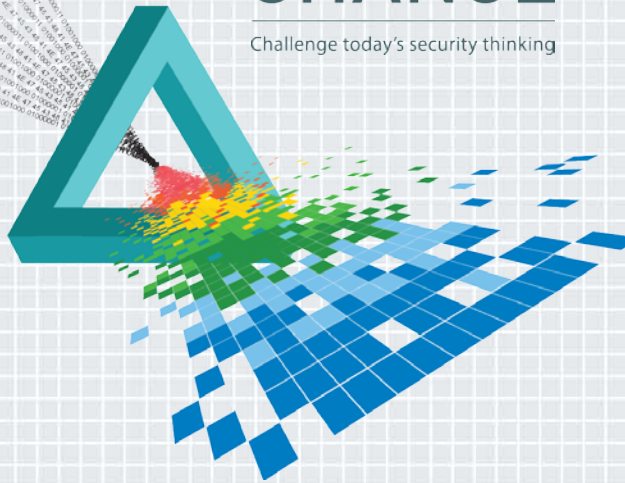
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



SESSION ID: HUM-W02

# From Bricks and Mortar to Bits and Bytes: A History and Future of Insider Threat

**Dr. Michael Gelles**
Director
Deloitte Consulting LLP

**Dr. Jesse Goldhammer**
Associate Dean for Business Development and Strategic Planning
University of California Berkeley
School of Information

# Agenda

- Common behaviors and triggers for insider events
- Evolution of the workplace and insider threats
  - Bricks and mortar workplace
  - Transitional workplace
  - Bits and bytes workplace
- Implications for today's insider programs
- Future uncertainties and their implications
- Applying this knowledge to your organization

# Defining Insider Threat

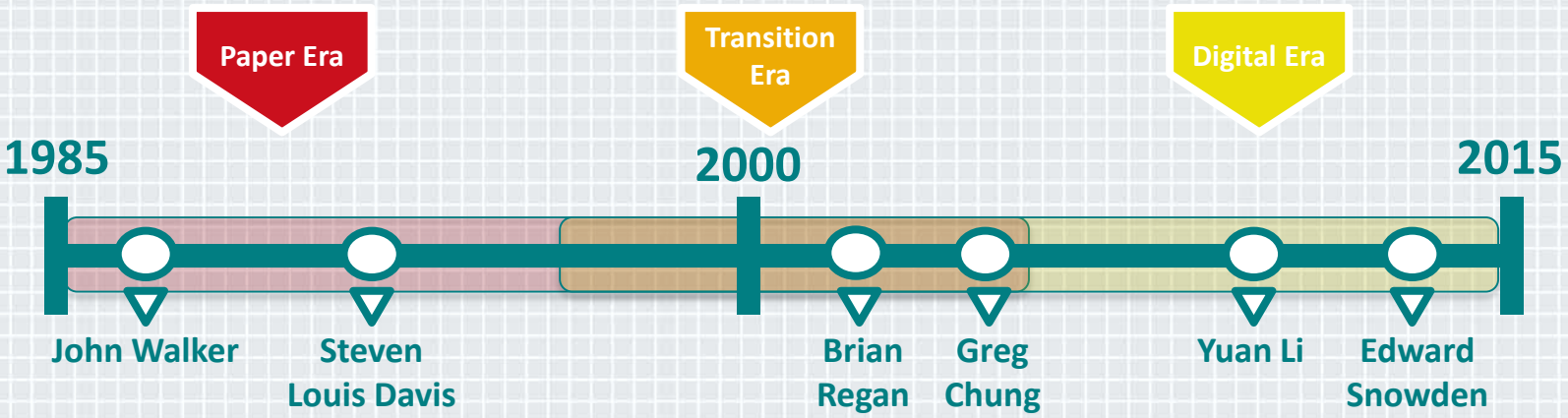
**Insider Threat:** A person who has the *potential to harm an organization for which they have inside knowledge or access*.

An insider threat *can have a negative impact on any aspect of an organization*, including employee and/or public safety, reputation, operations, finances, and mission continuity.

# Behavior is Constant…

| Characteristics of Employees at Risk |
| --- |
| Not impulsive |
| No single motive |
| History of managing crises ineffectively |
| Pattern of frustration, disappointment |
| Seeks validation |
| Aggrandized view of abilities/ achievements |
| Strong sense of entitlement |
| Views self above the rules |
| Seeks immediate gratification/validation |

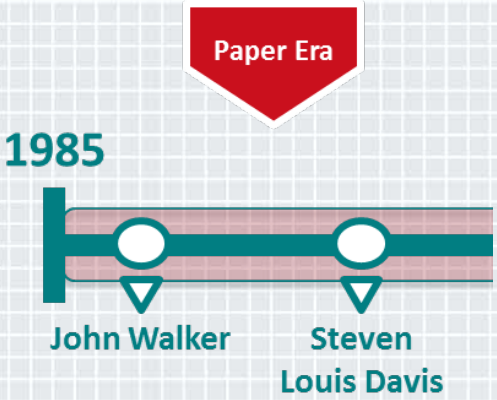
| If Needs Are Not Met, Employee Becomes… |
| --- |
| Rebellious |
| Passive aggressive |
| Destructive |
| Complacent |
| Self perceived value exceeds performance |
| Intolerant of criticism |
| Unable to assume responsibility for actions |
| Blaming of others |
| Minimizing of their mistakes or faults |




## …But Context Changes

Over the past 30 years, insiders have shifted from removing paper files to exfiltrating digital data

# The Bricks and Mortar Workplace




## Era Characteristics

- **Attributes:** Physical actions are observable, which leads to external constraints
- **Behavior:** Person-to-person handoffs of hard copy information
- **Insider Programs**: Counterintelligence focused and reactive

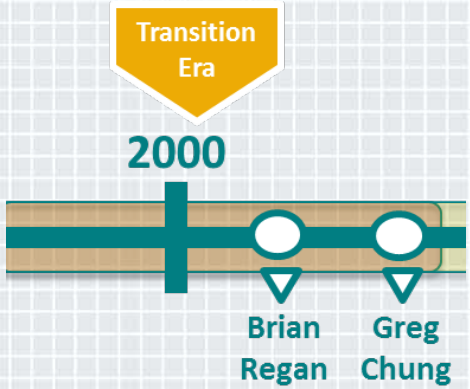
## John Walker (Navy)[1]

- **Access**: Navy Chief Warrant Officer and communications specialist
- **Rationale**: Validation; $500 - $1,000 a week
- **Exploit**: Helped the Soviet Union decipher more than one million encrypted messages

## Steven Louis Davis (Gillette)[2]

- **Access**: Lead Process Control Engineer with access to the development of a new system
- **Rationale**: Anger at supervisor; removed from position as lead developer
- **Exploit**: Sent confidential engineering drawings to several competitors

# The Transitional Workplace




## Era Characteristics

- **Attributes:** Unobservable virtual actions avoid external constraints – leaving only internal constraints
- **Behavior:** Download data using removable media
- **Insider Programs**: Use physical, behavioral, and some technology indicators

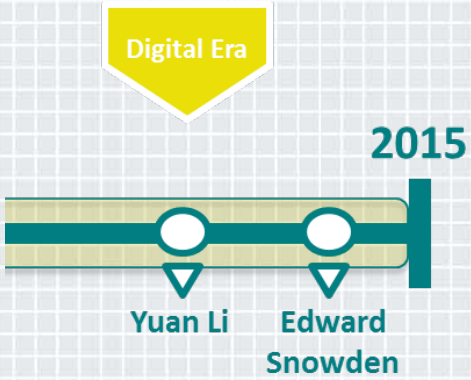
## Brian Regan (NRO)[3]

- **Access**: Signals intelligence specialist with access to Intelink
- **Rationale**: Validation; debt
- **Exploit**: Stole 15,000 pages, CD-ROMs, videos

## Greg Chung (Boeing)[4]

- **Access**: Stress analyst with a high security clearance and access to technical blueprints and designs
- **Rationale**: Allegiance; “contribute to the motherland”
- **Exploit**: Stole ‘hundreds of thousands of documents’ to bring to China under the guise of giving lectures

# The Bits and Bytes Workplace




## Era Characteristics

- **Attributes:** Tracking of virtual actions create external constraints
- **Behavior:** Machine to machine file transfer to exfiltrate data
- **Insider Programs**: Correlate virtual and non-virtual behavior

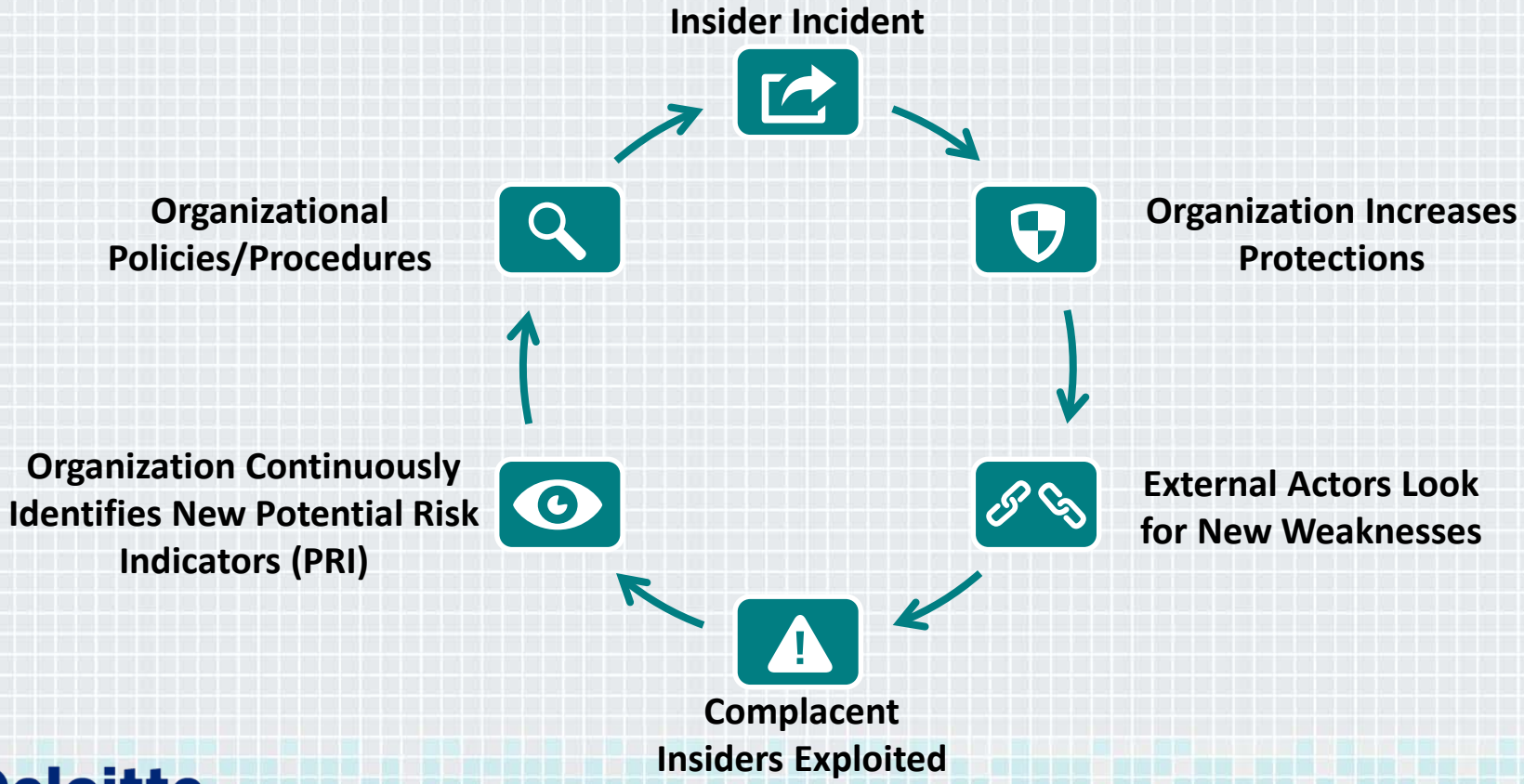
## Yuan Li (Sanofi Aventis)[5]

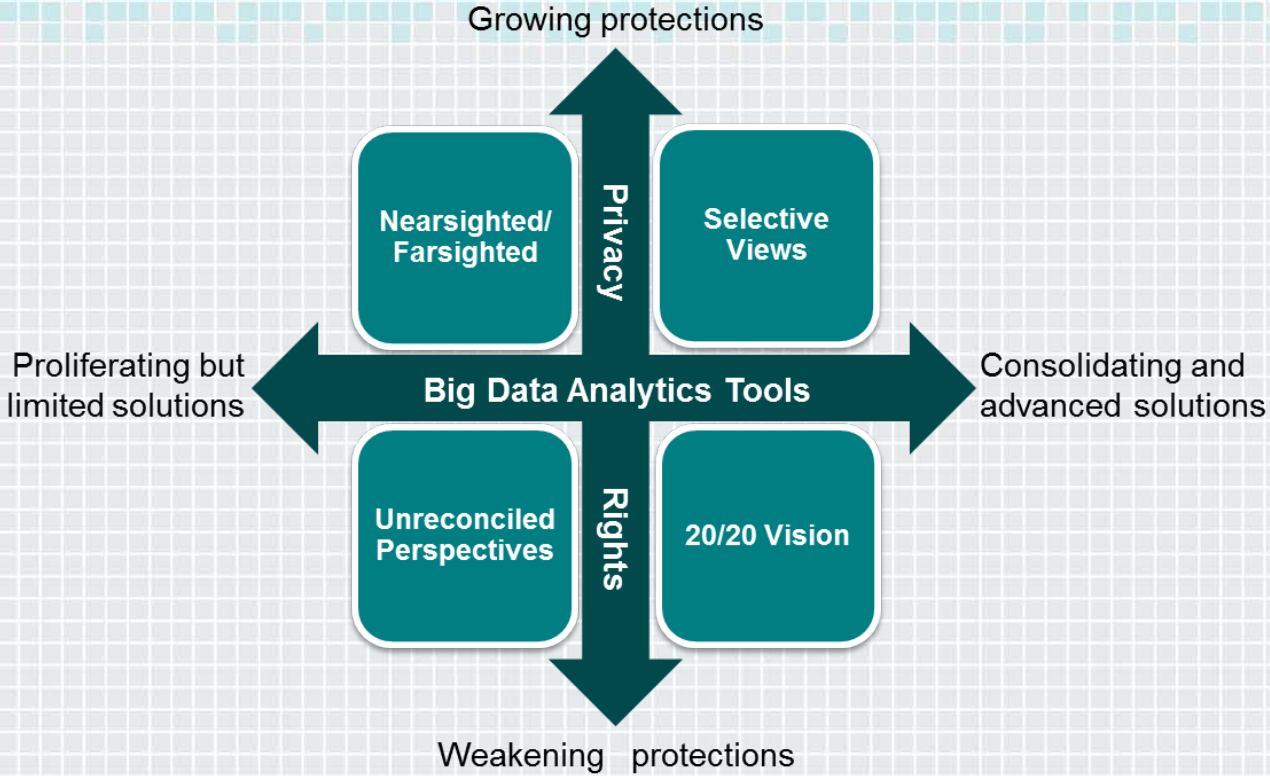
- **Access**: Research chemist with access to secret R&D work and lab test results
- **Rationale**: Greed/ allegiance; sold secrets to a Chinese chemical company she had stake in
- **Exploit**: Downloaded information to her home computer from internal databases to sell

## Edward Snowden (NSA)[6]

- **Access**: Network administrator with a high level of access to classified information
- **Rationale**: Validation; disagreement with US surveillance and privacy policies
- **Exploit**: Leaked classified information to the media, starting in May 2013

# Today's Evolving Insider Threat Program

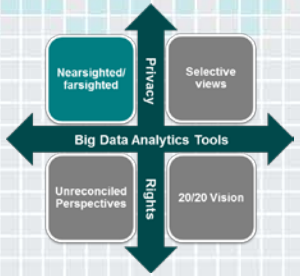





## An Uncertain Future

Changes in technology and privacy protections could alter the insider dynamic

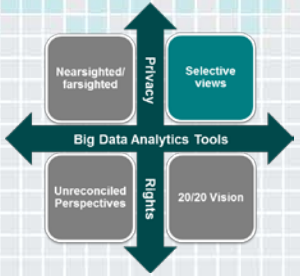
# Nearsighted/farsighted

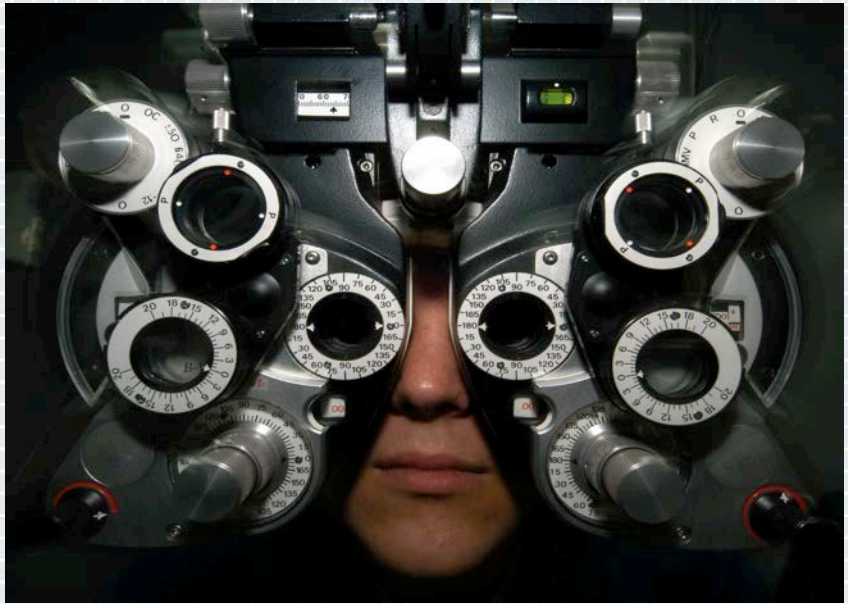



## Scenario Characteristics

- **Attributes:** Lots of data solutions, all of which are imperfect, in a privacy protected world
- **Threat:** Malicious insiders become more common and destructive while external actors actively recruit complacent insiders
- **Strategies**: Must find new ways to baseline risky behaviors and define new processes to carefully adhere to compliance guidelines

# Selective Views

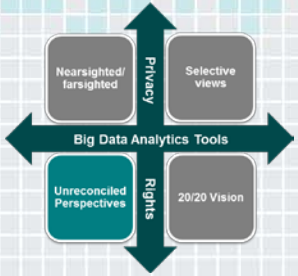


## Scenario Characteristics

- **Attributes:** Technology gets much more powerful, but is constrained by privacy protections
- **Threat:** Limited data collection creates opportunities for complacent and malicious insiders
- **Strategies:** Organizations leverage advanced technical tools to best utilize the data permitted for collection, invest in training and enhanced technical controls

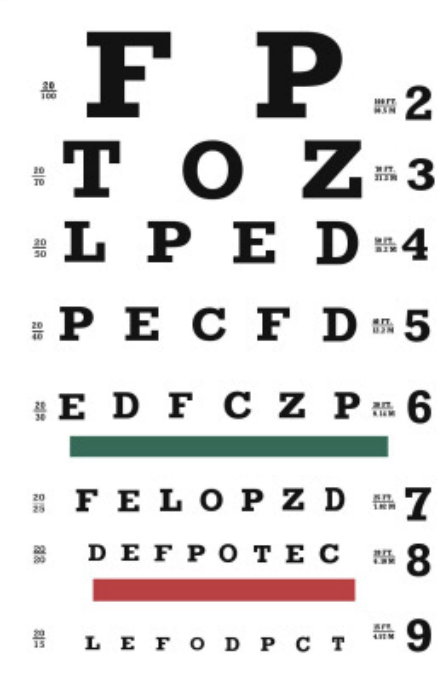
# Unreconciled Perspectives

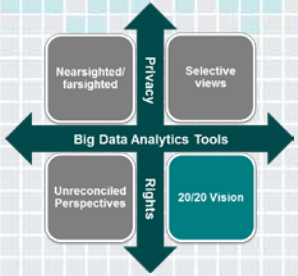




## Scenario Characteristics

- **Attributes:** Data solutions remain highly imperfect and dispersed while privacy protections diminish
- **Threat:** Malicious insiders become a more significant threat than complacent insiders who can be monitored, though ineffectually
- **Strategies**: Organizations increase investment in manpower to monitor disparate tools and training to curb complacent insiders

# 20/20 Vision




## Scenario Characteristics

- **Attributes:** Real-time insider threat mitigation capabilities become available and operate at scale
- **Threat:** Quick identification of malicious insiders shifts the focus to external actors who recruit complacent insiders
- **Strategies**: Significant insider technology investments accompanied by process changes to improve ROI

# Applying this Knowledge to Protect your Organization

- Identify your critical assets
- Determine your “risk appetite” and “risk tolerance”
- Catalog potential risk indicators in your organizational data
- Understand organization’s culture and how it can be targeted
- Continually evaluate program effectiveness to meet evolving threats

# Want More Information?


- Mike Gelles: mgelles@deloitte.com
- Jesse Goldhammer: jgoldhammer@berkeley.edu


## Sources


1) Sontag, Sherry; Drew, Christopher; Annette Lawrence Drew (1998). Blind Man's Bluff: The Untold Story of American Submarine Espionage. New York City: HarperCollins. ISBN 0-06-103004-X.
2) Tie, Robert. “Economic Espionage: How to Protect Your Clients’ Trade Secrets”. Fraud Magazine, September/October, 2008
3) "ESPIONAGE: Brian Regan Facts (DNI Briefing: SCI Today)". Special Security Office, Office of the Deputy Chief of Staff, G-2, Pentagon, July 2007.
4) Bhattacharjee, Yudhijit. “A New Kind of Spy: How China obtains American technological secrets”. The New Yorker Magazine, May 5, 2014.
5) Defense Security Service Counterintelligence Directorate. “Administration Strategy on Mitigating the Theft of U.S. Trade Secrets”. Web. February 2013.
6) Cole, Matthew; Brunker, Mike. "Edward Snowden: A Timeline". NBC News, May 26, 2014.