Insider Threats

Do more harm than external attackers?

Tim Schnurr, CRISC

Inquisitive IT

Tim Schnurr, CFA CRISC

2000s	Early 2010s	Late 2010s	2020s
Hedge Fund Analyst & Sell Side Research	Intellectual Property Valuation & Brokerage	Big 4 Large Company Cybersecurity	Small Company & HNW Individual Cybersecurity

External

Adversaries trying to breach and steal data, often including proprietary or sensitive data

What Can they identify and sell easily?

Internal

Internal actors trying to mis-appropriate valuable trade secrets to benefit

OR

Clicking on Links :)

Intent

Negligent

Careless actions to open risk.

Clicking on Links, Shadow IT like dropbox or personal email

Malicious

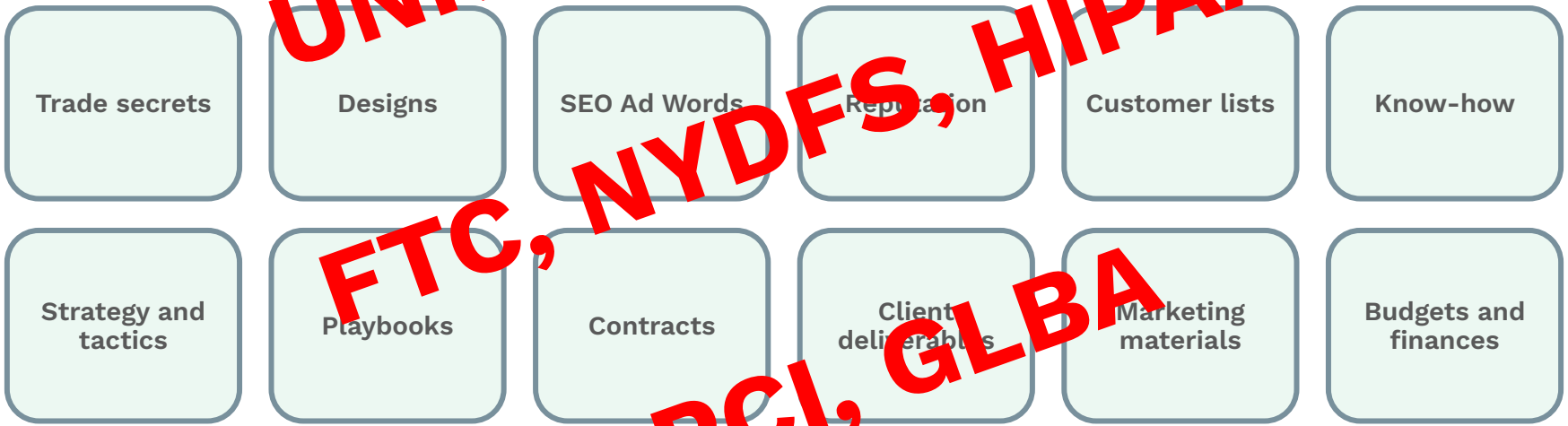
Intent to monetize for personal benefit.

What’s at Risk? Crown Jewels, IP (legally called Trade Secrets)

Every organization has confidential information (proprietary and private)

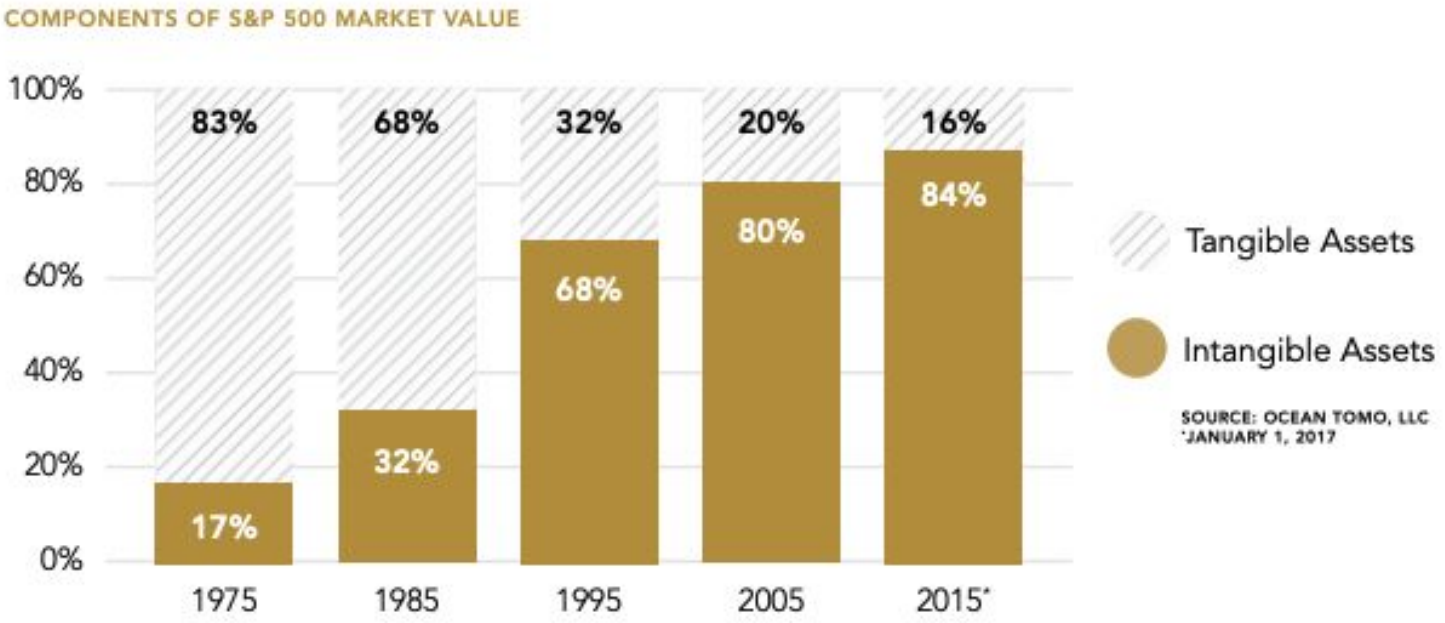
What's at Risk? Crown Jewels or IP

Every organization has confidential information (proprietary and private)



UNREGULATED BY FTC, NYDFS, HIPAA, PCI, GLBA

IP AS % OF COMPANY VALUE



MORE THAN 80% OF COMPANY VALUE RESIDES IN INTANGIBLE ASSETS OR IP

WHY NOW? OFFLINE TO ONLINE, DATA CREATION AND ACCESS

[1] Cybersecurity Insiders // [2] Ponemon Institute // [3] IBM // [4] Accenture

By the Numbers

60% Data breaches caused by insider threat incidents [1]

287 Average number of days to detect and contain an insider threat [3]

15M Average annual cost of an insider threat incident [2]

72% Organizations that have experienced an insider threat in the past year [4]

44% Increase in insider threats over the past two years [2]

[1] Cybersecurity Insiders // [2] Ponemon Institute // [3] IBM // [4] Accenture

Why Does Insider Threat Occur

Too often employees don’t realize they don’t own the work they created, rather the firm does

- ✔ **They can’t leave or exit with it - Acknowledge Duty**
- ✔ **Should be careful when sharing - Confidentiality (i.e., least trust, need to know)**
- ✔ **Additional security controls - Data Classification**
- ✔ **Role-based and access -**
- ✔ **Role-based training**

LARGELY UNREPORTED

NO DUTY TO DISCLOSE INSIDER “BREACH” - EMPLOYEE EXITS WITH FILES (NOT PRIVACY DATA)

Not Insurable

Shift in IP Strategy

IP Program

Patent

Public Disclosure – Gov't granted monopoly

Trade Secret

Private - Reasonable efforts to keep private
Coordinated with Risk & Compliance

Trade Secret Controls

Data Access Controls / Zer Trust

Digital Tracking & Logs

Who’s Responsible?

Insider threats (specifically IP Strategy) falls somewhere between cybersecurity, human resources, IT, legal, and risk-management departments

Cybersecurity

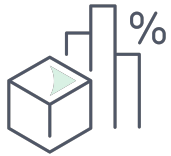
Not included in most frameworks (NIST, CIS, ISO)

HR

Not a focus until a bad employee exit

Legal

GC may not have IP background



Risk

We are not a tech company, so not a specific worry

Also…

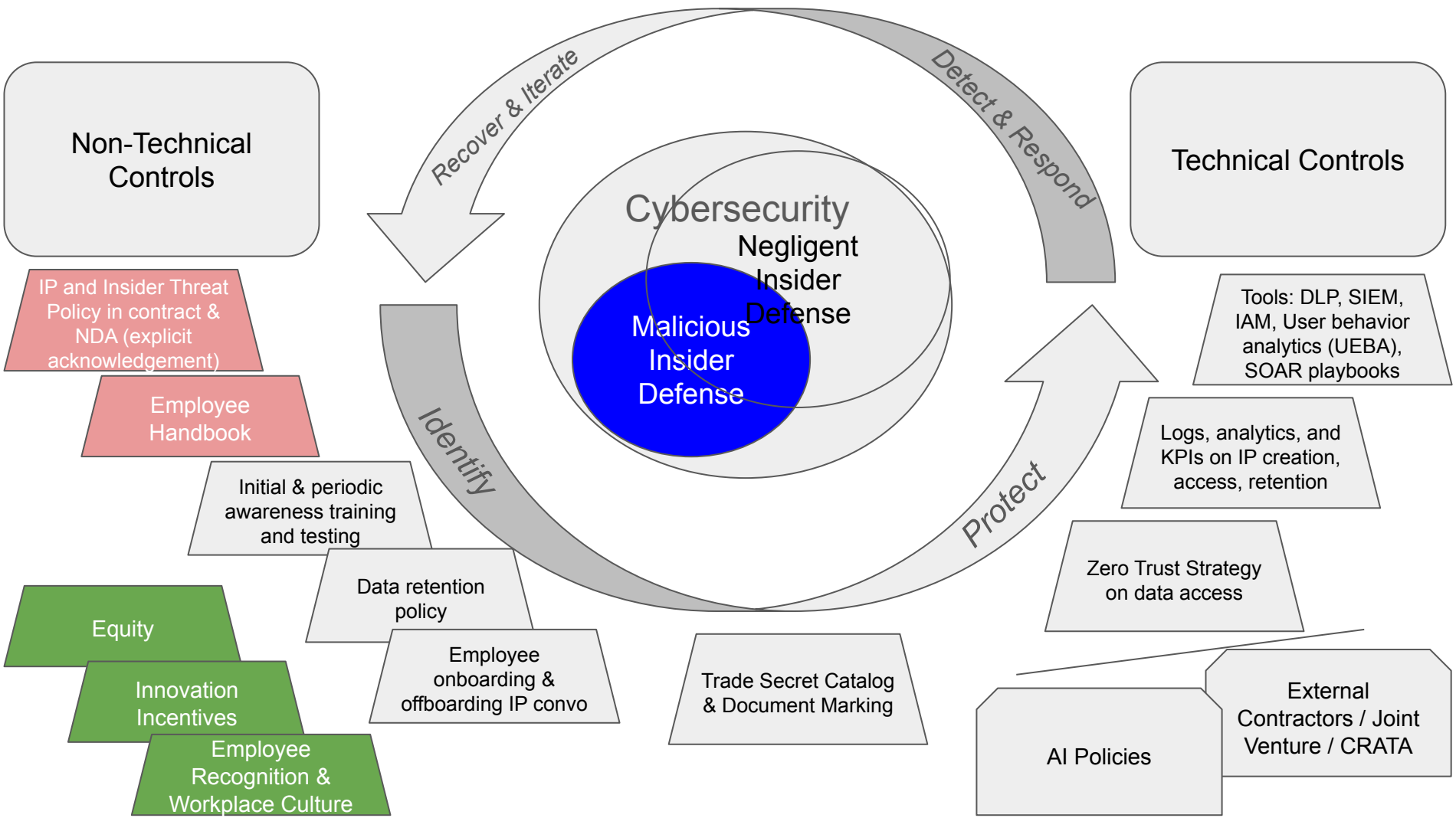
Small organizations likely have none of these roles

Effective Defense

- Leadership defined goals and policy
- Document Trade Secret Catalog (Meta-Data likely ideal) - IDENTIFY
- Employee handbook and training (obligation confirmation) - Onboarding and Offboarding
- Incorporate into Cyber Training
- Data Classification
- Enforce with Tools (Can’t depend on Whistleblowers) - PROTECT - DETECT

Tools and Enforcement

- ✔ Data classification tools
- ✔ Data access tools
- ✔ Logs
- ✔ Policies & Alerts
- ✔ Watermarking and tracking


Non-Technical Controls
Technical Controls
Recover & Iterate
Detect & Respond
Identify
Protect
Cybersecurity
Negligent Insider Defense
Malicious Insider Defense
IP and Insider Threat Policy in contract & NDA (explicit acknowledgement)
Employee Handbook
Initial & periodic awareness training and testing
Data retention policy
Employee onboarding & offboarding IP convo
Equity
Innovation Incentives
Employee Recognition & Workplace Culture
Trade Secret Catalog & Document Marking
Tools: DLP, SIEM, IAM, User behavior analytics (UEBA), SOAR playbooks
Logs, analytics, and KPIs on IP creation, access, retention
Zero Trust Strategy on data access
AI Policies
External Contractors / Joint Venture / CRATA

Role Play Litigation

Imagine trying to convince a judge that an employee is guilty of stealing company assets. What evidence can be presented that the rules were conveyed, monitoring was sufficient, and the digital trail is clear, and the employee understood the duty and clearly violated that responsibility? - DEFEND TRADE SECRETS ACT 2016

Also a great way to increase your budget to senior leadership as you protect/guard firm value

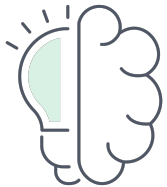
Key Takeaways

Non-technical Must Haves

Acknowledge duty of company ownership

Employee agreement, NDA, IP assignment

Employee handbook



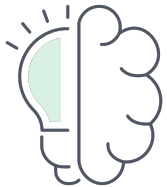
Ongoing training

Technical - Logs, Forensics, Alerting, Testing

Identify and Classify Data

Access Controls

Logging



Simulate

Questions and Comments