Pleasant Health

Managed IT Services, Security Compliance for Regulations

“Every contact leaves a trace” — Locard’s exchange principle

Privacy, Security, Compliance

Do the concepts of PSC apply to your business?

It depends, but probably.

Here are some questions to ask regarding your business:

Does your business have confidential data?

How long could your business survive if data was encrypted preventing access to documents?

How long would it take your business to recover if your data was wiped and had to start fresh?

Many of your businesses are already providing some kind of security.

Roofing – Security against elements

Insurance – Security against accidentals, health, auto, aging costs

Financial Advisor – Securing your future comfort level

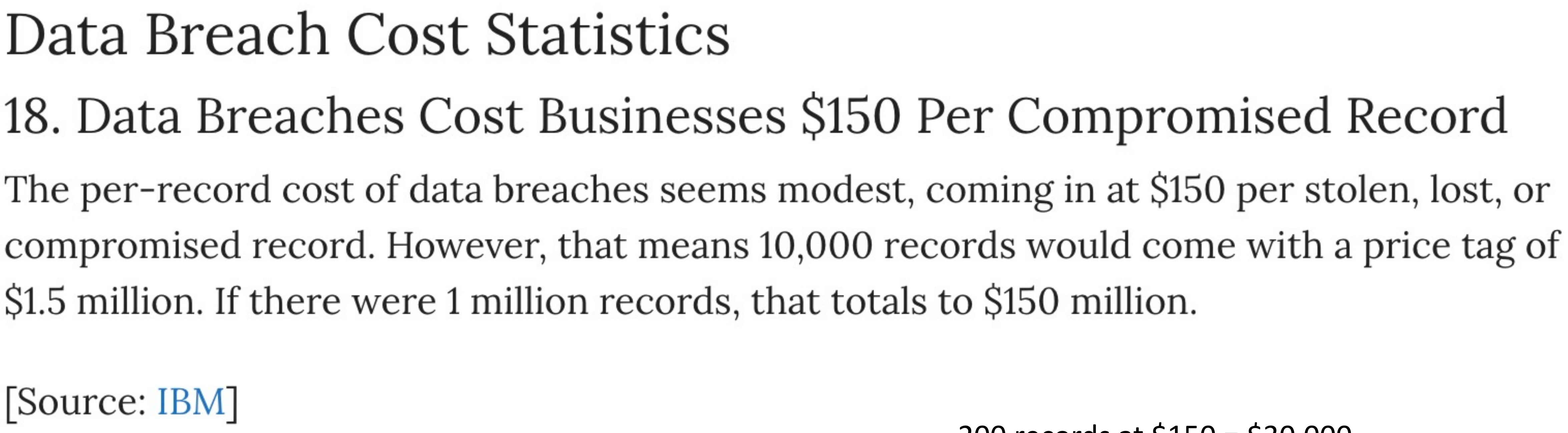
Jujutsu– Gentle Art of Personal Security

Pest Control – Securing against insect and rodents carrying disease and causing destruction

“The eye cannot see what the mind does not know”

Why worry about computer security?

How many customers do you have “data records” of?



Data Breach Cost Statistics

18. Data Breaches Cost Businesses $150 Per Compromised Record

The per-record cost of data breaches seems modest, coming in at $150 per stolen, lost, or compromised record. However, that means 10,000 records would come with a price tag of $1.5 million. If there were 1 million records, that totals to $150 million.

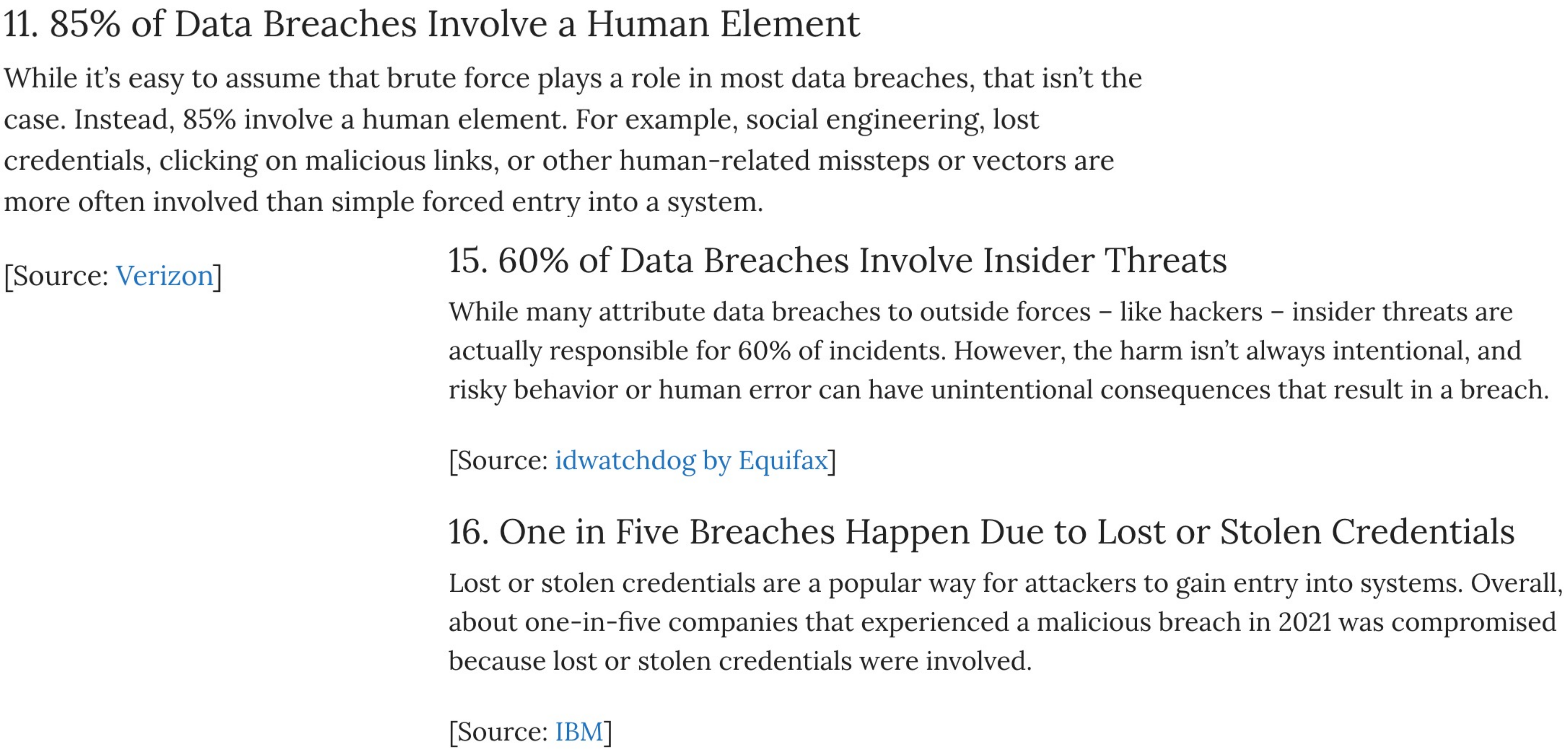
[Source: IBM]

200 records at $150 = $30,000

https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

What are some of the causes of security incidents?

https://firewalltimes.com/data-breach-statistics/



11. 85% of Data Breaches Involve a Human Element

While it’s easy to assume that brute force plays a role in most data breaches, that isn’t the case. Instead, 85% involve a human element. For example, social engineering, lost credentials, clicking on malicious links, or other human-related missteps or vectors are more often involved than simple forced entry into a system.

[Source: Verizon]

15. 60% of Data Breaches Involve Insider Threats

While many attribute data breaches to outside forces – like hackers – insider threats are actually responsible for 60% of incidents. However, the harm isn’t always intentional, and risky behavior or human error can have unintentional consequences that result in a breach.

[Source: idwatchdog by Equifax]

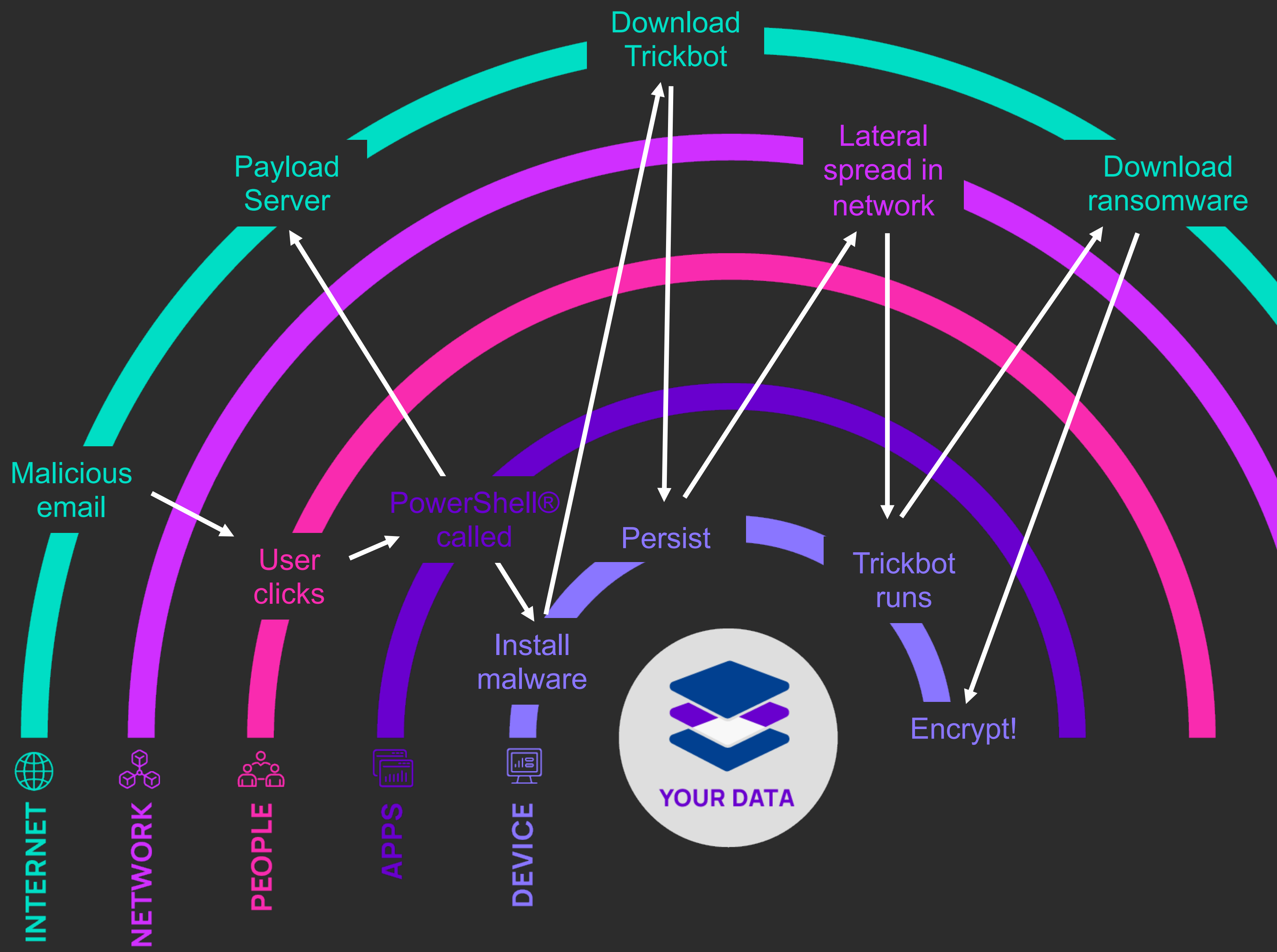
16. One in Five Breaches Happen Due to Lost or Stolen Credentials

Lost or stolen credentials are a popular way for attackers to gain entry into systems. Overall, about one-in-five companies that experienced a malicious breach in 2021 was compromised because lost or stolen credentials were involved.

[Source: IBM]

Sample kill chain for Ryuk ransomware

- Attack touches all layers
- Some more than once
- Varies by attack or threat variant



Essential security has expanded

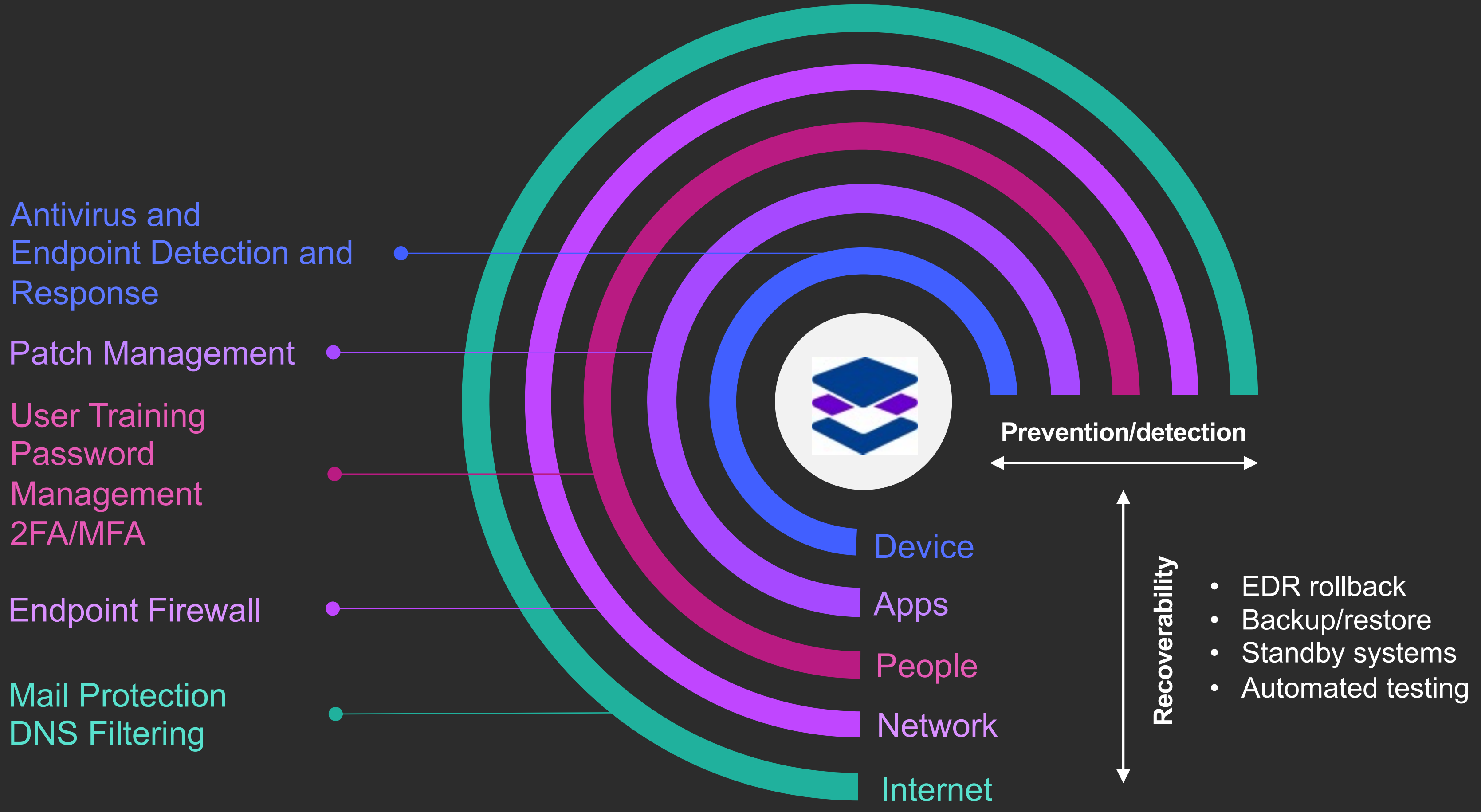
- AV
- EDR
- Patch
- Firewall
- Backup

+

- Mail protection
- DNS Filtering
- Password management
- EDR with rollback
- Recovery testing

+

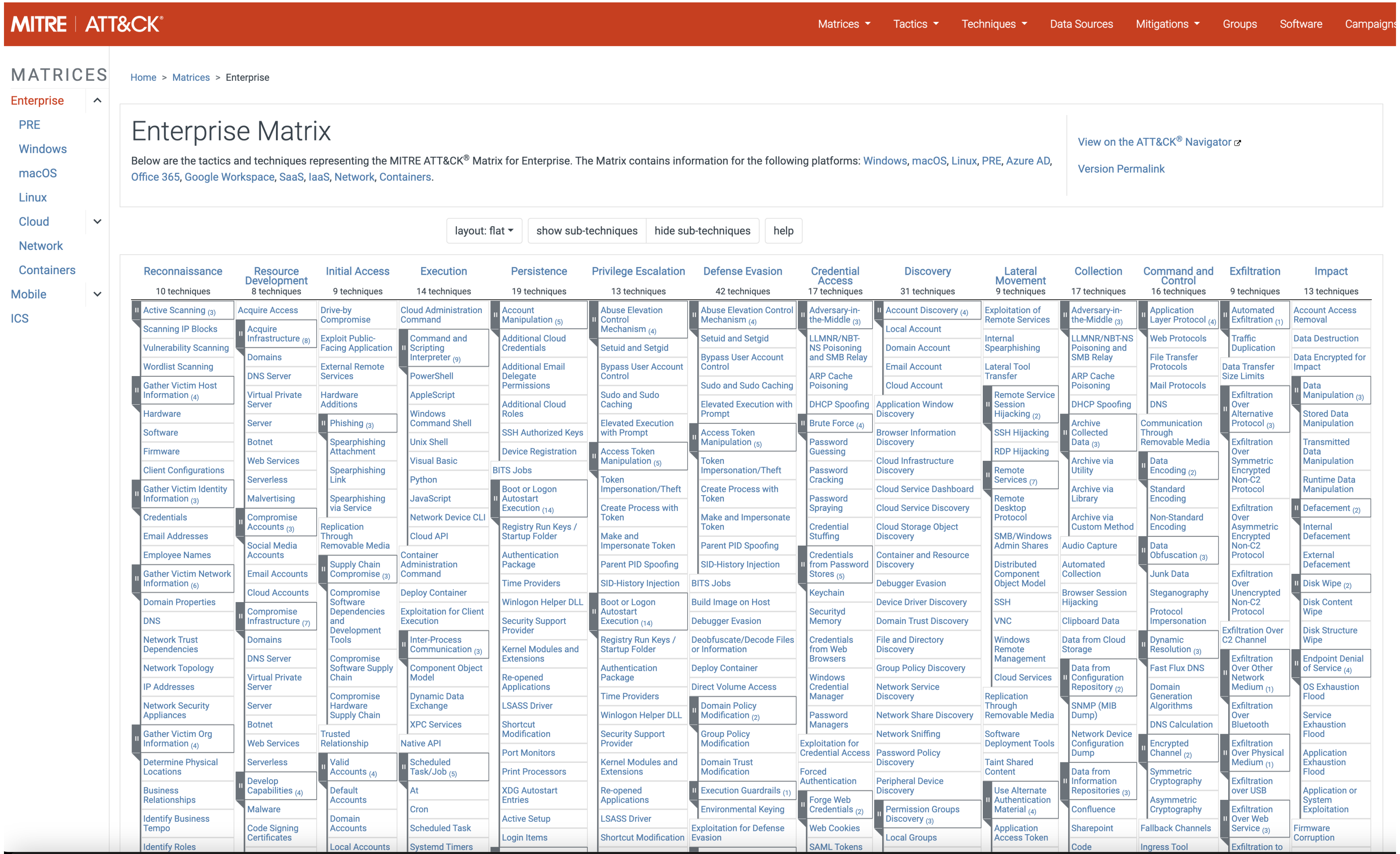
- User training
- Pen testing



- EDR rollback
- Backup/restore
- Standby systems
- Automated testing

How do security professionals keep this all straight?

https://attack.mitre.org/matrices/enterprise/



Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers.

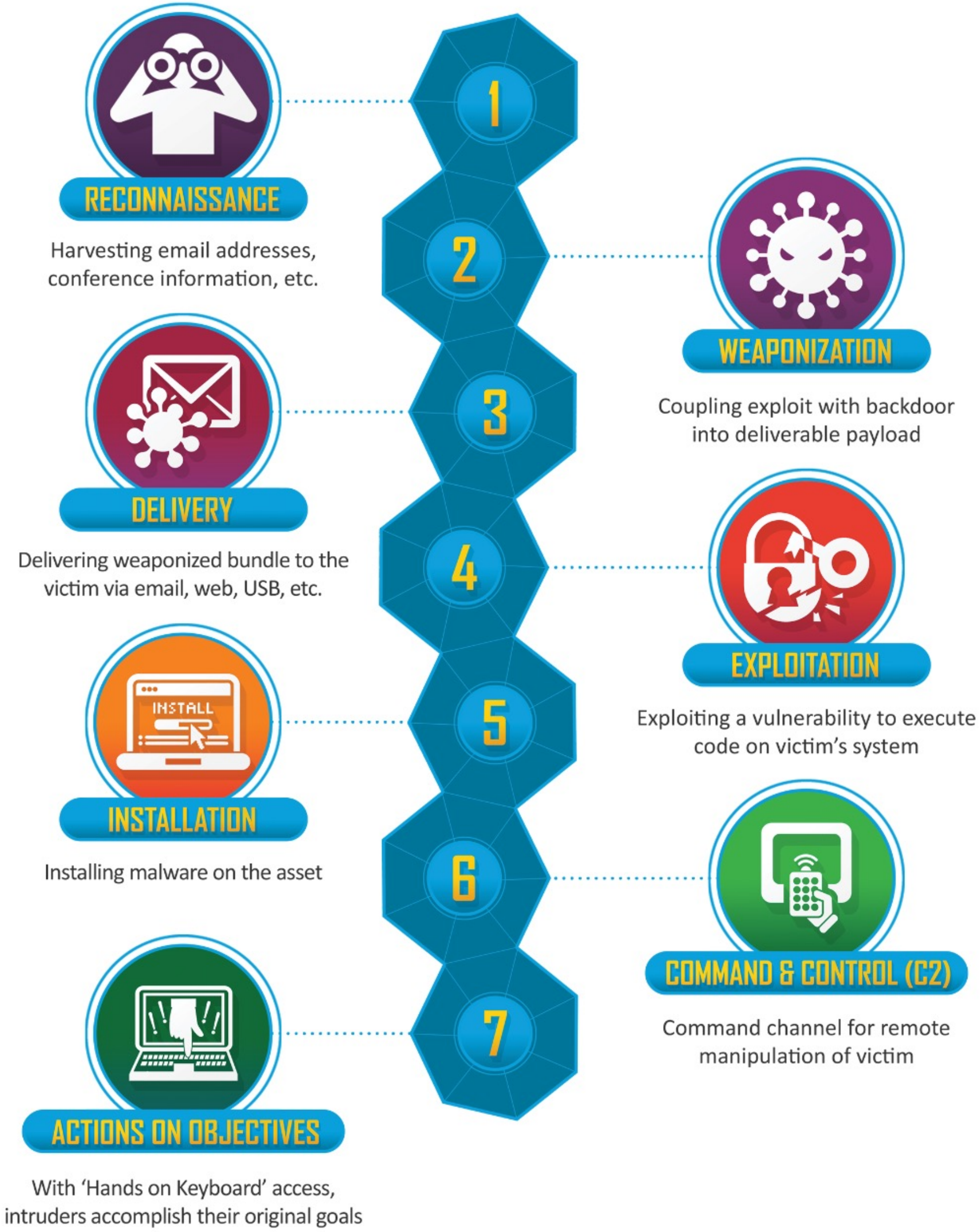
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	9 techniques	14 techniques	19 techniques	13 techniques	42 techniques	17 techniques	31 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Scanning IP Blocks	Acquire Infrastructure (8)	Exploit Public-Facing Application	Command and Scripting Interpreter (9)	Additional Cloud Credentials	Setuid and Setgid	Setuid and Setgid	LLMNR/NBT-NS Poisoning and SMB Relay	Local Account	Internal Spearphishing	LLMNR/NBT-NS Poisoning and SMB Relay	Web Protocols	Traffic Duplication	Data Destruction
Vulnerability Scanning	Domains	External Remote Services	PowerShell	Additional Email Delegate Permissions	Bypass User Account Control	Bypass User Account Control	ARP Cache Poisoning	Domain Account	Lateral Tool Transfer	ARP Cache Poisoning	File Transfer Protocols	Data Transfer Size Limits	Data Encrypted for Impact
Wordlist Scanning	DNS Server	Hardware Additions	AppleScript	Additional Cloud Roles	Sudo and Sudo Caching	Sudo and Sudo Caching	DHCP Spoofing	Email Account	Remote Service Session Hijacking (2)	DHCP Spoofing	Mail Protocols	Exfiltration Over Alternative Protocol (3)	Data Manipulation (3)
Gather Victim Host Information (4)	Virtual Private Server	Phishing (3)	Windows Command Shell	SSH Authorized Keys	Elevated Execution with Prompt	Elevated Execution with Prompt	Brute Force (4)	Cloud Account	SSH Hijacking	Archive Collected Data (3)	DNS	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Stored Data Manipulation
Hardware	Server	Spearphishing Attachment	Unix Shell	Device Registration	Access Token Manipulation (5)	Access Token Manipulation (5)	Password Guessing	Application Window Discovery	RDP Hijacking	Archive via Utility	Communication Through Removable Media	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Transmitted Data Manipulation
Software	Botnet	Spearphishing Link	Visual Basic	BITS Jobs	Token Impersonation/Theft	Token Impersonation/Theft	Password Cracking	Browser Information Discovery	Remote Services (7)	Archive via Library	Data Encoding (2)	Exfiltration Over Unencrypted Non-C2 Protocol	Runtime Data Manipulation
Firmware	Web Services	Spearphishing via Service	Python	Boot or Logon Autostart Execution (14)	Create Process with Token	Create Process with Token	Password Spraying	Cloud Infrastructure Discovery	Remote Desktop Protocol	Archive via Custom Method	Standard Encoding	Exfiltration Over C2 Channel	Defacement (2)
Client Configurations	Serverless	Replication Through Removable Media	JavaScript	Registry Run Keys / Startup Folder	Make and Impersonate Token	Make and Impersonate Token	Credential Stuffing	Cloud Service Dashboard	SMB/Windows Admin Shares	Audio Capture	Non-Standard Encoding	Exfiltration Over Other Network Medium (1)	Internal Defacement
Gather Victim Identity Information (3)	Malvertising	Supply Chain Compromise (3)	Network Device CLI	Authentication Package	Parent PID Spoofing	Parent PID Spoofing	Credentials from Password Stores (5)	Cloud Service Discovery	Distributed Component Object Model	Automated Collection	Data Obfuscation (3)	Exfiltration Over Bluetooth	External Defacement
Credentials	Compromise Accounts (3)	Compromise Software Dependencies and Development Tools	Cloud API	Time Providers	SID-History Injection	SID-History Injection	Keychain	Cloud Storage Object Discovery	SSH	Browser Session Hijacking	Junk Data	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Email Addresses	Social Media Accounts	Compromise Software Supply Chain	Container Administration Command	Winlogon Helper DLL	Boot or Logon Autostart Execution (14)	BITS Jobs	Securityd Memory	Container and Resource Discovery	VNC	Clipboard Data	Steganography	Exfiltration over USB	Disk Content Wipe
Employee Names	Email Accounts	Compromise Hardware Supply Chain	Deploy Container	Security Support Provider	Registry Run Keys / Startup Folder	Build Image on Host	Credentials from Web Browsers	Debugger Evasion	Windows Remote Management	Data from Cloud Storage	Protocol Impersonation	Exfiltration Over Web Service (3)	Disk Structure Wipe
Gather Victim Network Information (6)	Cloud Accounts	Trusted Relationship	Exploitation for Client Execution	Kernel Modules and Extensions	Authentication Package	Debugger Evasion	Windows Credential Manager	Device Driver Discovery	Cloud Services	Data from Configuration Repository (2)	Dynamic Resolution (3)	Exfiltration to	Endpoint Denial of Service (4)
Domain Properties	Compromise Infrastructure (7)	Valid Accounts (4)	Inter-Process Communication (3)	Re-opened Applications	Time Providers	Deobfuscate/Decode Files or Information	Password Managers	Domain Trust Discovery	Replication Through Removable Media	SNMP (MIB Dump)	Fast Flux DNS		OS Exhaustion Flood
DNS	Domains	Default Accounts	Component Object Model	LSASS Driver	Winlogon Helper DLL	Deploy Container	Exploitation for Credential Access	File and Directory Discovery	Software Deployment Tools	Network Device Configuration Dump	Domain Generation Algorithms		Service Exhaustion Flood
Network Trust Dependencies	DNS Server	Domain Accounts	Dynamic Data Exchange	Shortcut Modification	Security Support Provider	Direct Volume Access	Forced Authentication	Group Policy Discovery	Taint Shared Content	Data from Information Repositories (3)	DNS Calculation		Application Exhaustion Flood
Network Topology	Virtual Private Server	Local Accounts	XPC Services	Port Monitors	Kernel Modules and Extensions	Domain Policy Modification (2)	Forge Web Credentials (2)	Network Service Discovery	Use Alternate Authentication Material (4)	Confluence	Encrypted Channel (2)		Application or System Exploitation
IP Addresses	Server		Native API	Print Processors	Re-opened Applications	Group Policy Modification	Web Cookies	Network Share Discovery	Application Access Token	Sharepoint	Symmetric Cryptography		Firmware Corruption
Network Security Appliances	Botnet		Scheduled Task/Job (5)	XDG Autostart Entries	LSASS Driver	Domain Trust Modification	SAML Tokens	Network Sniffing		Code	Asymmetric Cryptography		
Gather Victim Org Information (4)	Web Services		At	Active Setup	Shortcut Modification	Execution Guardrails (1)		Password Policy Discovery			Fallback Channels		
Determine Physical Locations	Serverless		Cron	Login Items		Environmental Keying		Peripheral Device Discovery			Ingress Tool		
Business Relationships	Develop Capabilities (4)		Scheduled Task			Exploitation for Defense Evasion		Permission Groups Discovery (3)					
Identify Business Tempo	Malware		Systemd Timers					Local Groups					
Identify Roles	Code Signing Certificates												

The first step in Privacy, Security and Compliance is an inventory.

Why?

In any directed cyber attack, the bad guys first step is recon. They will be performing an inventory of your business to determine what they can attack.

On the right is Lockheed Martin's Cyber Kill Chain®



1 RECONNAISSANCE

Harvesting email addresses, conference information, etc.

2 WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

3 DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION

Installing malware on the asset

6 COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals

What do you include in your inventory?

Technology the business has – mobile devices, network, PCs, printers, shredders, IoT devices, etc…

Software the business uses – local, Software as a Service like Quickbooks Online, Xero Accounting, Stripe/Square, M365, Google Enterprise, Wix, Social media logins…

Data the business has and where is it – Payroll data in Quickbooks, SSNs, W-2, W-4, I-9, incorporation docs, bills+account numbers and contacts/responsible parties, CRM customer lists, invoices, trade secrets, formulations, login info, PHI…. Printed, electronic, stone tablets

Third Parties the business uses – Shared office space, cleaners, landlord of a leased office building, Accountant, Banks, CC processor

Locations where business is conducted or business assets may be present – Cars, Office locations, home along with the Keys to these locations. I encourage you to maintain a key inventory right beside your software access inventory which is tied with employee onboarding and offboarding procedure.

Personnel - Employees, Interns, Volunteers, anyone who has access to the components of company "inventory"

While gathering all of this you might as well lump in all other **Business Assets** including tools of the trade.

What do you do with your inventory?

This is a simple sample examination of **Technology** though the Privacy, Security and Compliance lenses.

Privacy: Are there cameras in locations where privacy is expected? What about an IoT speaker like Alexa or Google? Are phone calls recorded and is appropriate notification given?

Security: Are systems patched on a regular basis? Are computers configured to require a password? Being a small business, Is there a separation of personal and business devices? Do computers and mobile devices have their storage encrypted or a power-on (BIOS/hard drive) password? Do you follow a Cybersecurity Framework?

Compliance: Many regulations have provisions requiring security. Some examples are shown in a later slide.

Designing a Compliance program 30,000 ft view

Identify what regulations your business must comply with.
Not sure, consult with your attorney.

Test how you are complying

Document in case you must demonstrate compliance.

Repeat this process every year or if needed because of a major change to your business.

(This is not a complete list)

FEDERAL Regulations and Agencies:
(FCC) (FDA) (ATF) (FTC) (SEC) (IRS)
Health Insurance Portability and Accountability Act (HIPAA)
Americans with Disabilities Act (ADA)
Fair Labor Standards Act (FLSA)
Occupational Safety and Health Act (OSHA)
Family and Medical Leave Act (FMLA)
Equal Employment Opportunity Commission (EEOC)
Sarbanes-Oxley Act (SOX)
Office of Foreign Assets Control (OFAC)
Gramm-Leach-Bliley Act (GLBA)
Employee Retirement Income Security Act (ERISA)
Alcohol and Tobacco Tax and Trade Bureau (TTB)
Federal Motor Carrier Safety Administration (FMCSA)
Children's Online Privacy Protection Act (COPPA)
Fair Credit Reporting Act (FCRA)
Federal Acquisition Regulation (FAR)
Defense Federal Acquisition Regulation Supplement (DFARS)
International Traffic in Arms Regulations (ITAR)
Export Administration Regulations (EAR)
Cybersecurity Maturity Model Certification (CMMC)

Compliance - What are the steps at 1,000 feet?

Identify what you have to comply with

Create an **Inventory**

Create a set of **controls**. Use a framework to assist in compliance.

Perform a **Risk Analysis**

Document what was analyzed and deficiencies in a risk register.

Remediate and **Document** actions of fixing or create, with what auditors call, a “compensating control”.

Documentation demonstrates compliance and improvement. Documentation keeps attorneys and regulators happy.

Repeat

FEDERAL Regulations and Agencies:

(FCC) (FDA) (ATF) (FTC) (SEC) (IRS)

Health Insurance Portability and Accountability Act (HIPAA)

Americans with Disabilities Act (ADA)

Fair Labor Standards Act (FLSA)

Occupational Safety and Health Act (OSHA)

Family and Medical Leave Act (FMLA)

Equal Employment Opportunity Commission (EEOC)

Sarbanes-Oxley Act (SOX)

Office of Foreign Assets Control (OFAC)

Gramm-Leach-Bliley Act (GLBA)

Employee Retirement Income Security Act (ERISA)

Alcohol and Tobacco Tax and Trade Bureau (TTB)

Federal Motor Carrier Safety Administration (FMCSA)

Children's Online Privacy Protection Act (COPPA)

Fair Credit Reporting Act (FCRA)

Federal Acquisition Regulation (FAR)

Defense Federal Acquisition Regulation Supplement (DFARS)

International Traffic in Arms Regulations (ITAR)

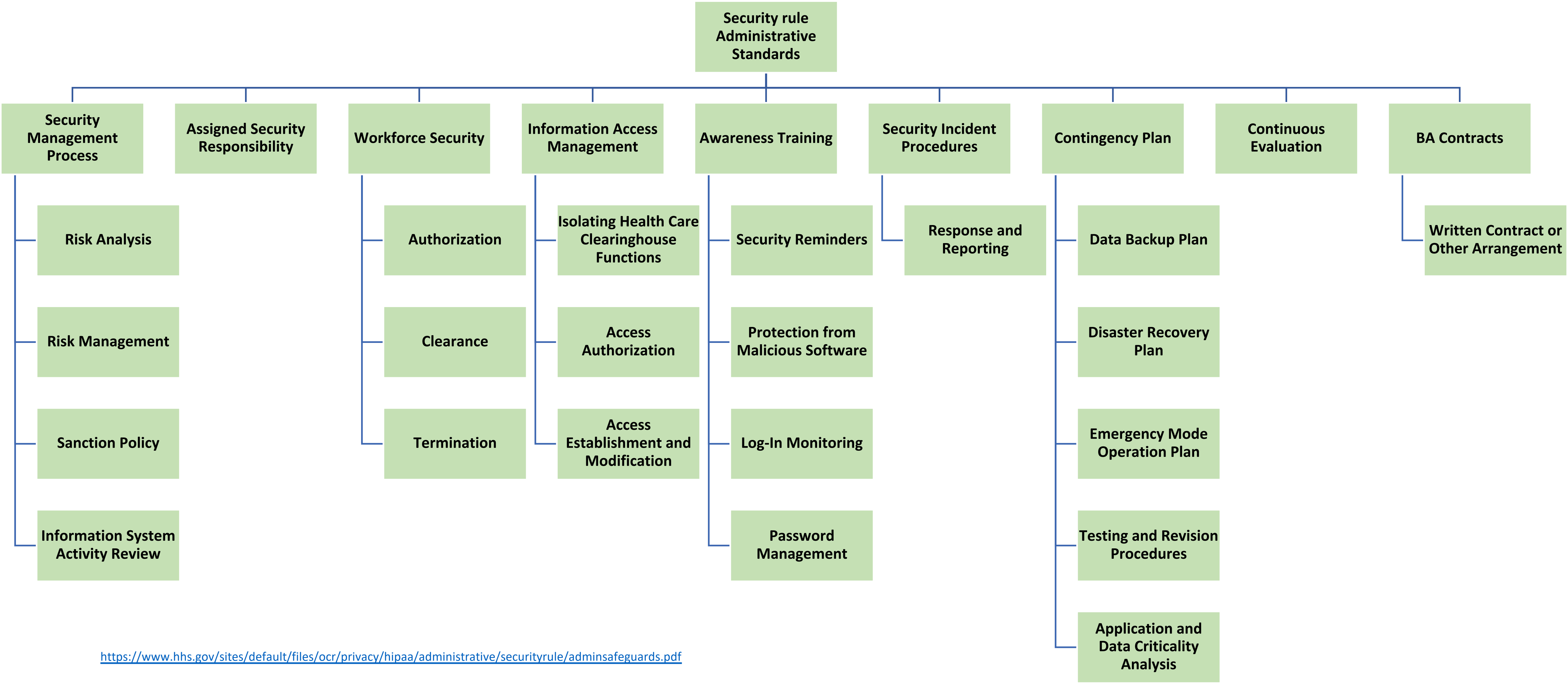
Export Administration Regulations (EAR)

Cybersecurity Maturity Model Certification (CMMC)

NIST CYBER SECURITY FRAMEWORK

PREPARE	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Organizational Communication	Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Development of Control Baselines	Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Enterprise Architecture	Governance	Data Security	Detection Processes	Analysis	Communications
Alignment with RMF	Risk Assessment	Info Protection Processes and Procedures		Mitigation	
	Risk Management Strategy	Maintenance		Improvements	
		Protective Technology			

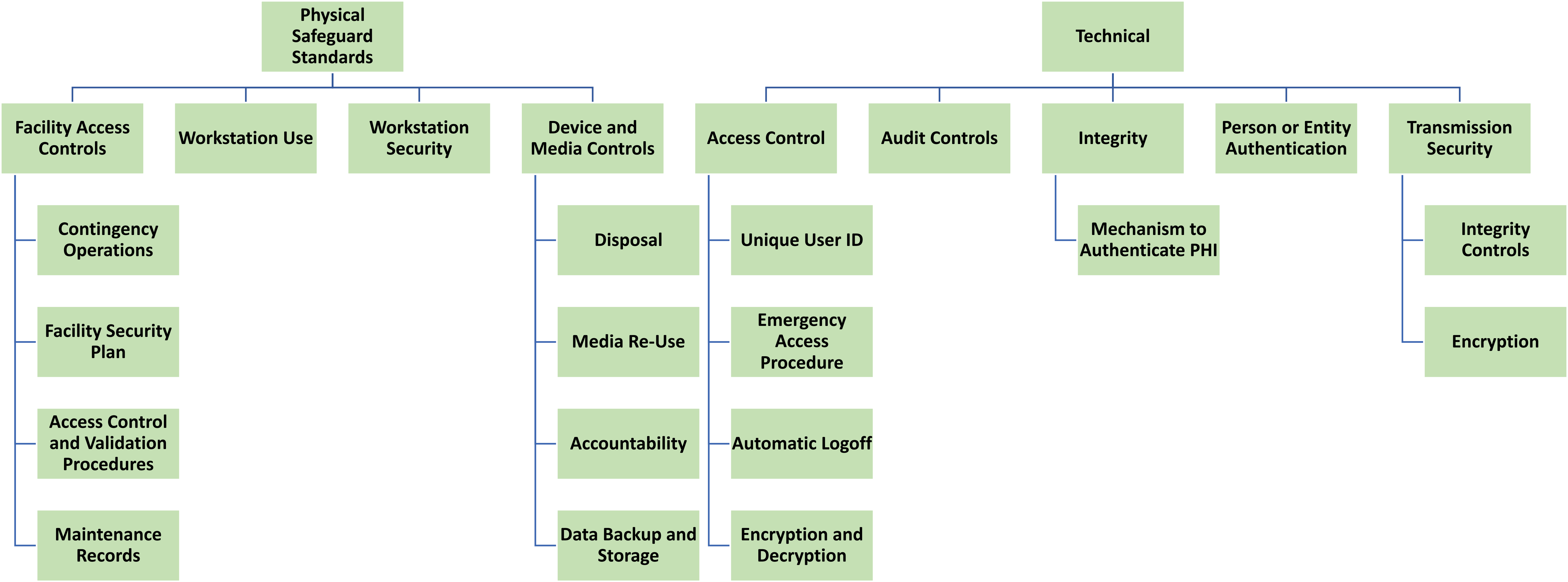
HIPAA Security Rule



- Security rule Administrative Standards
  - Security Management Process
    - Risk Analysis
    - Risk Management
    - Sanction Policy
    - Information System Activity Review
  - Assigned Security Responsibility
  - Workforce Security
    - Authorization
    - Clearance
    - Termination
  - Information Access Management
    - Isolating Health Care Clearinghouse Functions
    - Access Authorization
    - Access Establishment and Modification
  - Awareness Training
    - Security Reminders
    - Protection from Malicious Software
    - Log-In Monitoring
    - Password Management
  - Security Incident Procedures
    - Response and Reporting
  - Contingency Plan
    - Data Backup Plan
    - Disaster Recovery Plan
    - Emergency Mode Operation Plan
    - Testing and Revision Procedures
    - Application and Data Criticality Analysis
  - Continuous Evaluation
  - BA Contracts
    - Written Contract or Other Arrangement

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf

HIPAA Physical and Technical Rules



- Physical Safeguard Standards
  - Facility Access Controls
    - Contingency Operations
    - Facility Security Plan
    - Access Control and Validation Procedures
    - Maintenance Records
  - Workstation Use
  - Workstation Security
  - Device and Media Controls
    - Disposal
    - Media Re-Use
    - Accountability
    - Data Backup and Storage
- Technical
  - Access Control
    - Unique User ID
    - Emergency Access Procedure
    - Automatic Logoff
    - Encryption and Decryption
  - Audit Controls
  - Integrity
    - Mechanism to Authenticate PHI
  - Person or Entity Authentication
  - Transmission Security
    - Integrity Controls
    - Encryption

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

Small Business introduction to Privacy, Security and Compliance

Your business has a few intertwined variables to consider with how you can move ahead with compliance:

Time, Energy, Money, and Experience/Knowledge

> *"If you want to go fast, go alone.*
> *If you want to go far, go together."*
> *African proverb*

BUT WAIT
THERE'S MORE
memes.com

Other uses for an Inventory

1. Risk Management: The inventory is used to identify potential risks and vulnerabilities in your business. For example, outdated hardware or software can pose a security risk.

2. Business Continuity and Disaster Recovery: The inventory can support business continuity and disaster recovery planning. If a disaster occurs, you'll know exactly what needs to be replaced or restored.

3. Insurance Valuation and Claims Processing: Having a complete inventory can help you ensure that your business is adequately insured.

4. Asset Tracking: In case of theft or employee fraud, an updated inventory can help track the assets and possibly assist in recovery.

5. Financial Reporting and Audit: Detailed inventory information can assist in financial reporting and audits. It can provide a clear picture of the company's assets, their value, and depreciation, which is essential for accurate financial statements.

6. Operational Efficiency: Understanding what resources you have and where they are can improve operational efficiency. It can help identify redundancies, streamline processes, and optimize resource usage.

7. Strategic Planning: An inventory can inform strategic planning by providing a snapshot of the current state of your business. It can help identify areas where investment is needed, guide decisions about technology adoption, and support capacity planning.

8. Employee Management: By tracking which employees have access to which resources, the inventory can help manage roles and responsibilities more effectively. It can also support risk management, onboarding and offboarding processes.

9. Vendor Management: If your inventory includes information about software and hardware vendors, it can support vendor management activities, such as contract renewal, negotiation, relationship management, and cost control.

10. Regulatory Compliance: While this is part of your original use case, it's worth emphasizing that an inventory can be crucial for demonstrating compliance with various regulations. It can help you prove that you're managing your assets responsibly and protecting sensitive data.

11. Mergers and Acquisitions: If your company is involved in a merger or acquisition, a detailed inventory can facilitate the due diligence process by providing clear information about the company's assets and liabilities.

Small Business introduction to Privacy, Security and Compliance

I missed highlighting one large category of Data inventory which may apply to PSC.

Contracts/Agreements

In HIPAA there is a requirement for a BAA:
Business Associate Agreement (BAA): A BAA is a contract between a HIPAA-covered entity and a business associate (a person or entity performing certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity). The BAA ensures that the business associate will appropriately safeguard protected health information.

There are a lot of other agreements that you should gather and review for requirements that fall under Privacy, Security or Compliance. Your neighborhood small business attorney Ashley Storm Ruleman would love to hear from you if you need assistance with contracts and agreements.

Federal Trade Commission

This slide is a high-level summary and is not a prescriptive list of compliance items.

FTC safeguard rule section 314.1(h) lists 13 examples of the types of financial institutions:

mortgage lenders, payday lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors that aren’t required to register with the SEC.

Section 314.2(h) of the Rule lists four examples of businesses that *aren’t* a “financial institution.” In addition, the FTC has exempted from certain provisions of the Rule financial institutions that “maintain customer information concerning fewer than five thousand consumers.”

What’s the point of this slide?

If possible, limit the data you retain to the MINIMUM NECESSARY!!!
Doing so reduces your risk.

Introduction to STRIDE
Title: **Understanding STRIDE for Threat Modeling**

•STRIDE is a threat modeling methodology developed by Microsoft. It stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.

•It helps in identifying potential threats in the system and categorizing them based on the type of threat.

Bullet Points:

1. **Spoofing**: Illegitimate use of legitimate services by faking the identity.
2. **Tampering**: Unauthorized modification of data.
3. **Repudiation**: Ability to deny an action without the possibility of proof.
4. **Information Disclosure**: Exposure of information to individuals who are not supposed to have access to it.
5. **Denial of Service (DoS)**: Denying legitimate users access to a service.
6. **Elevation of Privilege**: An unprivileged user gaining privileged access.

1."Passwords are like underwear. You shouldn’t leave them out where people can see them. You should change them regularly. And you shouldn’t loan them out to strangers." - Chris Pirillo – old C-NET/TechTV show host

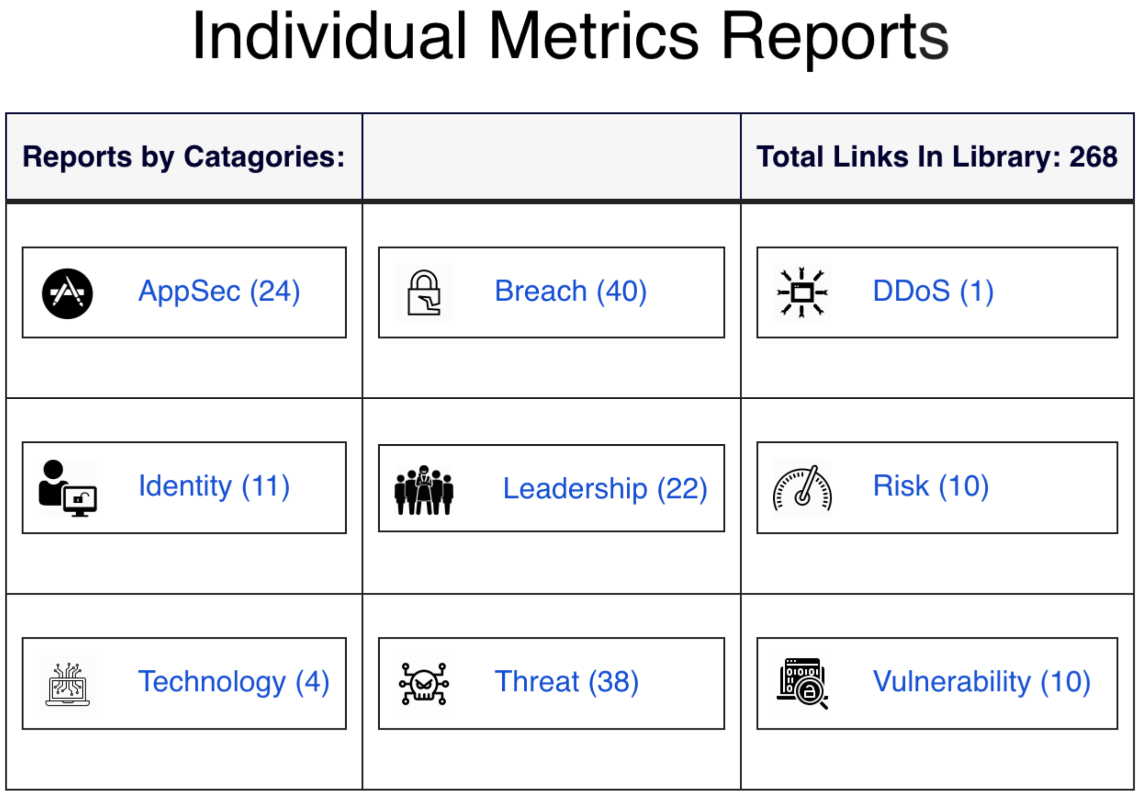
2."Security is always excessive until it’s not enough." - Robbie Sinclair

3."Amateurs hack systems, professionals hack people." - Bruce Schneier – Security Technologist

Where can I get more of these scary stats?

https://pleasanthealth.net/2023-data-breach-investigations-report-dbir.pdf#page=17

Visit the link below to access the reports. Breach reports have the juiciest (in a nerd’s opinion) details.



Individual Metrics Reports

Reports by Catagories:		Total Links In Library: 268
AppSec (24)	Breach (40)	DDoS (1)
Identity (11)	Leadership (22)	Risk (10)
Technology (4)	Threat (38)	Vulnerability (10)

https://johnmasserini.com/resources/industry-statistical-reports/