



# Same Threat, Different Day: Minimizing Insider Threats and Risks

*(Or, why hope is **NOT** a strategy!)*

# Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0627

# The National Insider Threat Center



Center of insider threat expertise

Began working in this area in 2001 with the U.S. Secret Service

Mission: enable effective insider threat mitigation, incident management practices, and develop capabilities for deterring, detecting, and responding to evolving cyber threats

Action and Value: conduct research, modeling, analysis, and outreach to develop & transition socio-technical solutions to combat insider threats

# About Insider Threat

There is not one “type” of insider threat

Threat is to an organization’s critical assets

- People
- Information
- Technology
- Facilities

Based on the motive(s) of the insider

Impact is to Confidentiality, Availability, Integrity

Cyber attack = Cyber Impact

Kinetic attack = Kinetic Impact

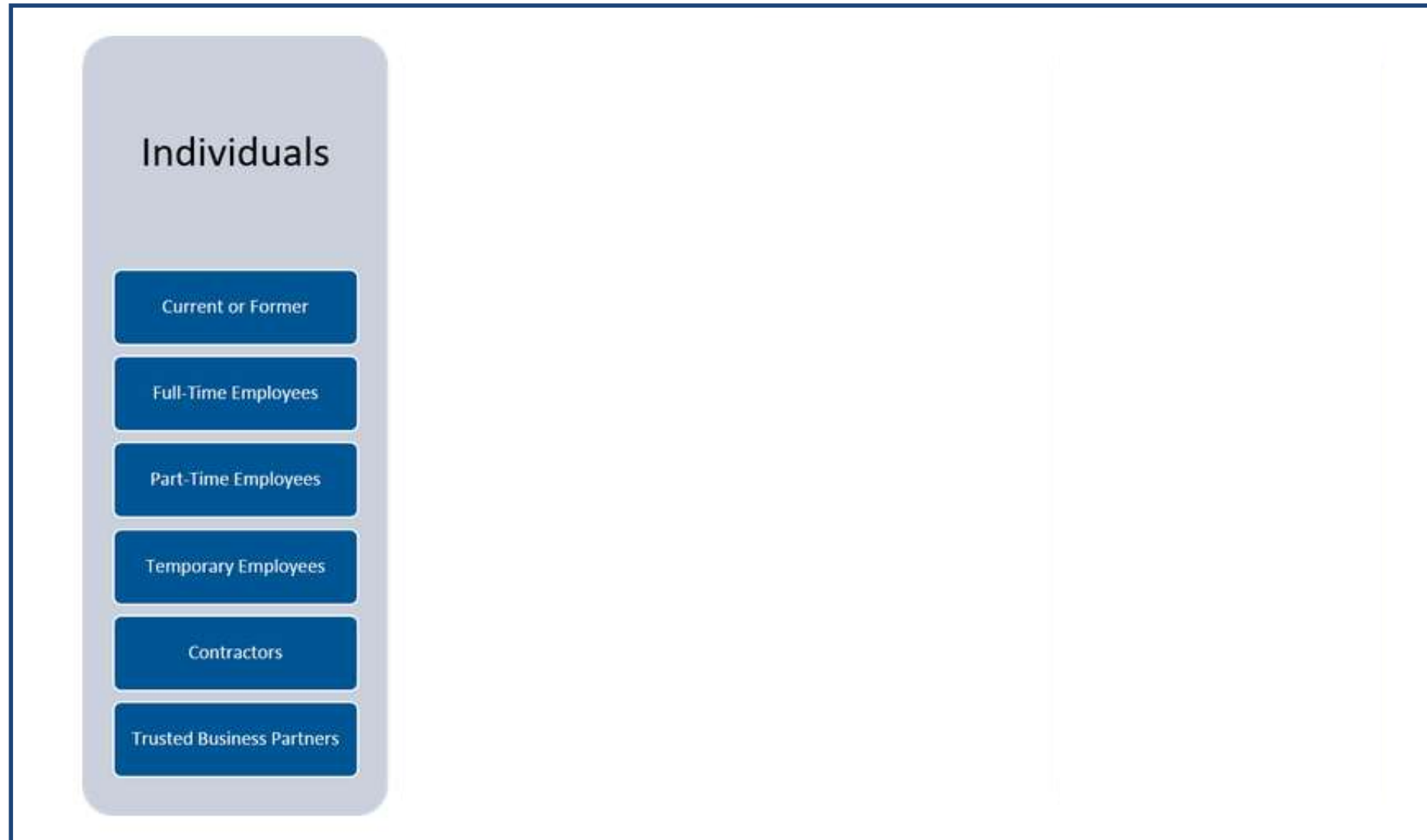
Cyber attack = Kinetic Impact

Kinetic attack = Cyber Impact

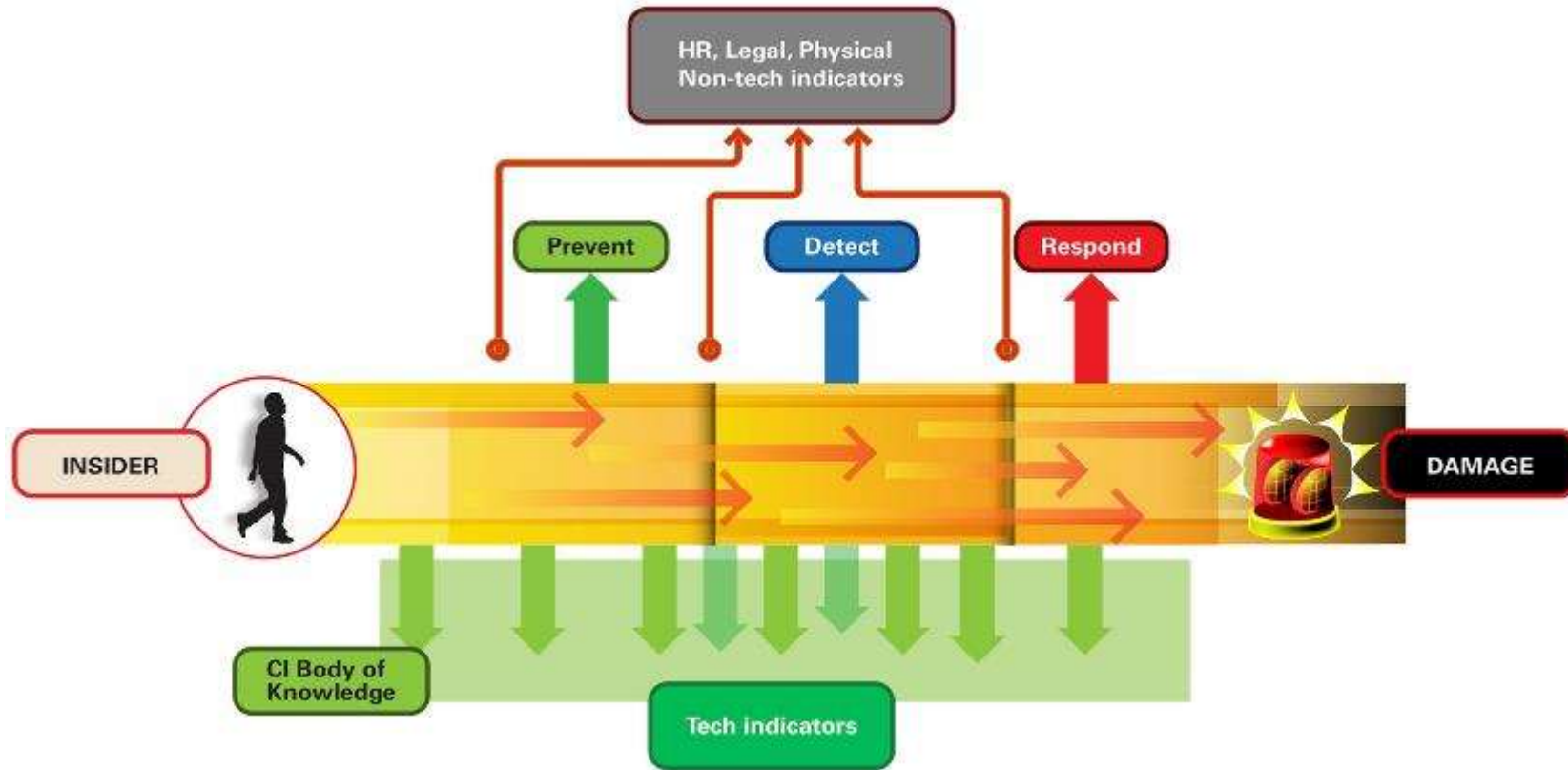
# What / Who is an Insider Threat?

The potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

# What / Who is an Insider Threat?



# Goal for an Insider Threat Program



*Opportunities for prevention, detection, and response for an insider incident*

# Types of Malicious Insider Incidents

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

# Types of Insider Activities - 1

## Insider IT Sabotage

An insider's use of IT to direct specific harm at an organization or an individual

- Deletion of information
- Bringing down systems
- Website defacement to embarrass organization

## Insider Theft of Intellectual Property

An insider's use of IT to steal intellectual property from the organization

- Proprietary engineering designs, scientific formulas, etc.
- Proprietary source code
- Confidential customer information
- Industrial Espionage and Trade Secrets

# Types of Insider Activities - 2

## Insider Fraud

An insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or theft of information which leads to fraud

- Payroll
- Reimbursement
- Unauthorized acquisitions

Theft and sale of confidential information

- SSN, PII, etc.
- Credit card numbers

Modification of critical data for a fee

- Driver's license records
- Criminal records
- Qualification for welfare, etc.

## Unintentional Insider Threat (UIT)

An insider whose actions or lack of action without malicious intent causes harm or the possibility of harm

# Types of Insider Activities - 3

## Insider National Security Espionage

- The act of communicating, delivering or transmitting information pertaining to the national defense of the United States to any foreign government or faction, with intent or reason to believe that is to be used to the injury of the United States or to the advantage of a foreign nation
  - Volunteers
  - Recruited in Place
  - Dispatched

## Insider Miscellaneous

- Unauthorized disclosure (information insider believed should be in the public domain)
- Providing address of a person to an acquaintance who physically harmed the individual
- Accessing records of high-profile individuals

# Types of Insider Activities - 4

## UIT - Four Categories:

**DISC** - accidental disclosure (e.g., via the Internet)

- sensitive information posted publicly on a website, mishandled, or sent to the wrong party via email, fax, or mail

**PHISHING/SOCIAL** - malicious code (UIT-HACKing, malware/spyware)

- an outsider's electronic entry acquired through social engineering (e.g., phishing email attack, planted or unauthorized USB drive) and carried out via software, such as malware and spyware

**PHYS** - improper/accidental disposal of physical records

- lost, discarded, or stolen non-electronic records, such as paper documents

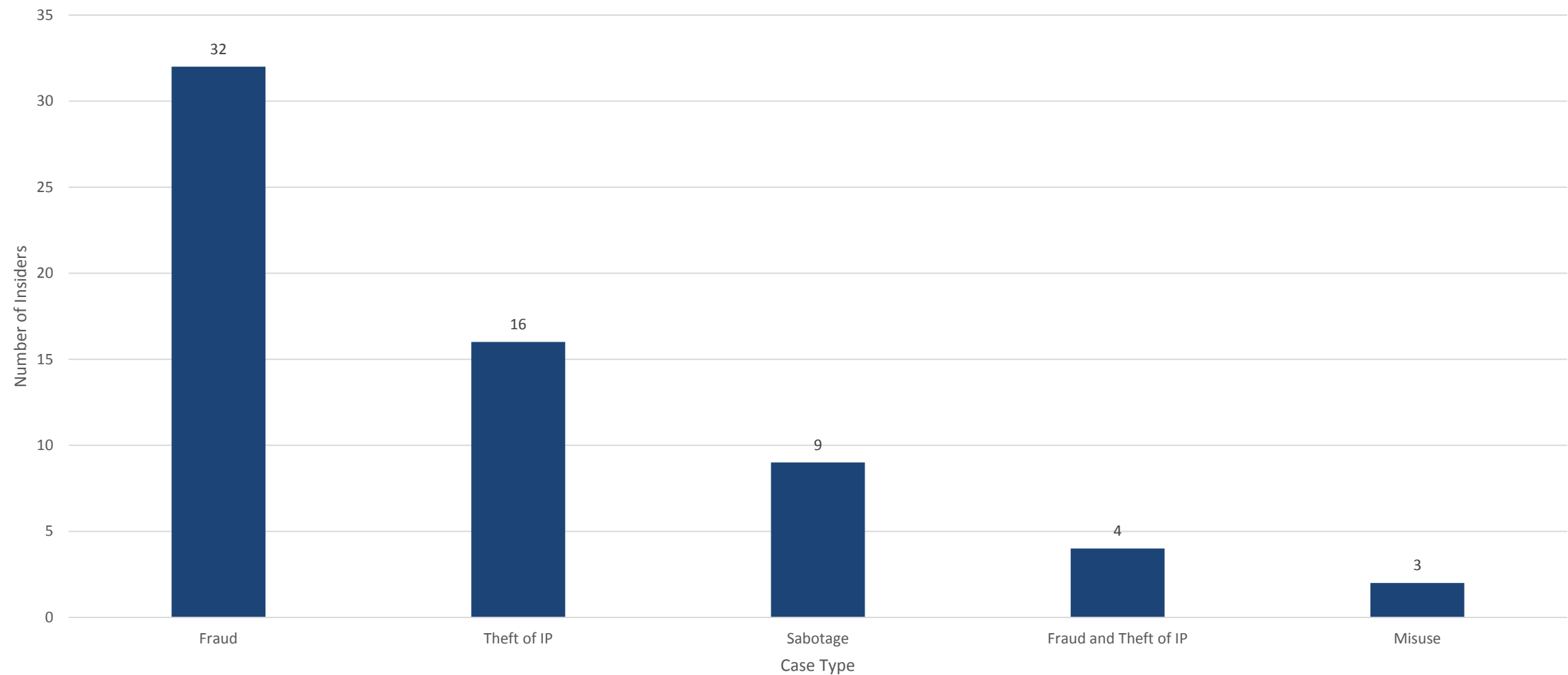
**PORT** - portable equipment no longer in possession

- lost, discarded, or stolen data storage device, such as a laptop, PDA, smart phone, portable memory device, CD, hard drive, or data tape

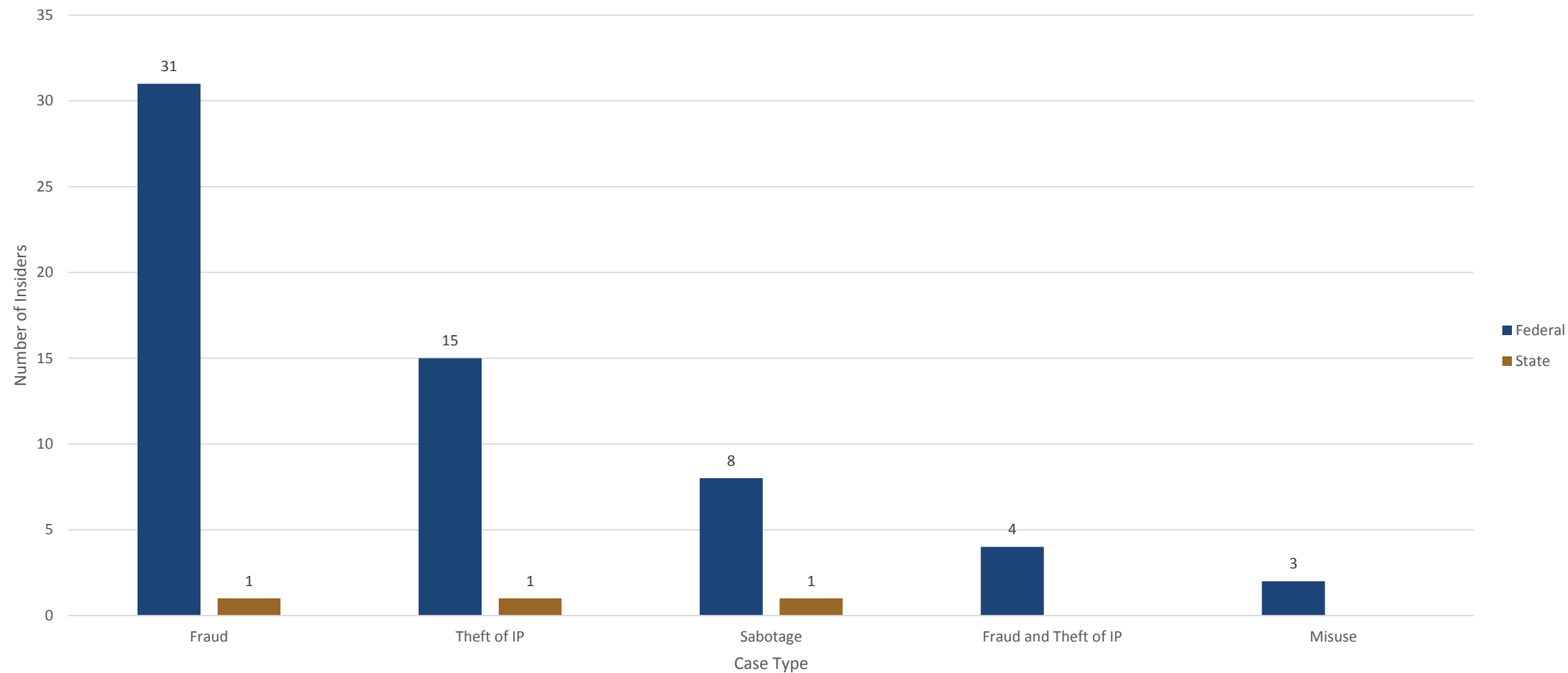
# Are There NYC Incidents?

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

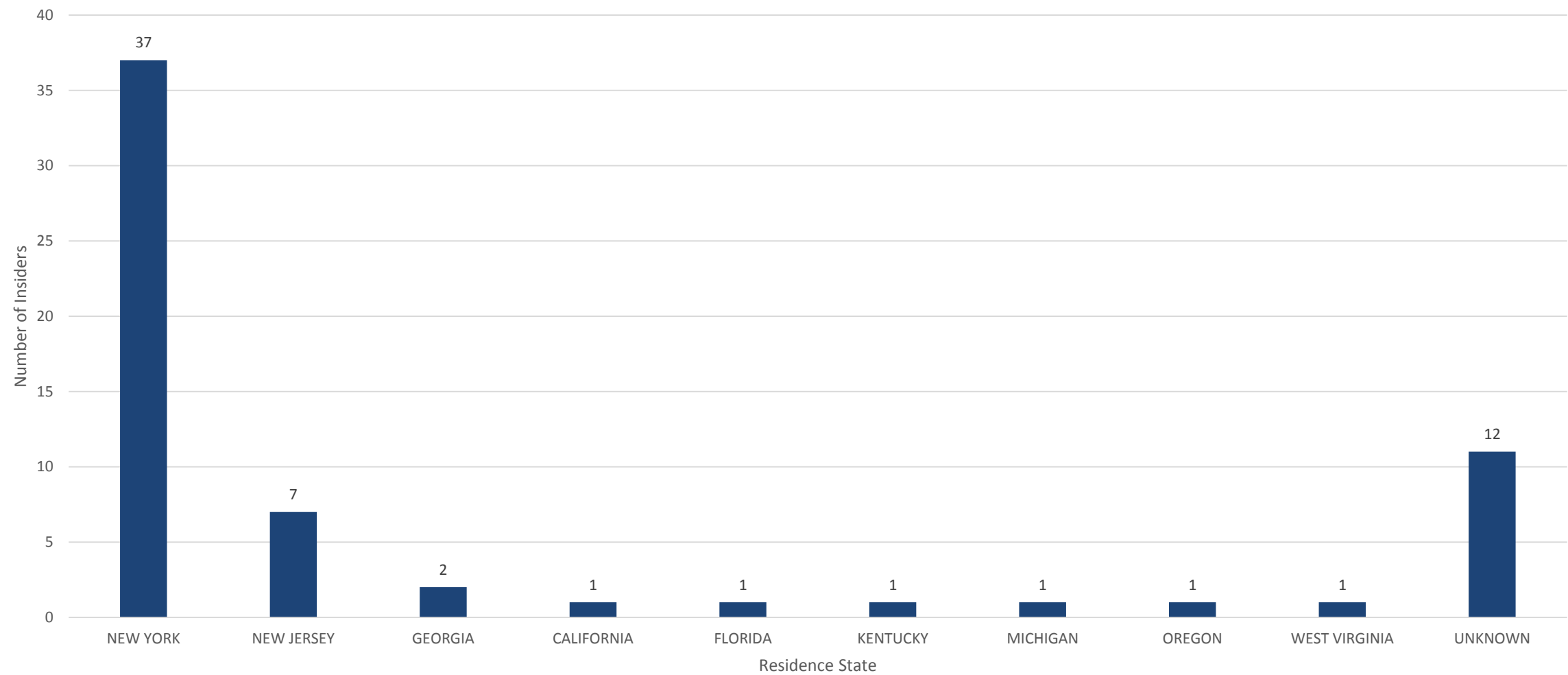
# Case Type



# Case Type by Level of Prosecution



# New York Incidents by Insider Residence



# Fraud

A DMV supervisor colludes with outsiders and other insiders to create fraudulent identification cards for profit with disregard for the impact to public safety.

The insider was a DMV supervisor that was part of a 7-person identity theft ring.  
The insider was paid by an outsider whom was the mastermind of the scheme.  
The outsider would receive requests from other outsiders.

When a request was received, the ring leader obtained stolen identities for customers and would provide a SSN to a DMV employee at another office. This employee would verify that the SSN could be used in the system.

Once approved, the ring leader would provide the customer with an identification package that included birth certificates, social security cards, pay stubs and bank cards to be used to obtain a DMV document.

The ring leader would then direct the customer to the insider's DMV office where they were a supervisor and could process the applications.

The scheme successfully sold more than 200 driver's licenses, learner's permits and ID cards for \$7,000 to \$10,000 each and made more than \$1,000,000 total.

The DMV has since taken steps to eliminate the gap in procedures that allowed the incident to continue.

The individuals that bought the fake identification included:

- A convicted sex offender,
- A criminal featured on "America's Most Wanted"
- An individual with drug and firearm convictions
- A convicted felon with two DUI convictions
- An undercover agent who claimed to be on the "no-fly" list

# Theft of IP

After leaving to work for a competitor, a former employee gains unauthorized access to their former supervisor's email account to exfiltrate IP.

The insider was a former employee of a financial services firm.

The insider had already moved on to a management position at a competitor during the time of the attack.

The insider compromised the email account of a former co-worker (supervisor) to send intellectual property (documents, business plans, presentations).

The targeted former co-worker never gave the insider access to this email account or password.

The insider sent these files to their new email account at their new employer, but there is no evidence that suggests that the insider's new employer was aware of the theft of intellectual property.

The former co-worker whose account the insider compromised received a message saying that an email failed to send - but the co-worker never sent such a message, which revealed their account was compromised.

The insider's involvement was confirmed using internet service provider (ISP) logs.

# IT Sabotage

A recently terminated field technician used the home computer of an unwitting coworker to delete critical data.

The insider was employed as a field technician by the victim organization, a computer consulting firm.

The insider's employment was terminated by the organization.

The insider would later claim the organization failed to reimburse them for equipment they had returned, which may have been the motivation for the attack.

On the evening of the insider's termination, the insider used a co-worker's home computer to remotely access the organization's network outside of working hours.

The insider used their former colleagues' usernames and passwords to attack the organization's network.

The insider wiped out files and data for several of the victim organization's most important clients, making the network inaccessible for days and causing some customers to permanently lose data.

The co-worker, unaware that the insider had used their computer to sabotage the network, reported the crime after the insider admitted that they had attacked the network.

The insider was ordered to pay approximately \$120,000 in restitution and sentenced to 1 year of imprisonment followed by 3 years of supervised release.



Common Sense Guide, Sixth Edition

# A Mitigation Strategy

# CSG, Sixth Edition

- Incorporates updated information based on analysis of ~2,500 insider threat incidents
- Provides new information on how GDPR might affect some of the BPs
- New Aspects of workplace violence and aggression tips added to BPs
- Key [research publication](#) was used to derive a new best practice (*The Critical Role of Positive Incentives for Reducing Insider Threat, Moore, et al.*)
- New mappings to other standards

# CSG, Sixth Edition – A New BP

	Best Practice	Best Practice Number from Version 5
1	Know and protect your critical assets.	1
2	Develop a formalized insider threat program.	2
3	Clearly document and consistently enforce policies and controls.	3
4	Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	4
5	Anticipate and manage negative issues in the work environment.	5
6	Consider threats from insiders and business partners in enterprise-wide risk assessments.	6
7	Be especially vigilant regarding social media.	7
8	Structure management and tasks to minimize insider stress and mistakes.	8
9	Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.	9
10	Implement strict password and account management policies and practices.	10
11	Institute stringent access controls and monitoring policies on privileged users.	11
12	Deploy solutions for monitoring employee actions and correlating information from multiple data sources.	12
13	Monitor and control remote access from all end points, including mobile devices.	13
14	Establish a baseline of normal behavior for both networks and employees.	14
15	Enforce separation of duties and least privilege.	15
16	Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.	16
17	Institutionalize system change controls.	17
18	Implement secure backup and recovery processes.	18
19	Close the doors to unauthorized data exfiltration.	19
20	Develop a comprehensive employee termination procedure.	20
21	Adopt positive incentives to align the workforce with the organization.	–

# A New Best Practice – BP 21

HR	Legal	Physical Security	Data Owners	IT	Software Engineering
✓	✓	✓	✓	✓	✓

## Best Practice: Adopt positive incentives to align workforce with organization.

Attracting employees to act in the interests of the organization through positive incentives reduces the baseline insider threat risk. Positive incentives that align the workforce values and attitudes with the organization’s objectives form a foundation on which traditional security practices that rely on forcing functions can be built to improve the effectiveness and efficiency of the insider threat defense.

This practice is related to Practice 5, “Anticipate and manage negative issues in the work environment,” and Practice 8, “Structure management and tasks to minimize insider stress and mistakes.” The difference is that this practice focuses on the use of positive incentives to improve employee attitudes independent of whether a specific negative issue or insider stress exists or is even identifiable. The detection of negative work issues or insider stress is not necessary in order to gain value by adopting positive incentives to reduce insider incident frequency.

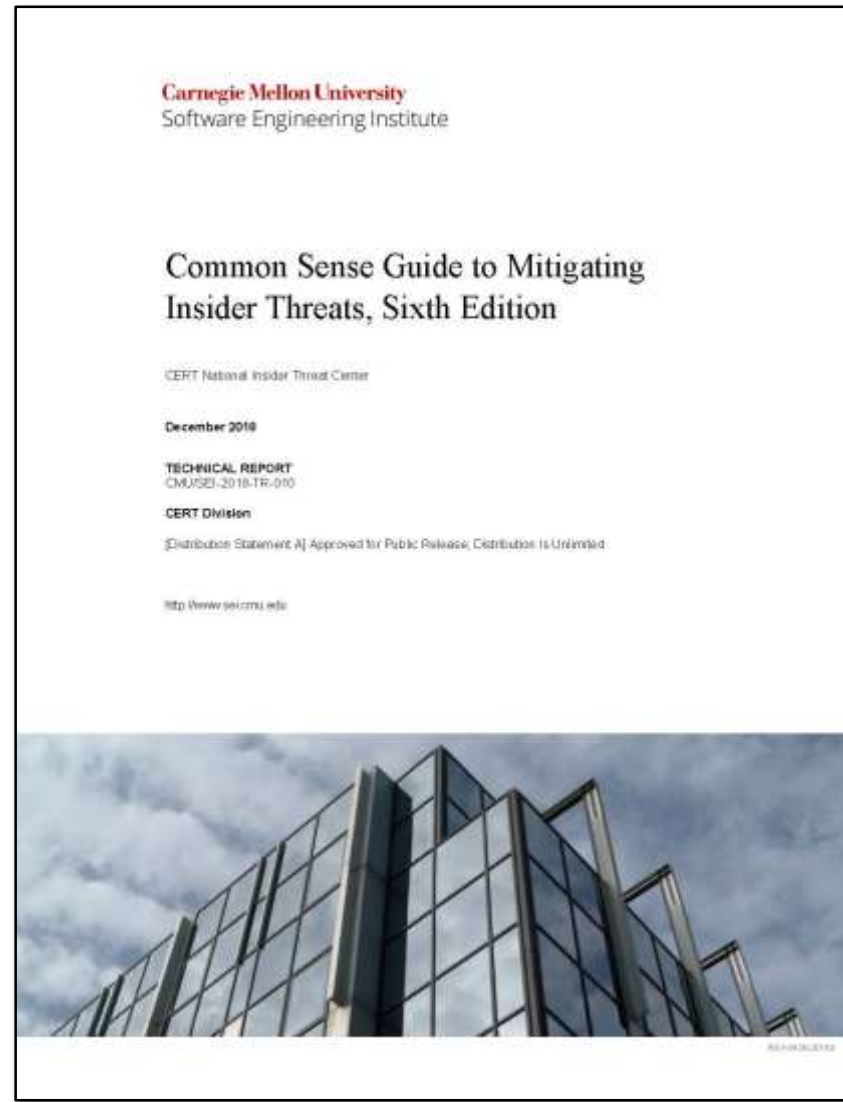
### 1. Protective Measures

Insider threat is unique in the realm of cybersecurity defense in that the potential threat agents—the

# CSG, Sixth Edition - Mappings

Best Practice	NIST 800-53 Rev. 4	National InT Policy & Min. Standards	NITTF InTP Maturity Framework	GDPR	CERT-RMM	ISO 27002	NIST CSF	CIS v7
1 - Know and protect your assets.	CP-2 CM-2 CM-8 PM-5 PM-8 RA-2	P-B-2 MS-G-1-b MS-G-1-c	ME8 ME11	Article 9 Article 32 Article 35	Asset Definition and Management Enterprise Focus	7.1.1 Inventory of Assets	ID.AM 1-6 ID.RA 1-6 ID.RM 1-3 PR.DS 1-7 PR.MA 1-2	Control 1 Control 2

# Common Sense Guide, Sixth Edition



***CERT's Common Sense Guide to Mitigating Insider Threats, Sixth Edition*** <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=540644>



Spring 2019 OSIT In-Person Meeting Updates

# Questions?

# Contact Information

## **CERT National Insider Threat Center**

Website: <http://www.cert.org/insider-threat/>

Blog: <http://www.cert.org/blogs/insider-threat/>

Email: [insider-threat-feedback@cert.org](mailto:insider-threat-feedback@cert.org)

## **Contact**

Michael Theis

Chief Engineer, Strategic Engagements

CERT National Insider Threat Center

Email: [mctheis@cert.org](mailto:mctheis@cert.org)