Cybersecurity Hygiene

SABM Feb 2021

Current State

- 87% of the Information Security spend is to keep attackers out
- We have to be right all the time, and the adversary only has to be right once
- What is missing
  1. We don't make it hard to get around
  2. We don't make it hard to get our stuff
  3. We don't make it hard use our stuff
  4. We don't make it hard to get out
  5. We don't make it hard to take a payload
- Why is this so?
  - Money
  - Effort
  - Time
  - Expertise

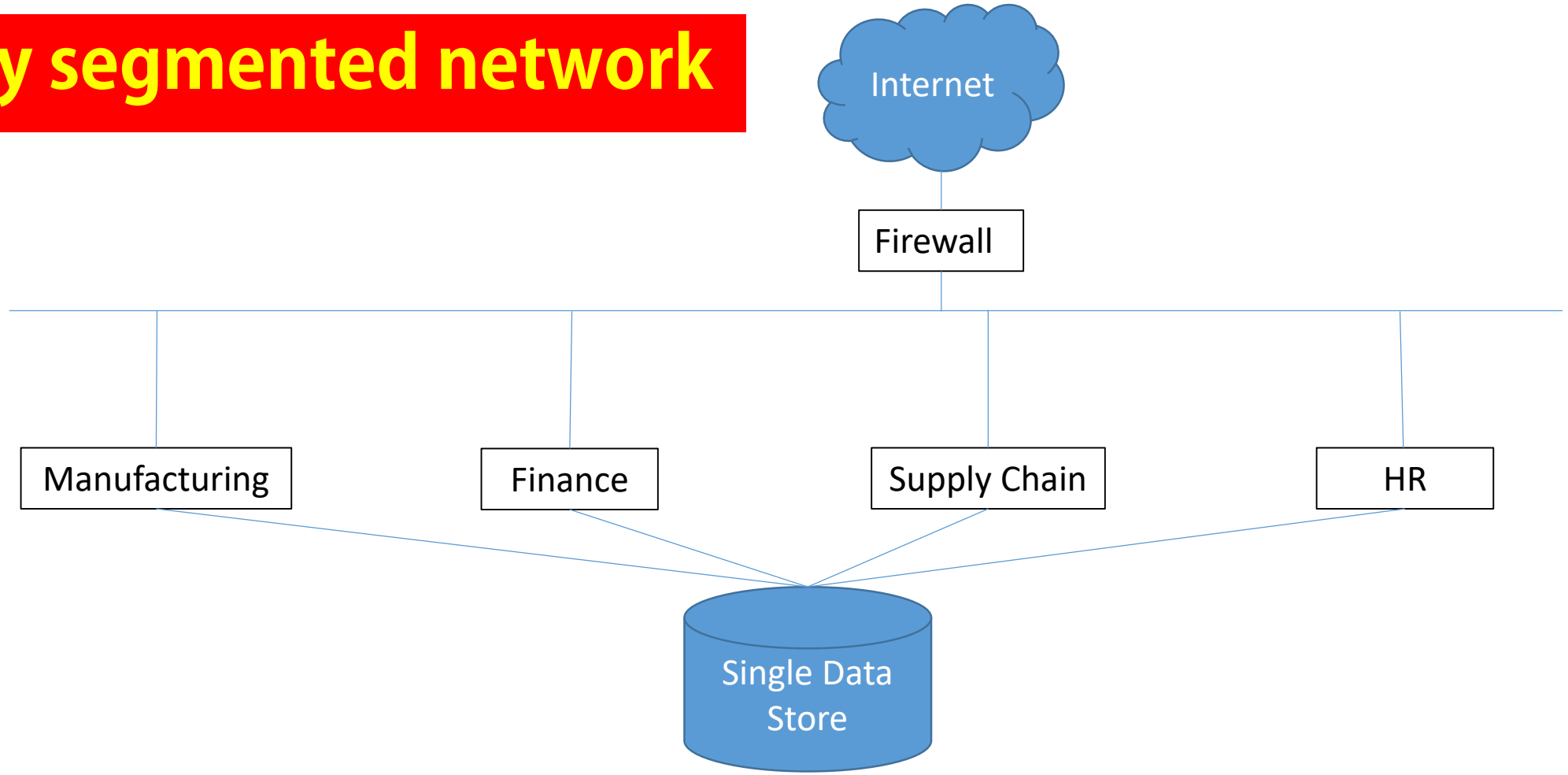
What You Can Do

- Ask questions of your tech folks
- Participate in work groups or teams to protect your data
- Raise awareness within your organization – beat the drum – especially if you are a data owner or have an interest
  - If you are Executive Management, be an evangelist
  - If you are not, work the management chain or Chain of Command
  - Everybody is responsible to keep data, and especially customer data safe
  - If organizational data is compromised, everyone in the organization will hurt
- IT and Cybersecurity work for you. You are their customer
- Ask your organization, how do we make it hard to get around, get our stuff, use our stuff, get out, take a payload?

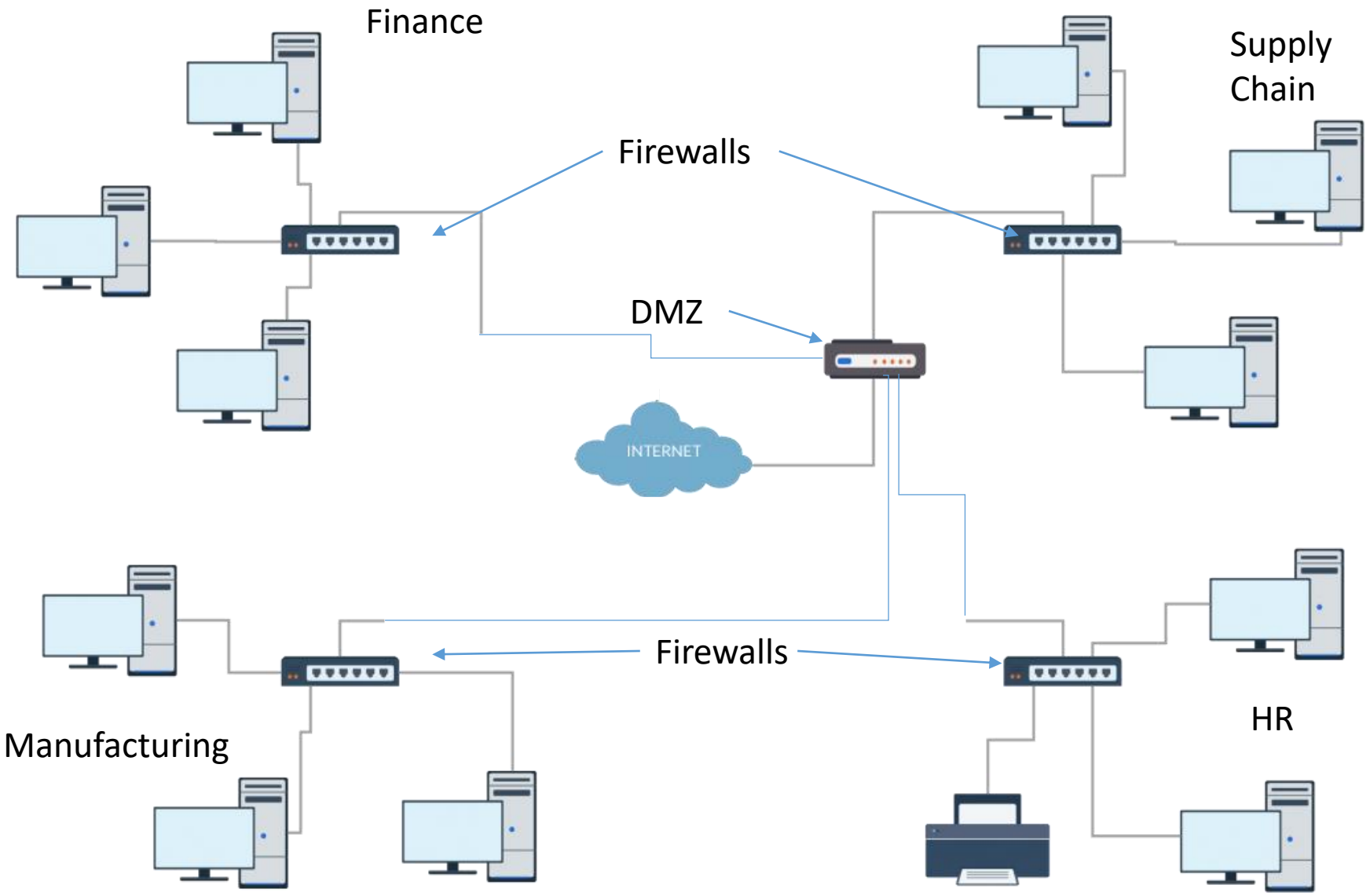
How To Do It – Make it Hard to Get Around

Make it hard to get around. Segment the network

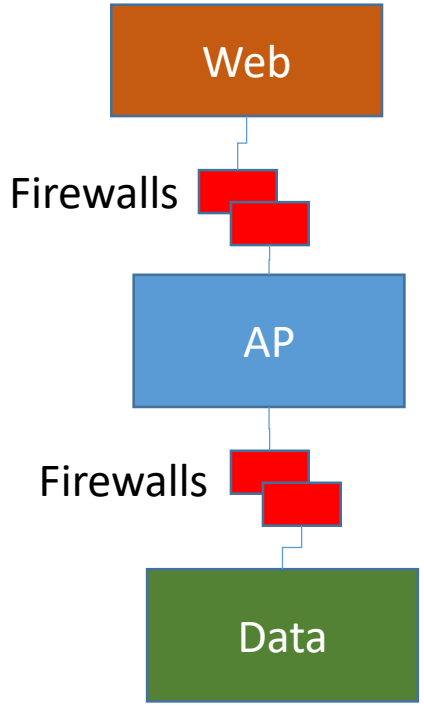
Poorly segmented network



Well-segmented Network



1. Hard to get around
2. Hard to get at our stuff



Make it Hard to Use Our Stuff

- Encrypt all data at rest
- Encrypt data in transit
- Separate data
- Bake security into applications
  - Input validation
  - Data transmissions and calls
  - User interactions
  - User interfaces
  - Beware aggregation and inference

Make it Hard to Get Out

- Filter and look for patterns
  - Firewalls
  - Routers
  - Anti-virus – not just known, but aberrations in traffic
  - Intrusion Detection Systems (IDS)
  - Intrusion Protection Systems (IPS)
- If unauthorized access
  - Close doors behind them so they can’t get out
  - Don’t let them leave by the same route
  - Segmentation offers multiple checkpoints to pass

Make it Hard to Take a Payload

- Filter outbound content
  - Personally Identifiable Information (PII)
  - Financial Information
  - Protected Health Information (PHI)
  - Controlled Unclassified Information (CUI)
  - Classified Information
- Prevent exit
- Block paths & points of origin
- Just because you can, doesn't mean you should
- Risk vs. Cost

Other Tips

- Disciplined Asset Management – know where your stuff is
- Good endpoint security
  - Home WiFi
  - Secure the device
- 2-factor authentication for admins
- Be militant about not sharing passwords and accounts – especially root access
- Call backs for remote access
- Good people processes
  - Adding and terminating people
  - Watching for indicators of comprisable people, Money, Ideology, Compromise, Ego (MICE)

Other Tips

- Physical
  - Open ports
  - Tailgating
  - Employee awareness
  - Mantraps
  - Greeter or receptionist
  - Escort non employees
- Documented processes and procedures
- Mandatory annual and continual training
- Phishing drills
- Documented Incident Response capability that adheres to some standard (i.e. NIST 800-63)

Questions ?