IT Security in the Hybrid World

Randy Marchany

Virginia Tech IT Security Office and Lab

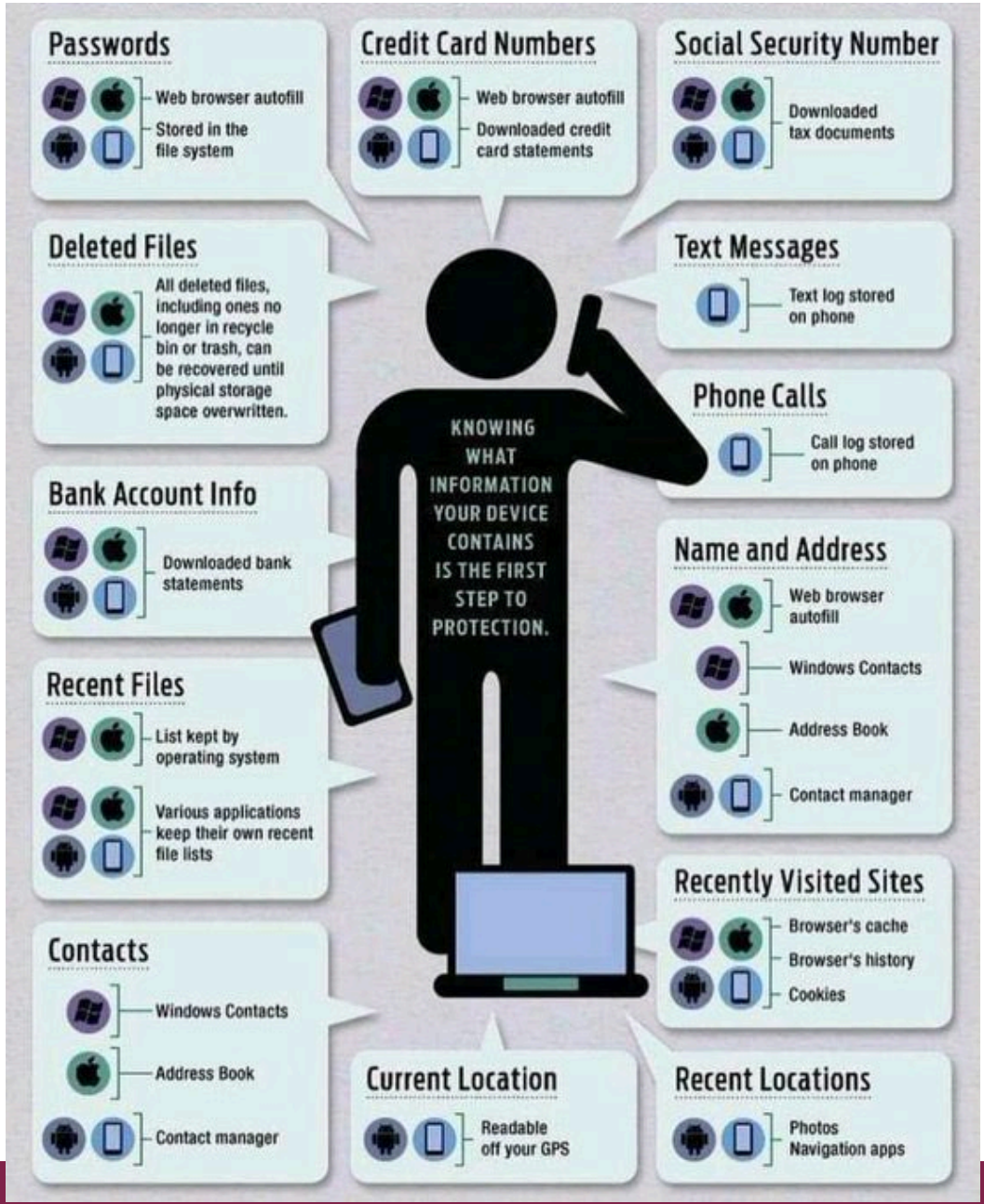
Threats

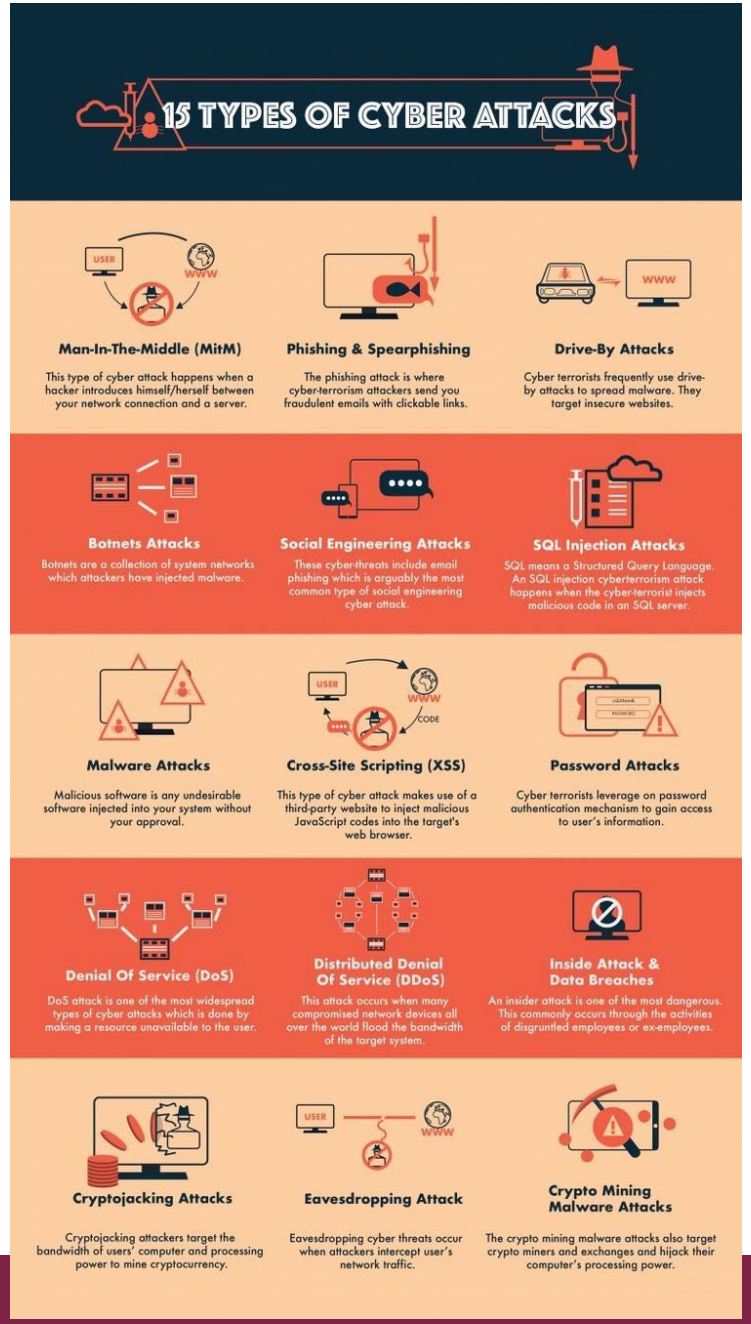
Hacker Attack Goals – over 30 years

Hacker attack goals are 1 or more of the following:

- **DATA theft/disclosure** aka data breaches
- **ATTACK** other sites using hacked assets
- **DESTRUCTION** of company data (deletion or ransomware).

- **DEFEND** accordingly


Passwords
Web browser autofill
Stored in the file system
Credit Card Numbers
Web browser autofill
Downloaded credit card statements
Social Security Number
Downloaded tax documents
Deleted Files
All deleted files, including ones no longer in recycle bin or trash, can be recovered until physical storage space overwritten.
Text Messages
Text log stored on phone
Phone Calls
Call log stored on phone
KNOWING WHAT INFORMATION YOUR DEVICE CONTAINS IS THE FIRST STEP TO PROTECTION.
Bank Account Info
Downloaded bank statements
Name and Address
Web browser autofill
Windows Contacts
Address Book
Contact manager
Recent Files
List kept by operating system
Various applications keep their own recent file lists
Recently Visited Sites
Browser's cache
Browser's history
Cookies
Contacts
Windows Contacts
Address Book
Contact manager
Current Location
Readable off your GPS
Recent Locations
Photos
Navigation apps



Time it takes a Hacker to Brute Force your password

@coders.bro

Numbers of Character	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 Secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100tn years	7qd years

Are you in green zone?

A Brave New World

Different Approach

- Data Protection is key
  - Find, Tag, Encrypt
- Data Flow
  - Where does our data go?
- Logs are crucial
  - Who, What, When, Where, How, Why
- Resilience
  - Can’t prevent ransomware attack
  - Recovery is key

Border? What Border?

- Internet 1.0 – static servers, endpoints
- Internet 2.0 – static servers, mobile endpoints
- Internet 3.0 – mobile servers (containers, serverless),
  mobile endpoints (laptops, phones,tablets, IoT, ICS)
- Internet 3.5 – Work From Home (WFH)
- **The new border is data, not the device or the network**

Zero Trust Networks(ZTN) Characteristics*

Vendors usually don't mention the 1st 3 Pillars

- Pillar 1: The network is always assumed to be **hostile**
- Pillar 2: Assume the hostiles are already **inside your network**
- Pillar 3: Network locality (segmentation) is **not sufficient** for deciding trust in a network
- Pillar 4: **Every** device, user and network flow is authenticated and authorized
- Pillar 5: **Policies** must be dynamic and calculated from as many sources of data as possible

** "Zero Trust Networks: Building Secure Systems in Untrusted Networks", Evan Gilman, Doug Barth*

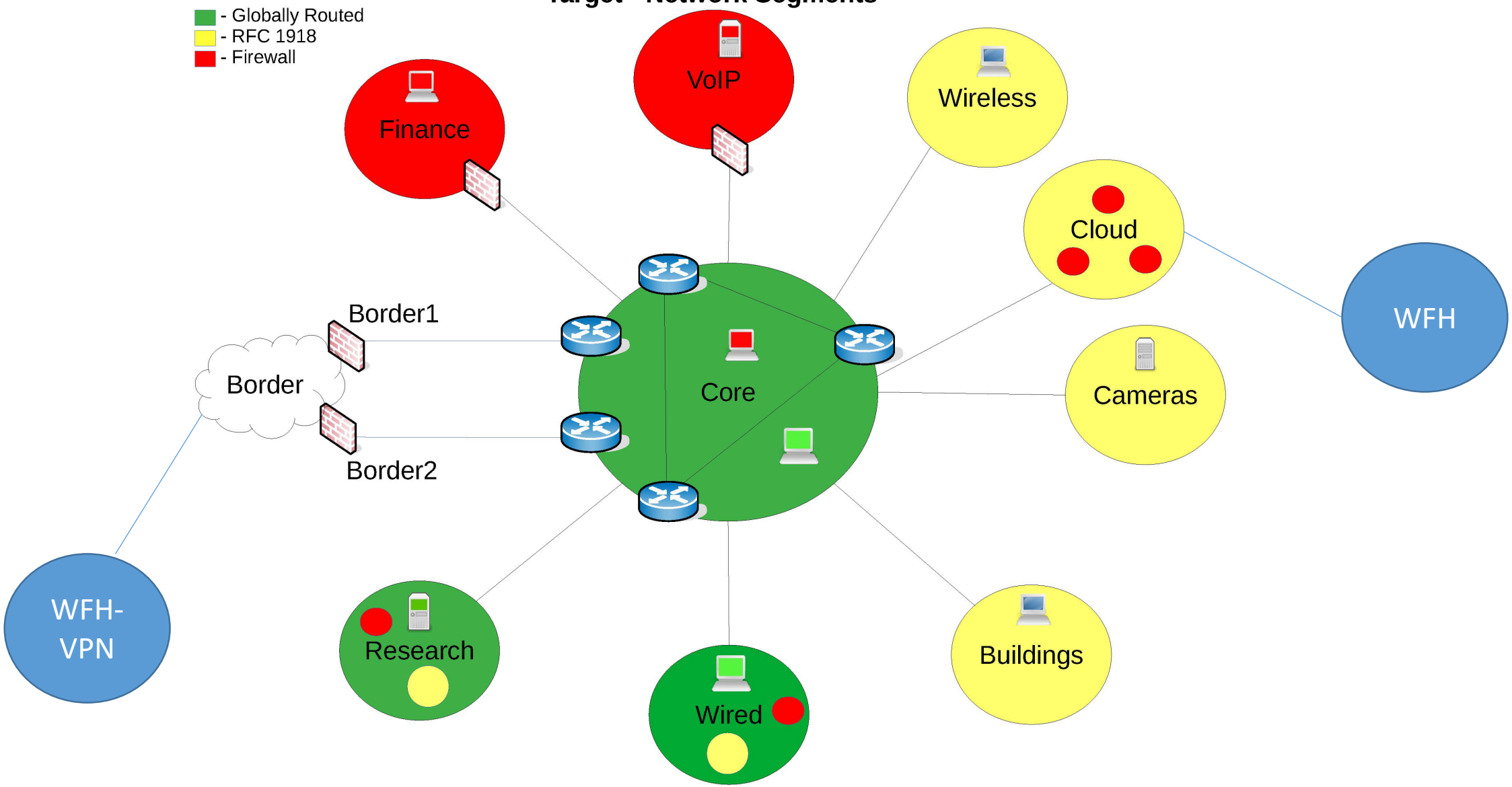
Times are a'changing – Gartner Predictions

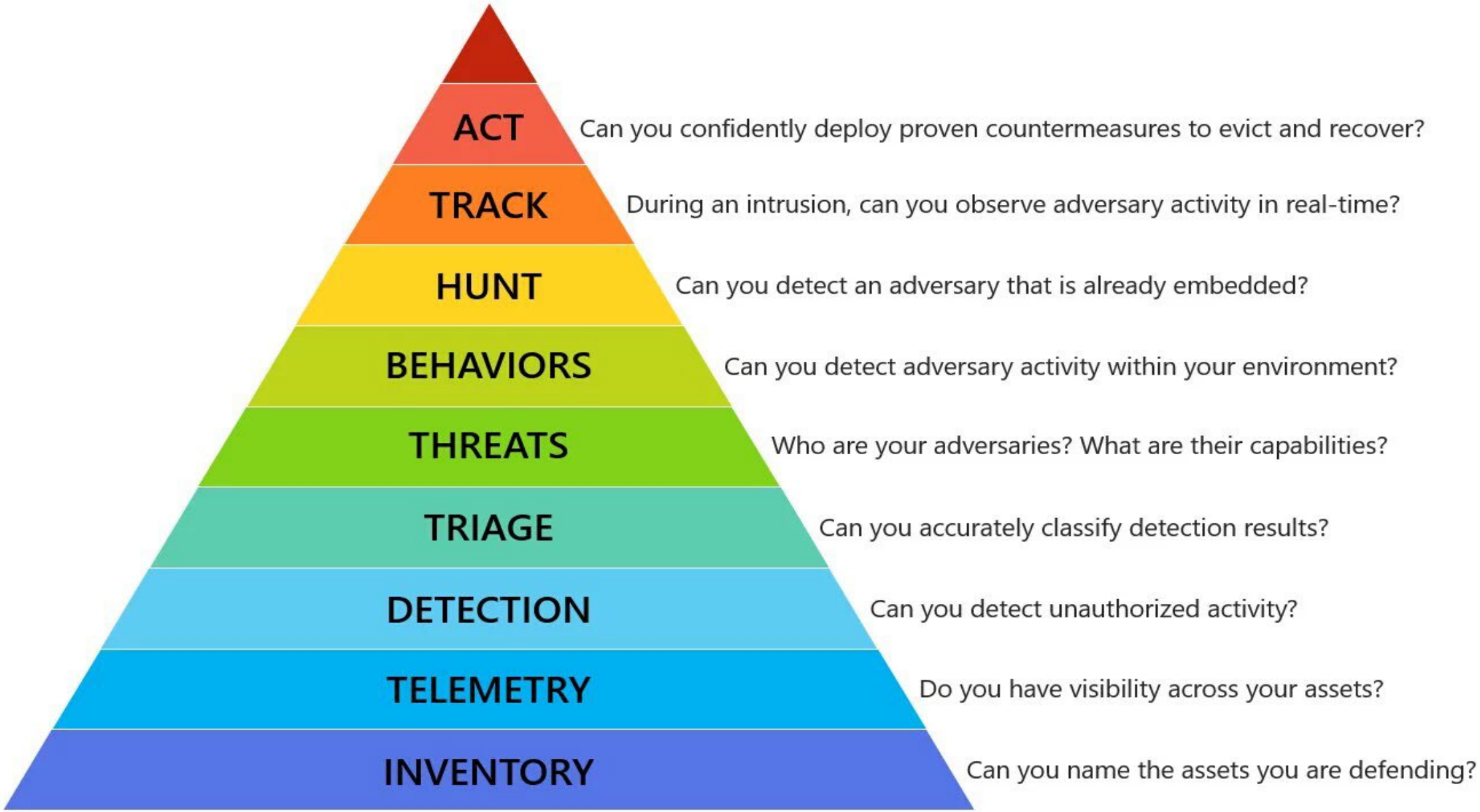
- **"Through 2023, government regulations requiring organizations to provide consumer privacy rights will cover 5 billion citizens and more than 70% of global GDP."**
- **"By 2025, 80% of enterprises will adopt a strategy to unify web, cloud services and private application access from a single vendor's SSE platform."**
- **"Sixty percent of organizations will embrace zero trust as a starting point for security by 2025. More than half will fail to realize the benefits."**
- **"By 2025, 60% of organizations will use cybersecurity risk as a primary determinant in conducting third-party transactions and business engagements."**
- Source: https://campustechnology.com/articles/2022/06/23/gartners-top-8-cybersecurity-predictions-for-the-coming-year.aspx?s=ct_nu_050722

Another View

- "As we **move our data outside of the firewall**, we have to adopt a zero-trust type model, " [Chris] Townshend said. "We are shifting our security enforcement out to the data itself, and **you have to have a security policy that follows that user no matter where that user is or what device they are using to access the data"**
    - "The new cyber landscape", Patrick Marshall, GCN Magazine, vol 37, #1
- In other words, **data & identity become the border.**

Target - Network Segments





Source: https://holisticinfosec.blogspot.com/2016/12/the-dfir-hierarchy-of-needs-critical.html
Figure source: https://github.com/swannman/ircapabilities

What's Changing?

- Border Monitoring
  - Line Speeds >100Gb, moving to 300-500Gb in 5 years
    - Bad News:Inline IDS/IPS/DLP not practical w/o impacting performance
    - Good News: some vendors are adjusting
- North-South traffic more important than East-West
- Vulnerability Scanning
  - ISP may interfere thinking it's an attack and block it
- Incident Response
  - Cutting off net access no longer under your control
- Cloud
  - Email, File sharing, Incident response, high risk data inventory affected

What’s Changing?

- VPN
  - Not necessarily a “security” feature
  - Home system may still be accessed from the net
  - Does force your packets to go thru your net
  - What services require VPN
    - ERP, etc.?
  - What services don’t require VPN
    - Email, Slack, Zoom, Teams?

A New Strategy

Net Access isn't Equal

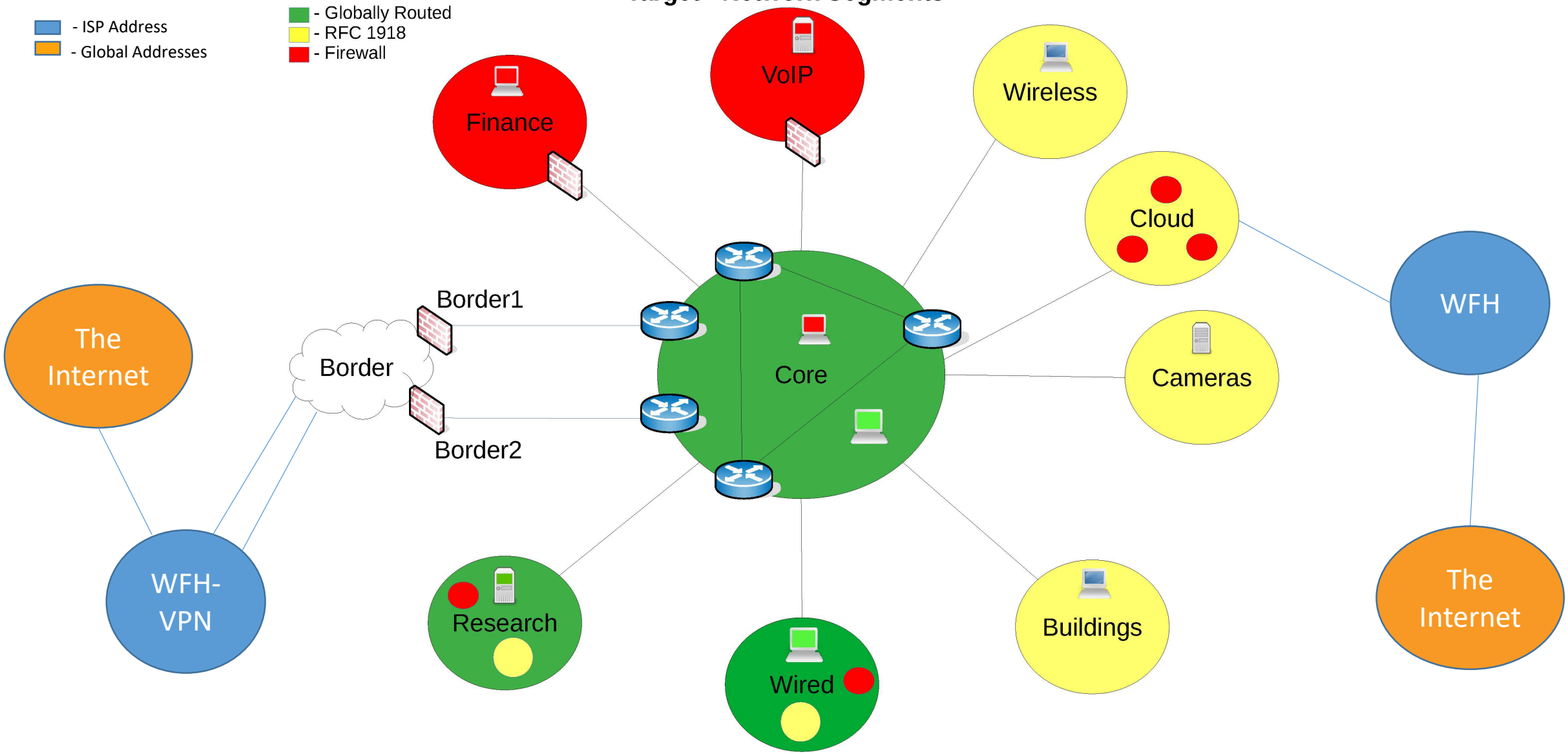
- Some areas have no internet access
- Some areas have poor internet access
- ISP rate based charge structure
  - Work zoom, school zoom, work downloads, streaming services = more expensive internet plans/fees

- EDITORIAL COMMENT – My Opinion only (Flame Retardant Suit On)
  - #WFH shows the Net has become a utility.
  - It should be regulated as such.
  - 21st Century version of Rural Electrification Project

Where Does It Go When It Goes Home?

- PROBLEM: Once data is on your home net, you lose data visibility
- Home systems become exfil targets
  - Infostealer class malware looks for PII
  - Attacker dumps from the home system
  - We don’t know if/when/where it went but the home ISP may
- SOLUTIONS (?)
  - TAG your data files (web bug)
  - File phones home instead of computer
  - Lot of work to implement

Target - Network Segments



Your Work Computer Became Your Home Computer

- Hopefully not!
- WFH not new but # of WFH computers has INCREASED
- Will your company tools work outside of your work network?
  - Active Directory?
  - Authentication? 2 factor?
  - Software Licensing?
  - Virtual Private Network (VPN)?

Your Home Computer Became Your Work Computer - 1

- If you use your home computer for work, you must follow your office's security requirements on it.

- **Create a separate userid for work stuff.** Keeps personal separate from work.
  - Browser history, photos, personal sensitive data vs. work sensitive data. Can limit ransomware damage.
- When you're done #WFH, you can delete that account

And Now Some Geek-Speak

- Can your IT scan computers at your house?
  - Probably not. May be blocked by your ISP
- Can you “disconnect” a host from your network?
  - ISP will get abuse complaints not your org.

- What network traffic visibility exists from computers at your house?
  - None probably unless you require VPN.
- What type of logs will you need to collect in this new WFH environment?

5 step

1 You

Someone creating a tremendous sense of urgency, often through fea intimidation, a crisis or ar important deadline.

Ultimately, the

Almost every home network starts with a wireless (often called Wi-Fi) network. This is what enables all of your devices to connect to the Internet. Most home wireless networks are contr separate, dedicate same way: by broa devices connect. T is a key part of pro following steps to

2 Home

Change the default administrator pass
The administrator a is what allows you t configure the settin your wireless netwo attacker can easily the default passwo the manufacturer h provided.

3 Passwords

When a site asks you to create a password, create a strong password: the more characters it has, the stronger it is. Using a passphrase is one of the simplest ways to ensure that you have a strong password. A passphrase is nothing more than a password made up of multiple words, such as "bee honey bourbon." Using a unique passphrase means using a different one for each device or online account. This way if one passphrase is compromised, all of your other accounts and devices are still safe.

Can't remember all those passphrases?

Use a password manager, which is a specialized program that securely stores all your passphrases in an encrypted format (and has lots of other great features, too!). Finally, enable two-step verification (also called two-factor or multi-factor authentication) whenever possible. It uses your password, but also adds a second step, such as a code sent to your smartphone or an app that generates the code for you. Two-step verification is probably the most important step you can take to protect your online accounts and it's much easier than you may think.

Not sure how to do these steps?

Ask your Internet Service Provider, check their website, check the documentation that came with your wireless access point, or refer to the vendor's website.

5 Steps to WFH Securely

Make sure each
computers, mob
programs and a
running the late
of its software.

Cyber attackers are constar
the software your devices u
they use special programs
using. Meanwhile, the comp
hard at work fixing them by
mobile devices install these updates promptly, you make it much harder for
someone to hack you. To stay current, simply enable automatic updating
whenever possible. This rule applies to almost any technology connected to a
network, including not only your work devices but Internet-connected TV's, baby
monitors, security cameras, home routers, gaming consoles or even your car.

5

Kids & Guests

Something you most likely don't have to worry about at the office is children, guests or other family members using your work laptop or other work devices.

Make sure family and friends understand they cannot use your work devices.

They can accidentally erase or modify information, or, perhaps even worse, accidentally infect the device.

https://www.sans.org/security-awareness-training/fact-sheet/

WFH Security Steps - Employees

Secure your home office (Physical)	Secure your home router – change default password
Separate work and personal devices	Encrypt your devices (bitlocker, FileVault, dm-crypt, etc., Android, IOS)
Use supported and updated OS versions, software	Automated login for work devices at home
2FA work device logins	Enable “Find my device” feature
Wipe HW before share, sell or dispose. Backup first!	Use a VPN
Use antivirus, anti-malware software	
Invest in a password manager	

https://www.upguard.com/blog/working-from-home-security-tips

WFH Security Steps - Employers

Invest in Cybersecurity Training	Manage your 3rd party vendors and service providers
Implement adequate email security practices	Use access control
Invest in Cyber hygiene – may include home devices	Ensure web apps use secure connections (HSTS)
Use metrics to monitor cybersecurity performance	Enforce password strength rules on work devices
Invest in password managers	Encrypt all company devices

Simple Steps to Protect Your Computer

- Password protect your userid, screen lock
- Update your OS & software
- Think before click
- You have a firewall already
- Adjust browser security, privacy settings

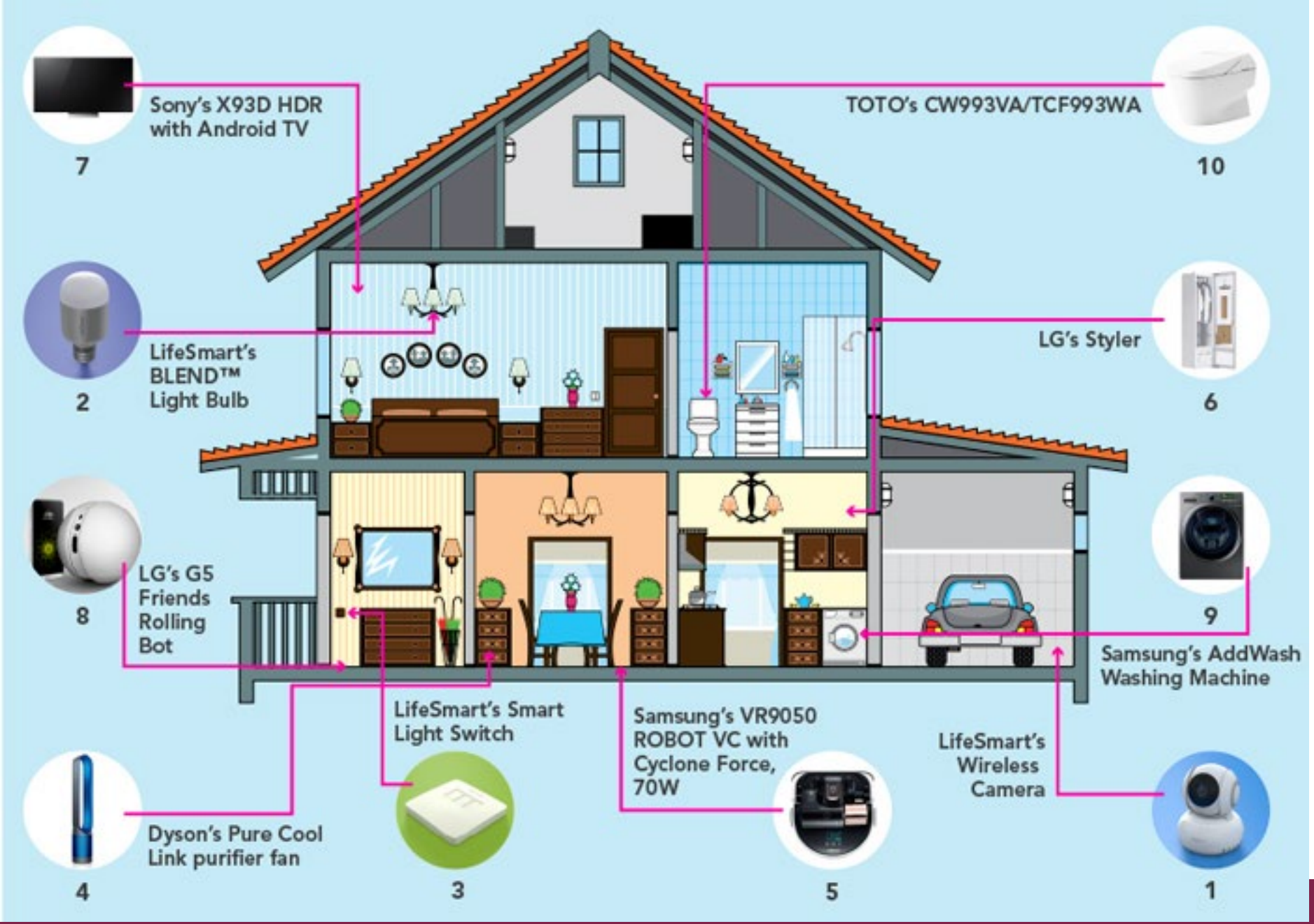
- Encrypt sensitive data
  - Use Microsoft Office tool
  - Remember your password!
- https://www.us-cert.gov/ncas/tips/ST15-002 "How to Secure Your Home Network"
- https://privacy.net/how-to-secure-your-computer/

https://privacy.net/how-to-secure-your-computer/

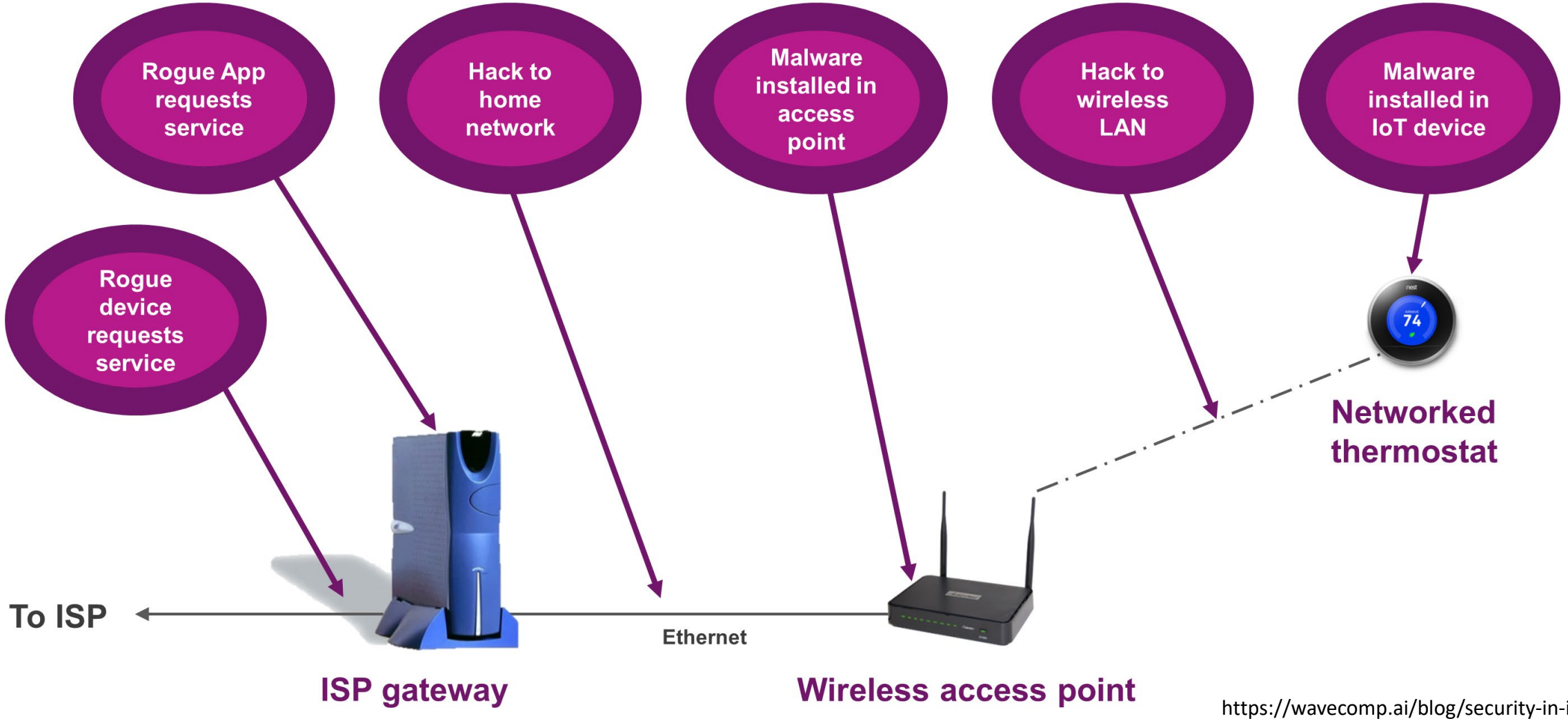
Your Home Network and Work Network

- Your home network is an extension of the work network

- Does your home **computer** meet any regulatory requirements imposed on the data you use?
- Does your home **network** meet any regulatory requirements imposed on the data you use?


Sony's X93D HDR with Android TV
7
TOTO's CW993VA/TCF993WA
10
LifeSmart's BLEND™ Light Bulb
2
LG's Styler
6
LG's G5 Friends Rolling Bot
8
9
Samsung's AddWash Washing Machine
LifeSmart's Smart Light Switch
Samsung's VR9050 ROBOT VC with Cyclone Force, 70W
LifeSmart's Wireless Camera
Dyson's Pure Cool Link purifier fan
4
3
5
1

Security attacks



https://wavecomp.ai/blog/security-in-iot-devices/

WFH, IoT, Mobile, Oh My!

Times are a'changing – Gartner Predictions

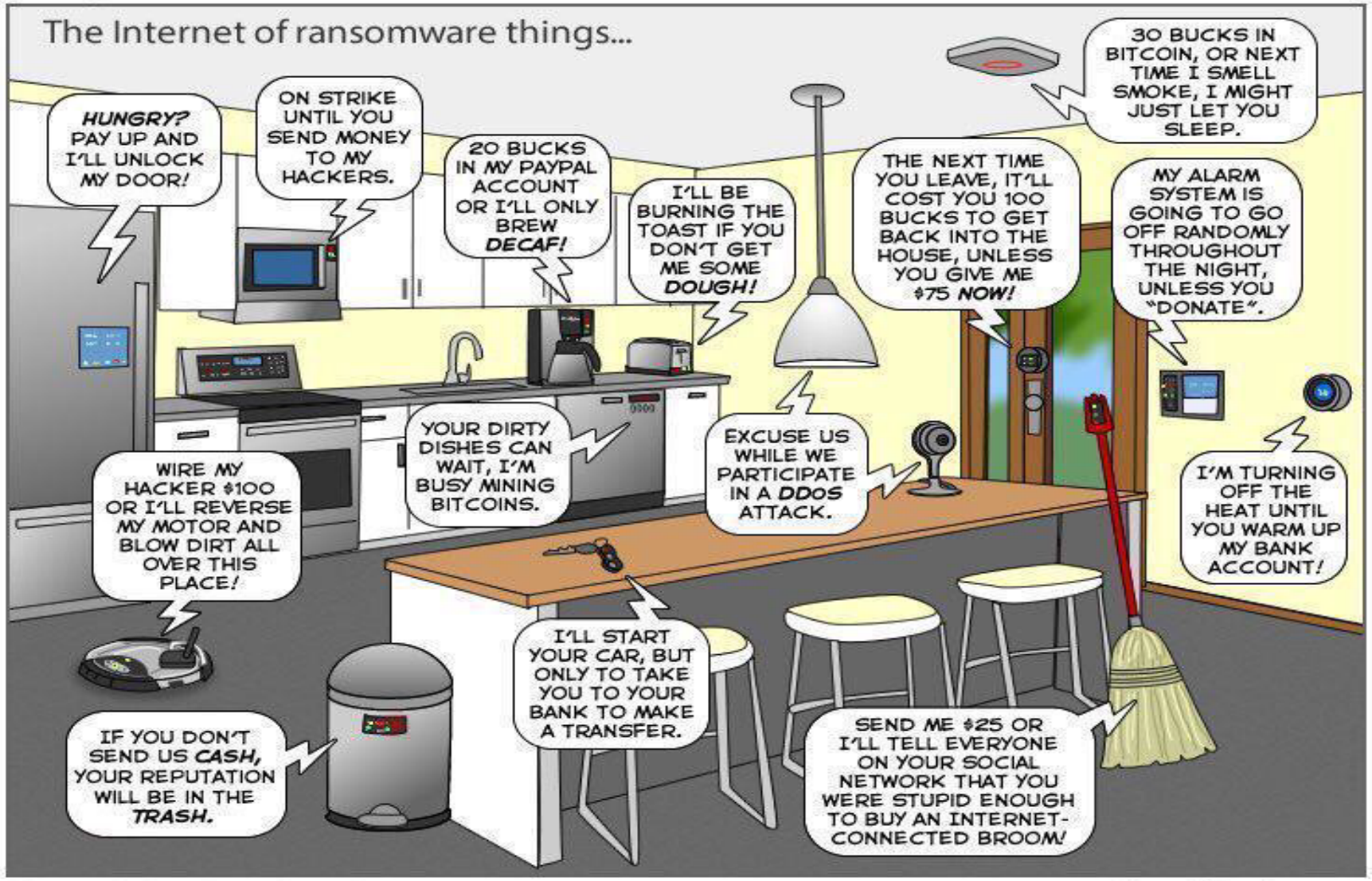
- **"By 2025, threat actors will have weaponized operational technology environments successfully to cause human casualties."**
- **"Through 2025, 30% of nation states will pass legislation that regulates ransomware payments, fines and negotiations…"**
- **"By 2025, 70% of CEOs will mandate a culture of organizational resilience to survive coinciding threats from cybercrime, severe weather events, civil unrest and political instabilities."**
- **"By 2026, 50% of C-level executives will have performance requirements related to risk built into their employment contracts."**
- Source: https://campustechnology.com/articles/2022/06/23/gartners-top-8-cybersecurity-predictions-for-the-coming-year.aspx?s=ct_nu_050722

What's a Thing?

- A Thing is physical object that contains 1 or more devices
- Sensor – sense the physical environment
  - Thermometers, Thermostats, weight scales
  - Measure something
- Actuator – affect the physical environment
  - Brakes, pedals, pistons
  - Does something

  - https://www.cosic.esat.kuleuven.be/school-iot/slides/IoTChallenges.pdf

The Joy of Tech™ by Nitrozac & Snaggy



You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com

Schneier's Example – Car Attack*

- Confidentiality, Availability, Integrity
- Confidentiality
  - Know who you are so we target your car
- Availability
  - Disable your car's brake system
- Integrity
  - Change the settings on your car's "stay in lane" feature
  - Tell it to be 2 ft to the left of the center line

- *"Click Here to Kill Everybody", by Bruce Schneier, ISBN: 978-0-393-60888-5

Amazon Echo Saves All Your Voice Data, Police Are Now Accessing It, Here's How to Hear & Delete It

By **Matt Agorist** - December 28, 2016

128.173.200.142 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

hp/jetdirect

Hosting Gmail rapid7 list CollegiateTimes netscan Dashboard DhcpTool - Help black ColdFusion Administra... webcam FreeBSD Handbook W3C Demo Token candi1

Gmail - Inbox (1) - tilley.rb@gmail.com | NeXpose Security Console :: Device Su... | http://198.82.143....v=hp.ConfigDevice | 128.173.200.142

NPI3F1C76 / 128.173.200.142

hp LaserJet 4200

Information | Settings | Networking

CONFIGURATION
- Network Settings
- Other Settings
- Privacy Settings
- Select Language

SECURITY
- Settings
- Authorization
- Mgmt. Protocols

DIAGNOSTICS
- Network Statistics
- Protocol Info
- Configuration Page

Other Links
- Help
- Support
- HP Home

Settings

Status | Wizard | Restore Defaults

Authorization

Administrator Password:	Not Set
Jetdirect Certificate:	Installed
Access Control:	Disabled

Web Interface

Encrypt All Web Communication:	Disabled
Encryption Strength:	Low (DES-56-bit, RC4-128-bit or 3DES-168-bit)

SNMPv1/v2

Status:	Enabled
Get Community Name:	Not Set (Defaults to "public")
Set Community Name:	Not Set (Defaults to "public")

SNMPv3

Status:	Disabled

Other Protocols

IPX/SPX:	Enabled
AppleTalk:	Enabled
DLC/LLC:	Enabled
9100 Printing:	Enabled
LPD Printing:	Enabled
IPP Printing:	Enabled
FTP Printing:	Enabled
SLP Config:	Enabled
mDNS:	Enabled
Multicast IPv4:	Enabled
RCFG:	Enabled

Done | JSESSIONID=undefined

List of Default Passwords

https://datarecovery.com/rd/default-passwords/

SEARCH

LET'S CHAT | START DATA RECOVERY | CASE STATUS | 800.237.4200

Datarecovery.com

Services | Data Loss Prevention | About | Contact | Clients | R&D | News

View All R&D Articles

Default Passwords

June 23, 2014

This page serves as a repository for the default passwords for various devices and applications.

Hardware devices listed include network devices such as routers, modems, and firewalls, along with various storage devices and computer systems. This is a substantial list, but it is not regularly updated. Revision numbers are therefore included where applicable in order to ensure accuracy.

If your device's listed password is incorrect or if you would like to submit a password for inclusion on this list, please send an email to support@datarecovery.com with this page's URL (http://datarecovery.com/rd/default-passwords/) in the subject line.

All of these admin passwords are provided for research purposes and for legal, legitimate use.

Manufacturer	Model/Name	Revision	Protocol	User	Password
3Com	-	1.25		root	letmein
3com	3comCellPlex7000	-		tech	tech
3COM	AccessBuilder	7000 BRI	SNMP	SNMPWrite	private
3COM	AirConnect Access	01.50-01	Multi	(none)	(none)

Categories

- COMPUTER FORENSICS
- DAMAGE
- DATA LOSS PREVENTION
- DATA RECOVERY KNOWLEDGE
- DATA RECOVERY NEWS
- DATA RECOVERY SERVICE
- DATA TYPES
- DATABASE
- EMAIL
- HARD DISK
- MAC/APPLE
- MEDIA

UNDOCK | START CHAT

List of Default Passwords | Shodan

https://www.shodan.io

Shodan | Developers | Book | View All...

SHODAN

Explore | Enterprise Access | Contact Us

New to Shodan? | Login or Register

The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account | Getting Started

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

56% of Fortune 100

1,000+ Universities

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

Summary

- Data Protection is key
  - Find, Tag, Encrypt
- Data Flow
  - Where does our data go?
- Logs are crucial
  - Who, What, When, Where, How, Why
- Resilience
  - Can’t prevent ransomware attack
  - Recovery is key

Contact information

- Randy Marchany, Marchany@vt.edu, 540-231-9523 (direct line), 540-231-1688 (office), Twitter: @randymarchany, Blog: randymarchany.blogspot
- http://security.vt.edu

References

- https://github.com/RUB-NDS/PRET
- https://www.nationalcyberscholarship.org/
- https://security.vt.edu
- https://foundation.mozilla.org/en/privacynotincluded
- https://www.ekransystem.com/en/blog/data-breach-investigation-best-practices