ADAPTING AND EVOLVING

Lessons Learned from Changing Security Landscapes

Courtney Healey
Insider Threat Program Manager
Cyber Security Operations
Courtney.Healey@equifax.com

10 September 2019

Confidential and Proprietary

Who We Are And What We Do

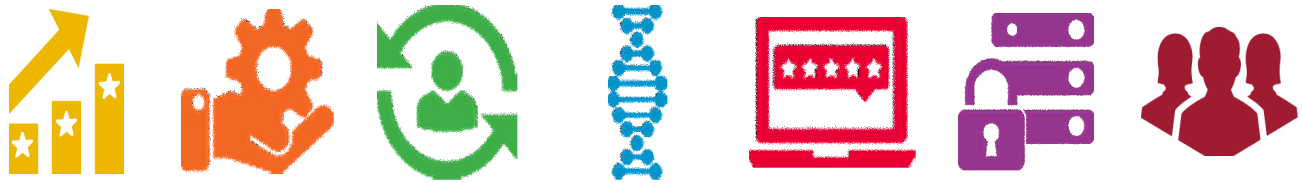
We are a global data, analytics, and technology company and we exist to help people live their financial best. We do that by blending unique data, analytics, and technology to create insights to power the world with knowledge to help make more informed decisions.

Our vision is to be the trusted leader that creates innovative solutions and insights that help customers drive growth and move people forward. To do that, we must focus on seven key areas: Growth, Technology, Customer-centricity, Data, Consumer-friendly CRA, Security, and One Team.

We have a passion and culture that promotes and rewards Integrity, Growth, Change, Unity, and Support.

Definition	A global data, analytics, and technology company
Purpose	Helping people live their financial best
Tagline	Powering the World with Knowledge
Position	At Equifax, we believe knowledge drives progress. We blend unique data, analytics and technology with a passion for serving customers globally, to create insights that power the decisions that move people forward.
Vision	To be the trusted global leader in data, advanced analytics, and technology that creates innovative solutions and insights that help customers drive growth and move people forward.

Imperatives



DRIVE GROWTH	CLOUD-FIRST TECHNOLOGY	CULTURE OF CUSTOMER CENTRICITY	MARKET-LEADING D&A	CONSUMER-FRIENDLY CRA	INDUSTRY LEADER IN SECURITY	EQUIFAX TEAM

Values	Integrity	Growth	Change	Unity	Support

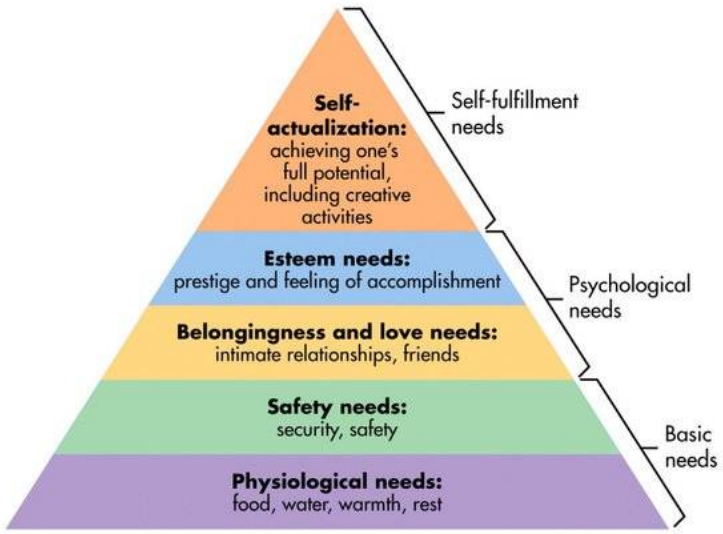
Strategic Questions for Insider Threat Programs

While there's no one-way to structure an InTP, we believe sharing our successes and failures in answering these questions can help you consider what you can do to maximize yours.

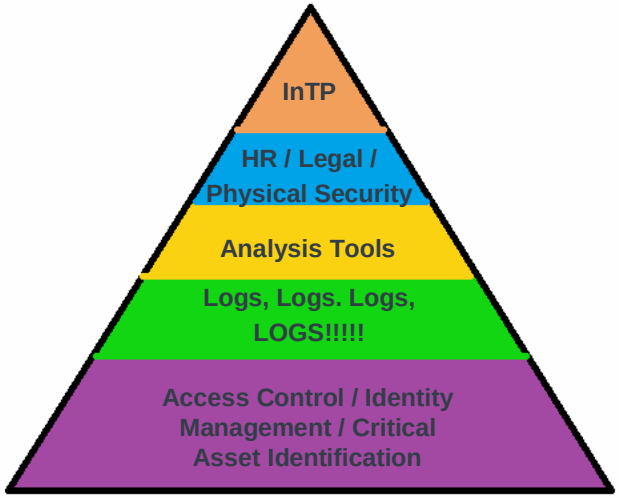
- Funding and executive buy-in…when should you get it?
- Where is the best place, organizationally, for an InTP to be placed to maximize effectiveness?
- What data should the InTP have and how do you get it?
- What tools and skillsets do you need?

Timing and Executive Buy-In

- Maslow's Hierarchy of Needs vs. InTP Hierarchy of Needs



https://simplyphsychology.org/maslow.html



If you are going to build a stand-alone program that functions proactively and reactively, you must already have addressed the other security needs.

Organizational Placement

Round 1 - Corporate Security

Reactive

- Analysts were co-located with the Internal Investigations
- Org silos created distance from data
- Limited ability to 'drive collection'; instead treated as 'case support'

Round 2 – Cyber Operations

Proactive

Analysts were co-located with SOC / Countermeasures / Red Team / Cyber Intel

Org structure created opportunities to collaborate regarding data needs

Merged human expertise with technical minds to drive internal 'intelligence' on potential ways an insider could cause harm

X-Factors : Leadership support, ability to bridge silos

Data – What and How

Equifax InTP Intelligence Cycle

- DLP / SIEM alerts
  - Data exfil
  - Physical access
  - Anomalous activity
- HR
  - upcoming terminations lists, discipline/disgruntlement concerns

Team Skills

- Social Science
  - Strong partnerships with BUs, Legal, HR, Audit, and other Security functions
  - Writing / Speaking
  - Intellectual curiosity
  - Truth to power personalities
  - Customer / Corporate priorities

- Technical / Cyber
  - Familiarity with DLP, UBA, SIEM tools
  - Documentation / Tracking / Case management
  - Incident Handling / Forensics a plus!

Questions / Discussion

- There are many ways your organization could configure and address the challenges discussed…but I think everyone here would agree that the one thing every program will have to do is adapt and evolve as technologies and laws change!

- What has/hasn't worked in your organization?