Computer Security: Cyber Essentials

DR. KAMI VANIEA

First, the news…

- http://www.sbrcentre.co.uk/images/site_images/20522_SmallBusinessTheCyberRiskReportVoRFINALFeb2016.pdf
- http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

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.

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.

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.

Establish an effective governance structure and determine your risk appetite.

Information Risk Management Regime

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.

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.

Maintain the Board's engagement with the cyber risk.

Produce supporting information risk management policies.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Establish an effective governance structure and determine your risk appetite.

Information Risk Management Regime

Maintain the Board's engagement with the cyber risk.

Produce supporting information risk management policies.

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

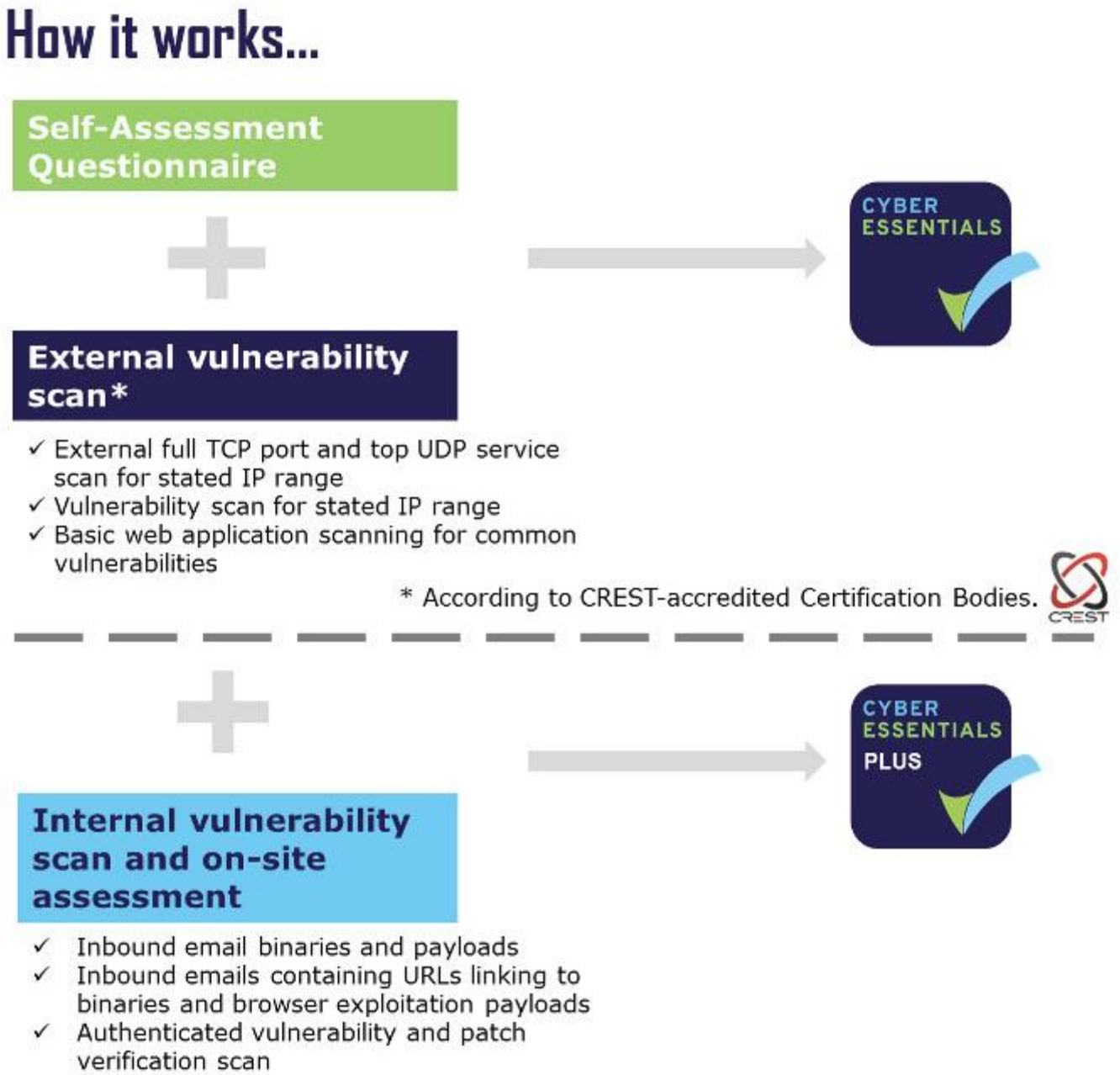
Cyber Security Essentials

It is a...

- Clear statement of the basic controls that all organisations should implement to mitigate the risk from common internet-based threats.
- Mechanism for organisations to demonstrate to customers, investors, insurers and others that they have taken essential precautions against cyber risks.
- Requirement for suppliers bidding for certain UK Government and large business contracts that handle personal information:
  - Professional services (commercial, financial, legal, HR and business services)
  - ICT (IT managed or outsourced services and ICT services).

Cyber Essentials Certification

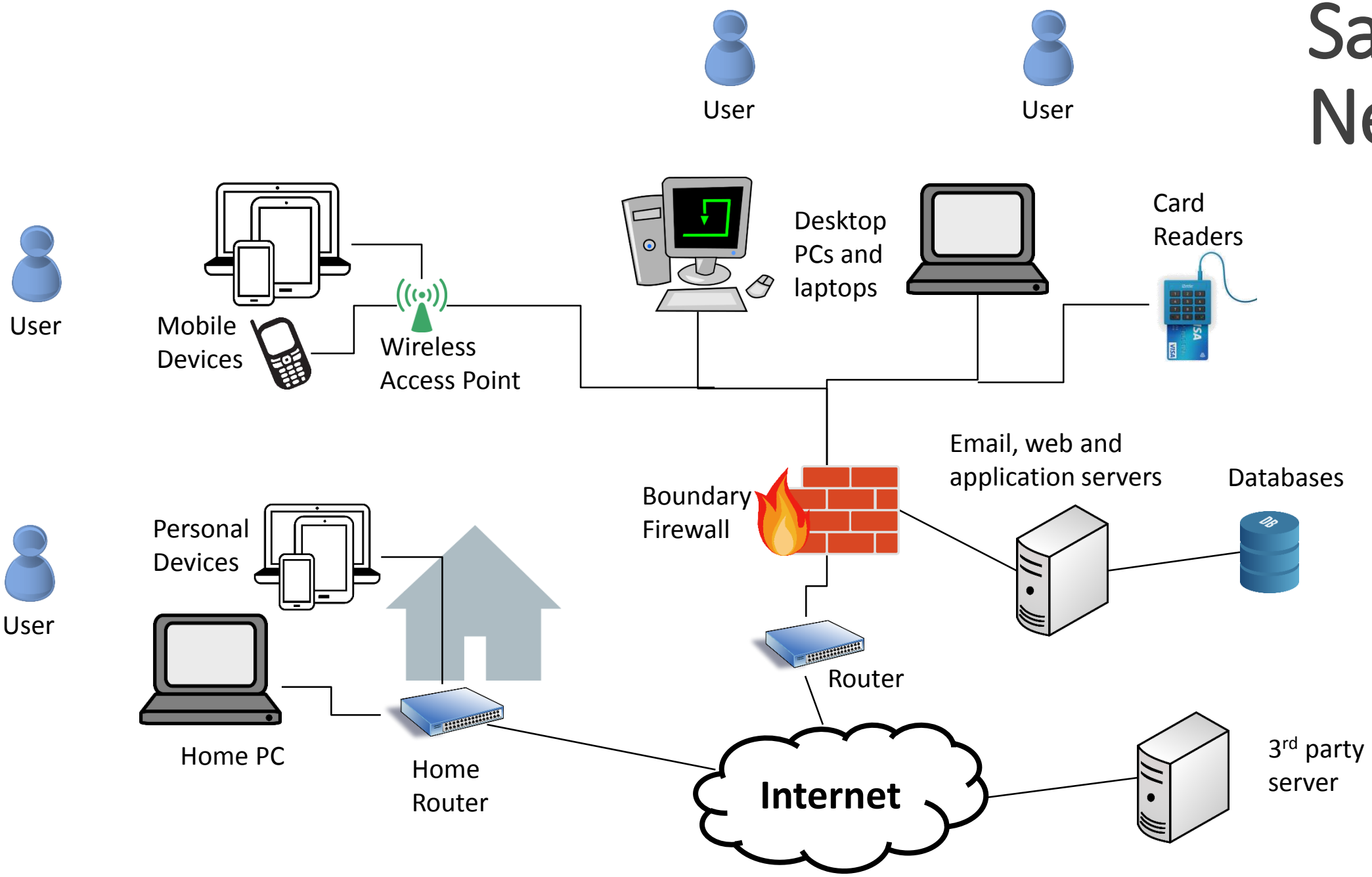
- Self-assessment
- External vulnerability scan by an approved tester
- Internal vulnerability scan by an approved tester



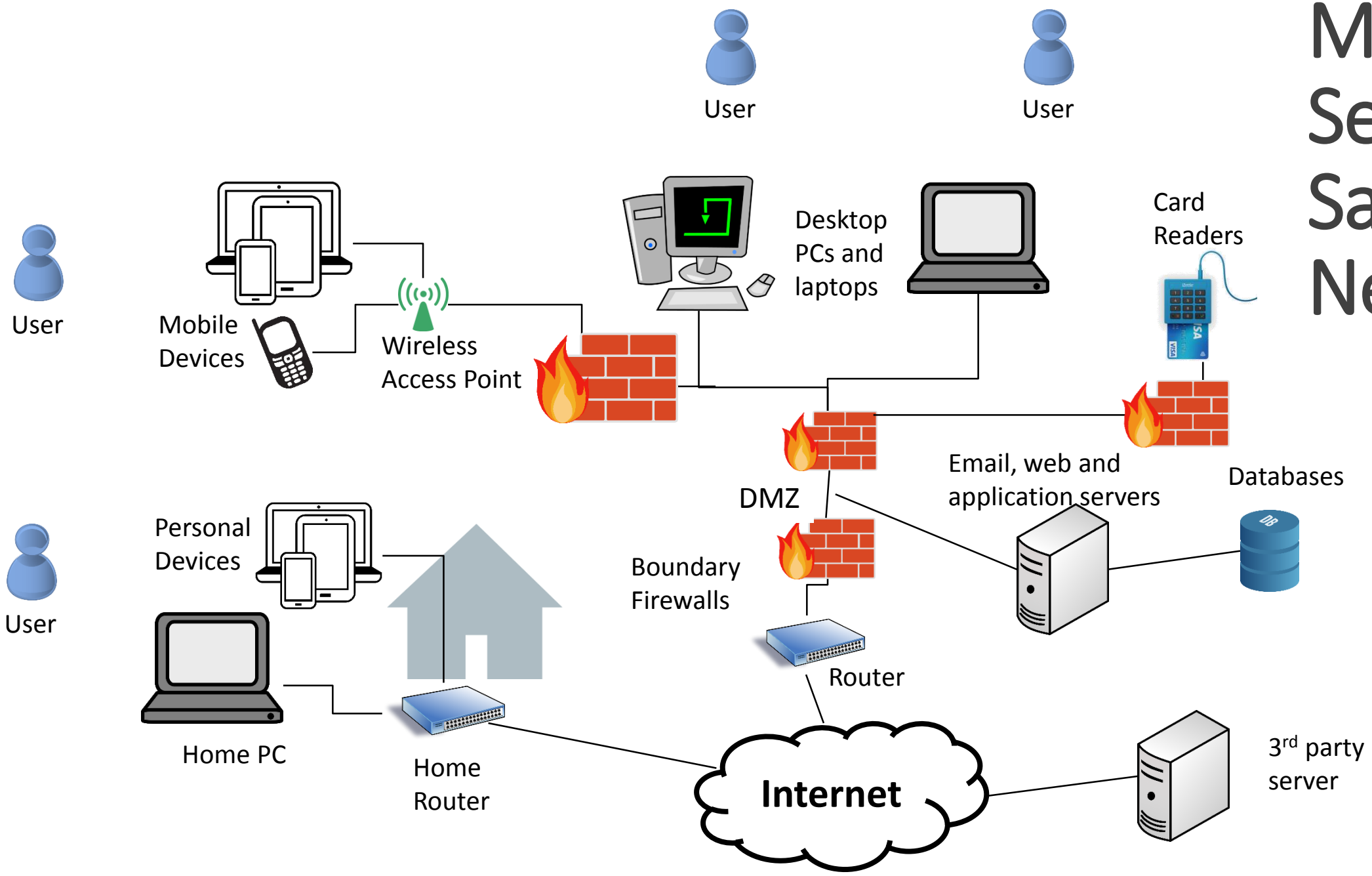
Cyber Essentials provides a good summary of what basic level protection looks like.

Cyber Essentials Controls

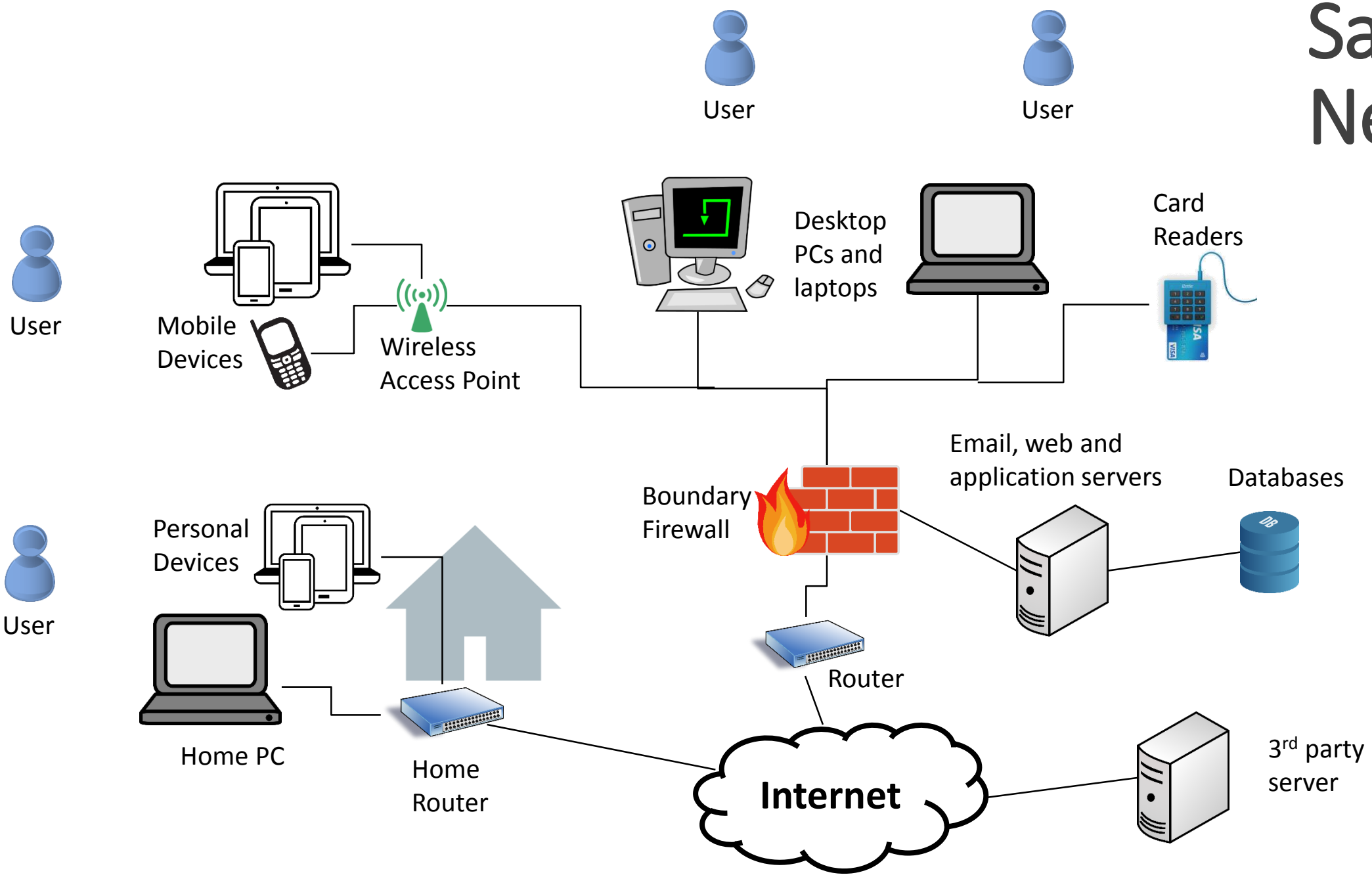
Sample Network



More Secure Sample Network



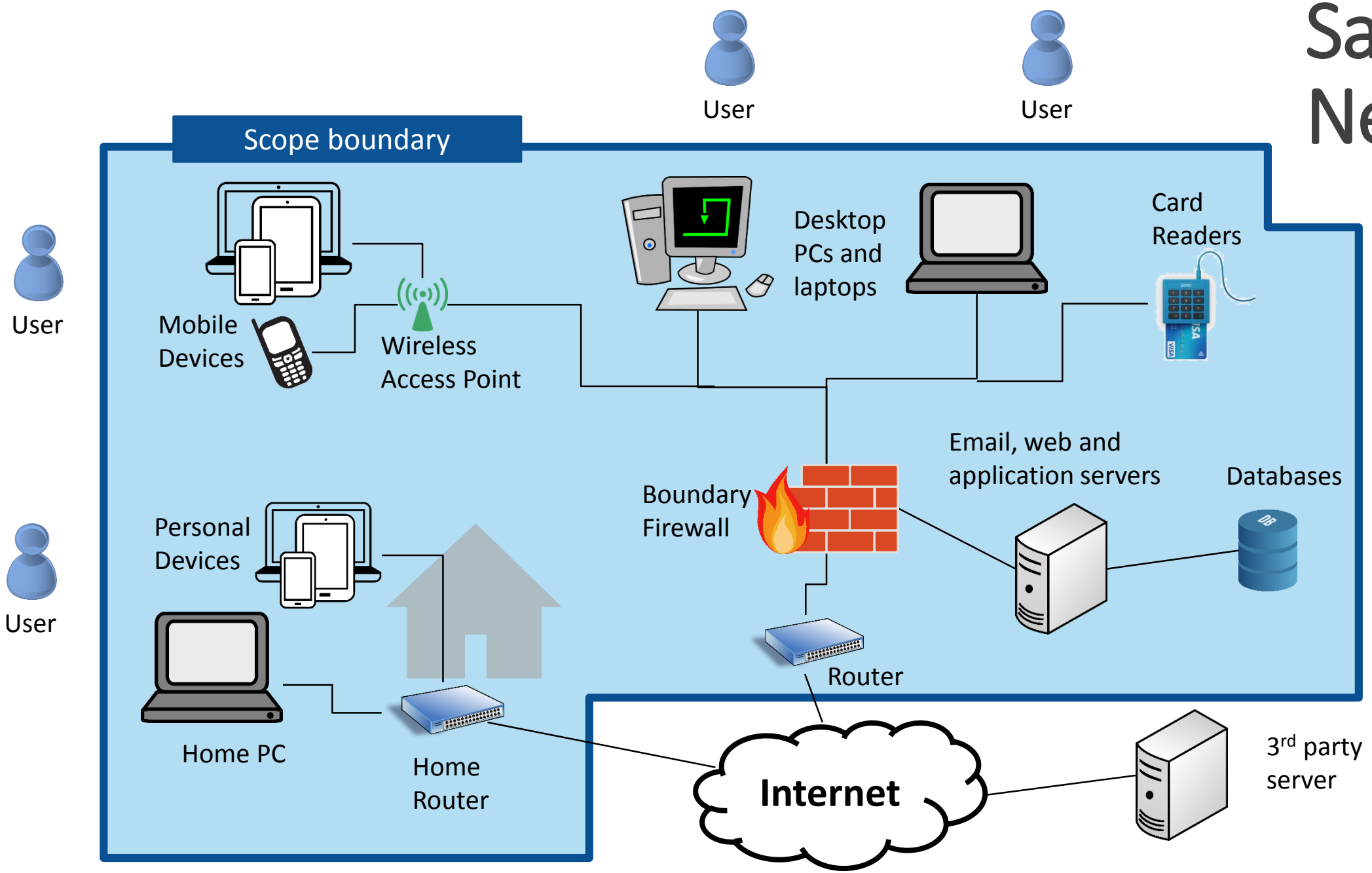
Sample Network



“A system which is unspecified can never be wrong, it can only be surprising.”

Step 1: Decide what you are going to protect and what is out of scope.

Sample Network



Cyber Security Essentials

Secure Configuration

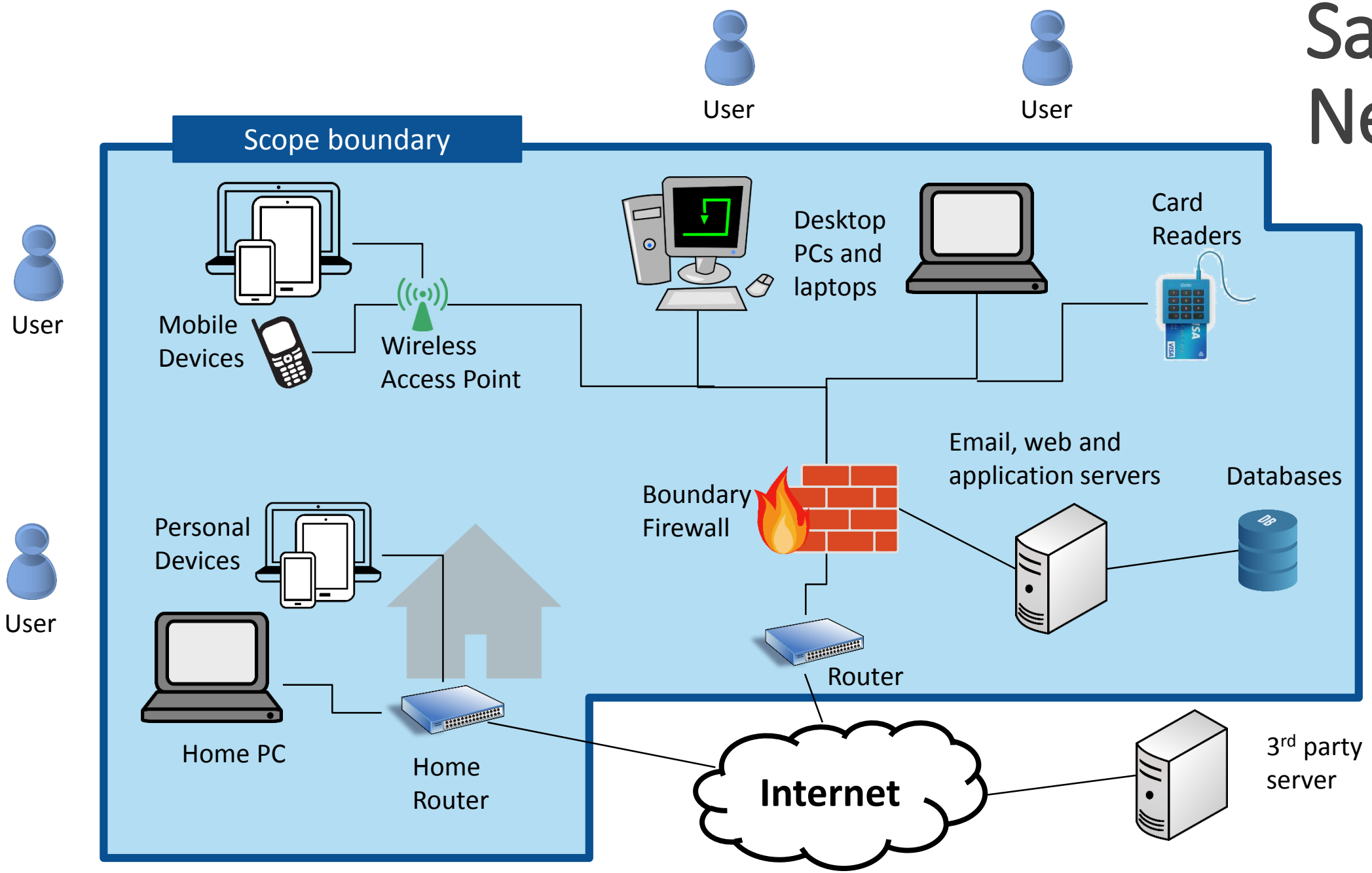
Objectives: Computers and network devices should be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.

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

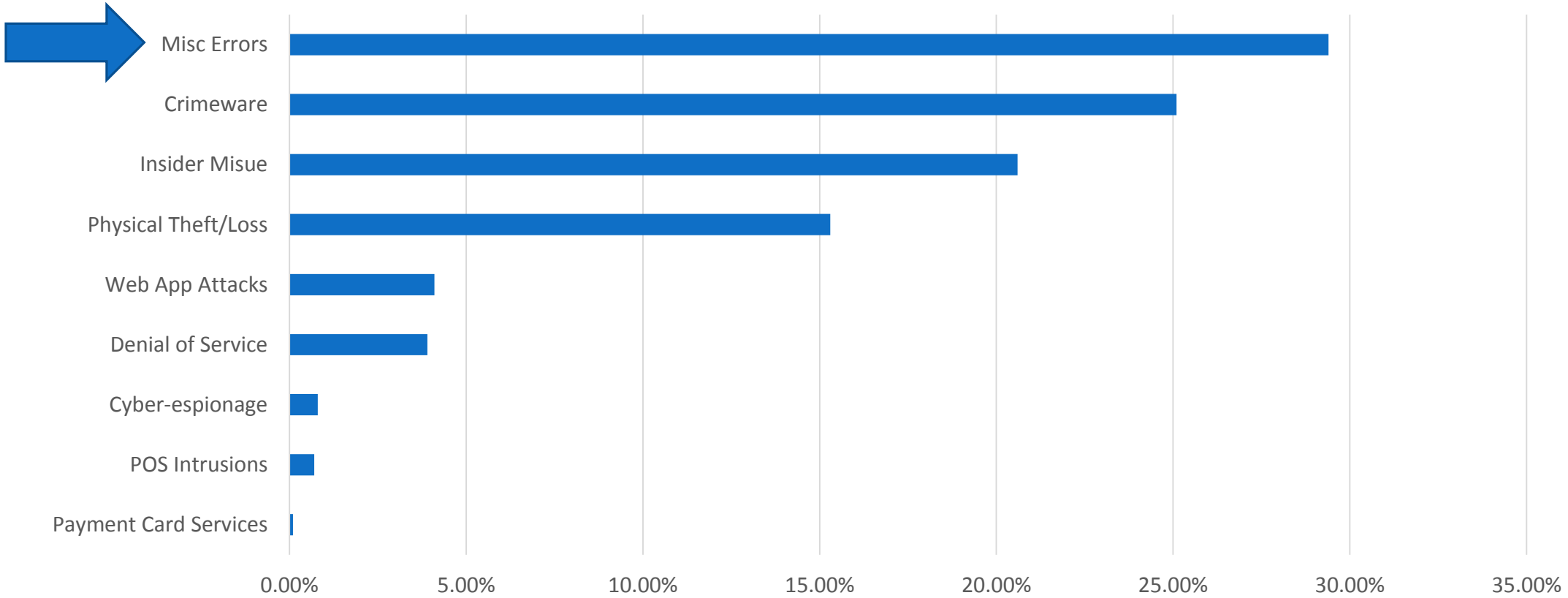
Secure Configuration

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



Server configuration error left the data world readable

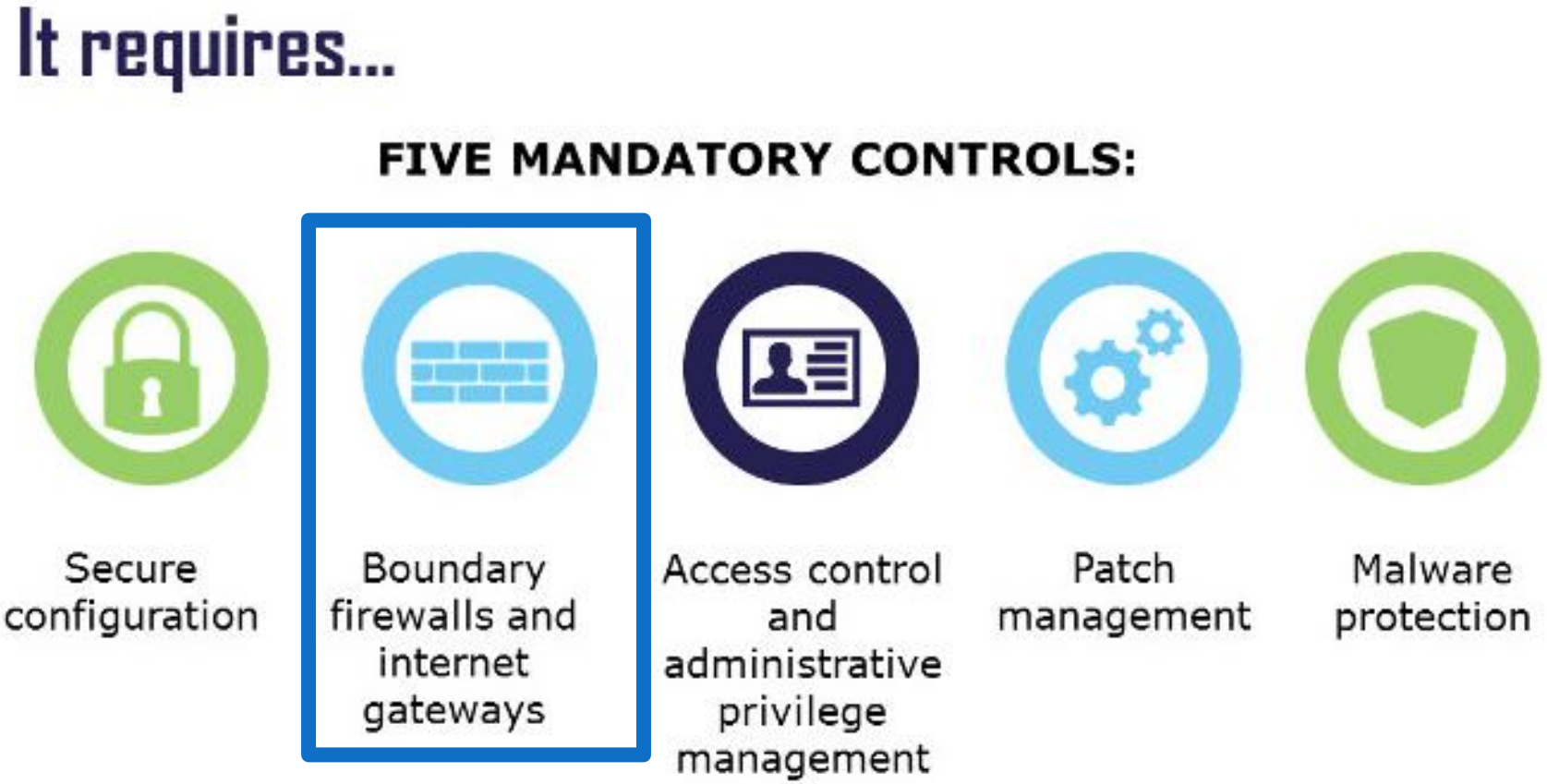
http://uk.reuters.com/article/us-usa-voters-breach-idUKKBN0UB1E020151229

CREDIT RSS | Tue Dec 29, 2015 | 2:20pm GMT

Database of 191 million U.S. voters exposed on Internet: researcher

Signs are pictured during a voter registration drive for National Voter Registration Day outside Convention Center in Los Angeles, California

Cyber Security Essentials

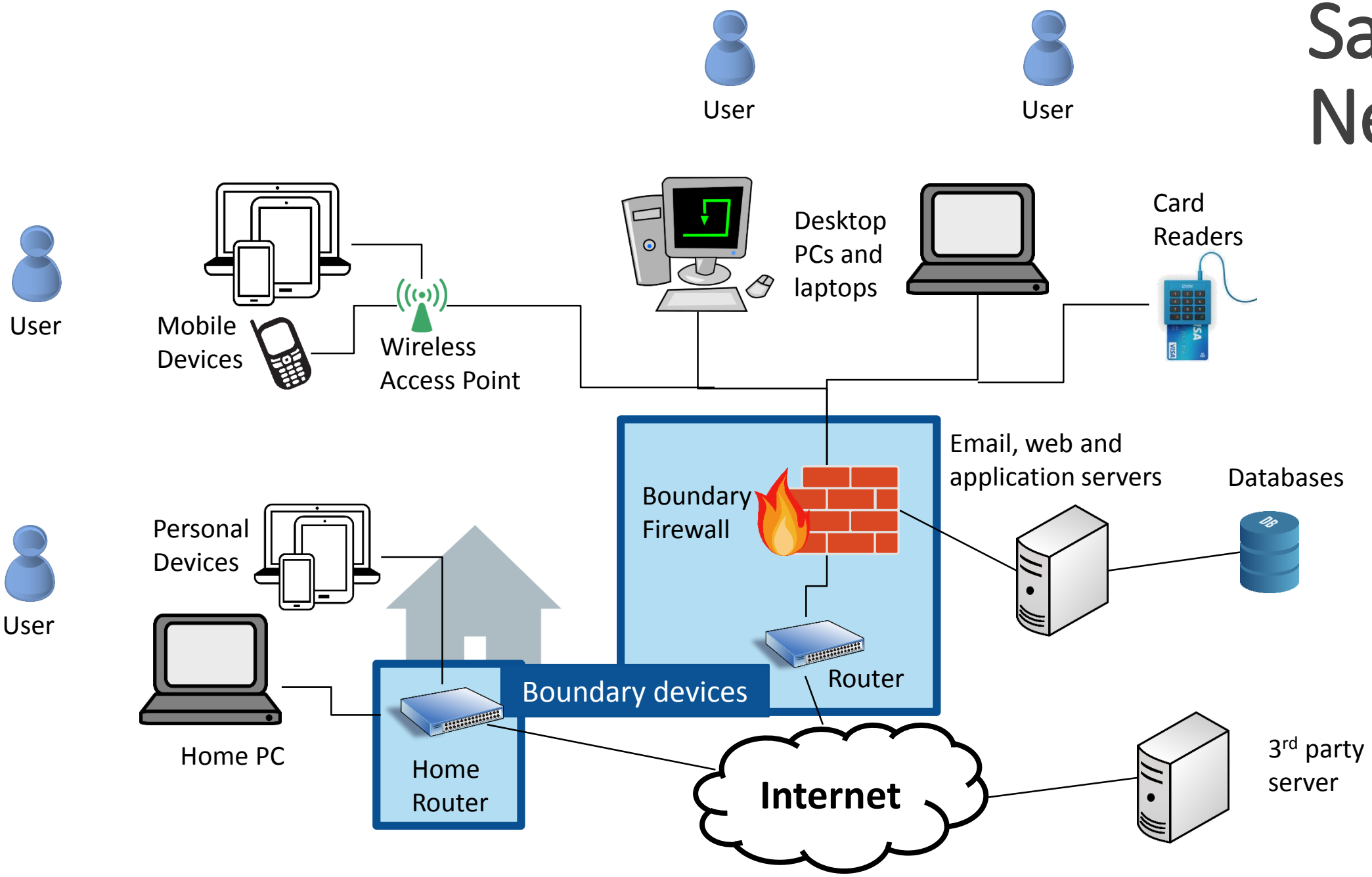


Boundary firewalls and internet gateways

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.

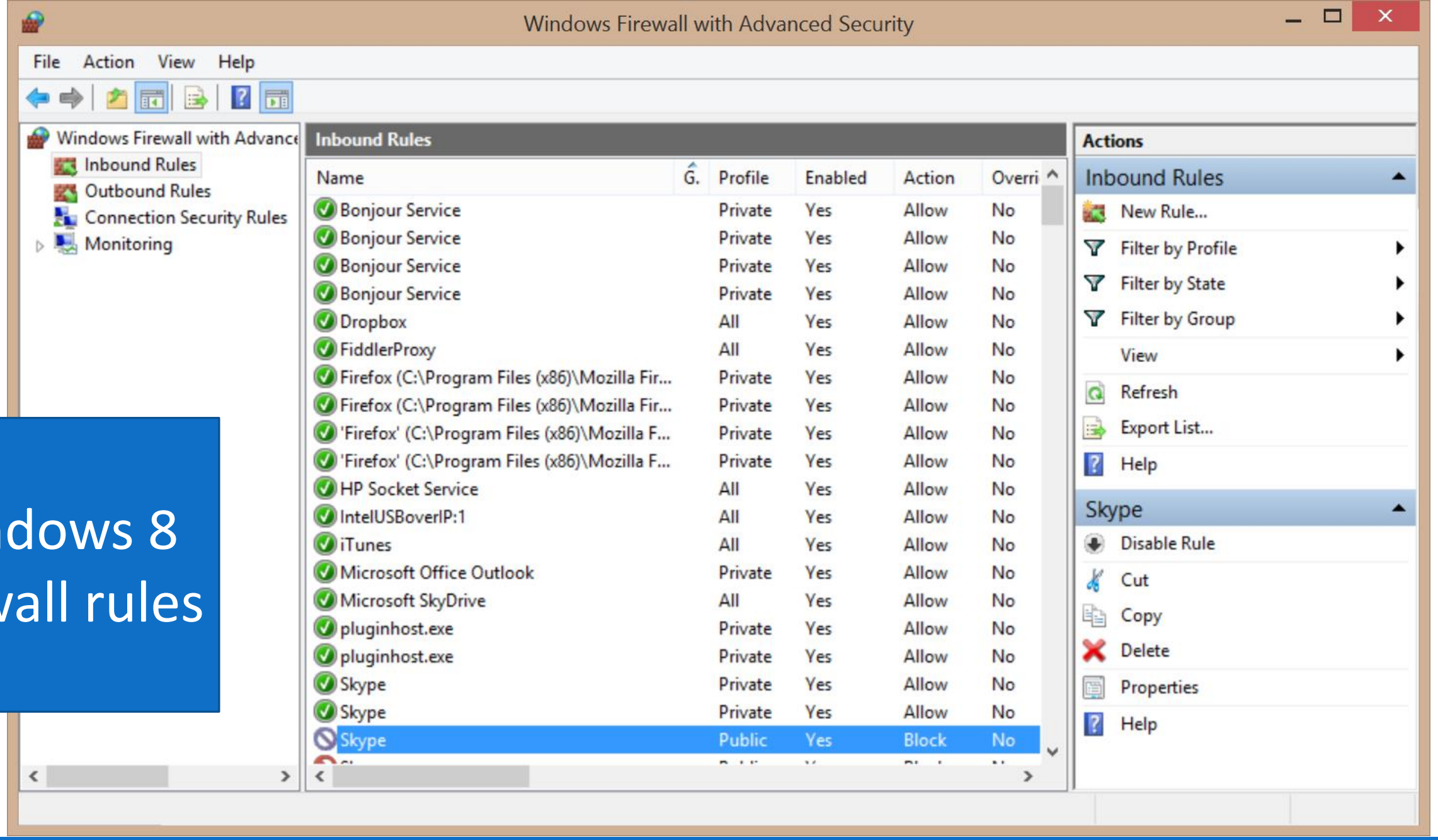
Sample Network



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



Two people sat out in a parking lot and breached the network which had no real security

http://www.nbcnews.com/id/17871485/ns/technology_and_science-security/t/tj-maxx-theft-believed-largest-hack-ever/#.UFi-HaRYtmg

T.J. Maxx theft believed largest hack ever

TJX cos. put number to loss Wednesday, acknowledges it could still go up

By Mark Jewell
Associated Press
updated

Print | Font: A A + −

BOSTON — A hacker or hackers stole data from at least 45.7 million credit and debit cards of shoppers at off-price retailers including T.J. Maxx and Marshalls in a case believed to be the largest such breach of consumer information.

For the first time since disclosing the theft more than two months ago, the parent company of nearly 2,500 discount stores put a number on how much card data was compromised — and it's a number TJX Cos. acknowledges could go still higher.

Experts say TJX's disclosures in a regulatory filing late Wednesday revealed security holes that persist at

Cyber Security Essentials

Access control and administrative privilege management

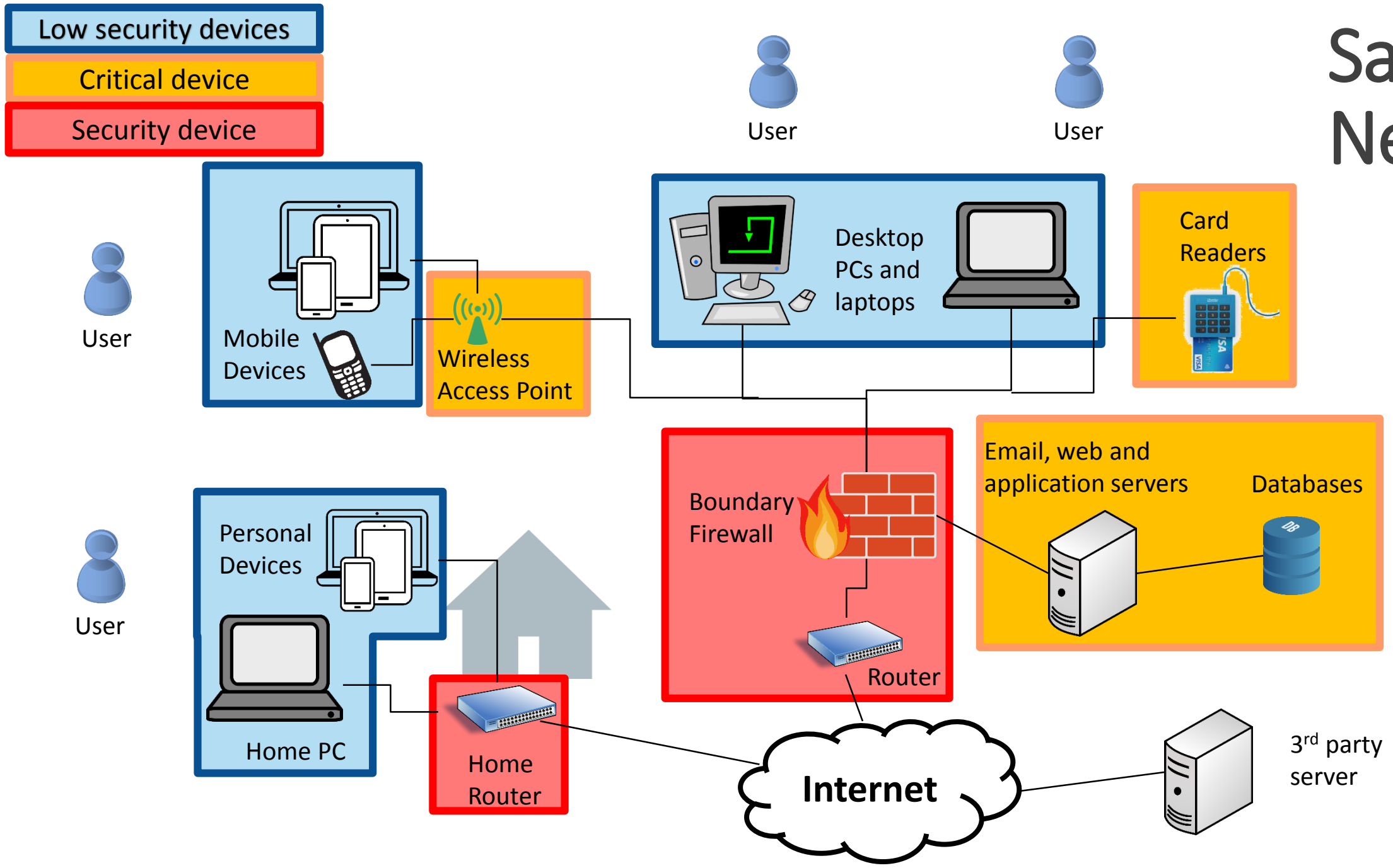
Objectives: User accounts, particularly those with special access privileges should be assigned only to authorized individuals, managed effectively and provide the minimum level of access to applications, computers and networks.

- 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



Investigation ongoing, current theory is that employees fell for a phishing attack

Massive breach at health care company Anthem Inc.

Elizabeth Weise, USATODAY 9:26 a.m. EST February 5, 2015

Anthem, the nation's second-largest health insurance company, is the latest target of a security breach. Eighty million customers, including the company's own CEO, are at risk of having their personal information stolen. VPC

SAN FRANCISCO - As many as 80 million

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

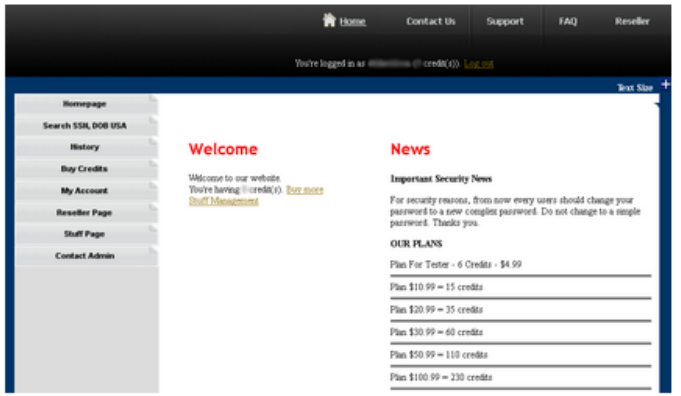
http://krebsonsecurity.com/2013/10/experian-sold-consumer-data-to-id-theft-service/

20 Experian Sold Consumer Data to ID Theft Service

OCT 13

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.



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

Malware protection

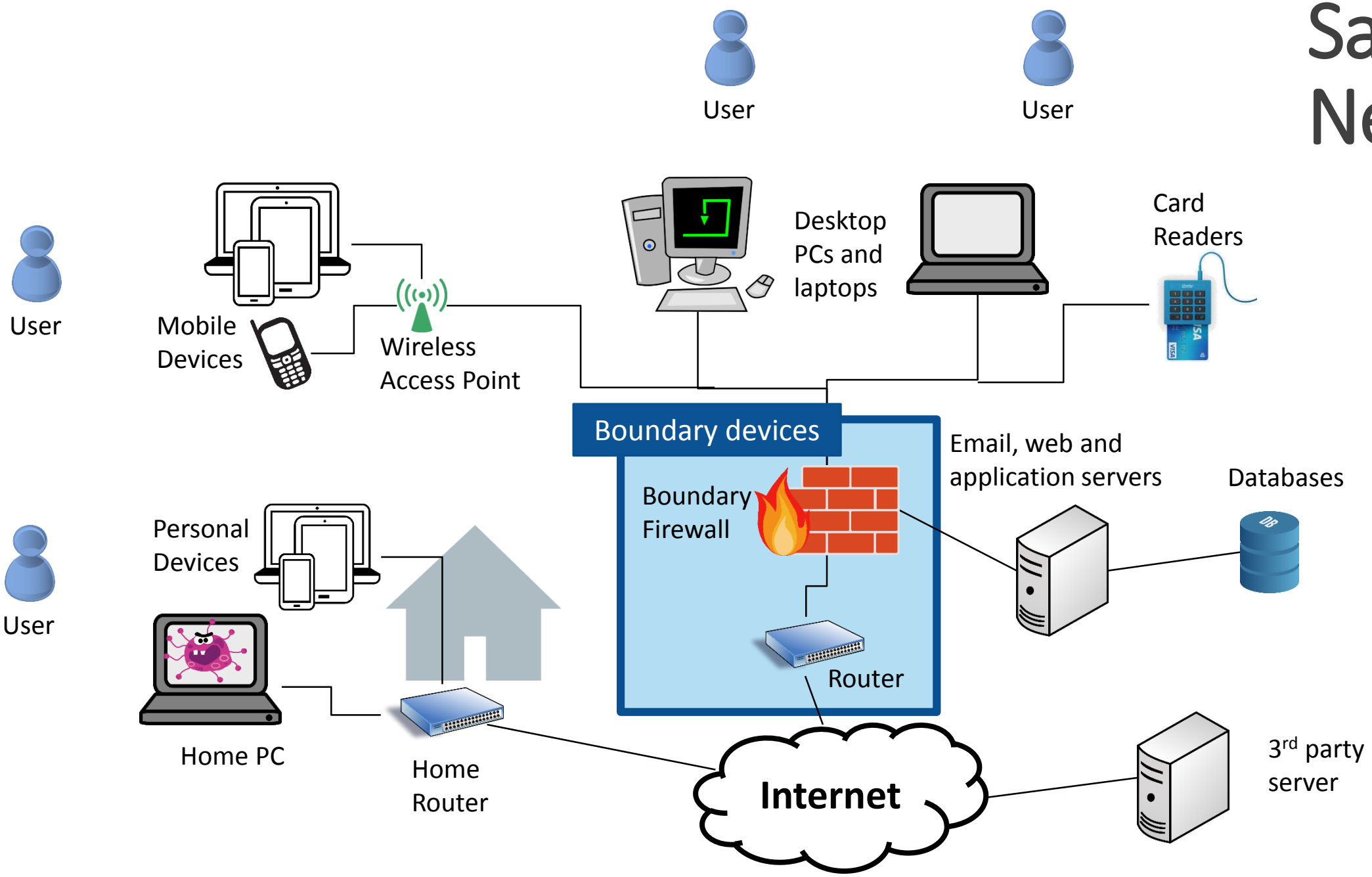
Objectives: Computers exposed to the internet should be protected against malware infection through the use of malware protection software.

- 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.

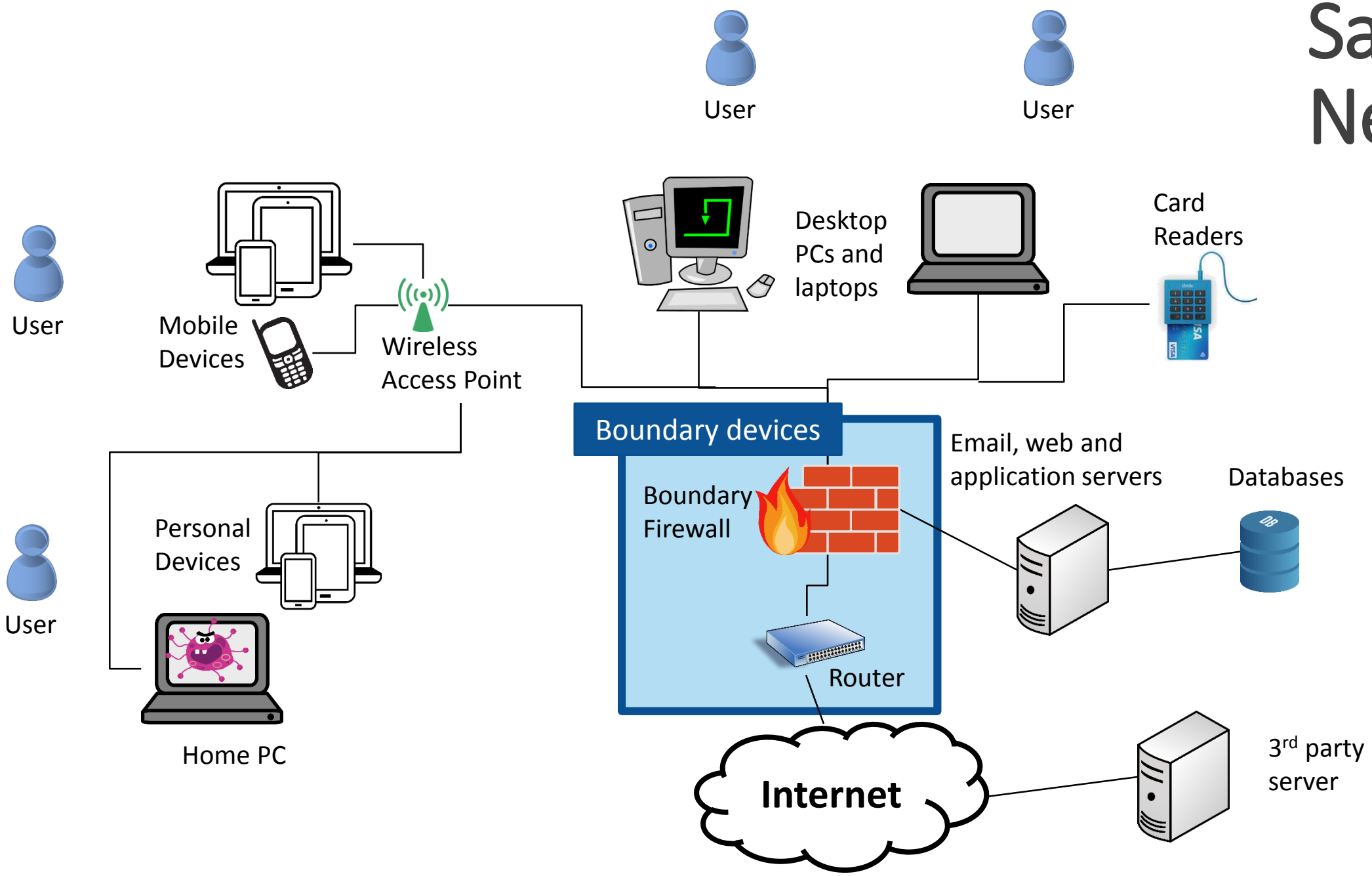
Malware protection

- 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 Washington Post

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 Washington Post

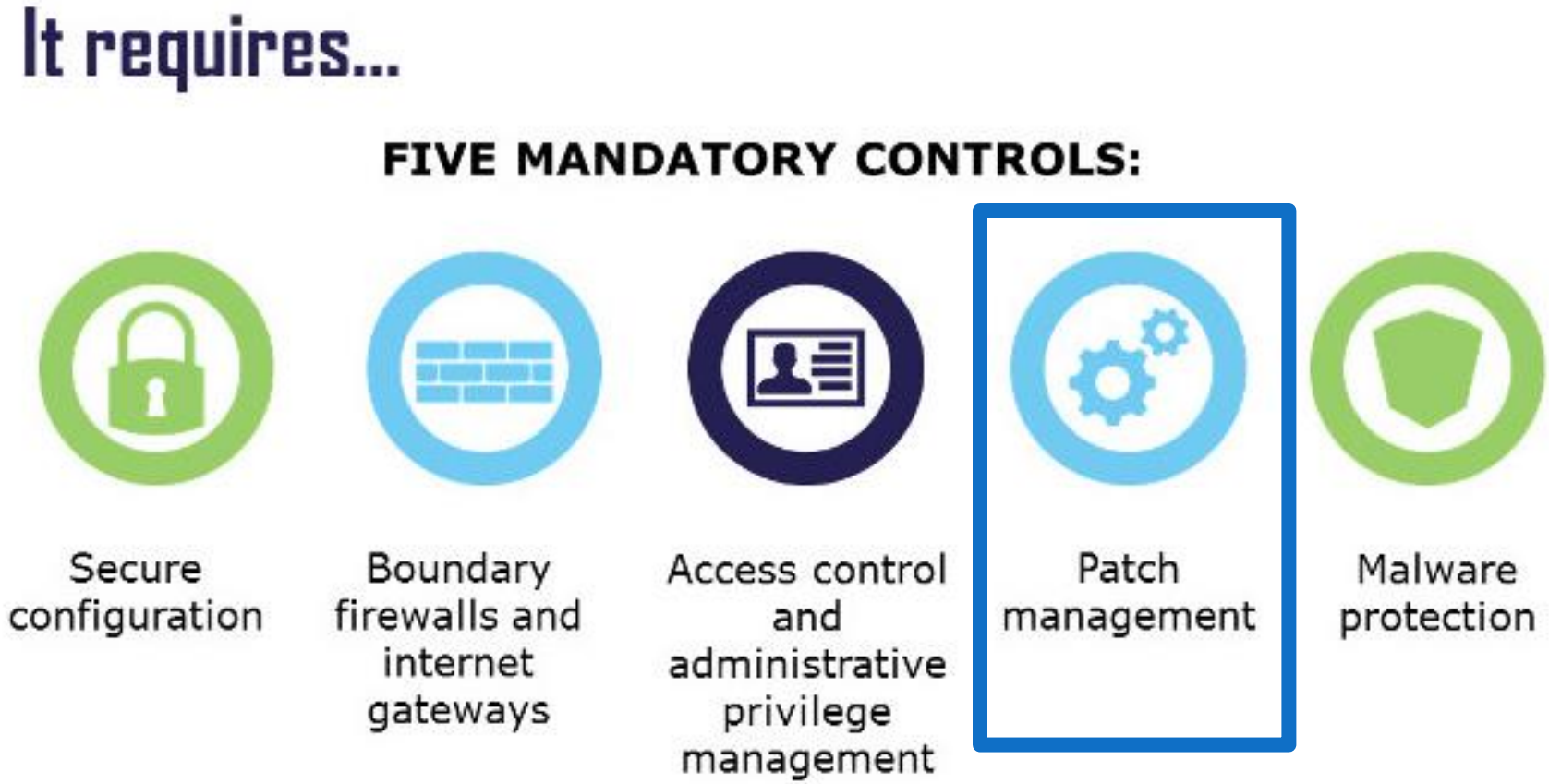
The Switch

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

Cyber Security Essentials



Patch management

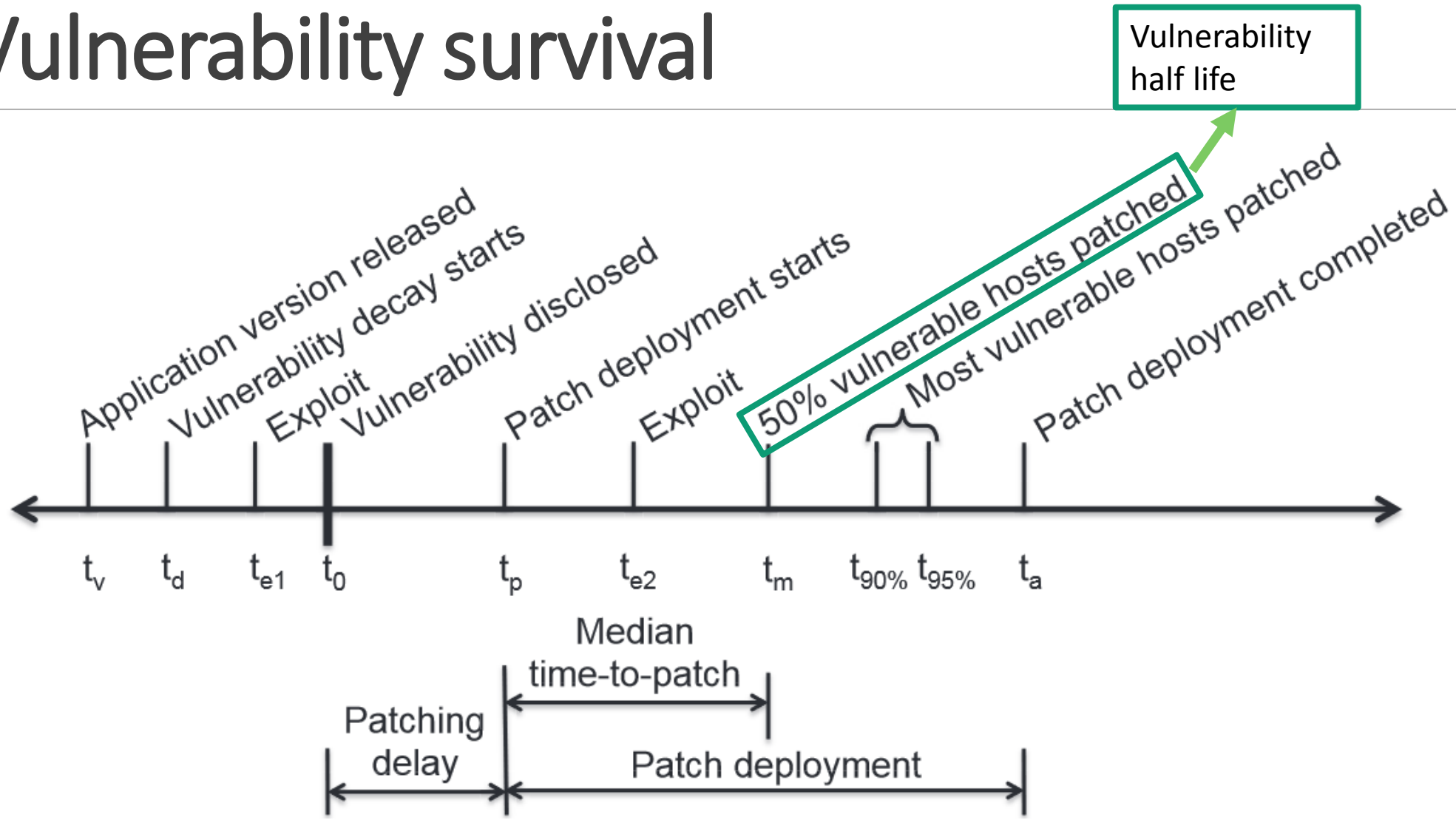
Objectives: Software running on computers and network devices should be kept up-to-date and have the latest security patches installed.

- 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.

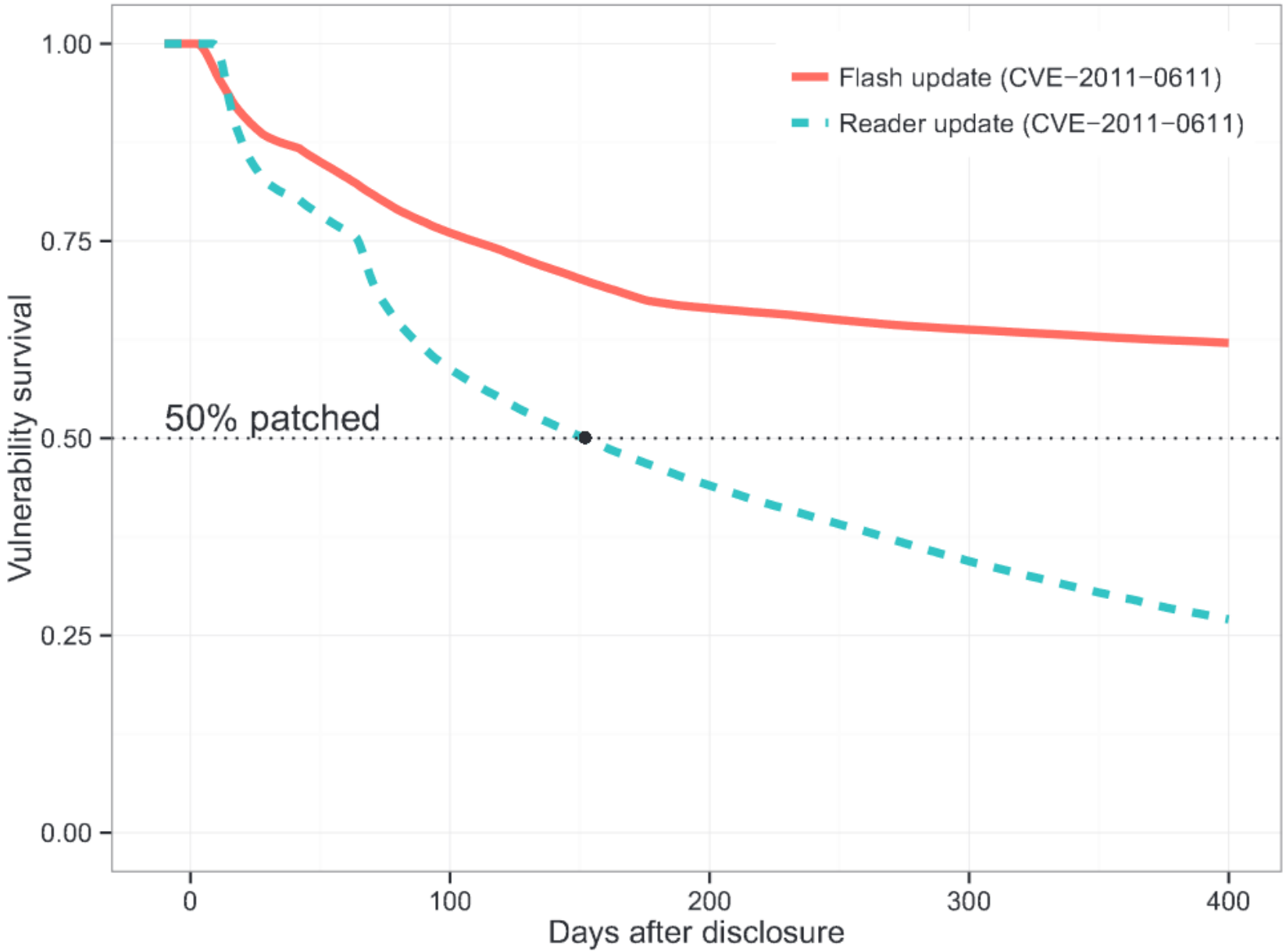
Vulnerability survival



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.



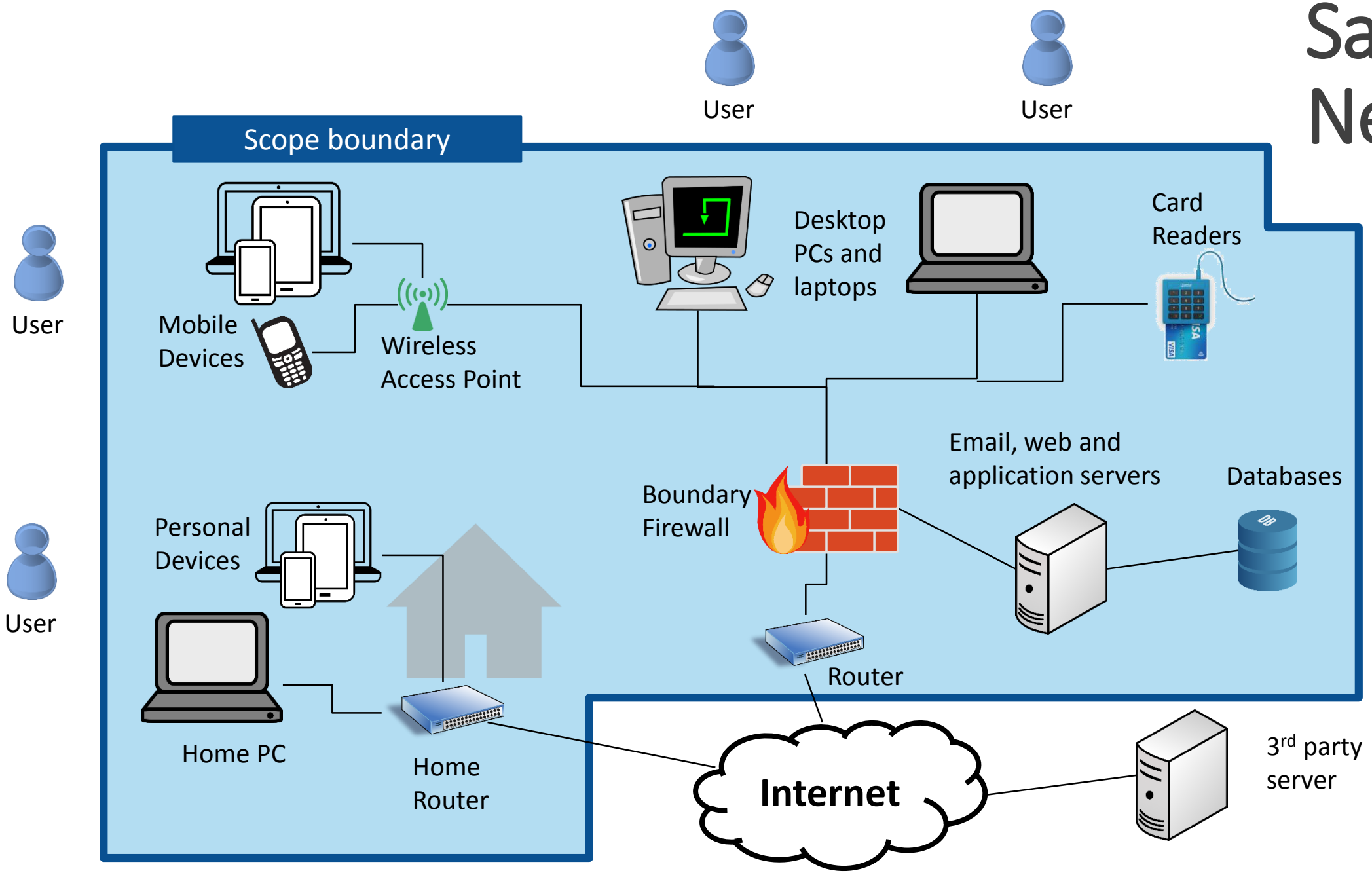
A. Nappa, R. Johnson, L. Bilge, J. Caballero, and T. Dumitraș, “The Attack of the Clones: A Study of the Impact of Shared Code on Vulnerability Patching,” in *IEEE Symposium on Security and Privacy*, San Jose, CA, 2015.

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

Sample Network



Questions