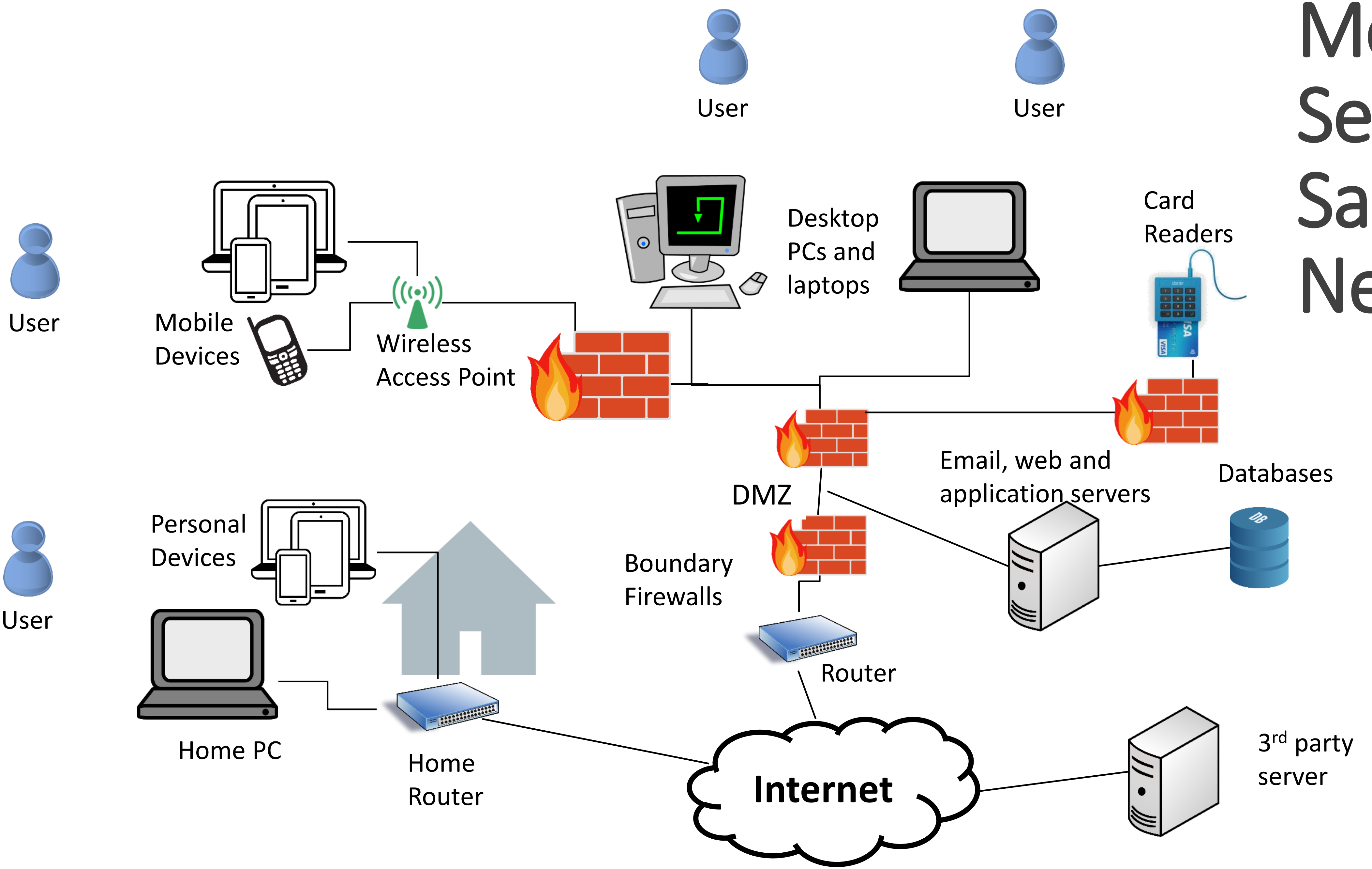
Cyber Essentials provides a good summary of what basic level protection looks like.

Cyber Essentials Controls

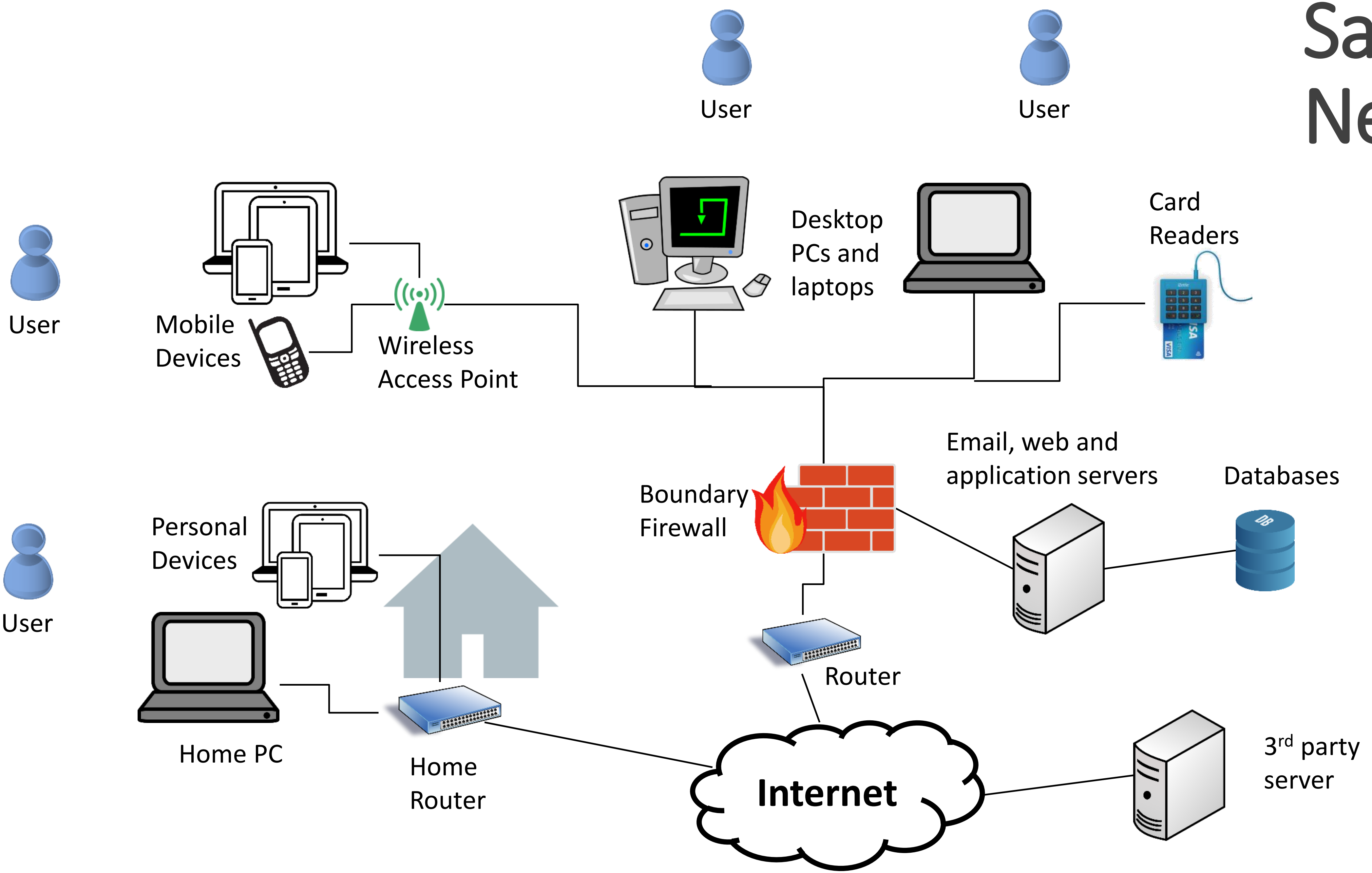
Sample Network



More Secure Sample Network

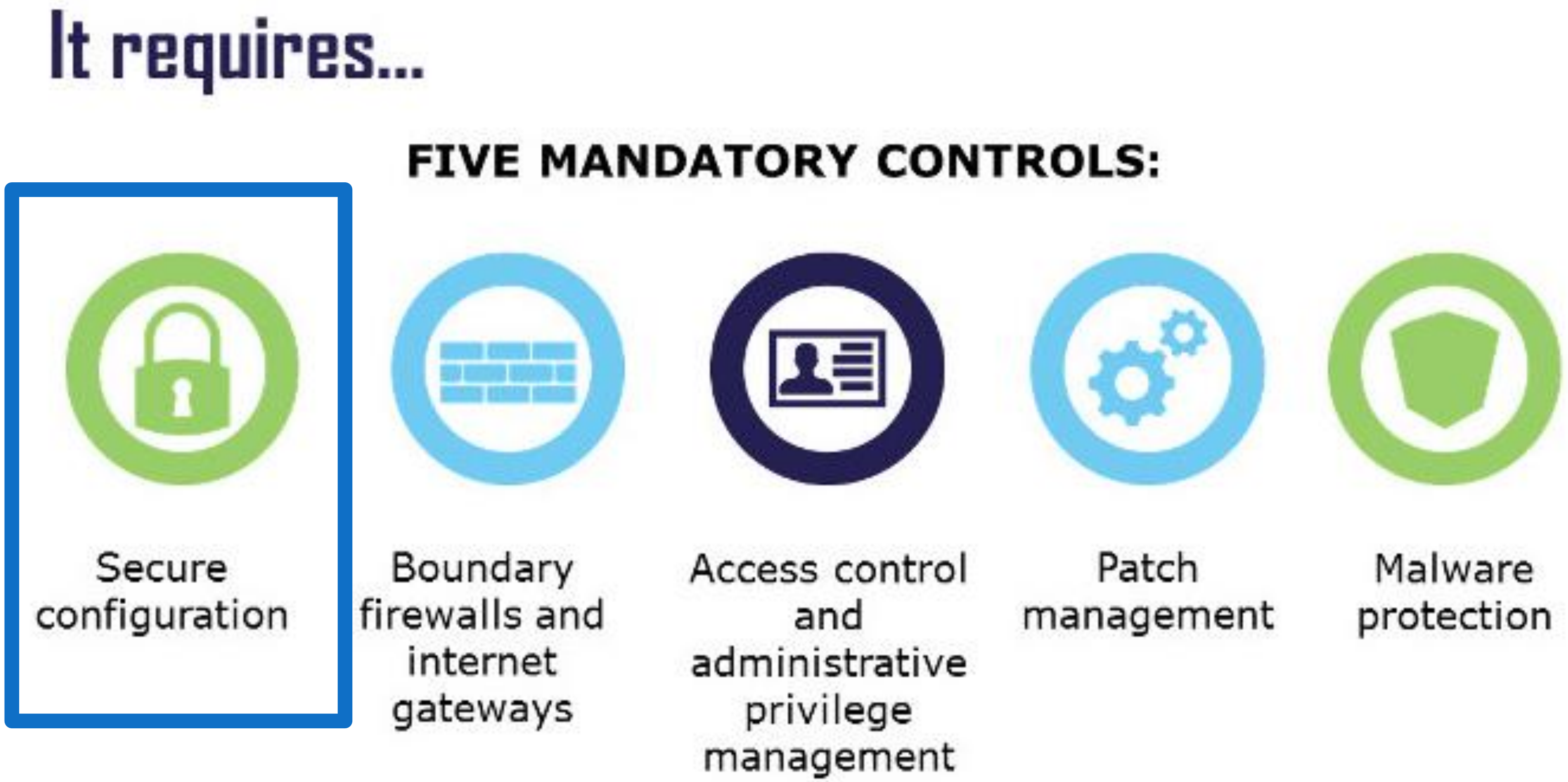


Sample Network



“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

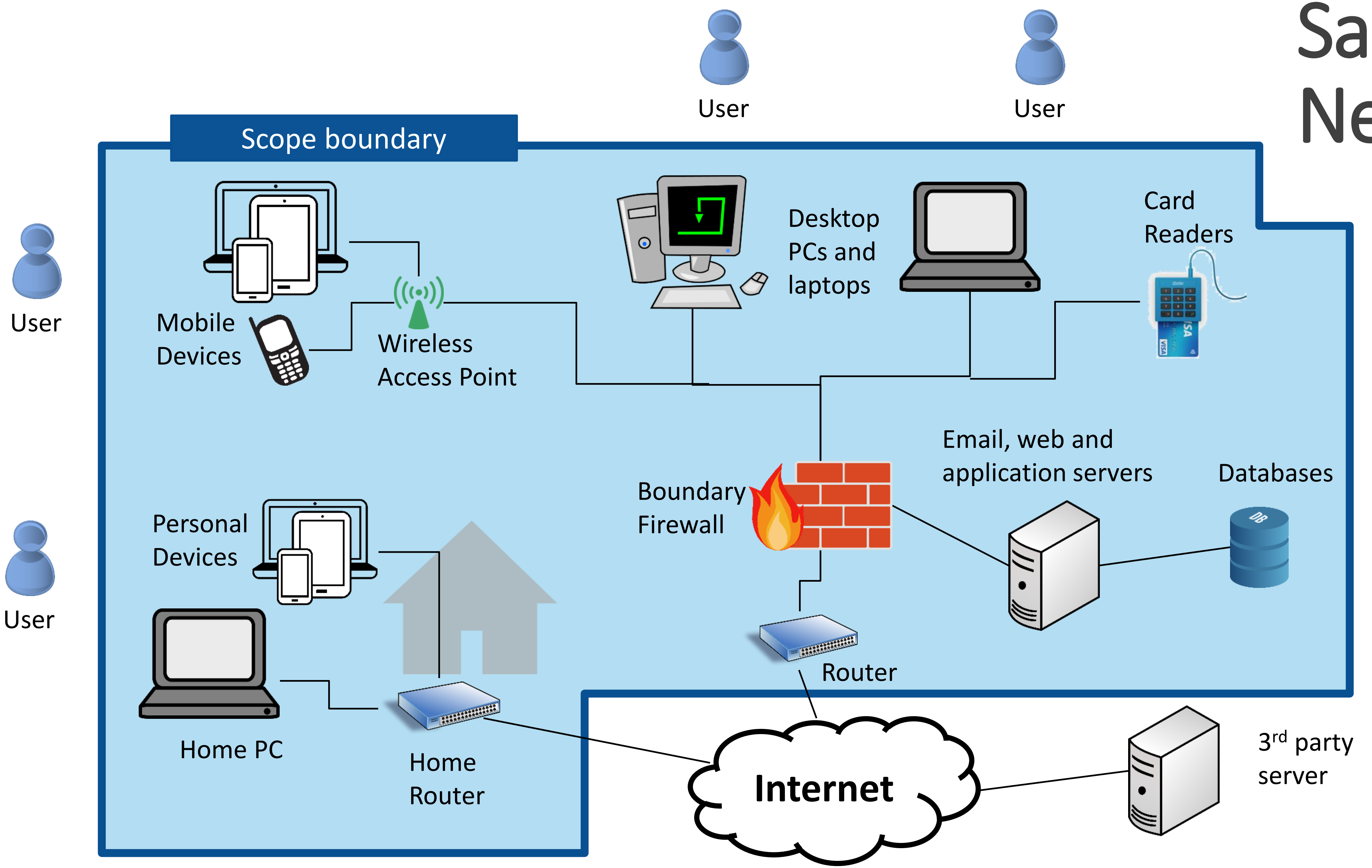
Objectives: Computers and network devices should be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.

- Default settings are not necessarily secure.
- Predefined passwords can be widely known.

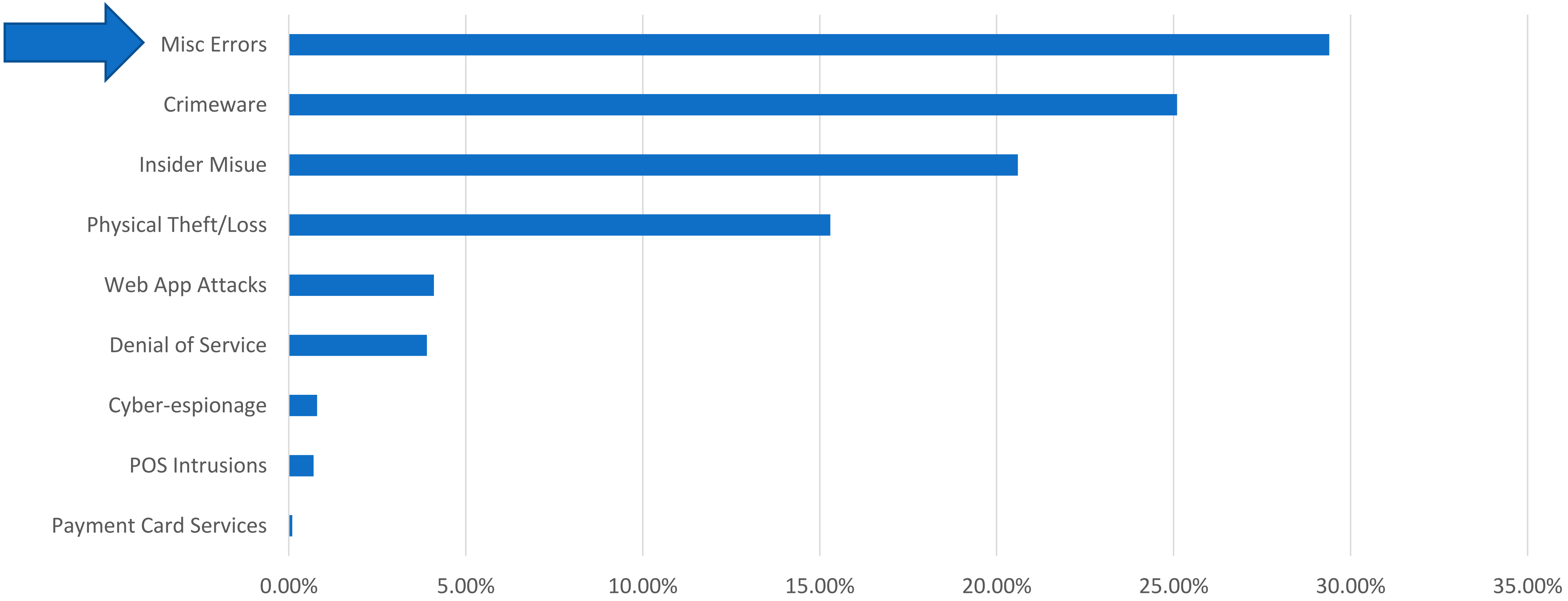
Secure Configuration

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

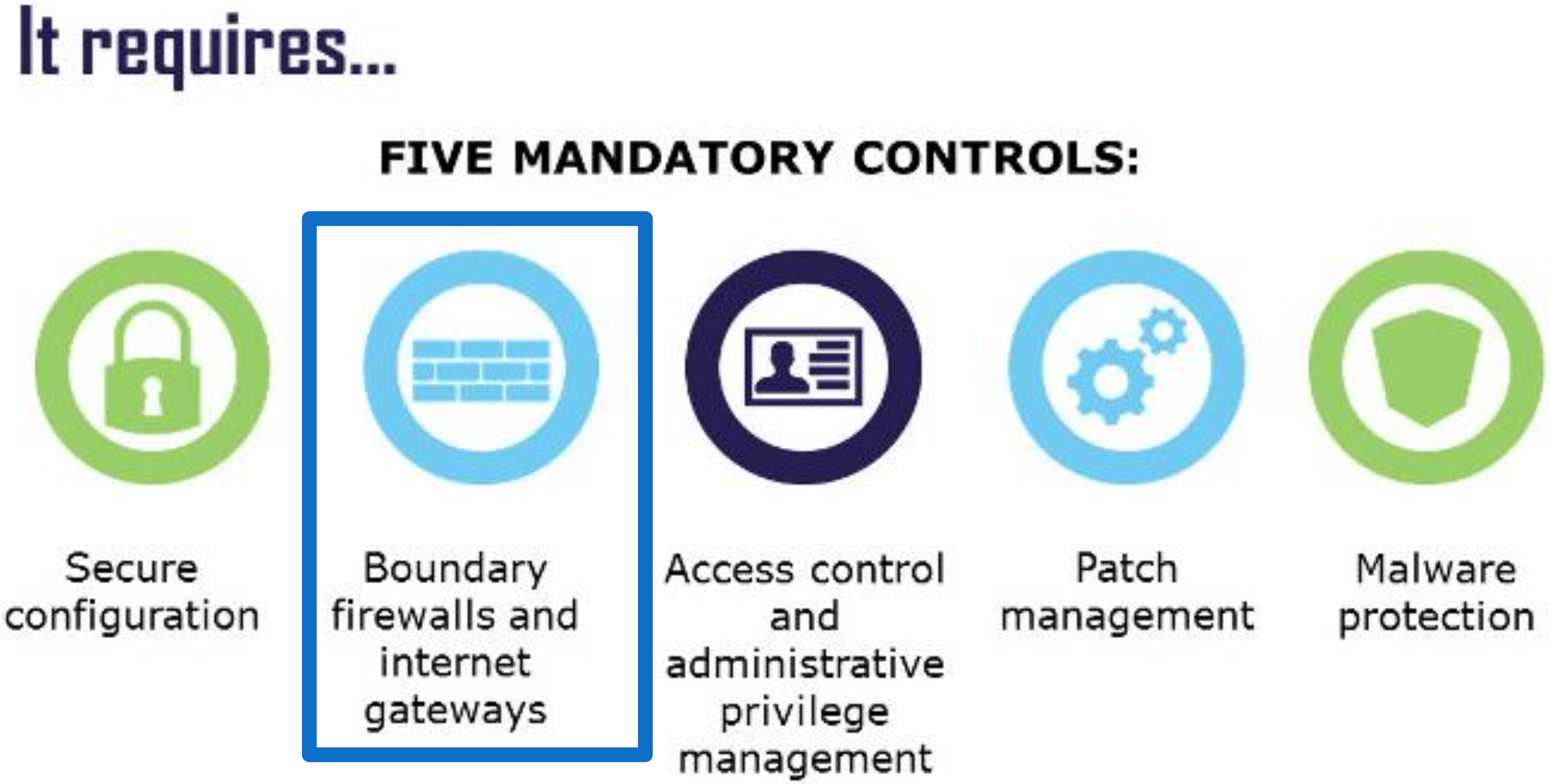


Configuration is a real problem



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

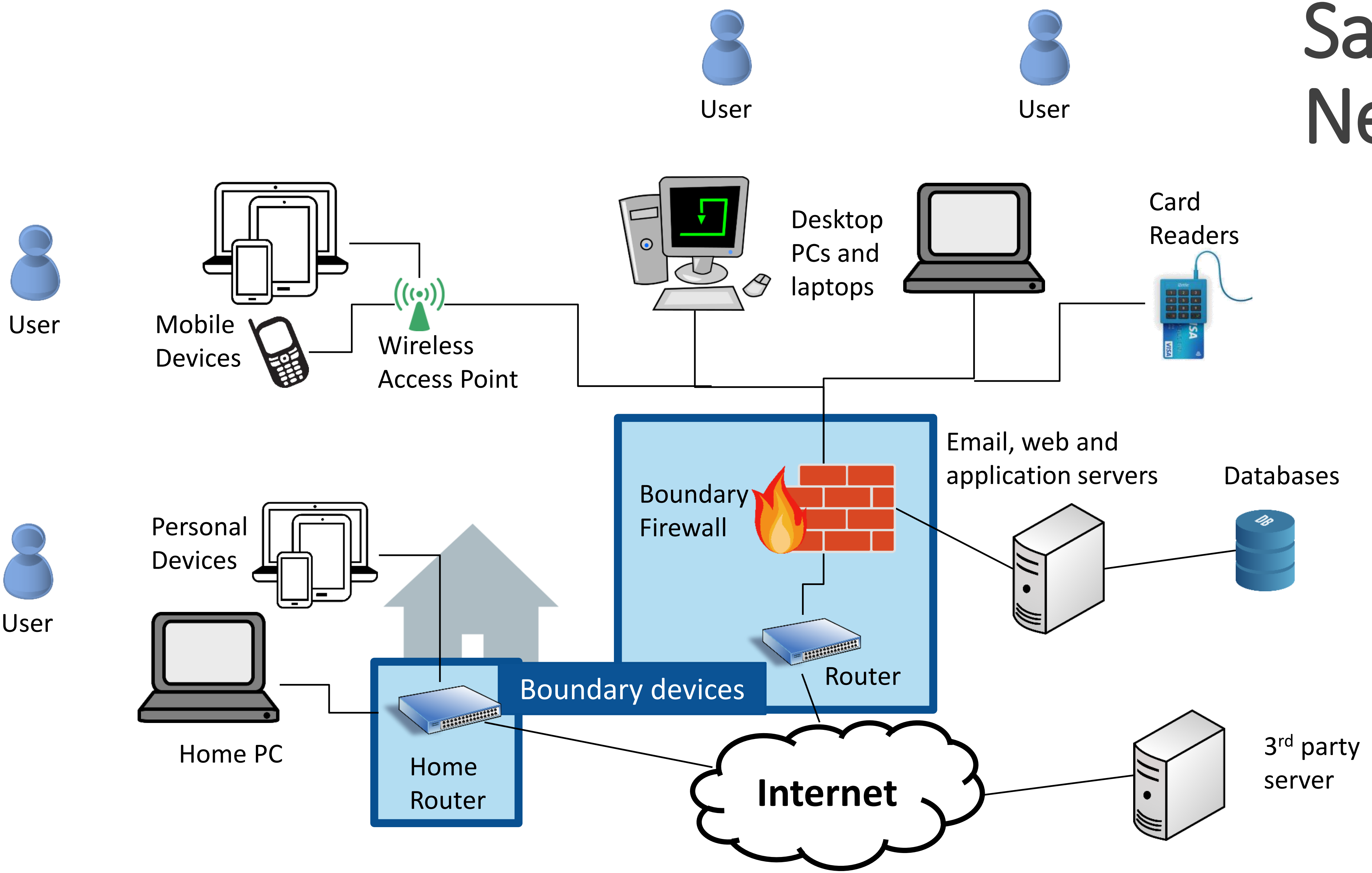
Malware protection

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.

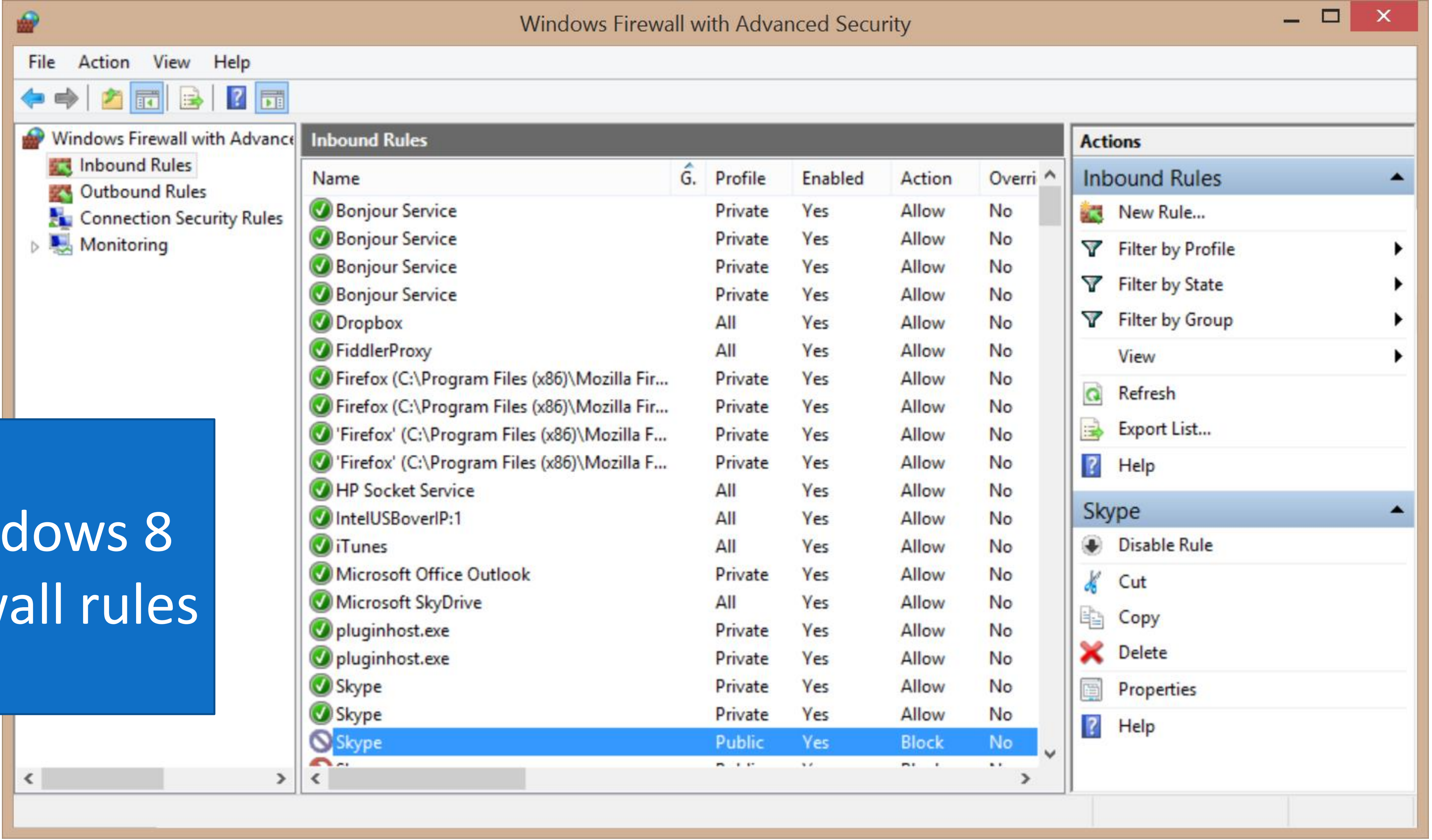
Sample Network



Boundary firewalls and internet gateways

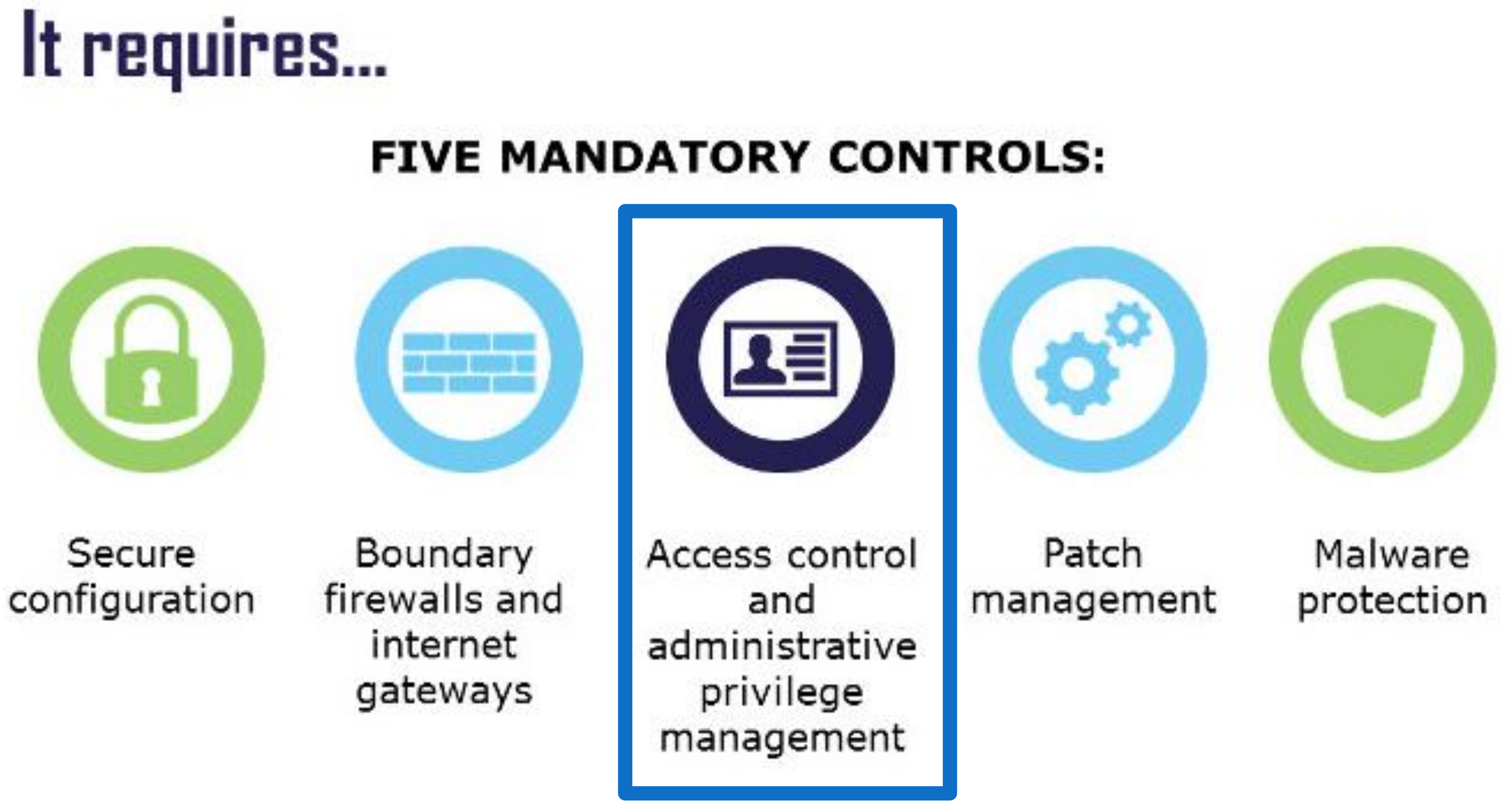
1. Change default administrator passwords for all network devices and firewalls.
2. Each rule that allows network traffic to pass through the firewall should be subject to approval by an authorized individual and documented.
3. Unapproved services, or services that are typically vulnerable to attack, 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



Name	G.	Profile	Enabled	Action	Overri
Bonjour Service		Private	Yes	Allow	No
Bonjour Service		Private	Yes	Allow	No
Bonjour Service		Private	Yes	Allow	No
Bonjour Service		Private	Yes	Allow	No
Dropbox		All	Yes	Allow	No
FiddlerProxy		All	Yes	Allow	No
Firefox (C:\Program Files (x86)\Mozilla Fir...		Private	Yes	Allow	No
Firefox (C:\Program Files (x86)\Mozilla Fir...		Private	Yes	Allow	No
'Firefox' (C:\Program Files (x86)\Mozilla F...		Private	Yes	Allow	No
'Firefox' (C:\Program Files (x86)\Mozilla F...		Private	Yes	Allow	No
HP Socket Service		All	Yes	Allow	No
IntelUSBoverIP:1		All	Yes	Allow	No
iTunes		All	Yes	Allow	No
Microsoft Office Outlook		Private	Yes	Allow	No
Microsoft SkyDrive		All	Yes	Allow	No
pluginhost.exe		Private	Yes	Allow	No
pluginhost.exe		Private	Yes	Allow	No
Skype		Private	Yes	Allow	No
Skype		Private	Yes	Allow	No
Skype		Public	Yes	Block	No

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

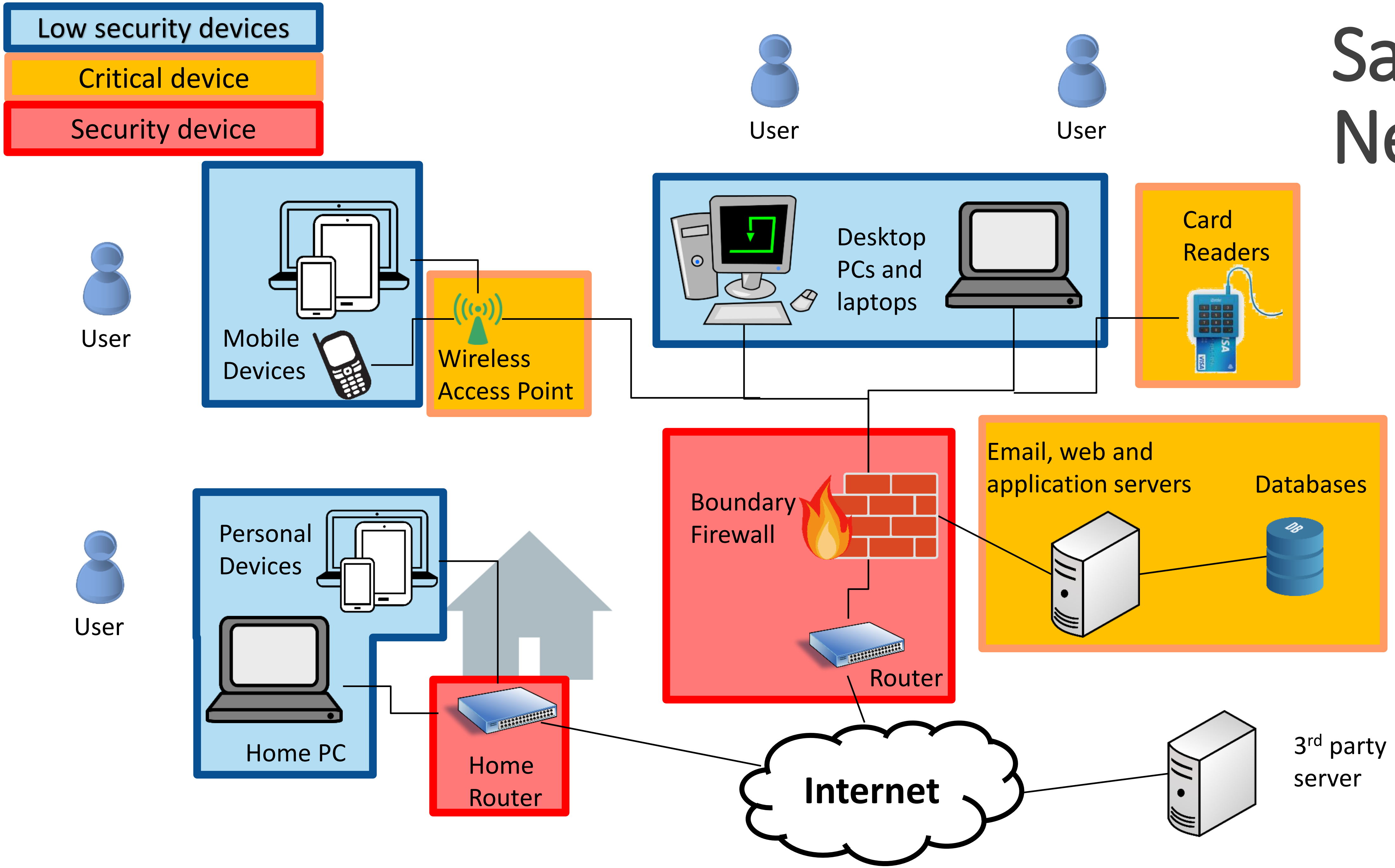
Objectives: User accounts, particularly those with special access privileges should be assigned only to authorized individuals, managed effectively and provide the minimum level of access to applications, computers and networks.

- 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.

Sample Network



One of the US companies that manages credit scores sold data to a person who ran an online ID Theft service.

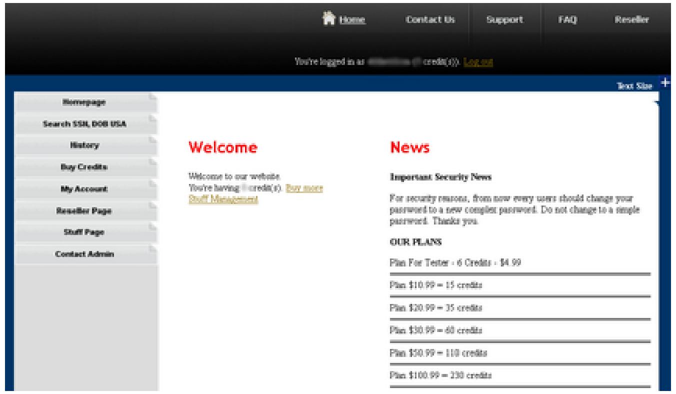
http://krebsonsecurity.com/2013/10/experian-sold-consumer-data-to-id-theft-service/

20
OCT 13

Experian Sold Consumer Data to ID Theft Service

An identity theft service that sold Social Security and drivers license numbers — as well as bank account and credit card data on millions of Americans — purchased much of its data from **Experian**, one of the three major credit bureaus, according to a lengthy investigation by KrebsOnSecurity.

In November 2011, this publication ran a story about an underground service called Superget.info, a fraudster-friendly site that marketed the ability to look up full Social Security numbers, birthdays, drivers license records and financial information on millions of Americans. Registration was free, and accounts were funded via WebMoney and other virtual currencies that are popular in the cybercriminal underground.



You're logged in as [redacted] credit(s). Log out

Welcome to our website.
You're having [redacted] credit(s). Buy more
Stuff Management

Important Security News

For security reasons, from now every users should change your password to a new complex password. Do not change to a simple password. Thanks you.

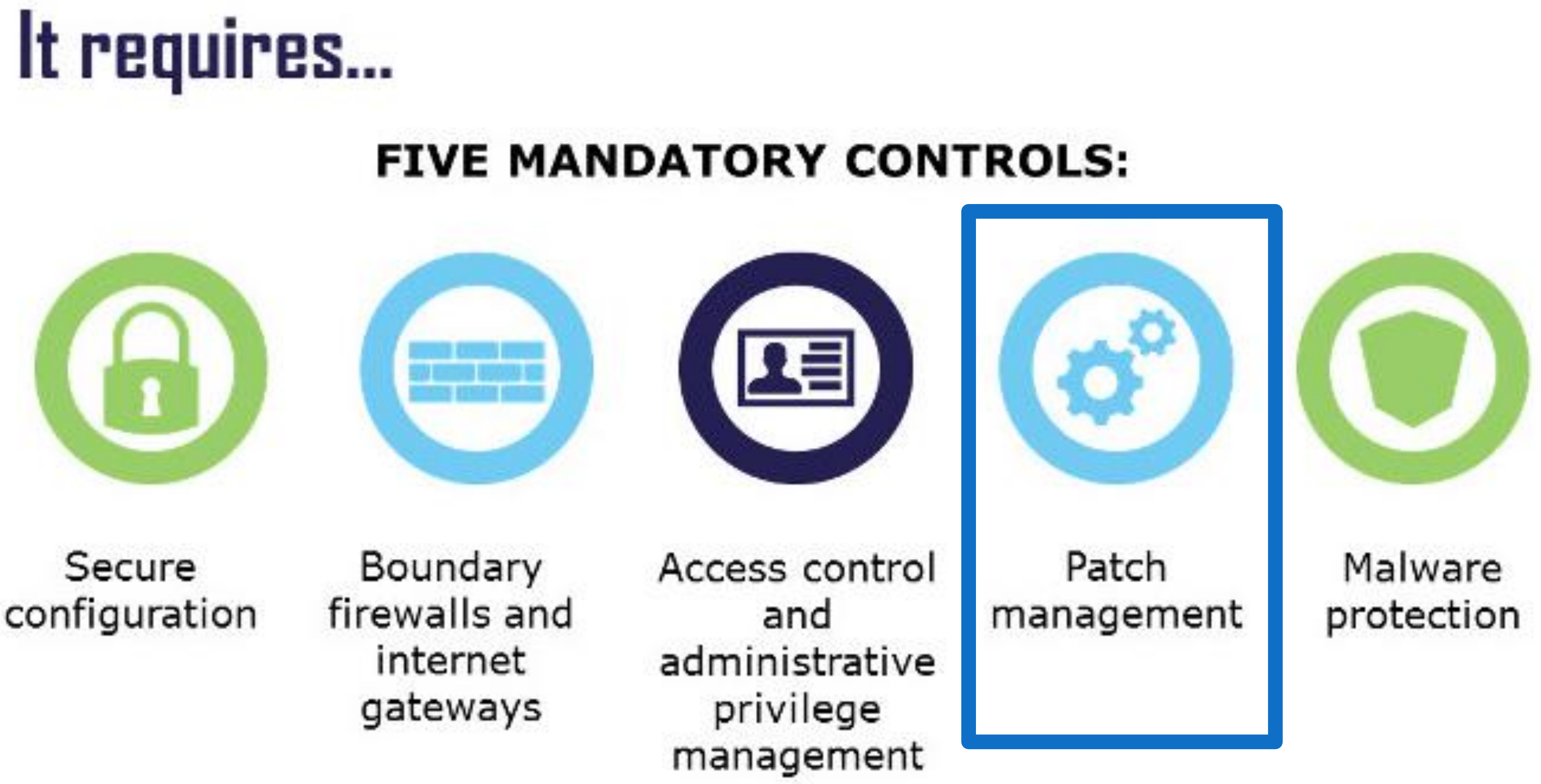
OUR PLANS

Plan For Tester - 6 Credits - $4.99
Plan $10.99 = 15 credits
Plan $20.99 = 35 credits
Plan $30.99 = 60 credits
Plan $50.99 = 110 credits
Plan $100.99 = 230 credits

superget.info home page

Each SSN search on Superget.info returned consumer records that were marked with a set of varying and mysterious two- and three-letter "sourceid:" identifiers, including "TH," "MV," and "NCO," among others. I asked readers who may have a clue about the meaning or source of those abbreviations to contact me. In the weeks following that post, I heard from many readers who had guesses and ideas, but none who seemed to have conclusive information.

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.

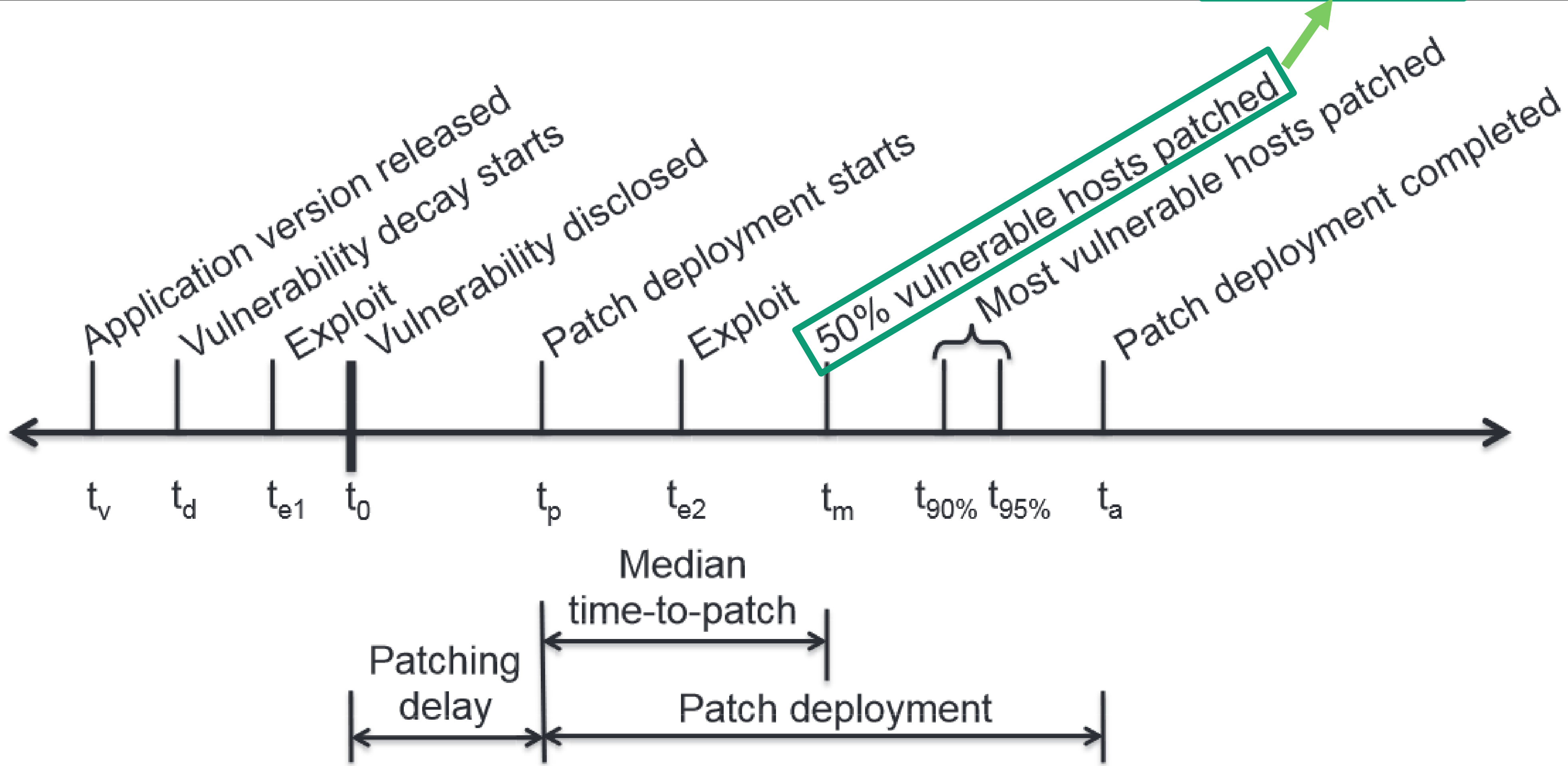
- Vulnerabilities in software are patched through updates.
- If you don’t install the update, the vulnerability is not patched.
- However, patching can cause compatibility problems. So you should always test the patches.

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

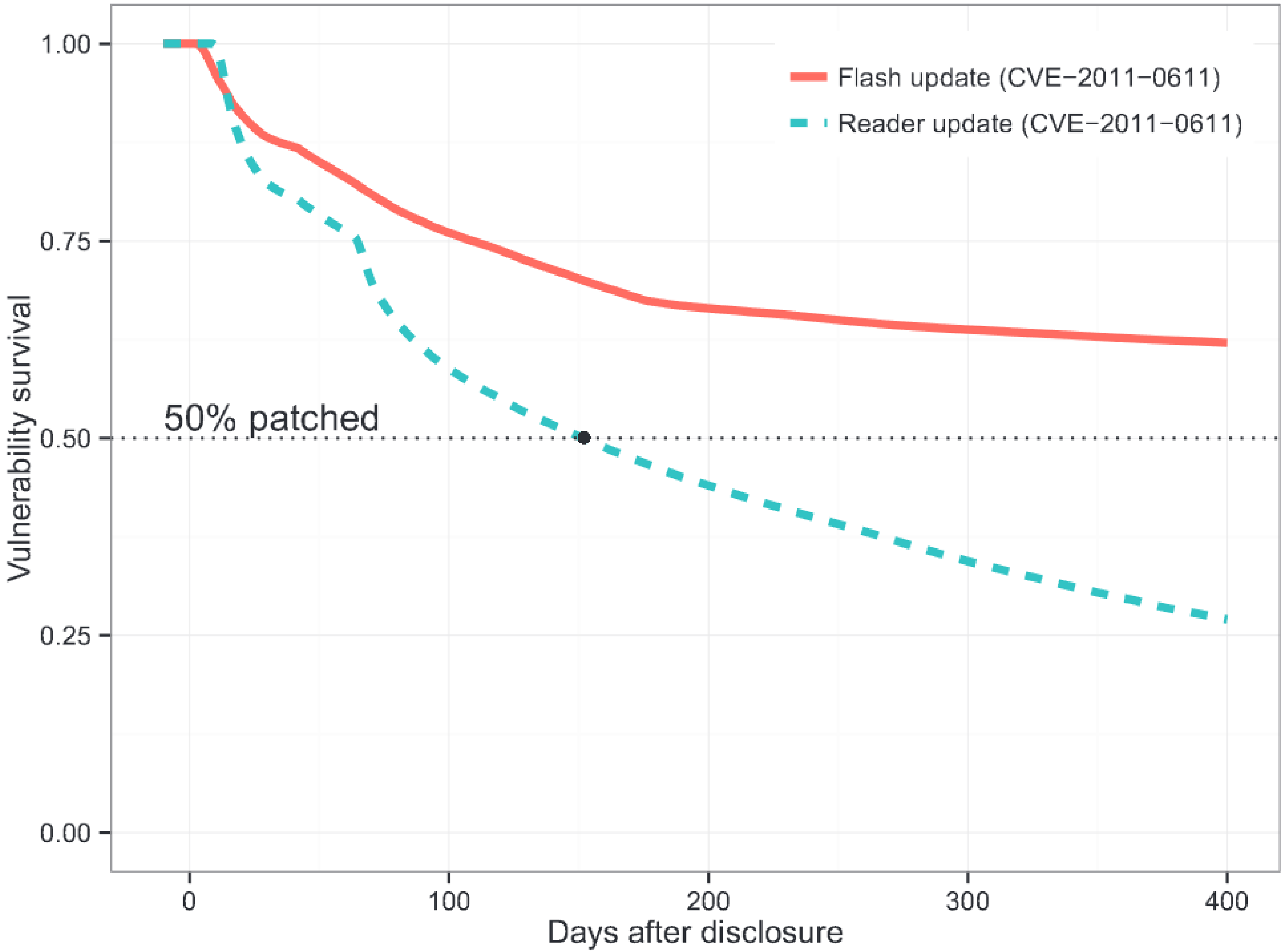
Vulnerability half life



A. Nappa, R. Johnson, L. Bilge, J. Caballero, and T. Dumitraș, "The Attack of the Clones: A Study of the Impact of Shared Code on Vulnerability Patching," in *IEEE Symposium on Security and Privacy*, San Jose, CA, 2015.

Vulnerability survival

- The % of computers patched X days after disclosure.



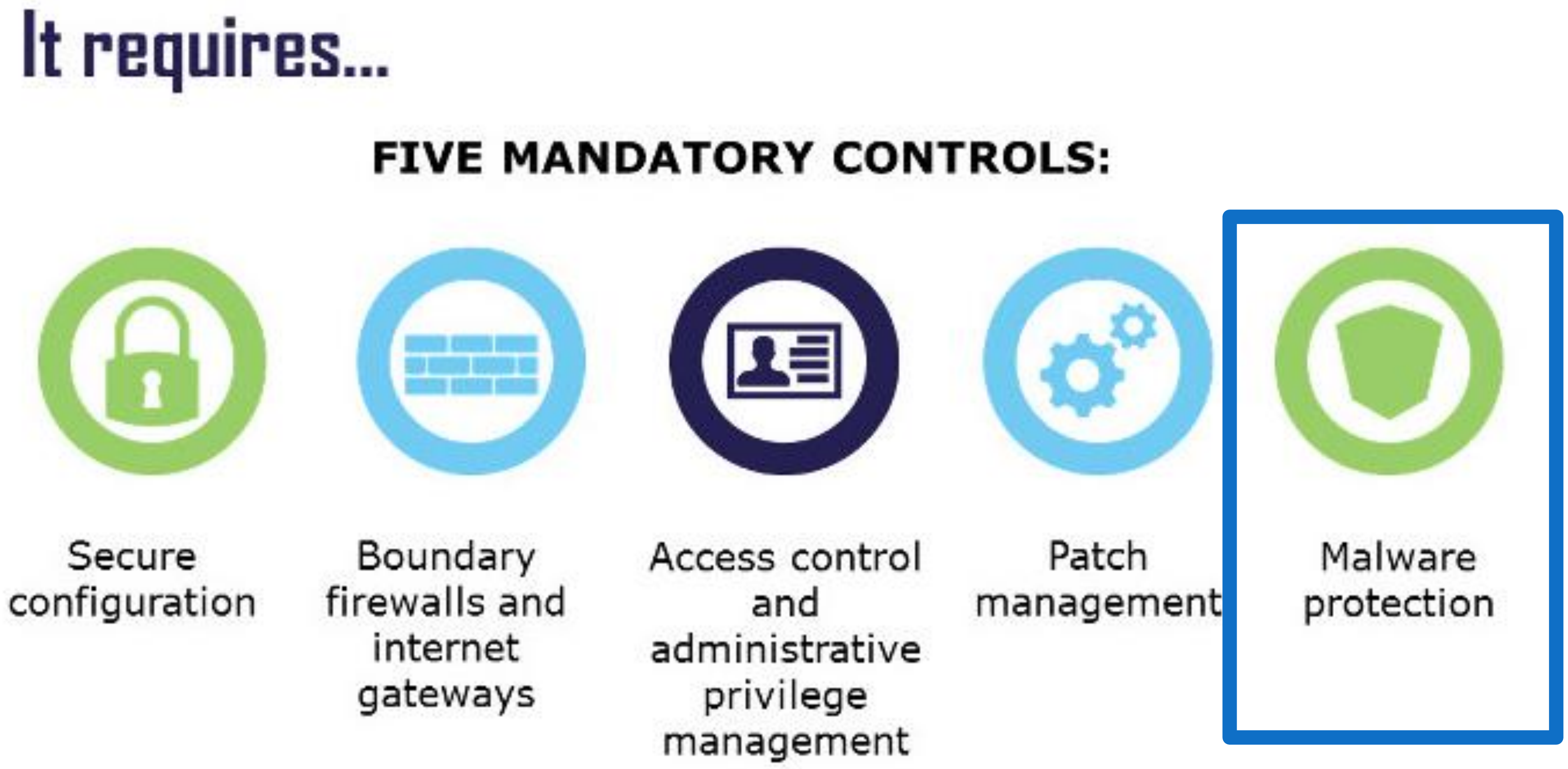
A. Nappa, R. Johnson, L. Bilge, J. Caballero, and T. Dumitraș, "The Attack of the Clones: A Study of the Impact of Shared Code on Vulnerability Patching," in *IEEE Symposium on Security and Privacy*, San Jose, CA, 2015.

Heartbleed

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

Errata Security Blog http://blog.erratasec.com/2014/06/300k-vulnerable-to-heartbleed-two.html

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

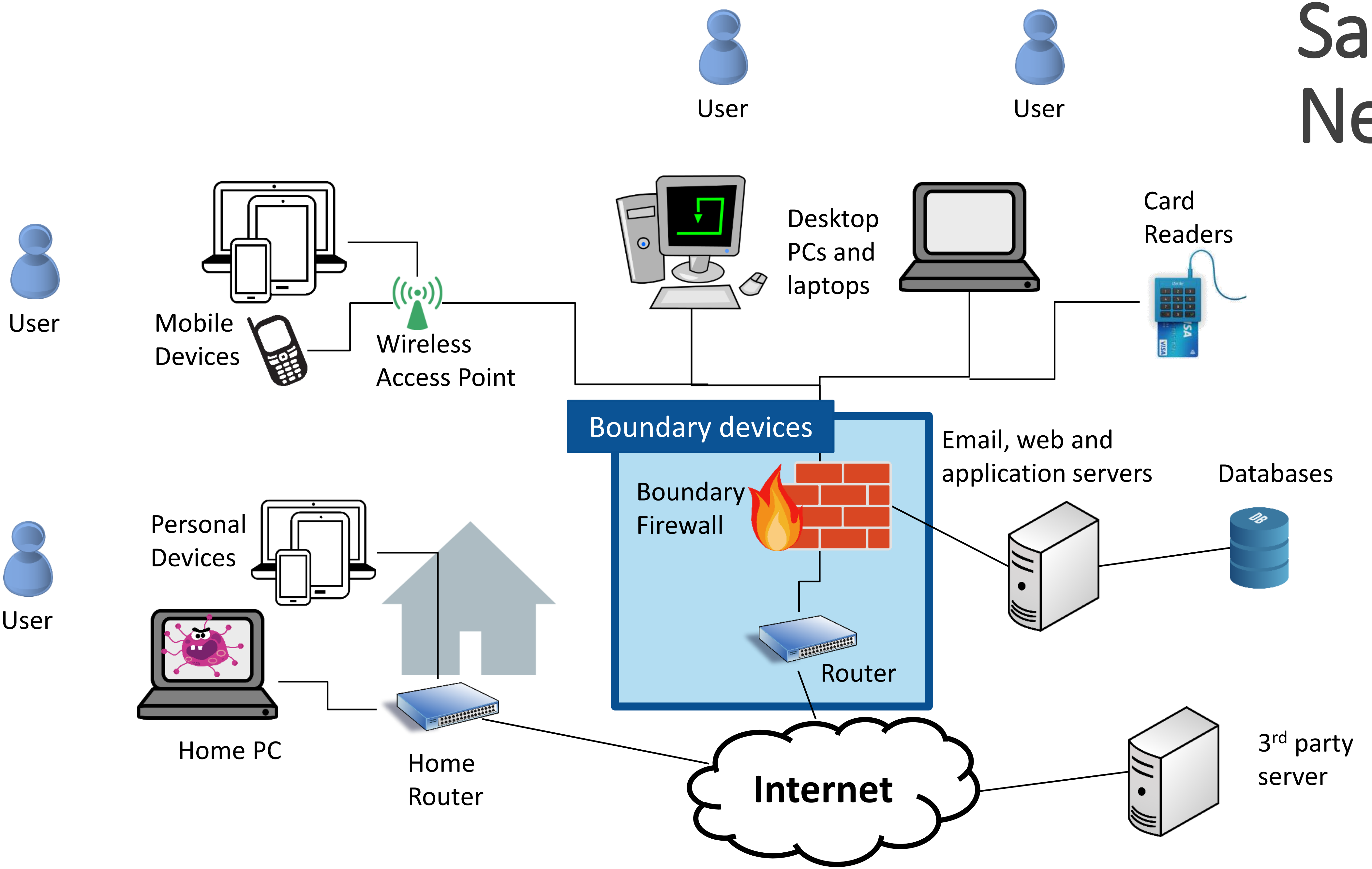
Objectives: Computers exposed to the internet should be protected against malware infection through the use of malware protection software.

- 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.

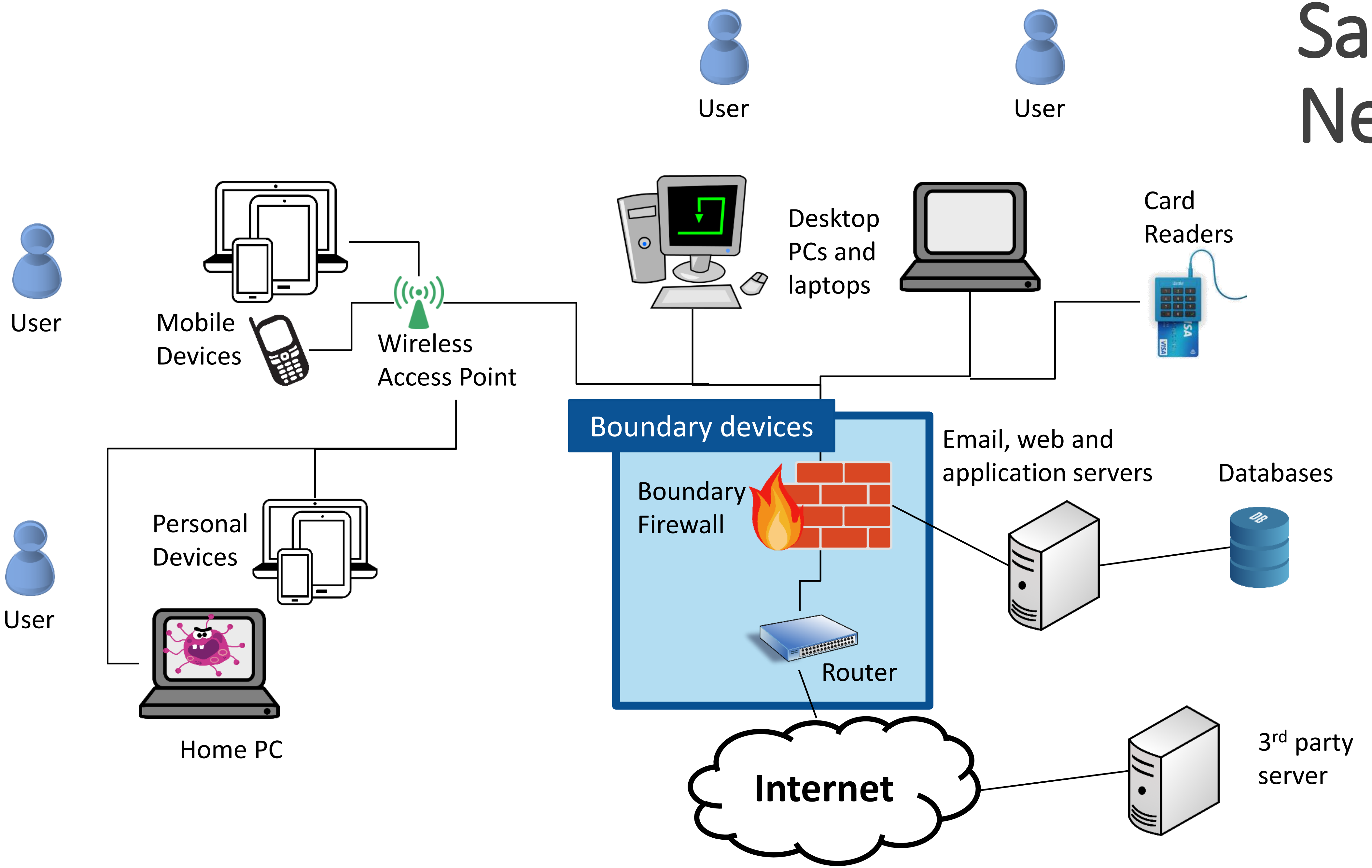
Malware protection

- 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.

Sample Network



Sample Network



The Switch

Thousands of visitors to yahoo.com hit with malware attack, researchers say

“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.”

https://www.washingtonpost.com/blogs/the-switch/wp/2014/01/04/thousands-of-visitors-to-yahoo-com-hit-with-malware-attack-researchers-say

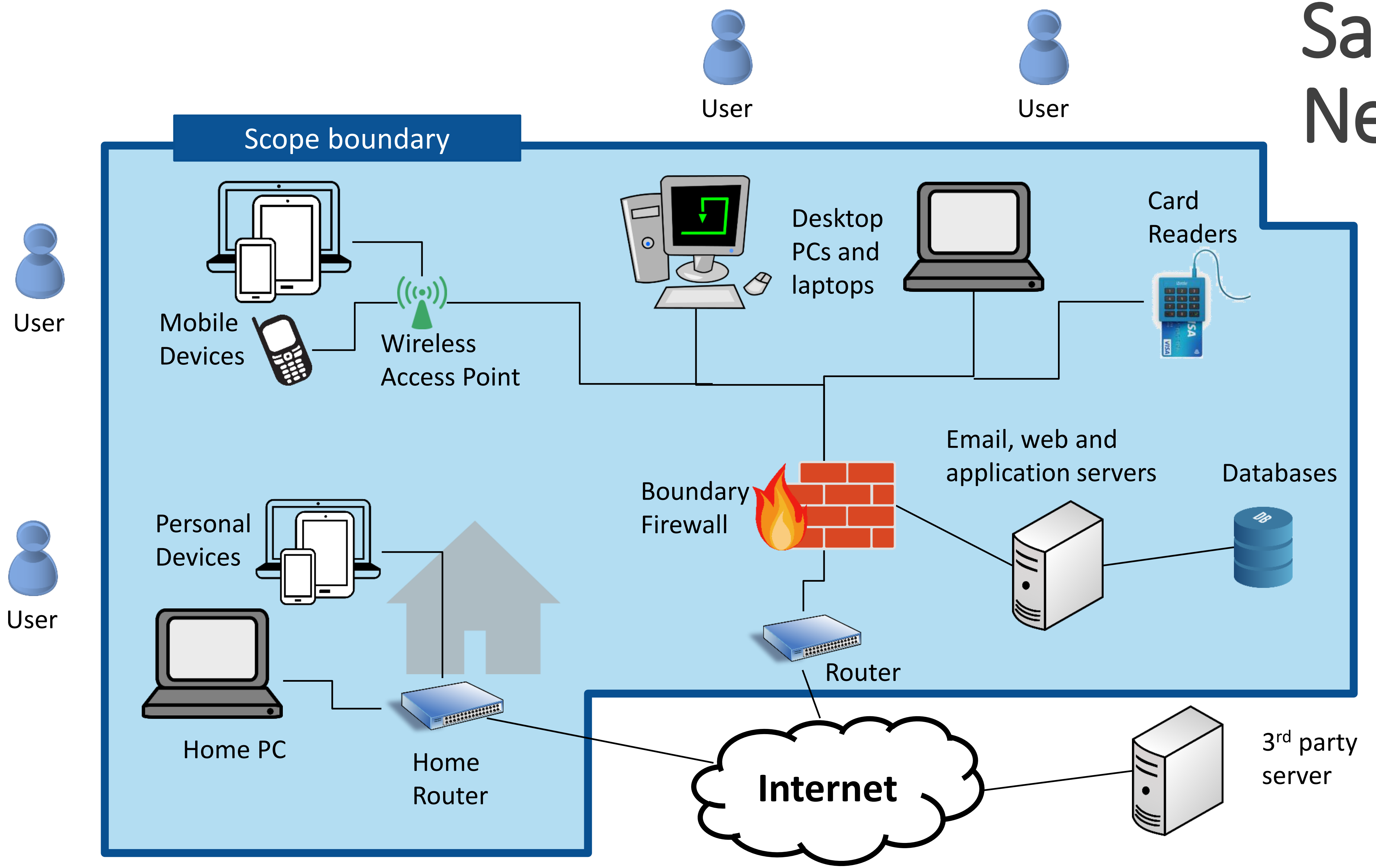
The Switch

Thousands of visitors to yahoo.com hit with malware attack, researchers say

“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.’”

https://www.washingtonpost.com/blogs/the-switch/wp/2014/01/04/thousands-of-visitors-to-yahoo-com-hit-with-malware-attack-researchers-say

Sample Network



Questions