Cyber Solutions, LLC

Cybersecurity: The 12 Pillars of Prevention

Dave Bell, President
Cyber Solutions, LLC.

Agenda

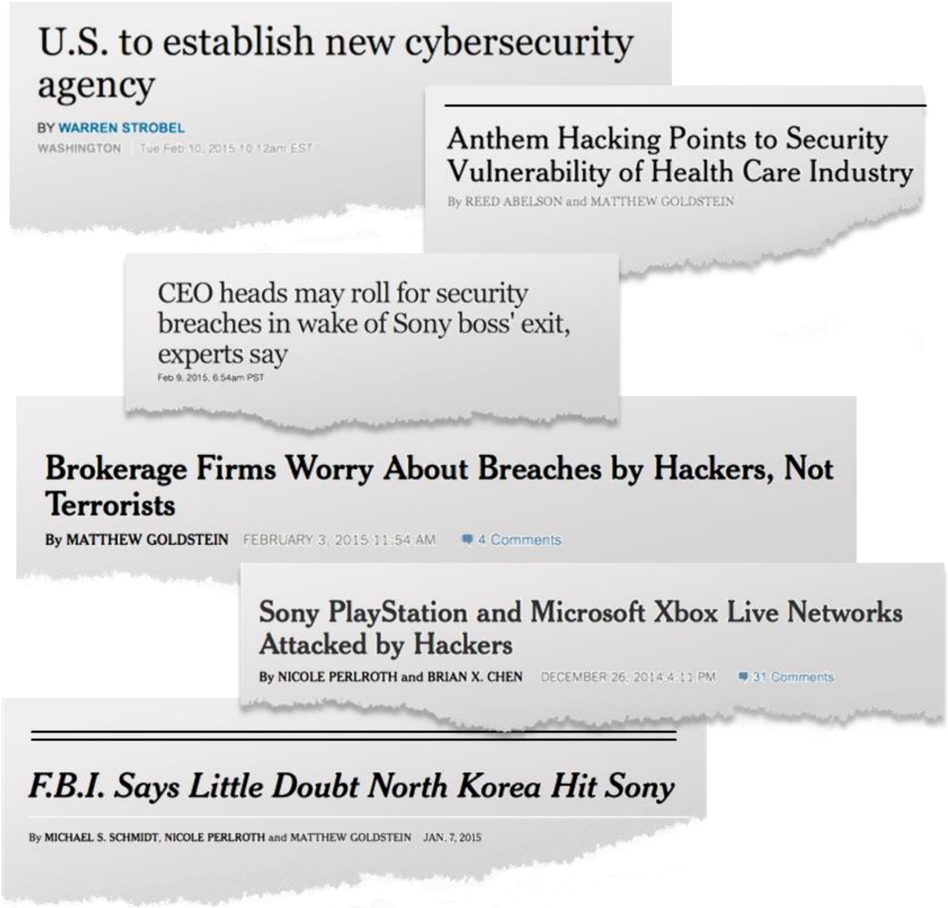
- The ever-changing “Landscape” of security
- 12 Pillars – Layered Protection
- Q & A

Cyber Solutions, LLC

Security Landscape

Security Breaches

A New Headline Every Day



U.S. to establish new cybersecurity agency

BY WARREN STROBEL

WASHINGTON | Tue Feb 10, 2015 10:12am EST

Anthem Hacking Points to Security Vulnerability of Health Care Industry

By REED ABELSON and MATTHEW GOLDSTEIN

CEO heads may roll for security breaches in wake of Sony boss' exit, experts say

Feb 9, 2015, 6:54am PST

Brokerage Firms Worry About Breaches by Hackers, Not Terrorists

By MATTHEW GOLDSTEIN FEBRUARY 3, 2015 11:54 AM 4 Comments

Sony PlayStation and Microsoft Xbox Live Networks Attacked by Hackers

By NICOLE PERLROTH and BRIAN X. CHEN DECEMBER 26, 2014 4:11 PM 31 Comments

F.B.I. Says Little Doubt North Korea Hit Sony

By MICHAEL S. SCHMIDT, NICOLE PERLROTH and MATTHEW GOLDSTEIN JAN. 7, 2015

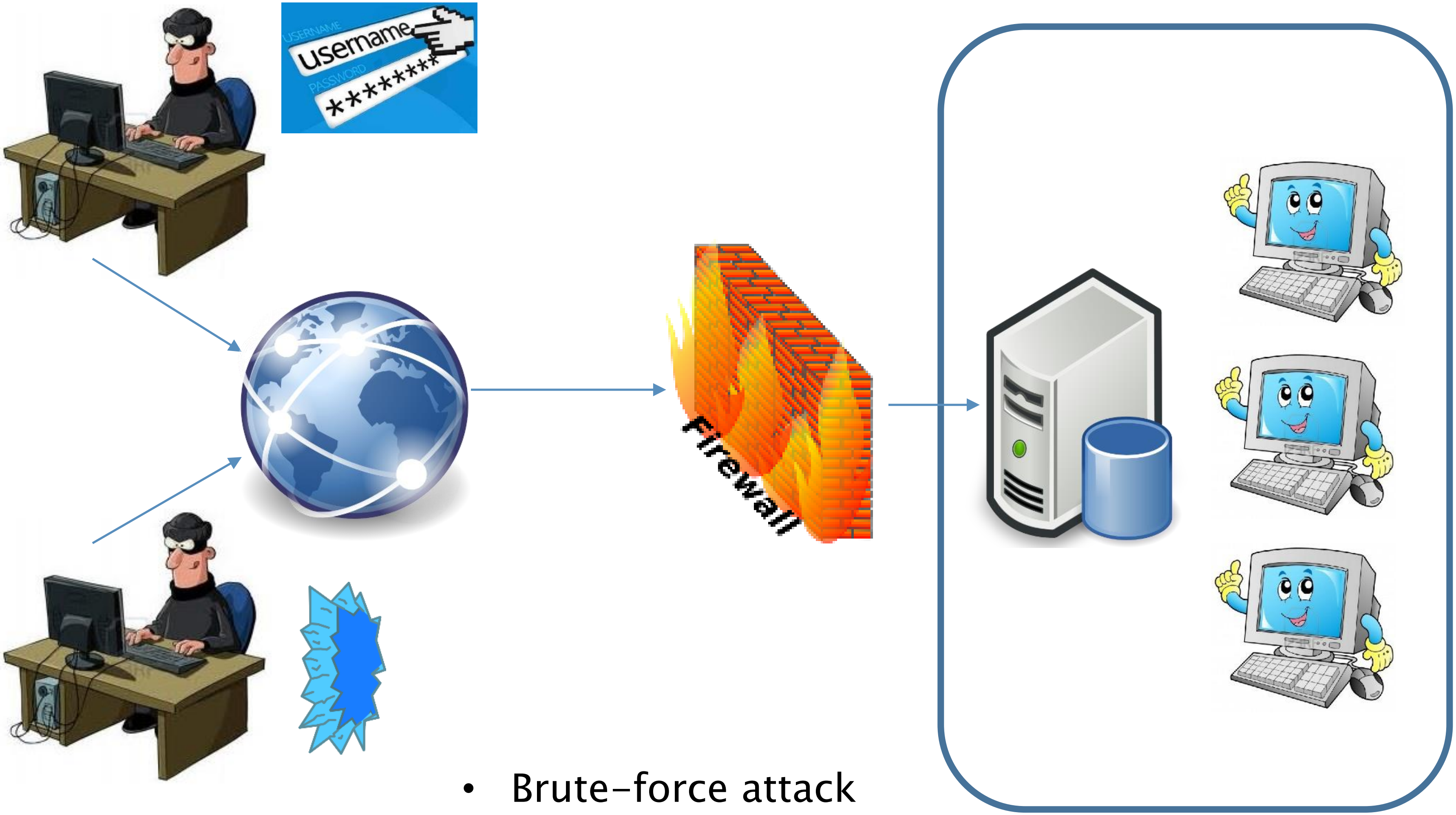
Cyber Solutions, LLC

Security Landscape

- Attack Types
  - Firewall penetration
  - Trojan horse strategy
  - More Ransomware!
    - WannaCry, CryptoLocker, etc
    - $1B industry in 2016

Cyber Solutions, LLC

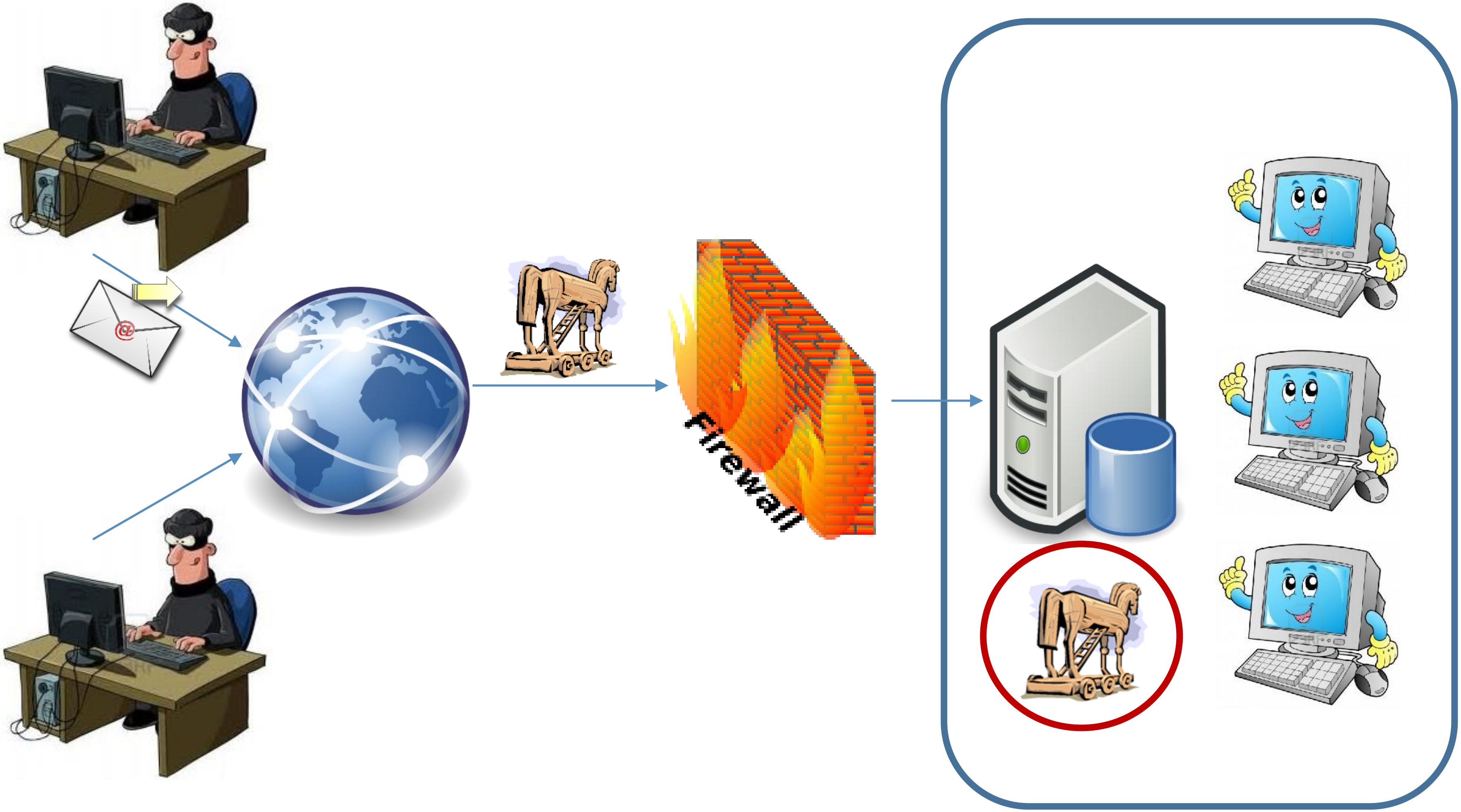
Firewall Penetration



- Brute-force attack
- Firewall vulnerabilities
- Insecure firewall ports (holes)

Cyber Solutions, LLC

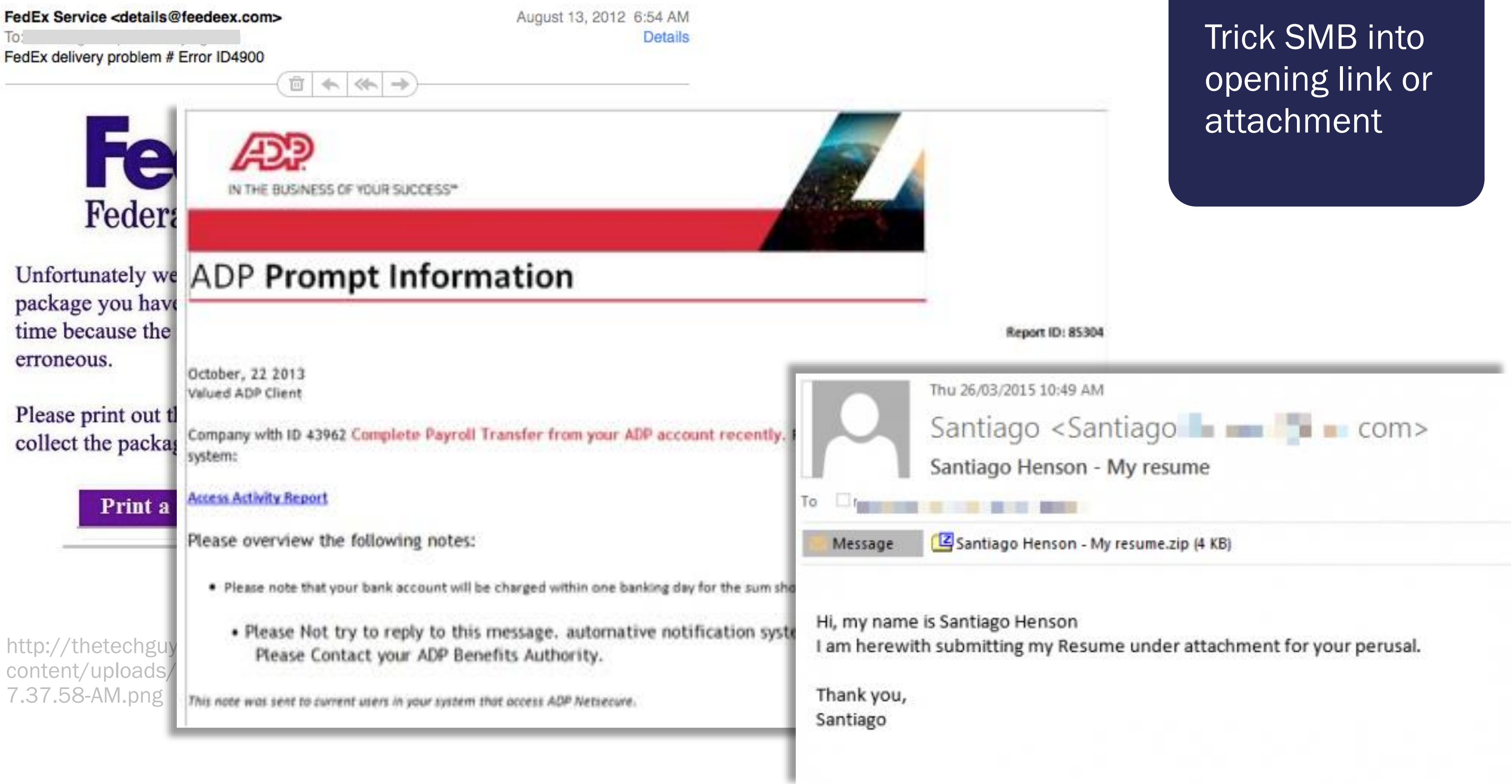
Trojan Horse Strategy



Trojan Horse Phishing Email

TACTIC

Trick SMB into opening link or attachment



FedEx Service <details@feedeex.com> August 13, 2012 6:54 AM

To: [redacted] Details

FedEx delivery problem # Error ID4900

Federa

Unfortunately we
package you hav
time because the
erroneous.

Please print out t
collect the packa

Print a

http://thetechguy
content/uploads/
7.37.58-AM.png

IN THE BUSINESS OF YOUR SUCCESS℠

ADP **Prompt Information**

Report ID: 85304

October, 22 2013
Valued ADP Client

Company with ID 43962 Complete Payroll Transfer from your ADP account recently.
system:

Access Activity Report

Please overview the following notes:

- Please note that your bank account will be charged within one banking day for the sum sho
- Please Not try to reply to this message. automative notification syst
  Please Contact your ADP Benefits Authority.

This note was sent to current users in your system that access ADP Netsecure.

Thu 26/03/2015 10:49 AM

Santiago <Santiago[redacted] com>

Santiago Henson - My resume

To [redacted]

Message | Santiago Henson - My resume.zip (4 KB)

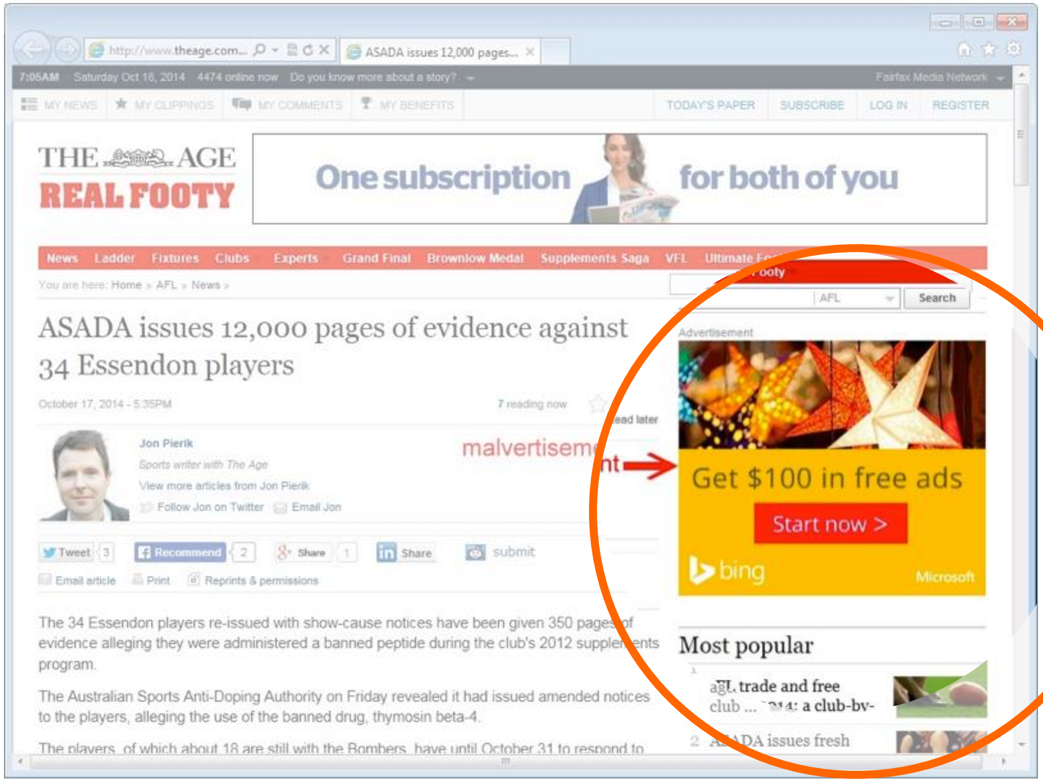
Hi, my name is Santiago Henson
I am herewith submitting my Resume under attachment for your perusal.

Thank you,
Santiago

Cyber Solutions, LLC

Trojan Horse – Malvertising

Malvertising Using Hijacked Images to Target SMBs



ASADA issues 12,000 pages of evidence against 34 Essendon players

October 17, 2014 - 5:35PM

Jon Pierik

Sports writer with The Age

View more articles from Jon Pierik

Follow Jon on Twitter Email Jon

The 34 Essendon players re-issued with show-cause notices have been given 350 pages of evidence alleging they were administered a banned peptide during the club's 2012 supplements program.

The Australian Sports Anti-Doping Authority on Friday revealed it had issued amended notices to the players, alleging the use of the banned drug, thymosin beta-4.

The players, of which about 18 are still with the Bombers, have until October 31 to respond to

Most popular

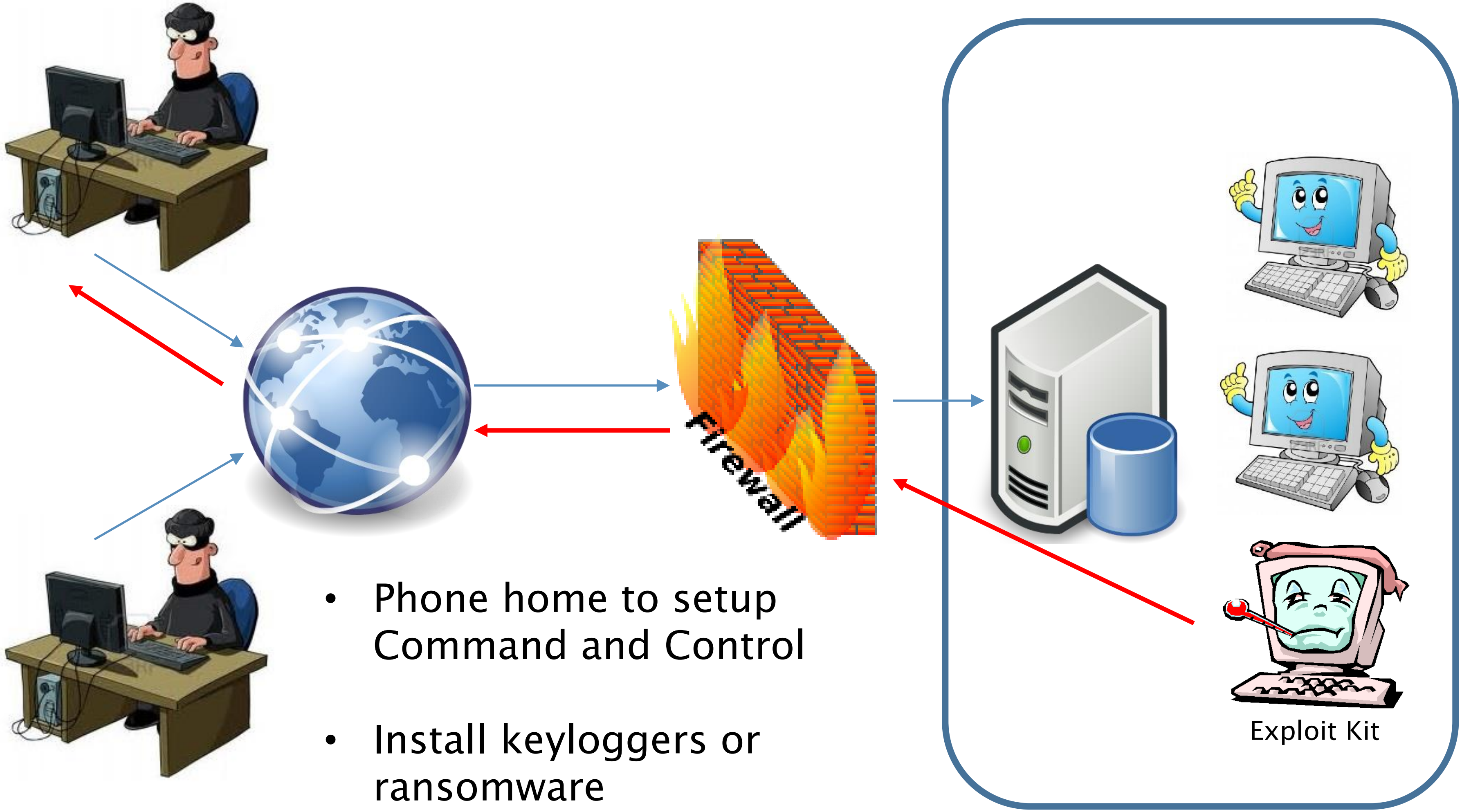
1 AFL trade and free agency 2014: a club-by-

2 ASADA issues fresh

Image: http://news.softpedia.com/news/CryptoWall-2-0-Delivered-Through-Malvertising-On-Yahoo-and-Other-Large-Sites-462970.shtml#sgal_0

Cyber Solutions, LLC

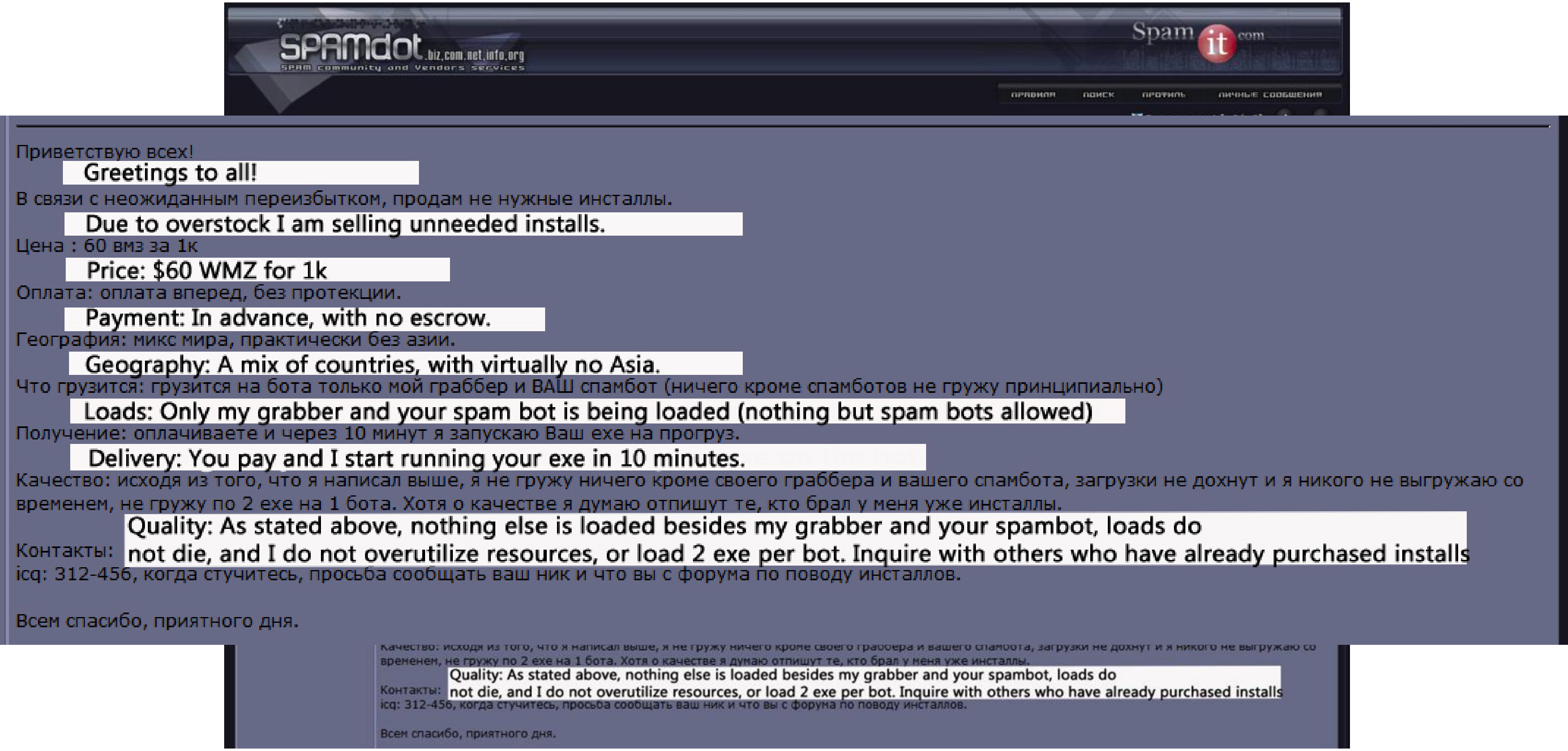
Once inside...



- Phone home to setup Command and Control
- Install keyloggers or ransomware
- Network enumeration – recon

Cyber Solutions, LLC

Cyber Crime Craigslist


SPAMdot.biz,com,net,info,org
SPAM community and Vendors services
Spam it com
правила
поиск
профиль
личные сообщения

Приветствую всех!

Greetings to all!

В связи с неожиданным переизбытком, продам не нужные инсталлы.

Due to overstock I am selling unneeded installs.

Цена : 60 вмз за 1к

Price: $60 WMZ for 1k

Оплата: оплата вперед, без протекции.

Payment: In advance, with no escrow.

География: микс мира, практически без азии.

Geography: A mix of countries, with virtually no Asia.

Что грузится: грузится на бота только мой граббер и ВАШ спамбот (ничего кроме спамботов не гружу принципиально)

Loads: Only my grabber and your spam bot is being loaded (nothing but spam bots allowed)

Получение: оплачиваете и через 10 минут я запускаю Ваш exe на прогруз.

Delivery: You pay and I start running your exe in 10 minutes.

Качество: исходя из того, что я написал выше, я не гружу ничего кроме своего граббера и вашего спамбота, загрузки не дохнут и я никого не выгружаю со временем, не гружу по 2 exe на 1 бота. Хотя о качестве я думаю отпишут те, кто брал у меня уже инсталлы.

Quality: As stated above, nothing else is loaded besides my grabber and your spambot, loads do not die, and I do not overutilize resources, or load 2 exe per bot. Inquire with others who have already purchased installs

Контакты:
icq: 312-456, когда стучитесь, просьба сообщать ваш ник и что вы с форума по поводу инсталлов.

Всем спасибо, приятного дня.

Качество: исходя из того, что я написал выше, я не гружу ничего кроме своего граббера и вашего спамбота, загрузки не дохнут и я никого не выгружаю со временем, не гружу по 2 exe на 1 бота. Хотя о качестве я думаю отпишут те, кто брал у меня уже инсталлы.

Quality: As stated above, nothing else is loaded besides my grabber and your spambot, loads do not die, and I do not overutilize resources, or load 2 exe per bot. Inquire with others who have already purchased installs

Контакты:
icq: 312-456, когда стучитесь, просьба сообщать ваш ник и что вы с форума по поводу инсталлов.

Всем спасибо, приятного дня.

Source: krebsonsecurity.com

Cyber Solutions, LLC

Price Per Infection

Region	2015 Average Price per 1,000 Infections	2015 Average Price per install
US	$70	$0.07
Europe	$105	$0.11
Asia	$140	$0.14
Australia	$140	$0.14

Data from Trend Micro Report: “Russian Underground 2.0”

Cyber Solutions, LLC

“Defense in Depth” Layers of protection

“Signature-based tools (antivirus, firewalls, and intrusion prevention) are only effective against 30-50% of current security threats.”

IDC
November 2011

Cyber Solutions, LLC

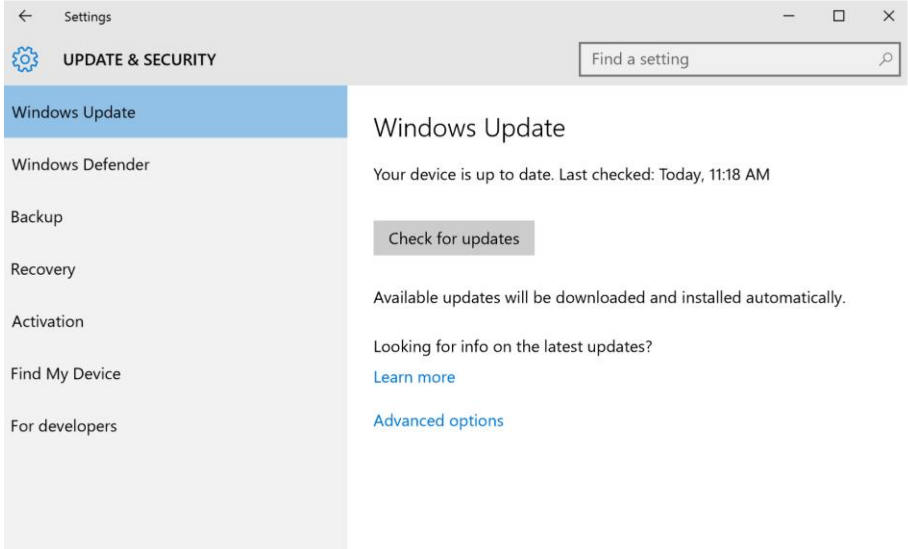
The 12 Pillars of Prevention

1. Patching/Updates
2. Advanced Endpoint Security
3. Spam filtering
4. Firewall – perimeter protection
5. Shadow IT
6. Backup and Disaster Recovery
7. Monitoring
8. Authentication Methods and Password Management
9. Due diligence – Employee education and AUP
10. Encryption
11. Wireless Networks
12. Cyber Insurance

Cyber Solutions, LLC

Pillar 1 – Patching/Updates

- 90% of infections could be prevented
- Windows/Office



Windows Update

Your device is up to date. Last checked: Today, 11:18 AM

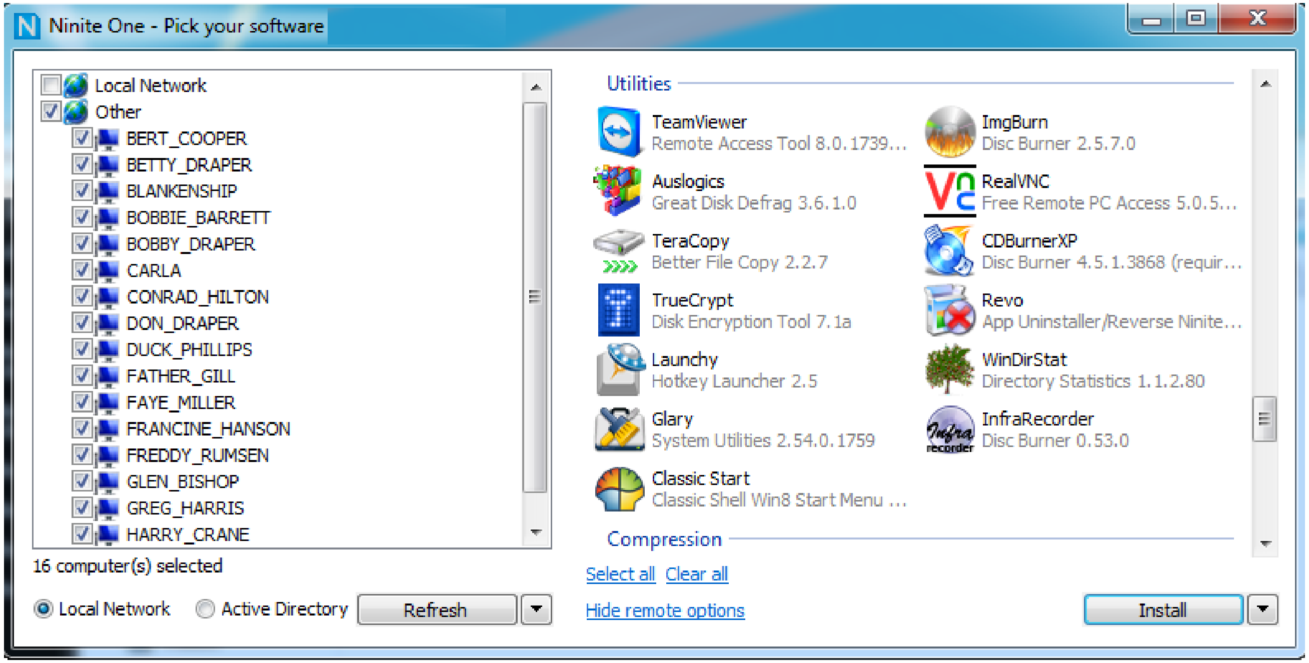
Available updates will be downloaded and installed automatically.

Looking for info on the latest updates?

Cyber Solutions, LLC

Patching/Updates

- Adobe, Java
- Ninite Pro subscription – www.ninite.com



Ninite One - Pick your software

- □ Local Network
- ☑ Other
  - ☑ BERT_COOPER
  - ☑ BETTY_DRAPER
  - ☑ BLANKENSHIP
  - ☑ BOBBIE_BARRETT
  - ☑ BOBBY_DRAPER
  - ☑ CARLA
  - ☑ CONRAD_HILTON
  - ☑ DON_DRAPER
  - ☑ DUCK_PHILLIPS
  - ☑ FATHER_GILL
  - ☑ FAYE_MILLER
  - ☑ FRANCINE_HANSON
  - ☑ FREDDY_RUMSEN
  - ☑ GLEN_BISHOP
  - ☑ GREG_HARRIS
  - ☑ HARRY_CRANE

16 computer(s) selected

● Local Network ○ Active Directory Refresh

Utilities

TeamViewer
Remote Access Tool 8.0.1739...

ImgBurn
Disc Burner 2.5.7.0

Auslogics
Great Disk Defrag 3.6.1.0

RealVNC
Free Remote PC Access 5.0.5...

TeraCopy
Better File Copy 2.2.7

CDBurnerXP
Disc Burner 4.5.1.3868 (requir...

TrueCrypt
Disk Encryption Tool 7.1a

Revo
App Uninstaller/Reverse Ninite...

Launchy
Hotkey Launcher 2.5

WinDirStat
Directory Statistics 1.1.2.80

Glary
System Utilities 2.54.0.1759

InfraRecorder
Disc Burner 0.53.0

Classic Start
Classic Shell Win8 Start Menu ...

Compression

Select all Clear all

Hide remote options

Install

Cyber Solutions, LLC

Pillar 1 – Takeaways

- Do not “set it and forget it”
- Use built-in Windows Updates
- Ninite Pro subscription for 3rd party apps

Cyber Solutions, LLC

Pillar 2 – Advanced Endpoint Security

- Signature-based vs. Cloud-based
- Don’t forget mobile devices!
  - Both iOS devices Android devices
- Cloud-based malware protection/Content Filtering

Cyber Solutions, LLC

Pillar 2 – Advanced Endpoint Security (Content Filtering)

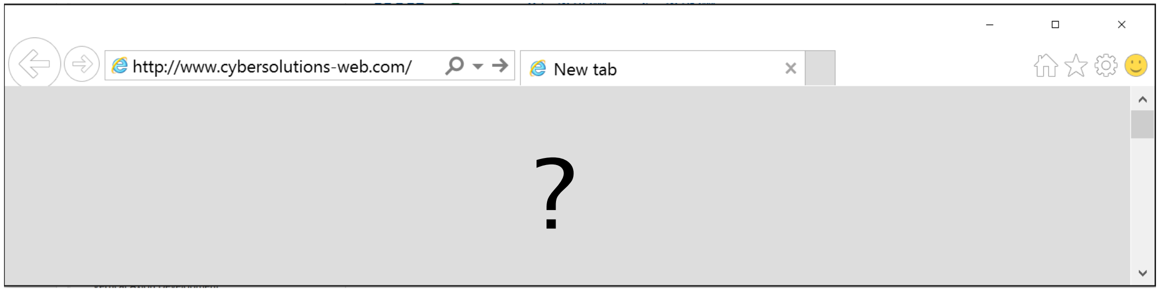
- What is DNS?
- Cloud-based malware protection
- Content filtering

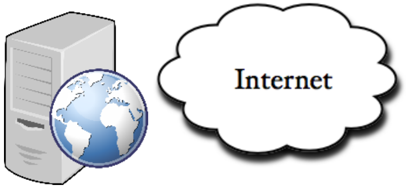
Cyber Solutions, LLC

What is DNS?

Step 1 – Browser does not know the IP address so it contacts DNS server

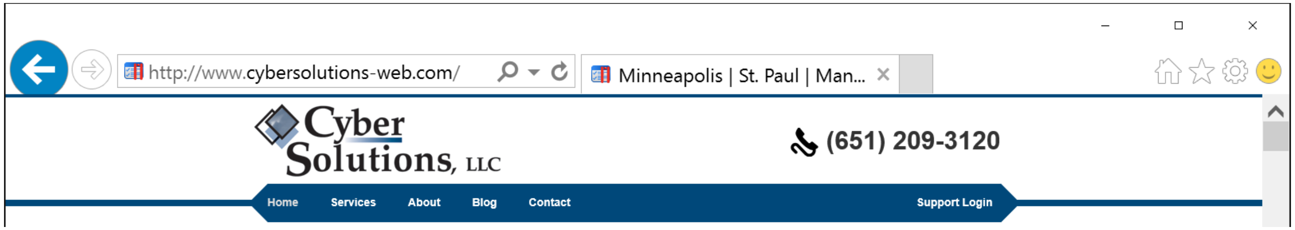
Example: www.cybersolutions-web.com = 1.2.3.4





Step 2 – DNS resolves web address to numeric IP address

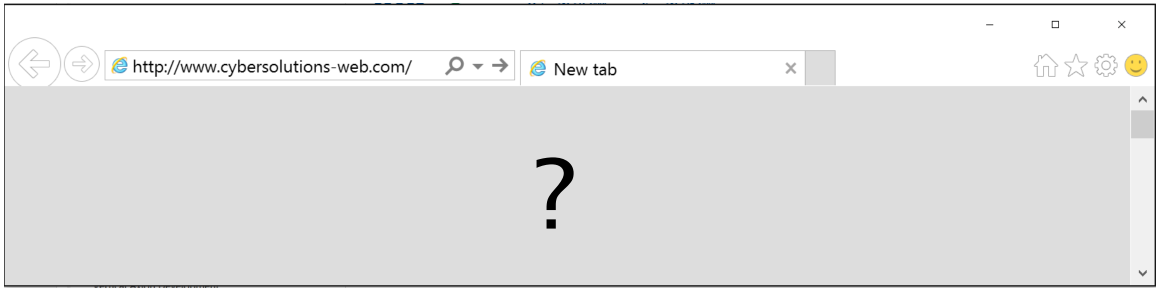
Step 3 – Browser uses IP address to contact web server and load web page

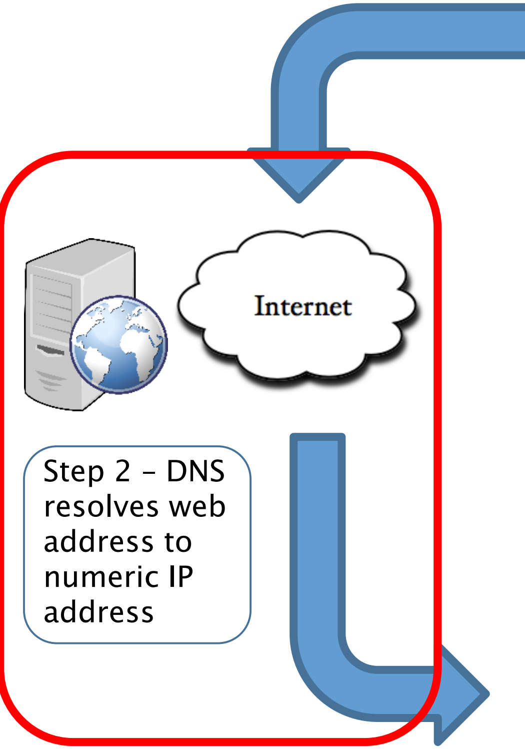


Filtering happens at DNS resolution

Example: www.cybersolutions-web.com = 1.2.3.4

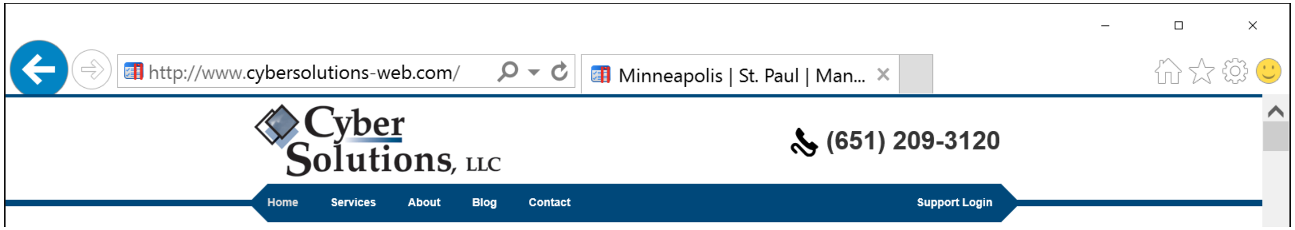
Step 1 – Browser does not know the IP address so it contacts DNS server





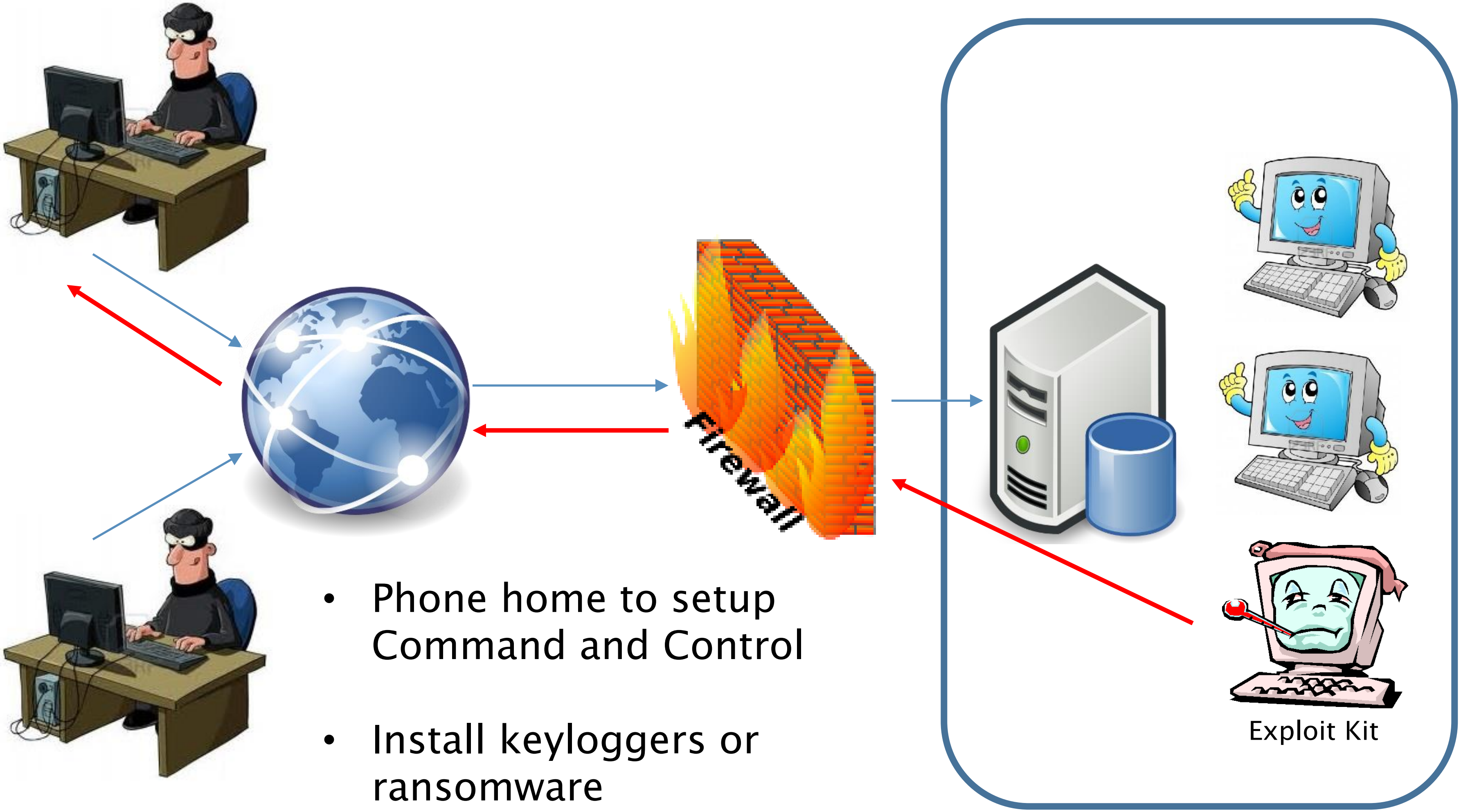
Step 2 – DNS resolves web address to numeric IP address

Step 3 – Browser uses IP address to contact web server and load web page



Cyber Solutions, LLC

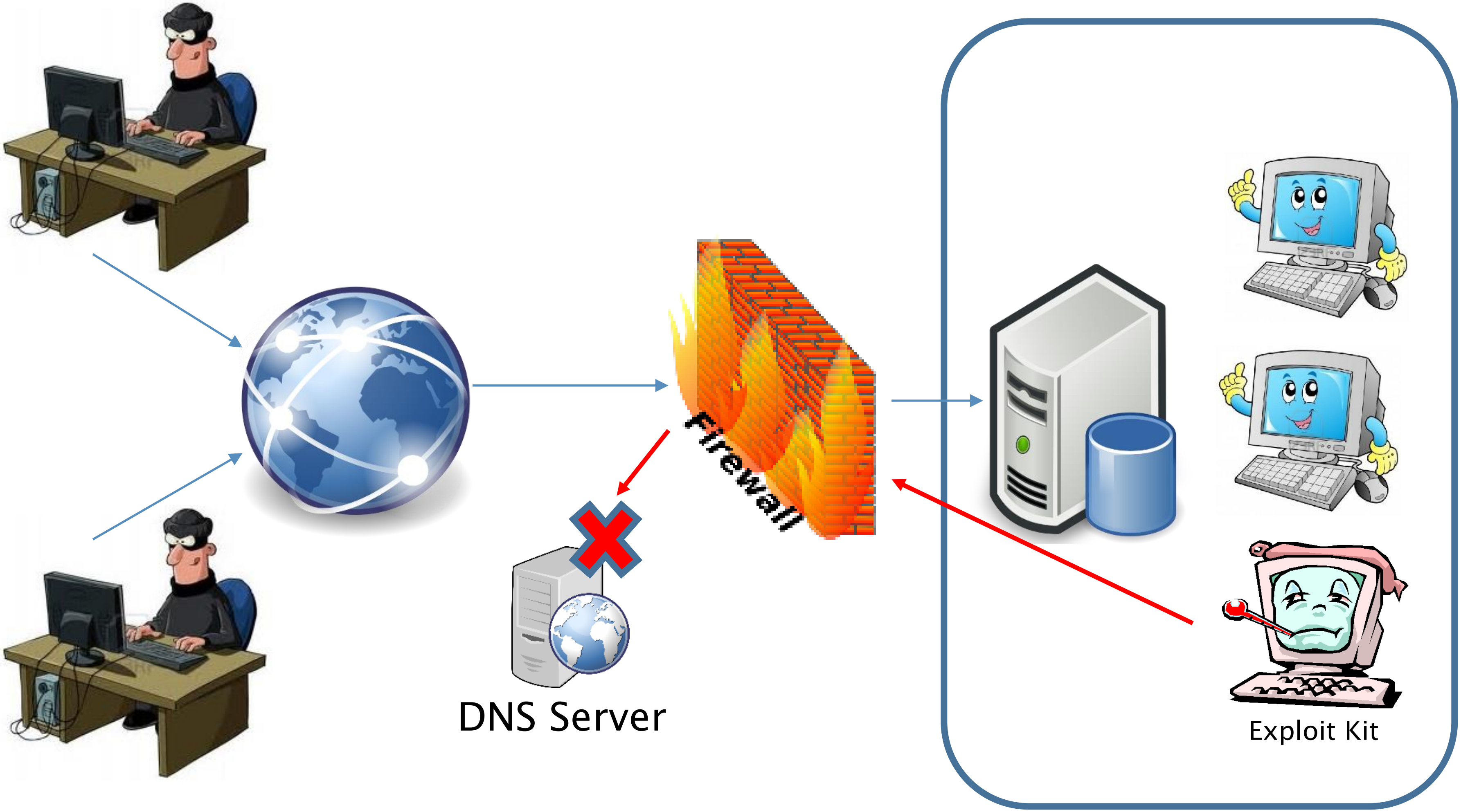
Command and Control



- Phone home to setup Command and Control
- Install keyloggers or ransomware
- Network enumeration – recon

Cyber Solutions, LLC

Blocking DNS traffic



Cyber Solutions, LLC

Cloud-based malware protection

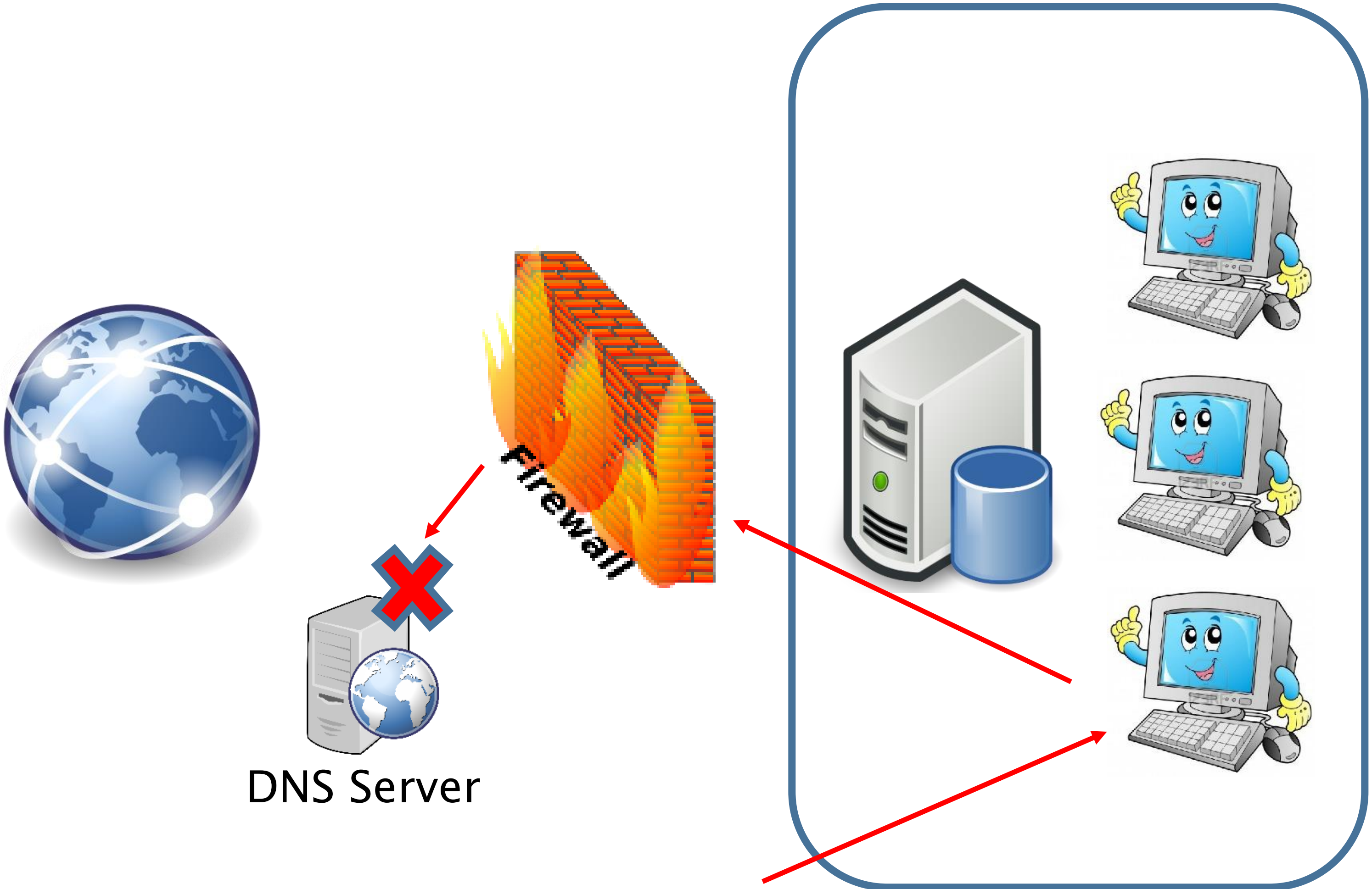
CONTAINMENT

Prevent "Phoning home"

- Block "Exploit Kit" from getting malware
  - Whether it's ransomware, keyloggers, spam senders or DDoS bots
- Stop Spyware/Keyloggers from uploading data
- Prevent Ransomware from getting an Encryption Key
- **Alert – and have team respond to alert**

Cyber Solutions, LLC

Content Filtering



www.socialmedia.com
www.inappropriate.com
www.infected.com

Pillar 2 – Takeaways

- www.webroot.com

- www.opendns.com

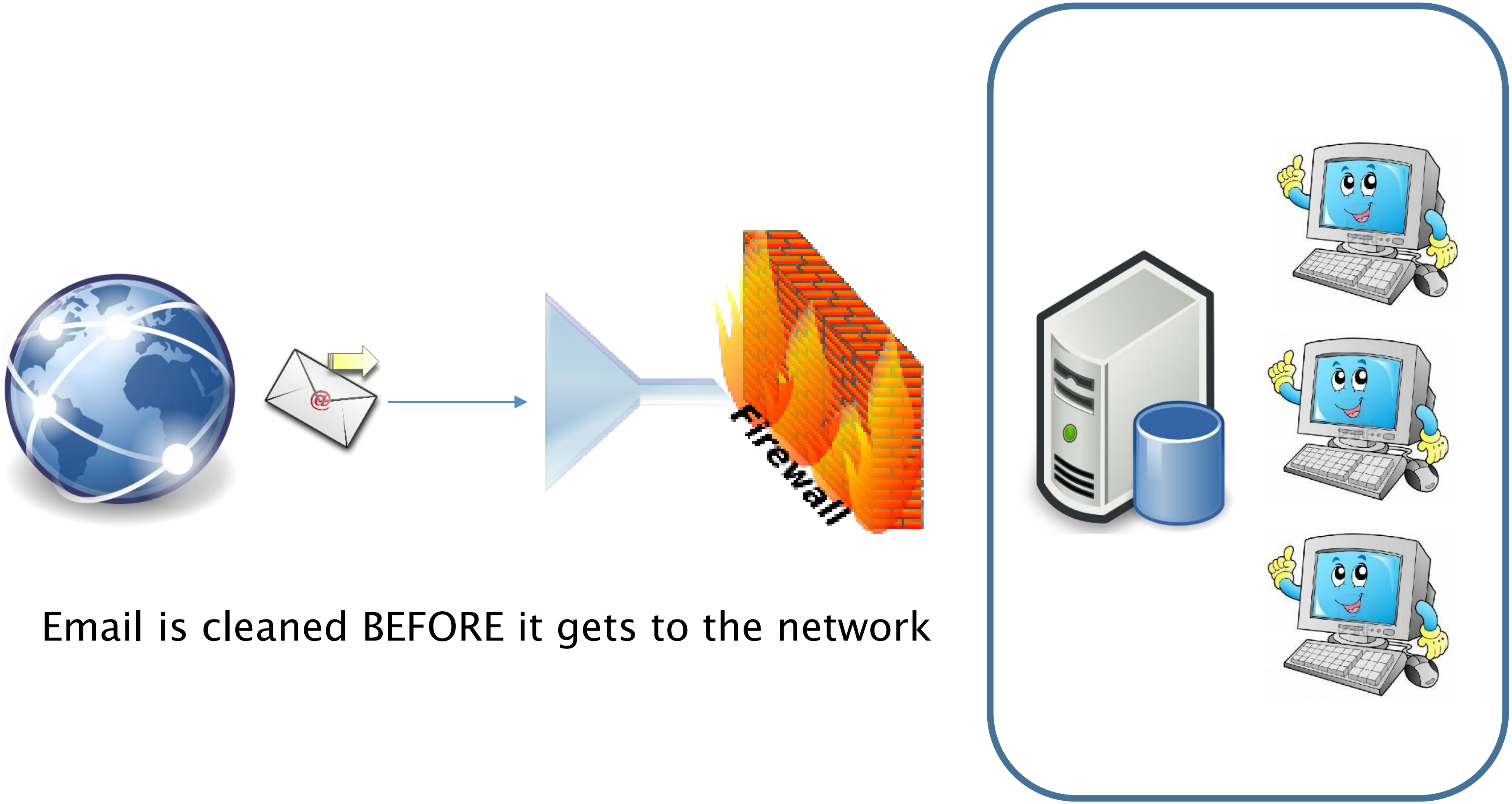
Cyber Solutions, LLC

Pillar 3 – Spam filtering

- Email provides an easy way to introduce malware
- Removes virus, malware, phishing and more
- Hosted filtering vs. Installed filtering

Cyber Solutions, LLC

Hosted Spam Filtering



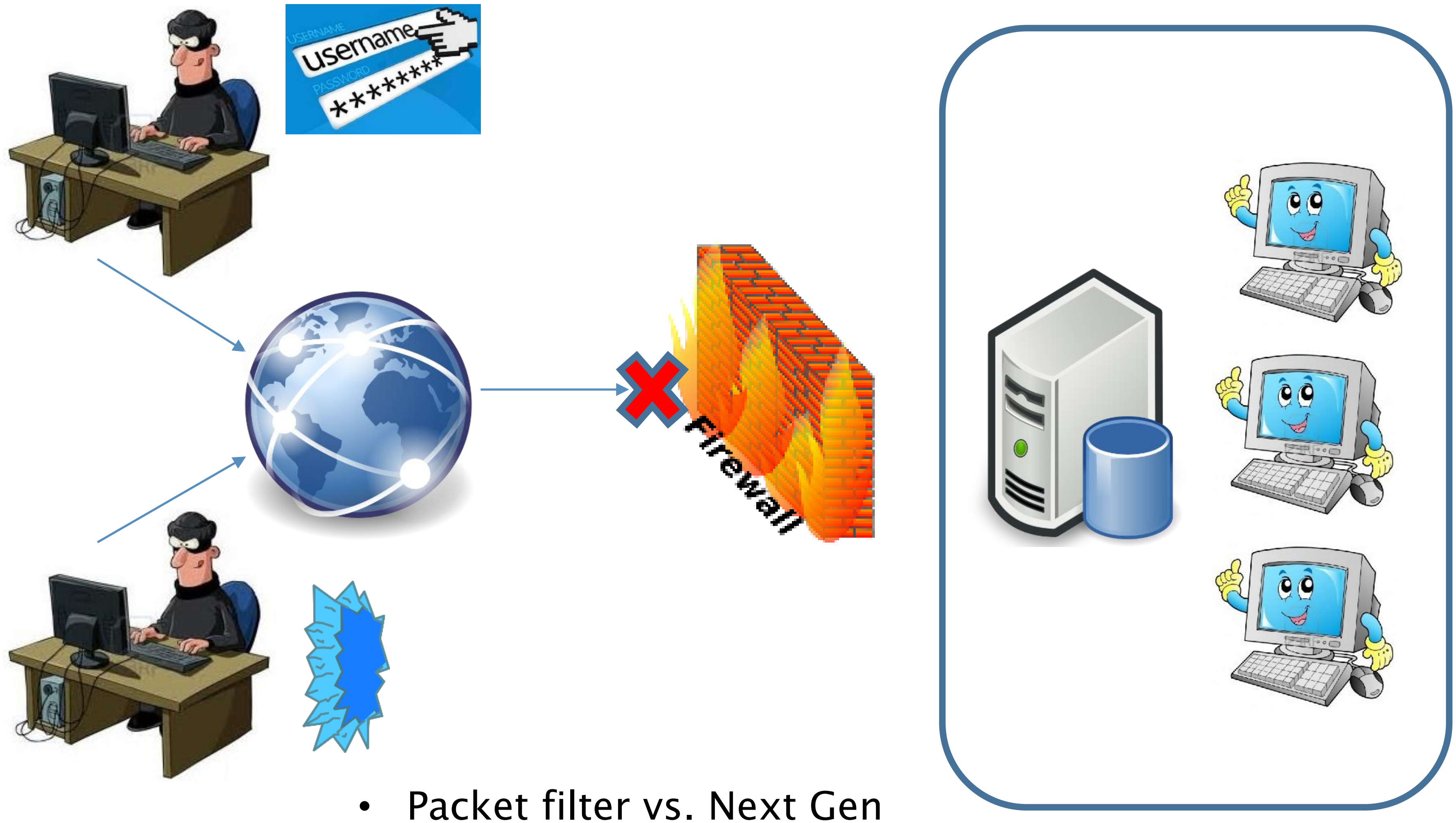
Email is cleaned BEFORE it gets to the network

Pillar 3 – Takeaways

- Built-in Outlook “Junk E-mail” is not great
- Consider additional cleaning thru 3rd party
  - Either hosted or installed
- Hosted Email through Office 365 is very good

Cyber Solutions, LLC

Pillar 4 – Firewall protection



- Packet filter vs. Next Gen
- Unified Threat Management
  - Gateway A/V, IDS, VPN

Cyber Solutions, LLC

Pillar 4 – Takeaways

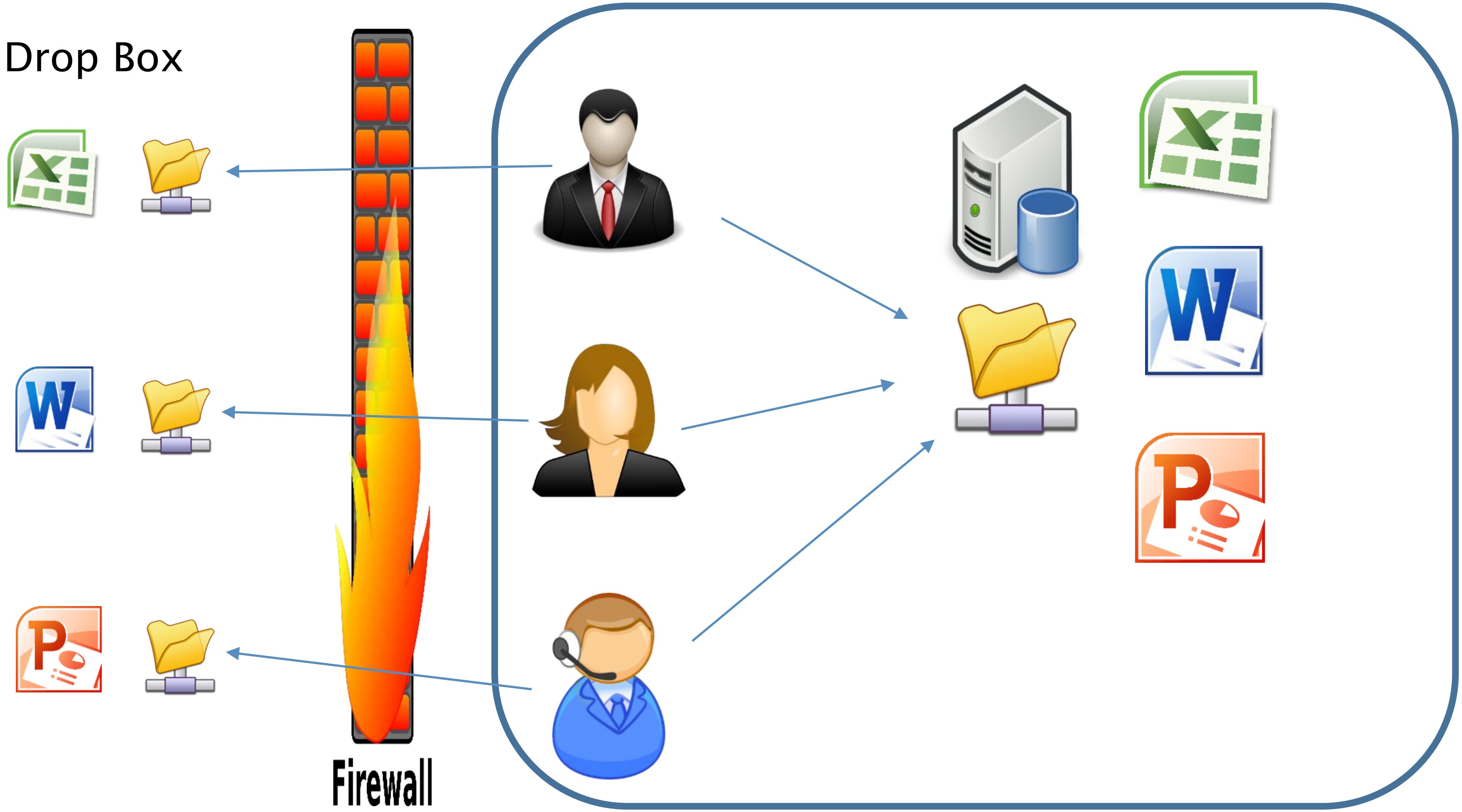
- Invest in a Business-Class firewall
  - WatchGuard Firebox or Dell SonicWall

- Include UTM – typically a subscription

- Start with "Deny-All" then only open what is necessary

Cyber Solutions, LLC

Pillar 5 – Shadow IT



Pillar 5 – Takeaways

- Avoid uncontrolled file sync services
- Include proper file handling in AUP

Cyber Solutions, LLC

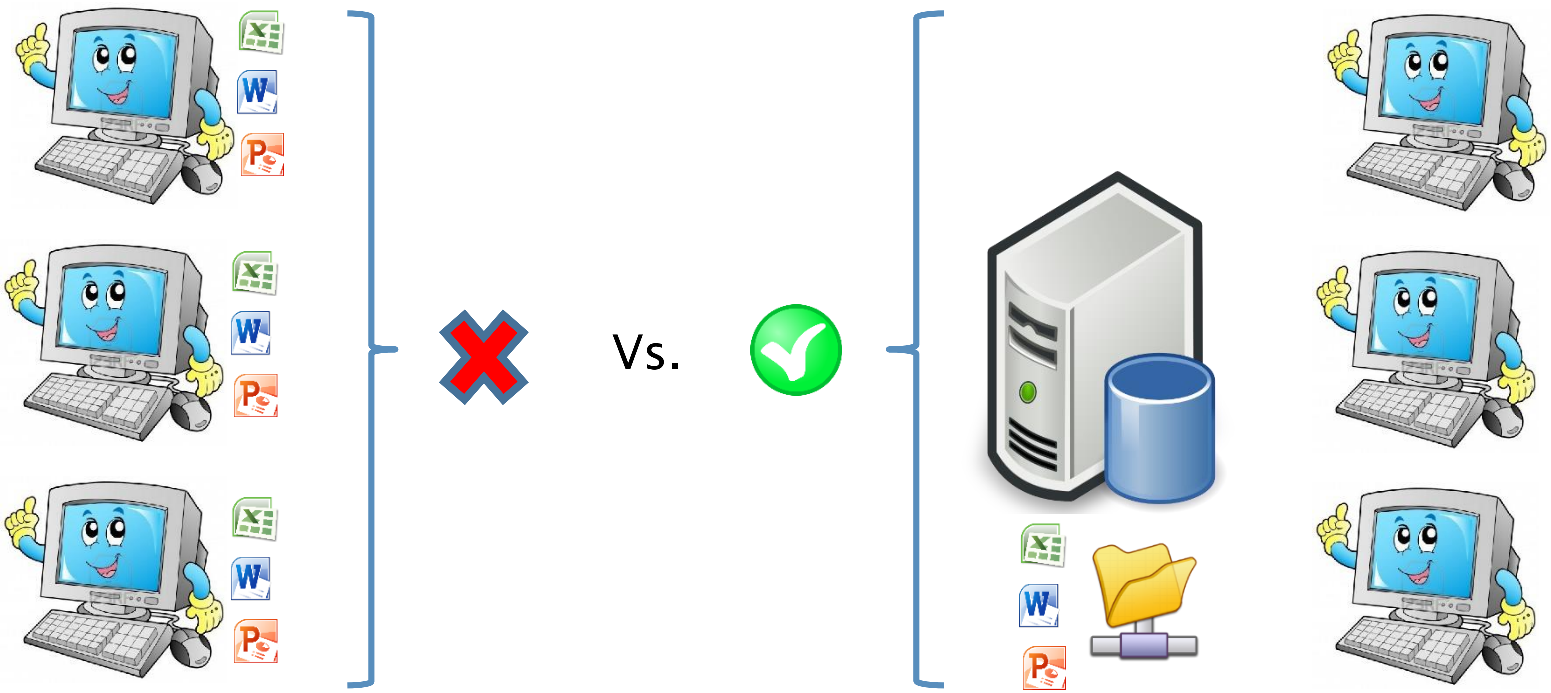
Pillar 6 – Backup and Disaster Recovery

- Centralize data
- Select the right backup software
- Replicate to a remote location

Cyber Solutions, LLC

Pillar 6 – Backup and Disaster Recovery

- Centralize data



Vs.

Cyber Solutions, LLC

Pillar 6 – Backup and Disaster Recovery

- Select the right backup software

File-based backups

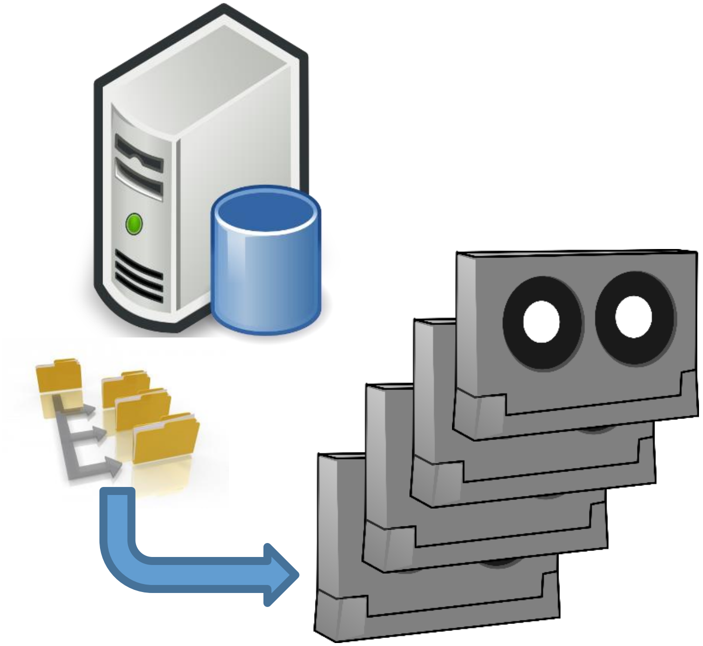
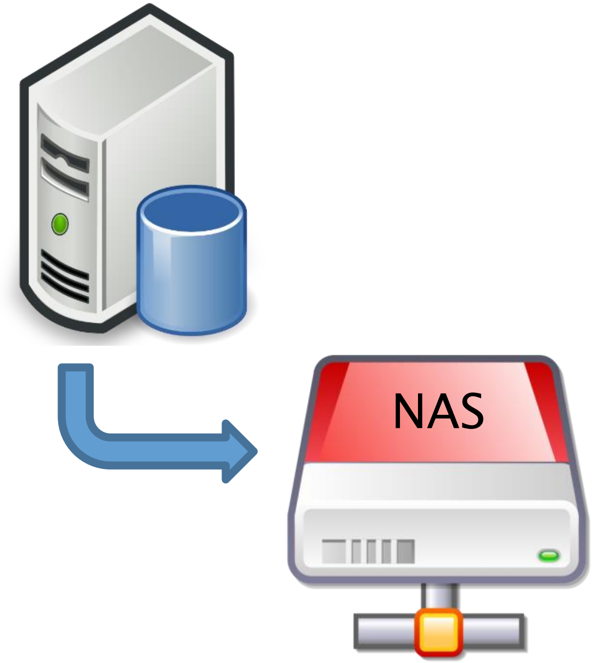


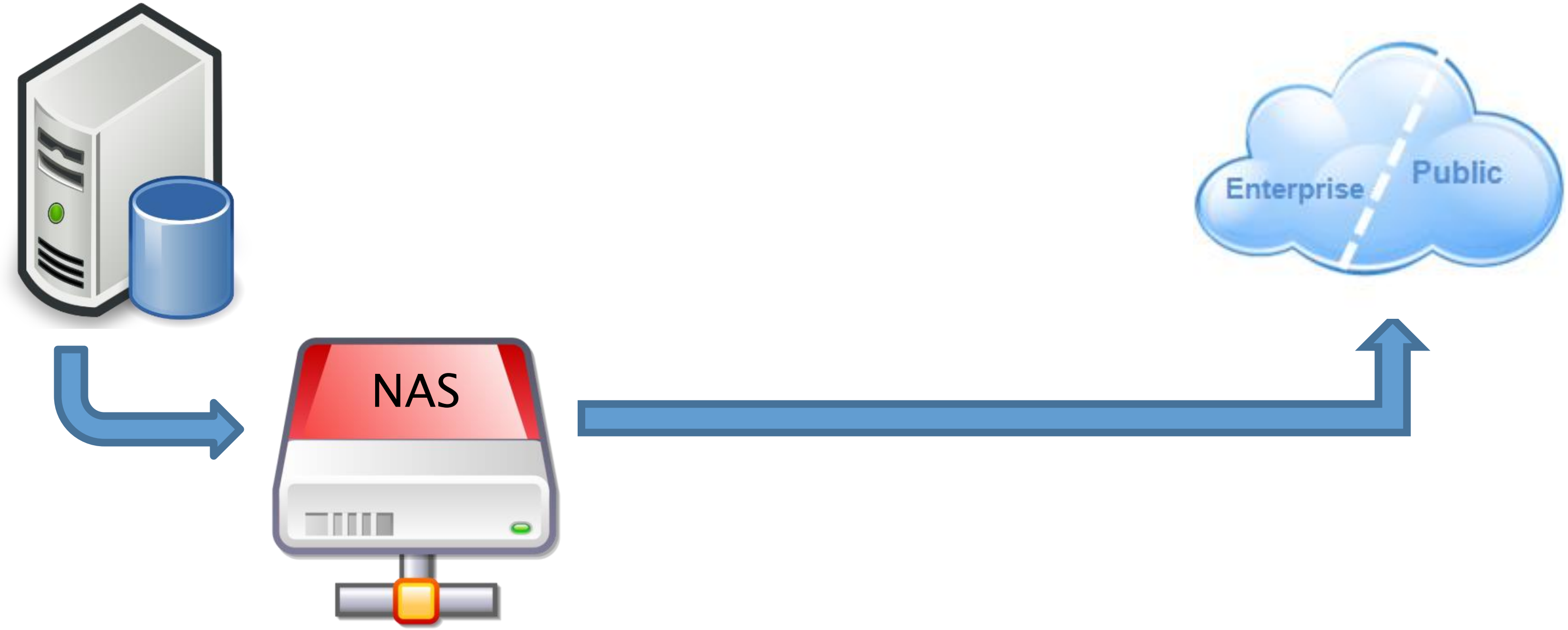
Image-based backups



Cyber Solutions, LLC

Pillar 6 – Backup and Disaster Recovery

- Replicate to a remote location



Cyber Solutions, LLC

Pillar 6 – Takeways

- Hourly backups
  - Protects against ransomware
- Consider bandwidth needs for replication
  - Replicate at night if necessary
- Test restore!
  - Even if just one file (but there are better ways)

Cyber Solutions, LLC

Pillar 7 – Monitoring

- “Set it and forget it” is not an option
- Regular Security Assessments
- Dark Web Research

Cyber Solutions, LLC

Pillar 7 – Takeaways

- Investing in tools to monitor is likely unrealistic
- It CAN be done manually
- Consider outsourcing

Cyber Solutions, LLC

Pillar 8 – Authentication Methods and Password Management

- Two-Factor Authentication (2FA)
  - Something you have PLUS something you know
    - Fob or cell phone

123456
1
2
123456

Cyber Solutions, LLC

Pillar 8 – Authentication Methods and Password Management

- You’ve heard it before, but are you listening?
  - Strong passwords include:
    - Upper-case
    - Lower-case
    - Special characters
    - Numbers

- Don’t use the same password

- Password management tools
  - LastPass – http://www.lastpass.com
  - KeePass – http://www.keepass.info

Cyber Solutions, LLC

Pillar 8 – Takeaways

- Create a password policy

- Consider Two-Factor authentication options

Cyber Solutions, LLC

Pillar 9 – Employee Education and Acceptable Use Policy

- Employees are your last line of defense
- Make sure they understand the risks
- Create an AUP and enforce it

Cyber Solutions, LLC

Pillar 9 – Takeaways

- Create knowledgeable email users
  - If it looks suspicious, it is. Delete it.
  - Spelling and grammatical errors are red flags
  - Hover over links to see unfamiliar web links

- Think before you click!

- Consider phishing simulation emails

Cyber Solutions, LLC

Pillar 10 – Encryption

- At rest vs. in transit (motion)
- Email
- BitLocker – Windows 10
  - O/S drive
  - USB drives
- Backup encryption

Cyber Solutions, LLC

Pillar 10 – Takeaways

- Evaluate data that leaves the network
  - Mobile data (USB, laptops)
  - Backup data
  - Email

- Utilize Windows built-in encryption (BitLocker)

- Utilize backup encryption

Cyber Solutions, LLC

Pillar 11 – Wireless Networks

- Determine need
- Easy to attack
- Guest wireless vs. internal wireless

Pillar 11 – Takeaways

- NO open networks – even guest

- Utilize current encryption
  - Use WPA2 with AES
    - TKIP is outdated
  - No WEP

Cyber Solutions, LLC

Pillar 12 – Cyber Insurance

- Average data breach costs $225/record*
  - Healthcare – $380/record

- Speed of containment is key
  - Have a plan

*Study conducted by Ponemon Institute and sponsored by IBM Security

Cyber Solutions, LLC

Pillar 12 – Takeaways

- Talk to your insurance agent

Cyber Solutions, LLC

Q & A

- Email: dbell@cybersolutions-web.com

Cyber Solutions, LLC