Insider Threat

Human Risk In A Digital Age

Sunette Runhaar

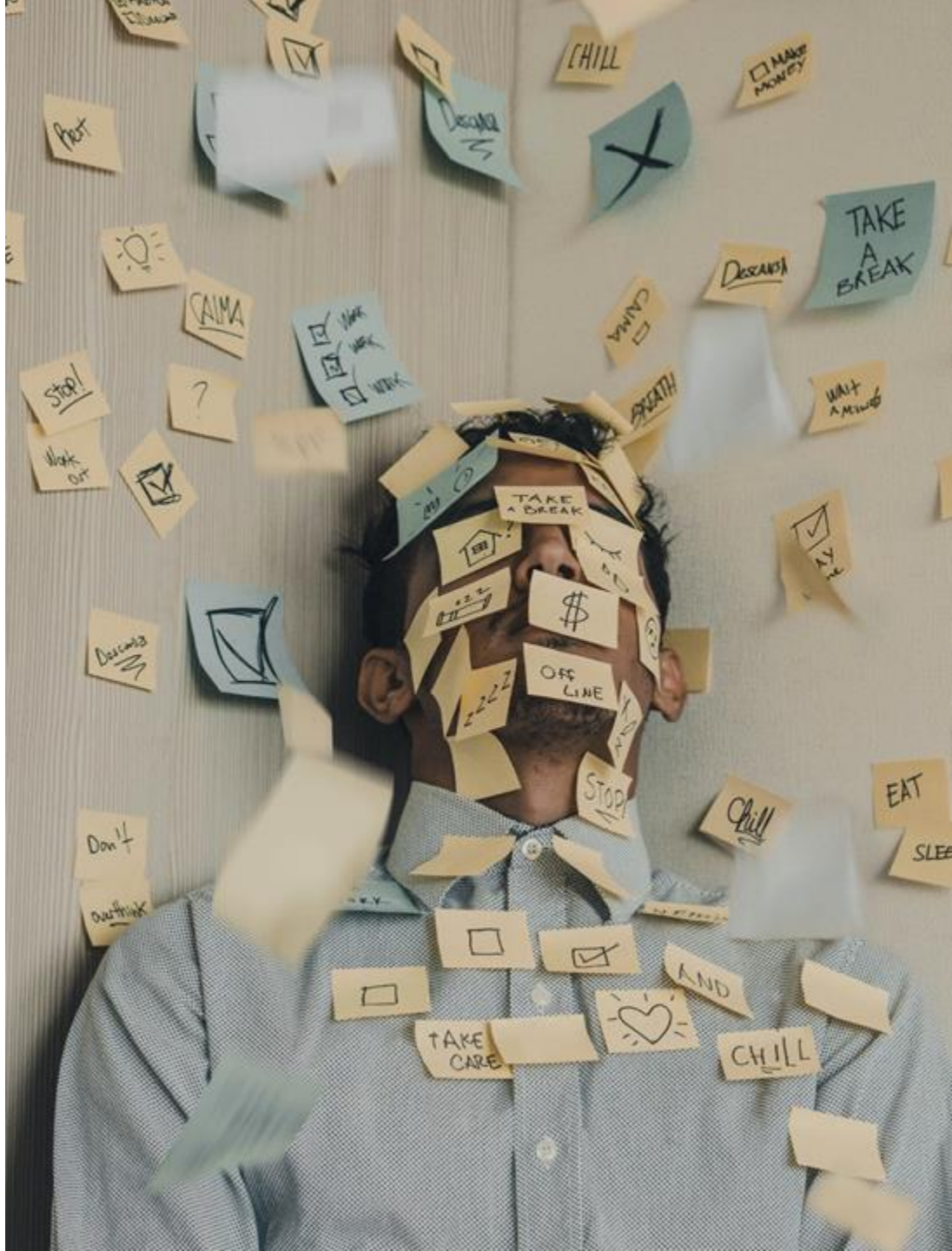
What Is an Insider Threat?

Insider

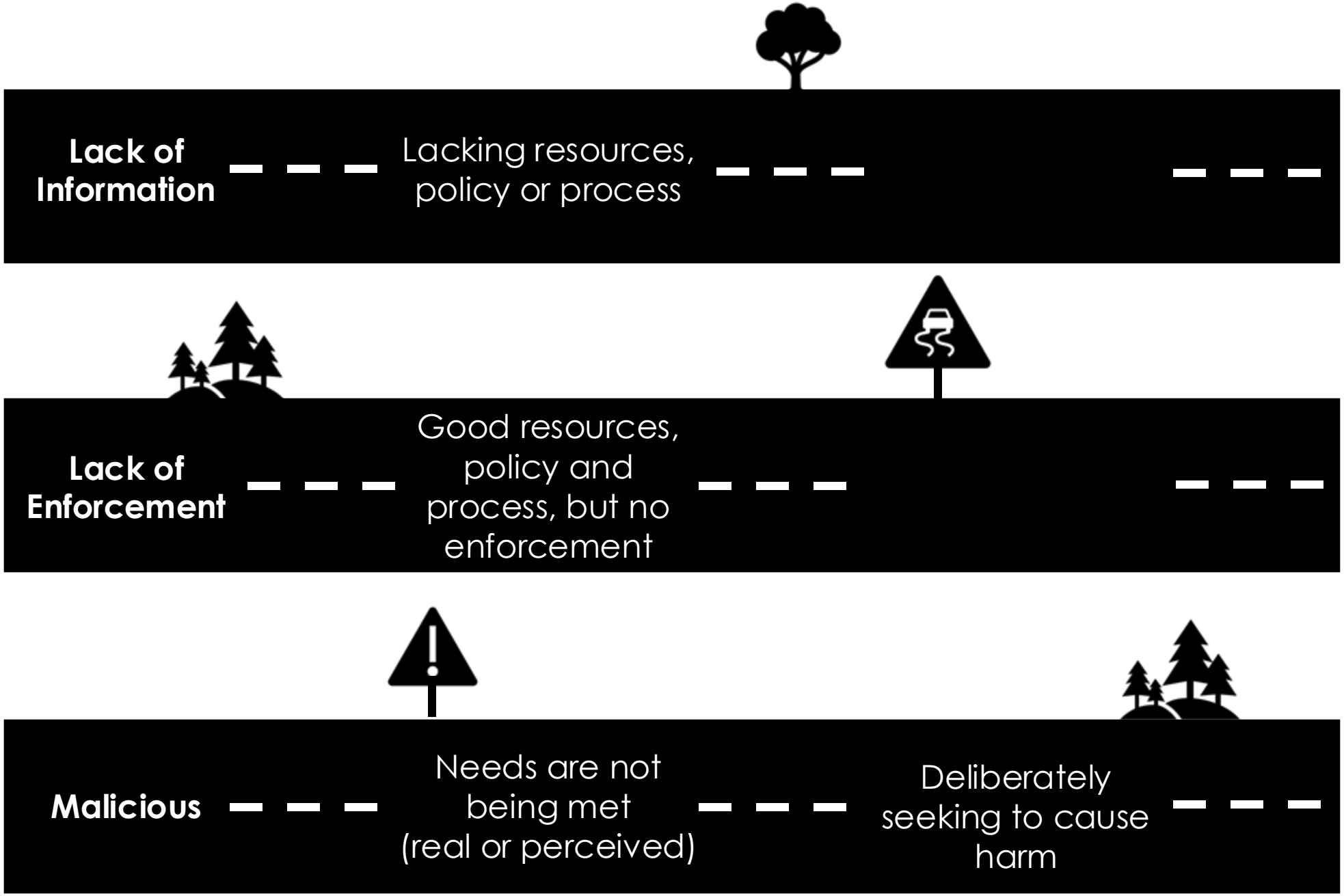
An individual who has (or had) legitimate and authorized access to an organization's assets.

Insider Threat

The risk that an insider will use their access to harm the organization, ***whether intentionally or unintentionally***.



How Do They Develop?



IP Theft

Espionage

Sabotage

Fraud

Data Breach

Media Leak

Malware

Violence

Real Needs Not Being Met

Hostile working environment

Discrimination and bias

Lack of development opportunities

Gaslighting

Favourtism

Concerns ignored/downplayed

Undervalued

Perception Of Needs Not Being Met

Miscommunication

Unclear expectations

Disconnected from team

Personal pressures affecting work

Perceived lack of action

Sense of entitlement

Case Study
The Critical Pathway

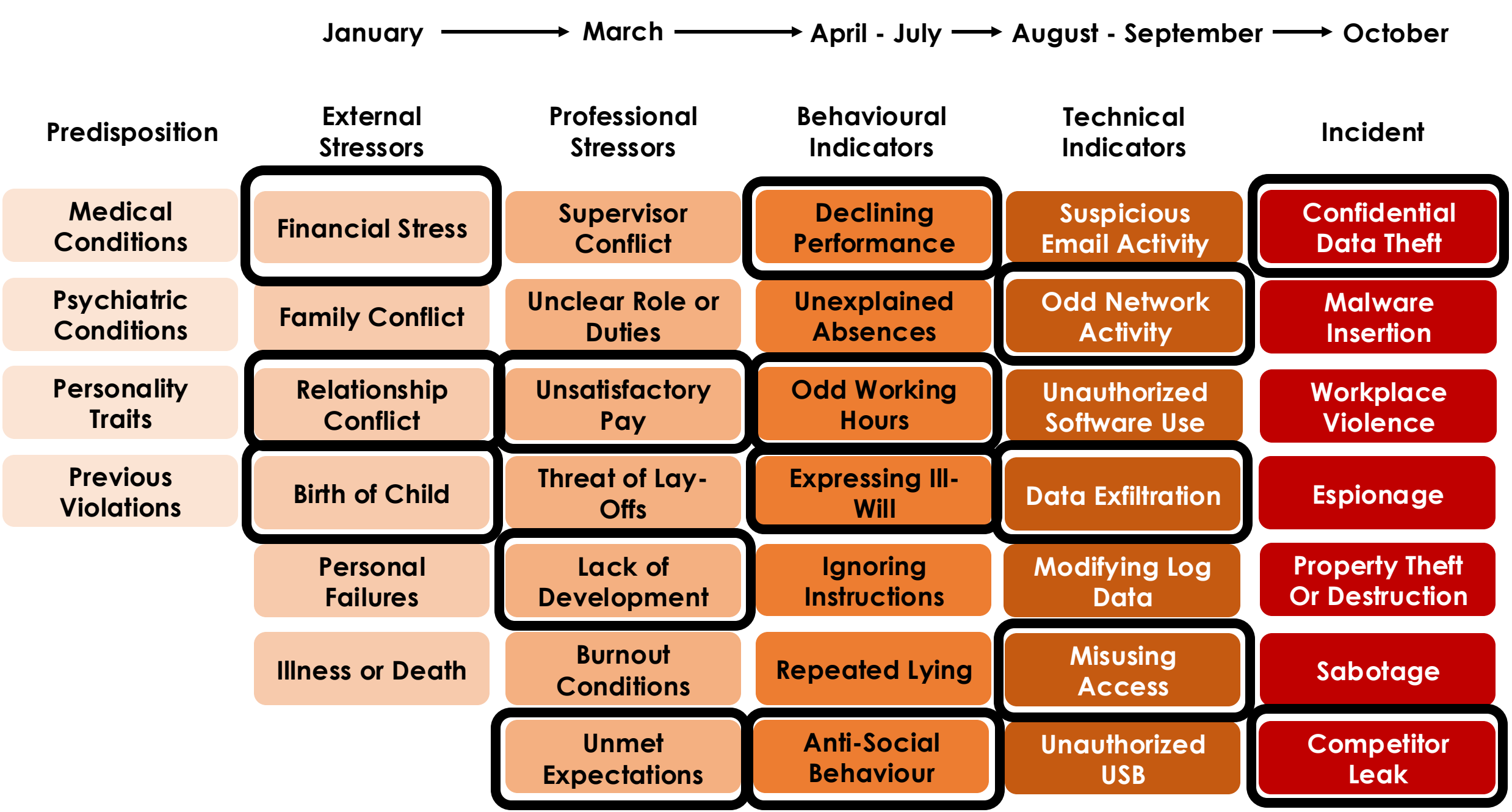
Predisposition	External Stressors	Professional Stressors	Behavioural Indicators	Technical Indicators	Incident
Medical Conditions	Financial Stress	Supervisor Conflict	Declining Performance	Suspicious Email Activity	Confidential Data Theft
Psychiatric Conditions	Family Conflict	Unclear Role or Duties	Unexplained Absences	Odd Network Activity	Malware Insertion
Personality Traits	Relationship Conflict	Unsatisfactory Pay	Odd Working Hours	Unauthorized Software Use	Workplace Violence
Previous Violations	Birth of Child	Threat of Lay-Offs	Expressing Ill-Will	Data Exfiltration	Espionage
	Personal Failures	Lack of Development	Ignoring Instructions	Modifying Log Data	Property Theft Or Destruction
	Illness or Death	Burnout Conditions	Repeated Lying	Misusing Access	Sabotage
		Unmet Expectations	Anti-Social Behaviour	Unauthorized USB	Competitor Leak

Long-term full-time employee

Workplace team

Loves a team lunch and Friday drink


Visibly excited to secure crown jewel IP
Just blocked your USB access


January
March
April - July
August - September
October
Predisposition
External Stressors
Professional Stressors
Behavioural Indicators
Technical Indicators
Incident
Medical Conditions
Psychiatric Conditions
Personality Traits
Previous Violations
Financial Stress
Family Conflict
Relationship Conflict
Birth of Child
Personal Failures
Illness or Death
Supervisor Conflict
Unclear Role or Duties
Unsatisfactory Pay
Threat of Lay-Offs
Lack of Development
Burnout Conditions
Unmet Expectations
Declining Performance
Unexplained Absences
Odd Working Hours
Expressing Ill-Will
Ignoring Instructions
Repeated Lying
Anti-Social Behaviour
Suspicious Email Activity
Odd Network Activity
Unauthorized Software Use
Data Exfiltration
Modifying Log Data
Misusing Access
Unauthorized USB
Confidential Data Theft
Malware Insertion
Workplace Violence
Espionage
Property Theft Or Destruction
Sabotage
Competitor Leak

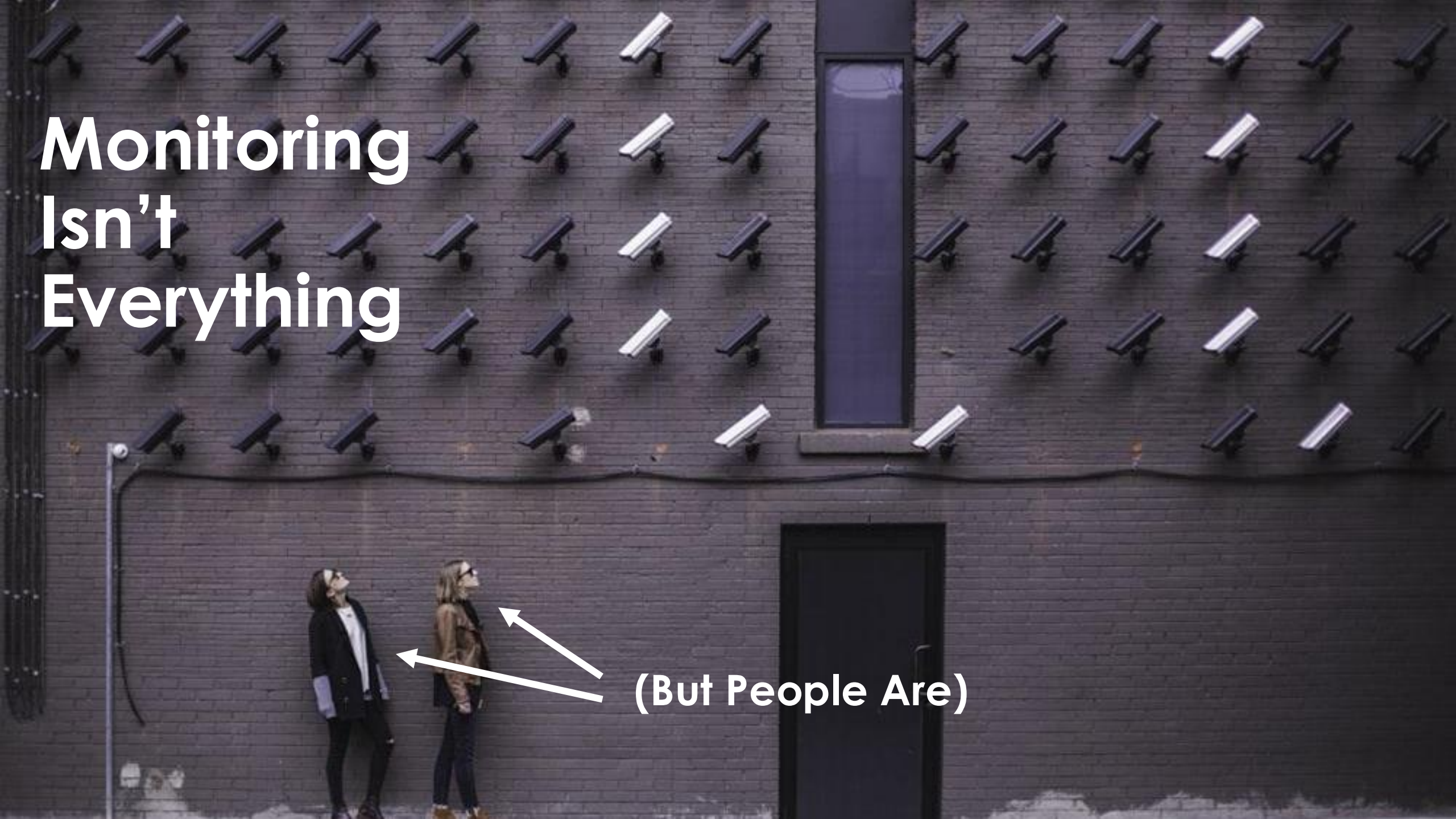
Discussion:

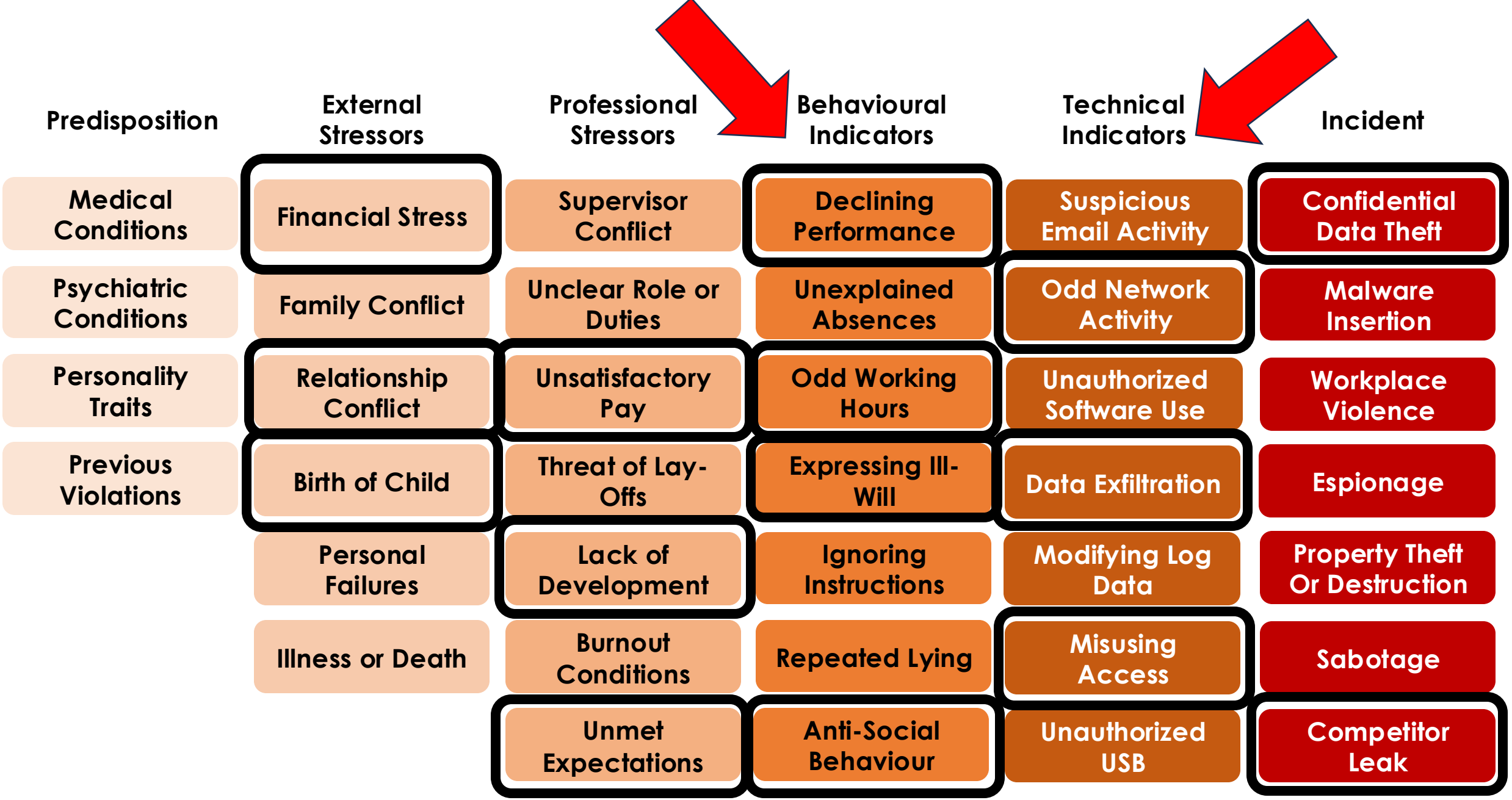
What Can We Learn From This?

Prioritize What You Can't Lose

Prepare For The Long Road


Specialist programs
Micro-segmentation, risky personas, etc.
Counter-espionage program
Data-driven approach
Learn from your data
See the organization as a whole
Monitor what you cannot control
Continuous and enhanced monitoring
Advanced: UEBA, UAM, or similar
Balance Trust & Control
Close or manage vulnerabilities
Raise awareness, build dialogue, and focus on wellness
Know your risk landscape
Cyber | Physical | Culture | Human | Third-party
Identify and protect what you can't lose
10 Year
Strategy


Monitoring
Isn't
Everything
(But People Are)


Predisposition
External Stressors
Professional Stressors
Behavioural Indicators
Technical Indicators
Incident
Medical Conditions
Psychiatric Conditions
Personality Traits
Previous Violations
Financial Stress
Family Conflict
Relationship Conflict
Birth of Child
Personal Failures
Illness or Death
Supervisor Conflict
Unclear Role or Duties
Unsatisfactory Pay
Threat of Lay-Offs
Lack of Development
Burnout Conditions
Unmet Expectations
Declining Performance
Unexplained Absences
Odd Working Hours
Expressing Ill-Will
Ignoring Instructions
Repeated Lying
Anti-Social Behaviour
Suspicious Email Activity
Odd Network Activity
Unauthorized Software Use
Data Exfiltration
Modifying Log Data
Misusing Access
Unauthorized USB
Confidential Data Theft
Malware Insertion
Workplace Violence
Espionage
Property Theft Or Destruction
Sabotage
Competitor Leak

Employee wellness is a security priority

Awareness matters

Q &A