Cybersecurity

Don’t Go It Alone

ALDEBARAN GROUP

Do you know what Cybersecurity is?

As defined by the Cybersecurity & Infrastructure Security Agency
CISA – www.cisa.gov

"Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information."

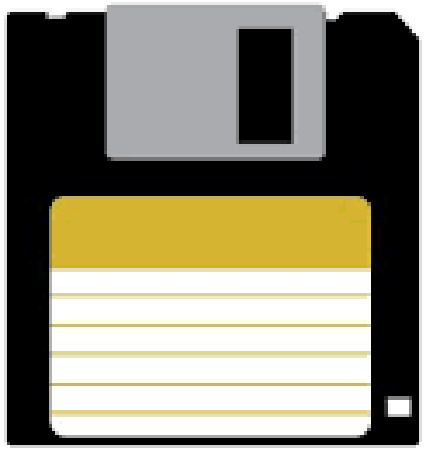
Do you know what Cybersecurity is?

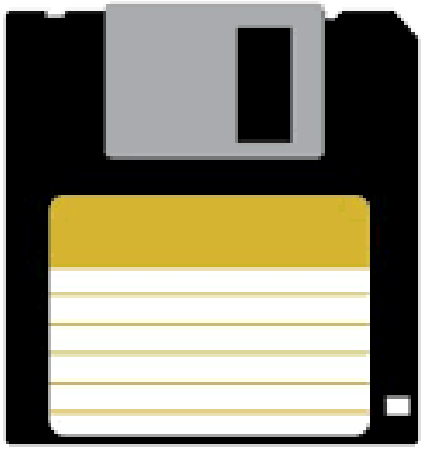
As defined by the Cybersecurity & Infrastructure Security Agency
CISA – www.cisa.gov

"Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information."

The Landscape Has Changed

Cybersecurity 1990





It’s You Against The World

Don’t Go It Alone

How we would **like** to think of our Cybersecurity…

How we **need** to think of our Cybersecurity…

What are the holes?

Insider Threats

External Threats

Poor Business Partners

(https://www.cisa.gov/defining-insider-threats)

Hole: Insider Threats

The potential for an **insider** to use their **authorized access** or understanding of an organization to **harm** that organization.

This harm can include **malicious, complacent, or unintentional acts** that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities.

(https://www.cisa.gov/defining-insider-threats)

Hole: Insider Threats

Intentional

- Stealing data
- Destroying data
- Permitting unauthorized access (credential sharing)

Unintentional User Induced Compromise

- Unintentional activation of unsafe hyperlinks, viruses, malware or ransomware
- Data Leakage (unsecure media/device loss/)
- Poor password/credential management

Unprotected Personal Devices

- Personal computers for remote access
- Out-of-date personal devices

(https://www.cisa.gov/defining-insider-threats)

Hole: **External Threats**

Bad actors **outside** an organization seeking to **gain unauthorized access to internal resources**.

Actors may be **nation states**, **organized hacking groups**, or **individuals**.

The bad actors use a variety of attack methods

Hole: **External Threats**

Malware	Hacking	Unauthorized Access
• Spyware • Ransomware • Viruses	• DDoS • Man-in-the-middle • Session Hijacking • Vulnerability Exploits	• Phishing • Compromising accounts • Social Engineering • Dark Web credentials

Hole: Poor Business Partners

Business partners **may not have robust security** and **data redundancy**, and they may **not be viable** businesses. These can put your data at risk.

Business partners may not accept responsibility for your losses due to failures in their platforms.

Hole: Poor Business Partners

Data Loss at Vendor

- Technical failure with insufficient backup
- Ransomware at vendor corrupts data
- Unauthorized access allows data deletion or exfiltration (Is vendor obligated to have recoverable data and is there an SLA on recovery

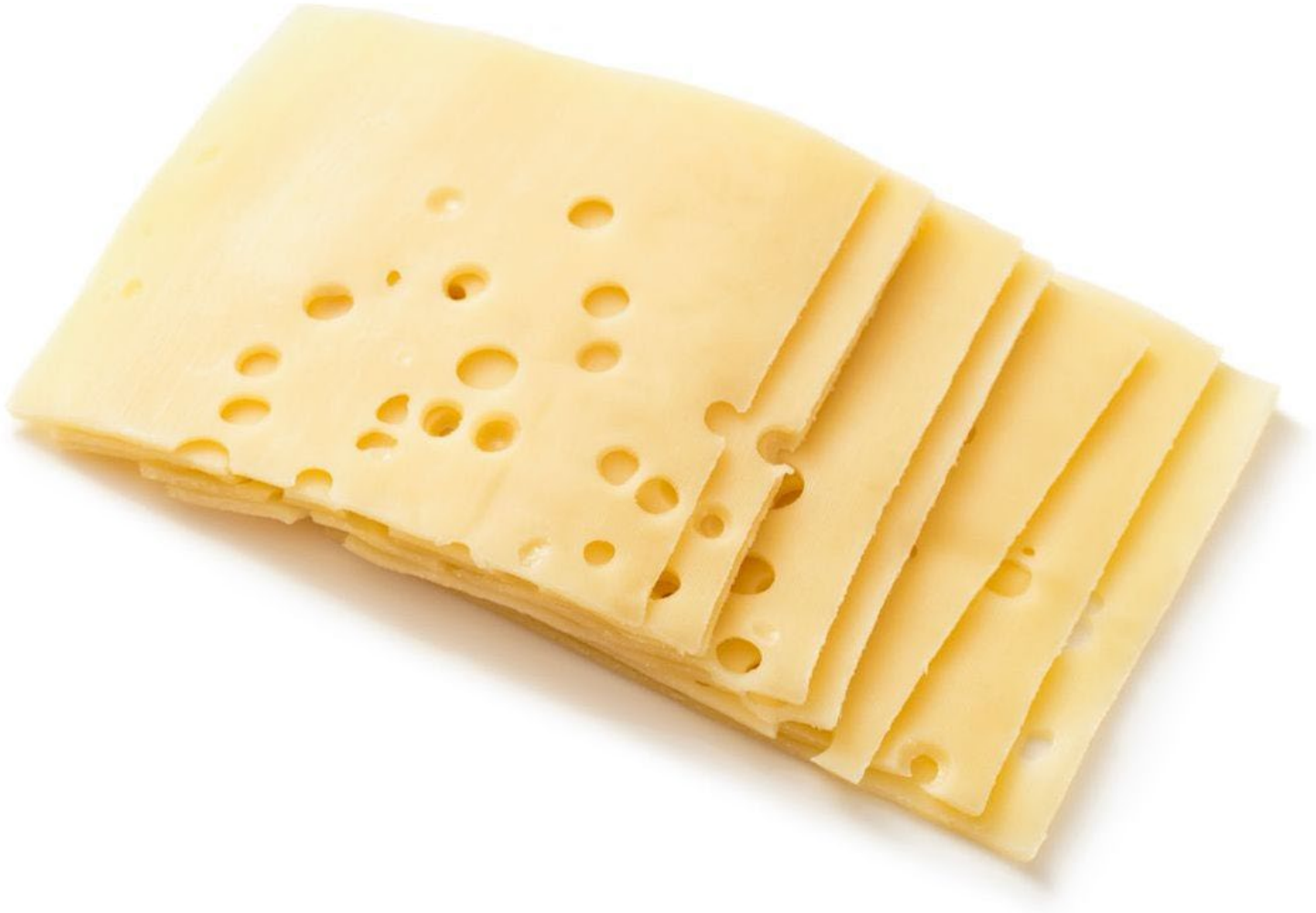
Vendor Failure

- Company Failure – Won't/can't return data
- Payment dispute – Vendor blocks access to data
- Vendor Unavailable (Ransomware, etc)

Supply Chain

- Authorized access for unsecure vendors (Target)
- Payloads delivered through 3rd party products through compromised software (Solarwinds)

Layers!



Layers Against Insider Threats

Physical Security

- Locked doors
- Locked computer screens
- Privacy screens
- Visitor Logging
- No un-checked entry

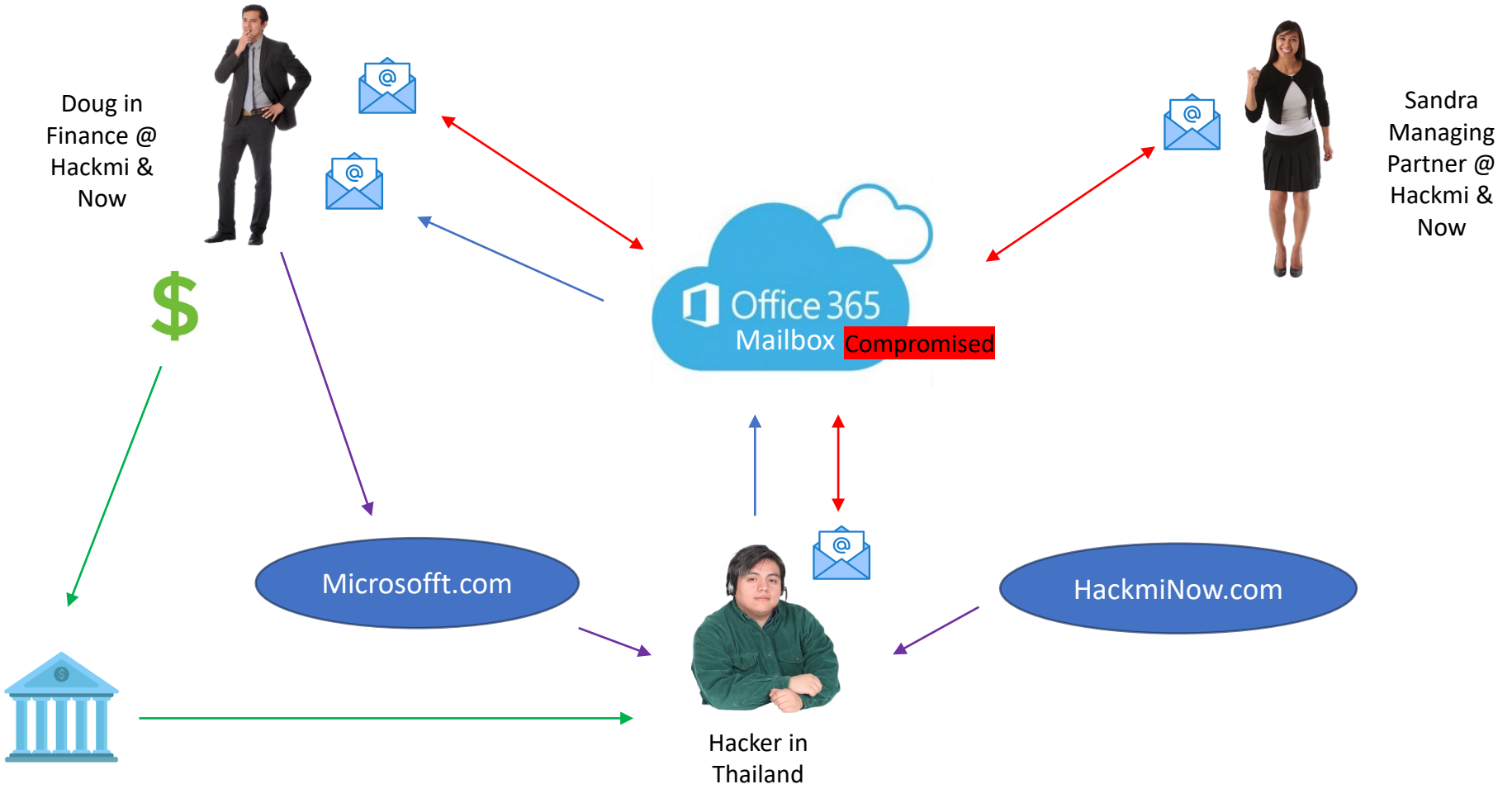
Personnel

- Policies and Procedures
- **Identification Requirements – ex. Finance and Shareholders**
- **Multi-Factor Authentication**
- Background Checks
- Auditing
- Least Privileged Access
- **Cybersecurity Training/ Phish Testing**
- No shared passwords
- Password Management

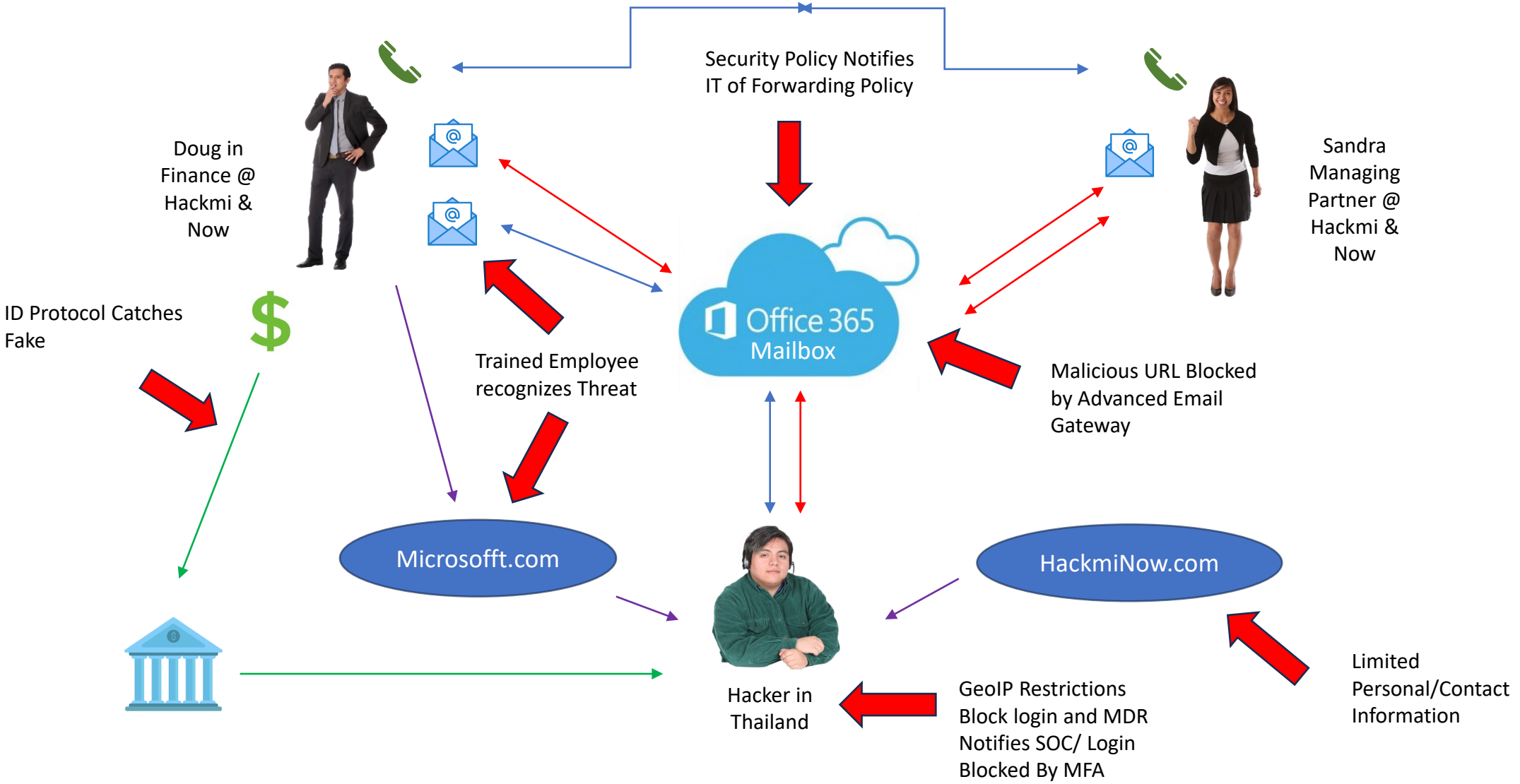
Threat Prevention and Remediation

- Application Control
- **Endpoint Detection and Response/Managed Detection and Response**
- **Advanced Email Protection**
- **Security Policies**
- Encrypted Media
- Robust Backup/Recovery/ Disaster Recovery
- Incident Response Planning

Example: Insider Threat @ Hackmi & Now



Example: Layers Against Insider Threat



Layers Against External Threats

Networking/Systems Management

- **Perimeter Protection – Firewall/Email Protection Services**
- **System Hygiene – Consistent and timely updates to hardware and software systems.**
- Penetration Testing

Identification

- **Multi-Factor Authentication**
- Single Sign On (SSO)
- **Least Privileged Access**
- Just In Time Passwords
- Unique, Long and Private Passwords
- No Shared Passwords
- Password Management
- Zero Trust

Threat Prevention/ Remediation

- **Endpoint/Managed Detection and Response**
- **Application Control/ Ringfencing**
- Cybersecurity Training for Staff/Phish Testing
- Incident Response Planning
- **Robust Backup/Recovery/ Disaster Recovery**

Example: External Threat

Hacker
In Slovenia

Exploits Remote Access device

Admin.User/PW

Firm Servers
Lateral Movement
Plants Ransomware

Deletes Backups/blocks access

Files Encrypted
Ransomware Activated
Backups Gone

Example: External Threat

Hacker
In Slovenia

Blocked by Geo-IP restrictions

Exploits Remote Access device

Admin.User/PW

Blocked by MFA

Fully patched device was not vulnerable

Firm Servers
Lateral Movement
Plants Ransomware

Blocked by MDR/App Control

Deletes Backups/blocks access

Files Encrypted
Ransomware Activated
Backups Gone

Blocked separate credentials/comm / Disconnected Off-site Cloud Backup

Blocked/halted by MDR/App Control

Layers Against Poor Business Partners

Administrative

- **Thorough vetting**
- Contractual Commitments
- Backups to other Cloud Providers
- Confidentiality Agreements
- **Require Cybersecurity Training/Phish Testing**

Technical

- Backups to other Cloud Providers
- **Multi-Factor Authentication**
- **Least Privileged Access/ only when needed**
- **Careful software vetting and monitoring.**
- Identification Protocols
- Unique, Long and Private Passwords
- **Robust Backup/Recovery/Disaster Recovery**

Example: Poor Business Partner

Physical Security Vendor

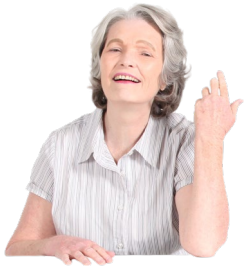
Physical Access Control Software

Access Firm Identity Provider with Excess Credentials

Malware Installed on Servers “Phones Home”

Firm Files Exfiltrated

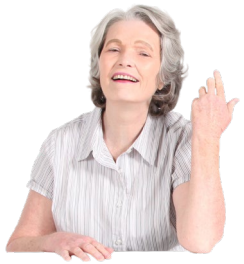
Hacker Controlled Servers



Hacker Phishes Security Vendor

Example: Poor Business Partner

Physical Security Vendor



Hacker Phishes Security Vendor

Thorough Vetting Ensures Security Protocols

Physical Access Control Software

Installed in Security Controlled Part of Network

Access Firm Identity Provider with Excess Credentials

IT Supplies Least Privileged Access Just In Time Credentials

Malware Installed on Servers "Phones Home"

Blocked by MDR/App Control

Firm Files Exfiltrated

Blocked by MDR

Blocked by Firewall Rules

Hacker Controlled Servers

AI the elephant in the room?

Can IT do this alone?

Can IT get all this done?

Just how good are your IT folks?

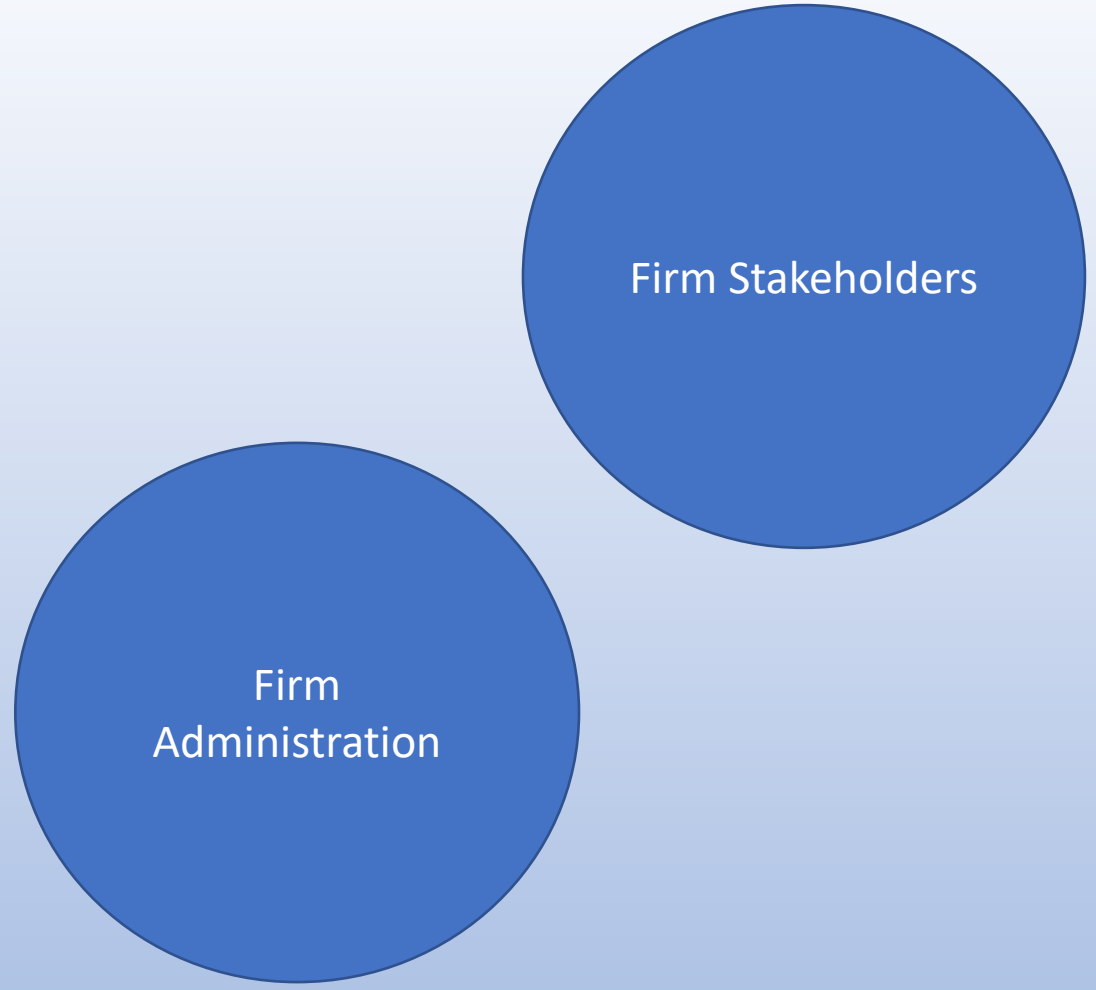
Do you know your team?

What can I do?

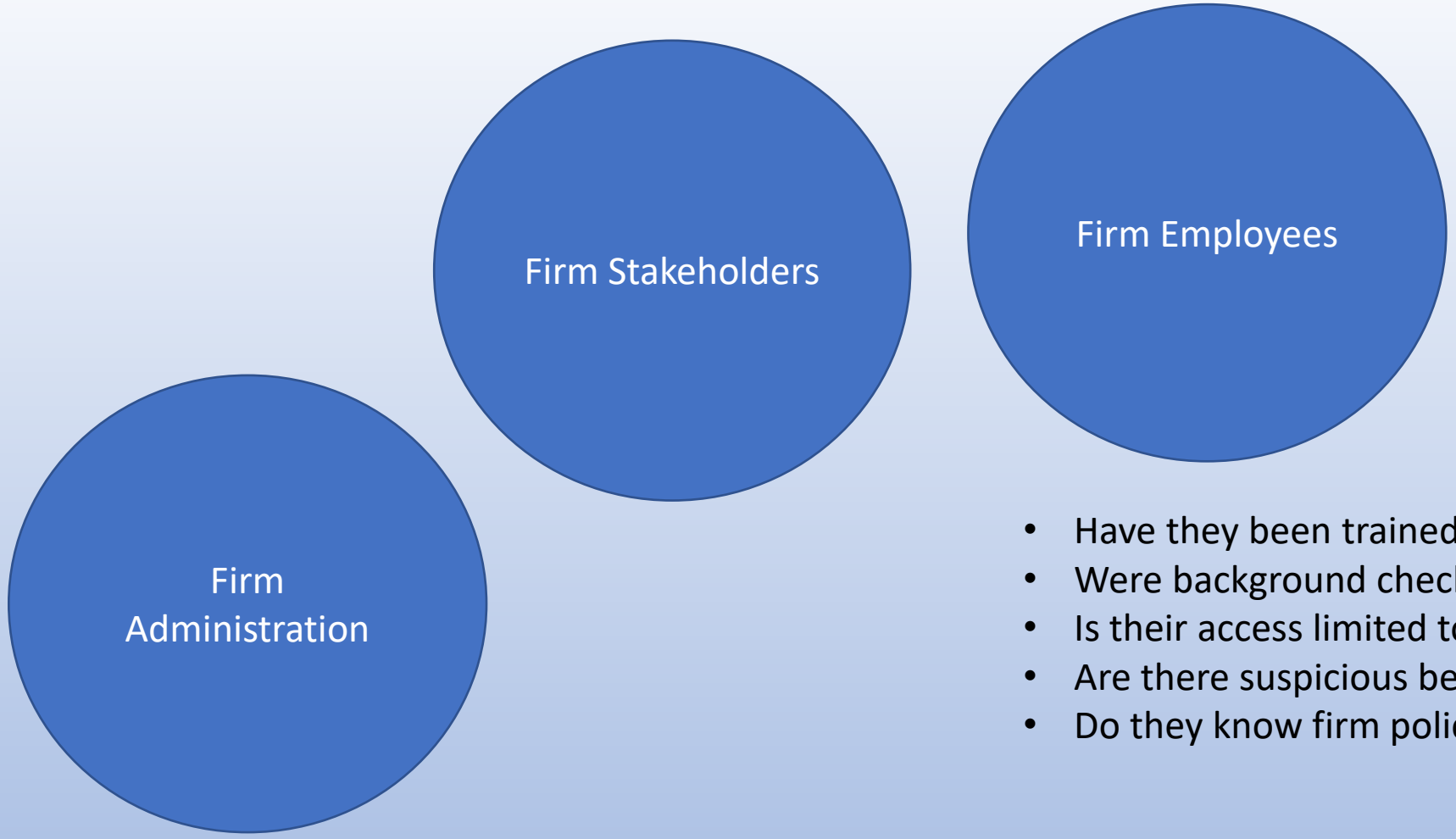
What can I do? Jump In!

- Initiate meetings/discussions specifically for cybersecurity
- Build a team that addresses cybersecurity issues regularly
- Attorney CLEs on ethics obligations re: cybersecurity
- Develop an attorney guru on cybersecurity issues
- Help ensure goals are aligned across the organization
- Ask questions and demand understandable and verifiable answers
- Translate risks into understandable terms for stakeholders
- Clean up the part of the house that you do control
- Promote security! DON'T complain about the hardships of security steps
- Be a part and know your part in Incident Response Plans

Do we remind employees to be vigilant?
Have I helped assemble a cybersecurity team?
Have I jumped in and asked questions?
Is our physical environment properly controlled?
Is IT aware of all the resources we access?
Does administration know its role in planning and incident response?
Would a cybersecurity framework be suited to help build our cybersecurity profile?



- Is Cybersecurity “on your radar”
- Do you know what’s at risk?
- Do you think we are safe?
- Are you confident we are safe?
- Do you/will you sit on the Cybersecurity Committee?
- Do you understand that threats are accelerating and that investing in security is no longer optional?
- Do our security practices meet our ethical/compliance obligations?



- Have they been trained to identify cyberthreats?
- Were background checks run?
- Is their access limited to the needs of their job?
- Are there suspicious behaviors?
- Do they know firm policies and procedures?

- What are your security protocols?
- What access do you need to our system?
- Have you been cleared by our IT Department?
- Do YOU have Cyber Insurance and how much?
- Have you experienced breaches?
- How do you handle breaches?

Firm Stakeholders

Firm Employees

Vendors

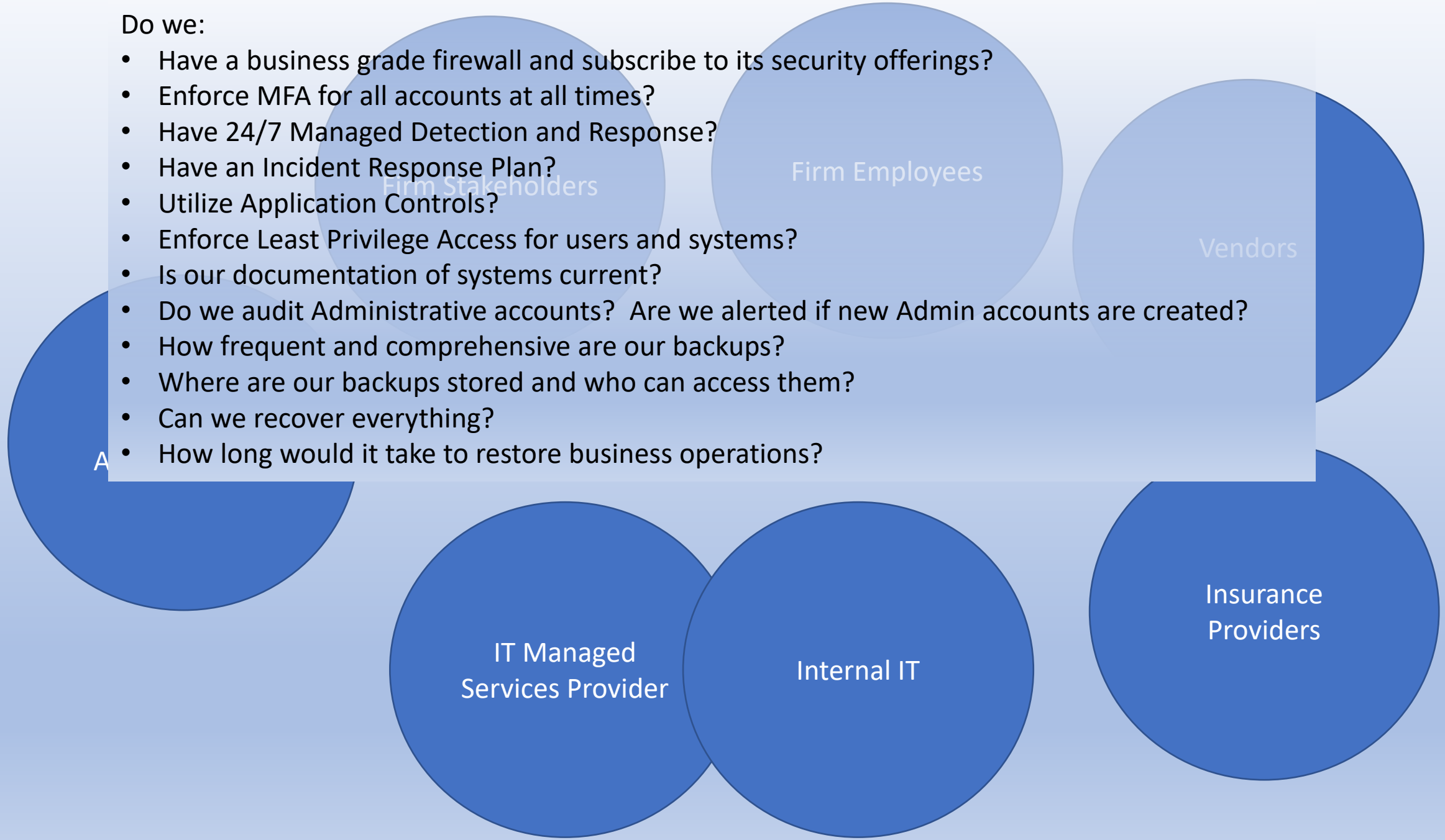
Firm Administration

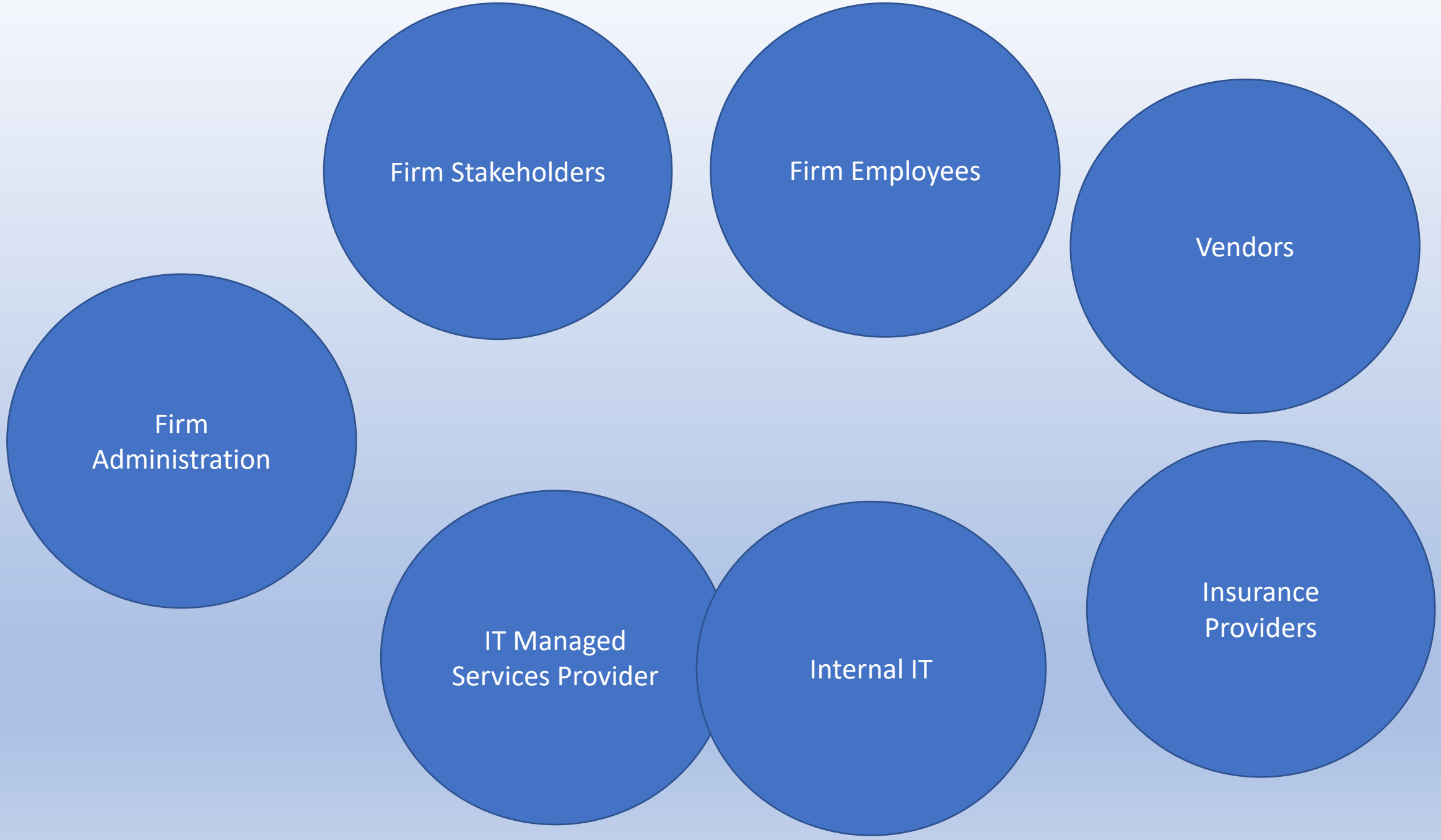
Insurance Providers

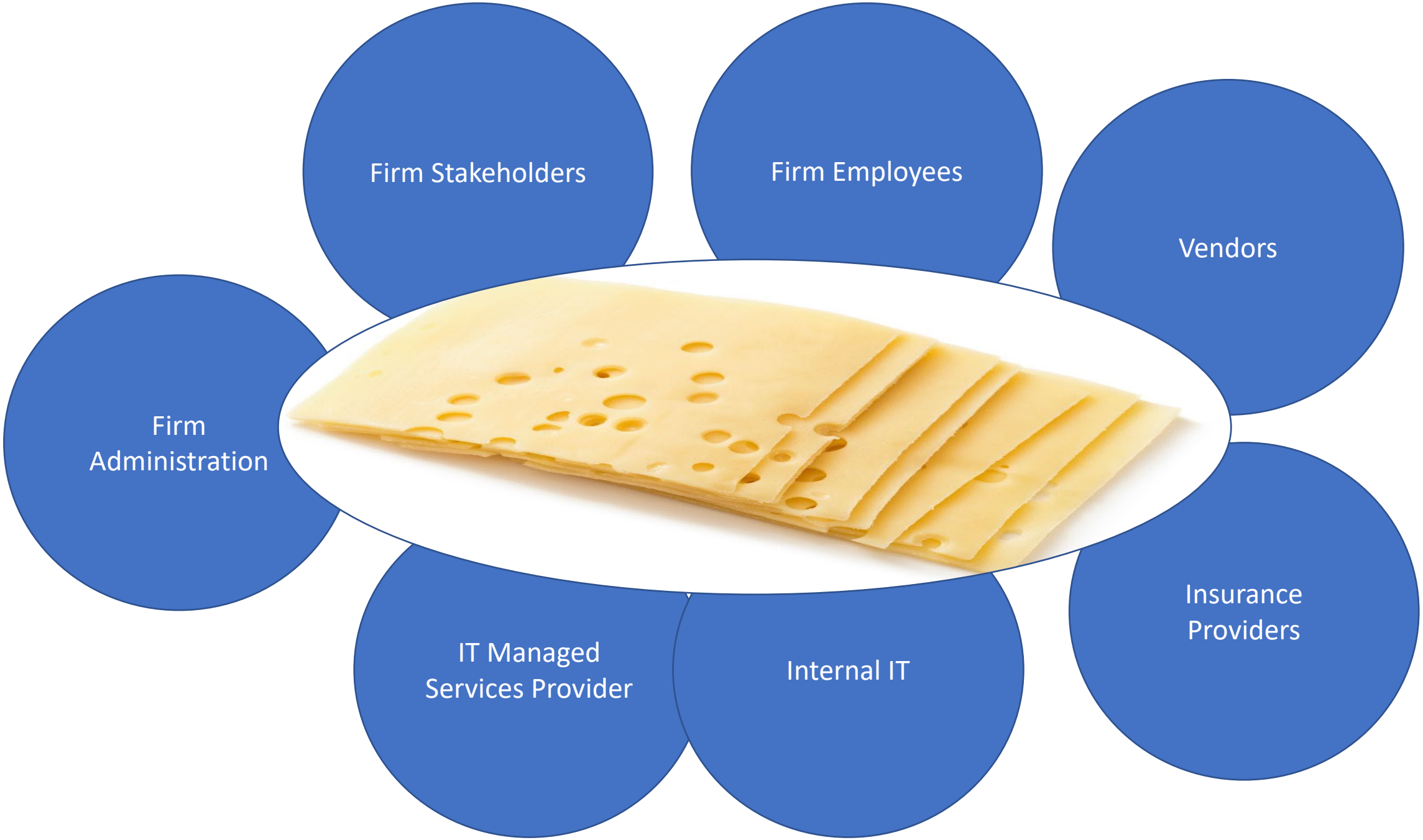
- What is our coverage?
- What types of events are covered?
- What can cause denial of claims?
- How do we confirm compliance?

Do we:

- Have a business grade firewall and subscribe to its security offerings?
- Enforce MFA for all accounts at all times?
- Have 24/7 Managed Detection and Response?
- Have an Incident Response Plan?
- Utilize Application Controls?
- Enforce Least Privilege Access for users and systems?
- Is our documentation of systems current?
- Do we audit Administrative accounts? Are we alerted if new Admin accounts are created?
- How frequent and comprehensive are our backups?
- Where are our backups stored and who can access them?
- Can we recover everything?
- How long would it take to restore business operations?




Firm Stakeholders
Firm Employees
Vendors
Firm Administration
IT Managed Services Provider
Internal IT
Insurance Providers


Firm Stakeholders
Firm Employees
Vendors
Firm Administration
Insurance Providers
IT Managed Services Provider
Internal IT

Questions/Discussion?

Resources

https://www.aldebarangroup.com/Cybersecurity-Webinar/