



# Malicious Insiders by Motive, Collusion, Recruitment, and Disgruntlement

Insights into the CERT National Insider Threat  
Center Incident Corpus

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

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.

DM19-0493

# A Note about the Cases

The statistics and figures represented in the remaining slides are limited to:

- Domestic incidents with publicly available information that were not dismissed or otherwise settled out of court
  - These incidents primarily took place in federal criminal courts
- Malicious insiders
- Cases identified as Fraud, Sabotage, Theft of IP, or Misuse

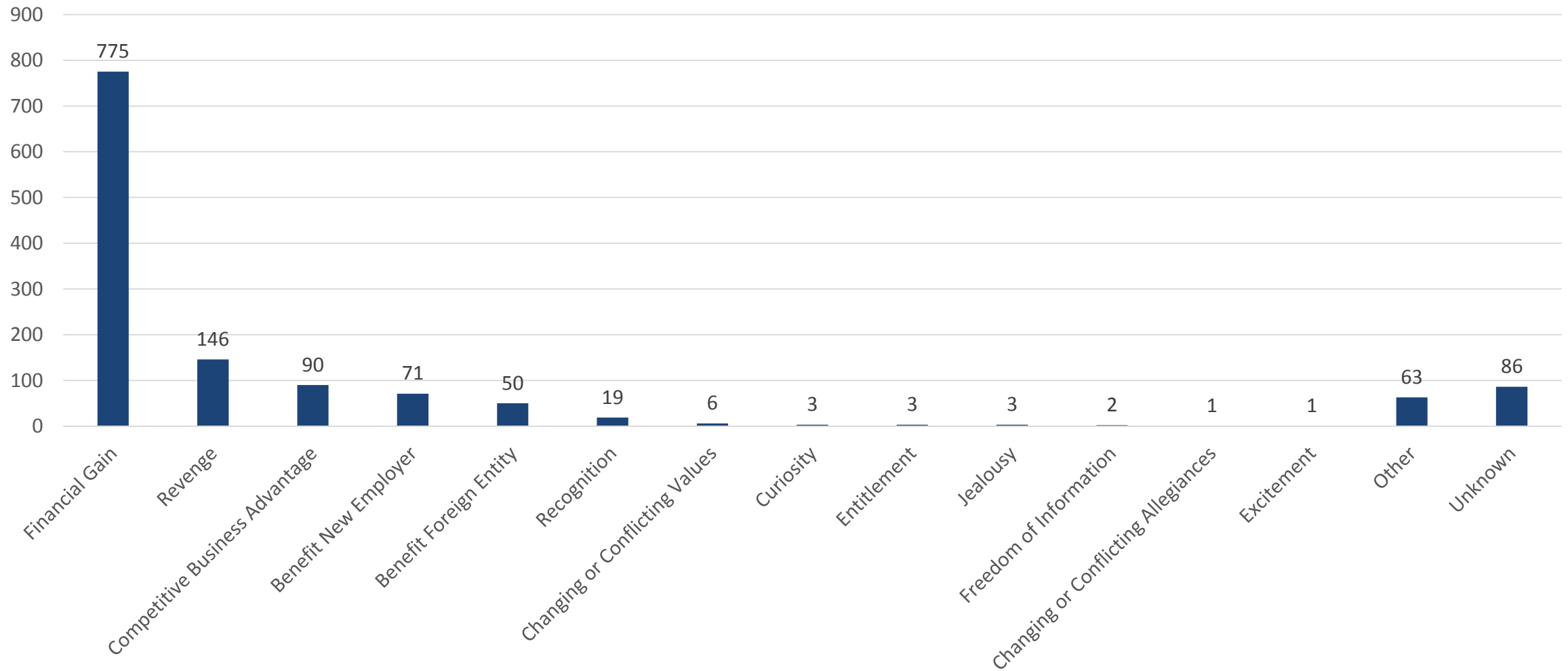
The categories of information are not intended to be exhausted of what is documented in the CERT Insider Threat Incident Corpus, but provide a sample of information.

# Objectives

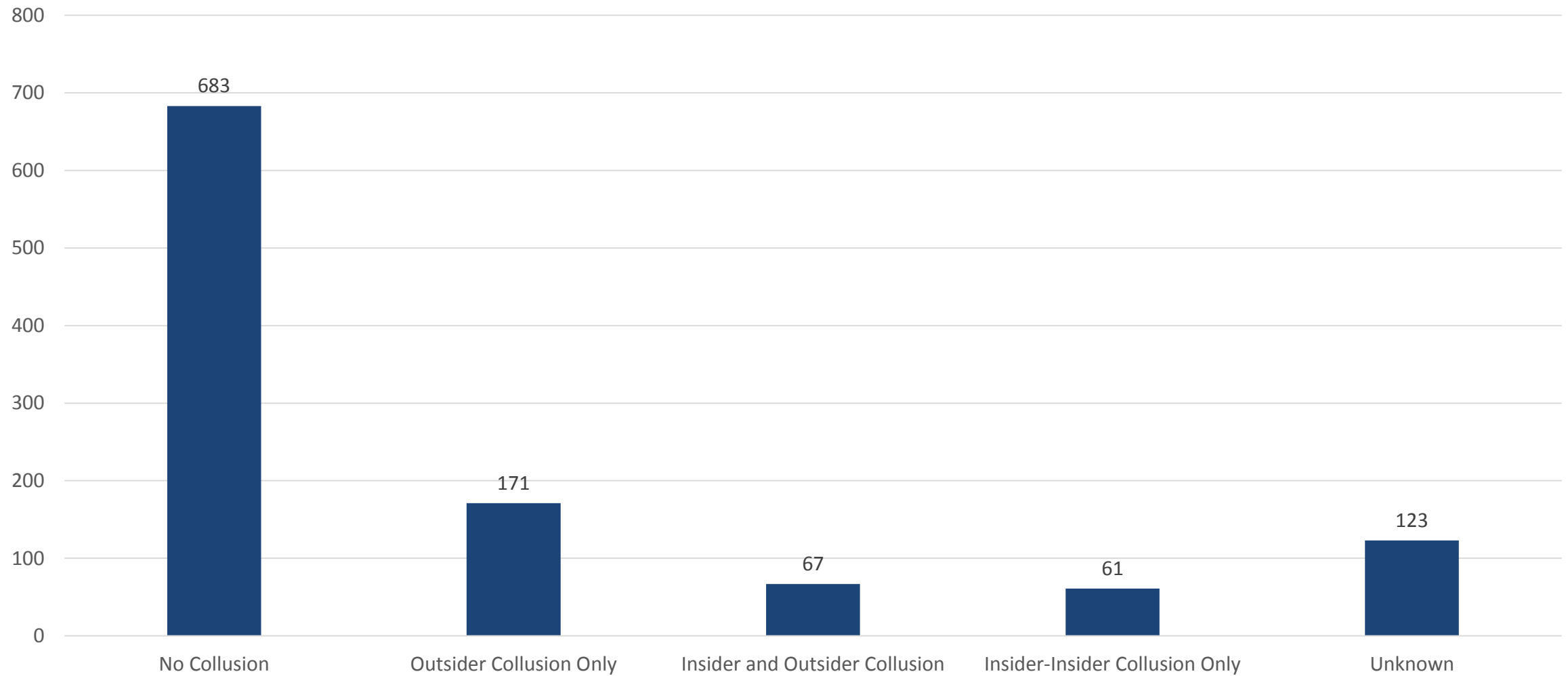
The information in the following slides will address the following information:

- **Why** did the insider commit a hostile act?
  - Motive
- **How** did the insider commit these hostile acts?
  - Recruitment
  - Collusion

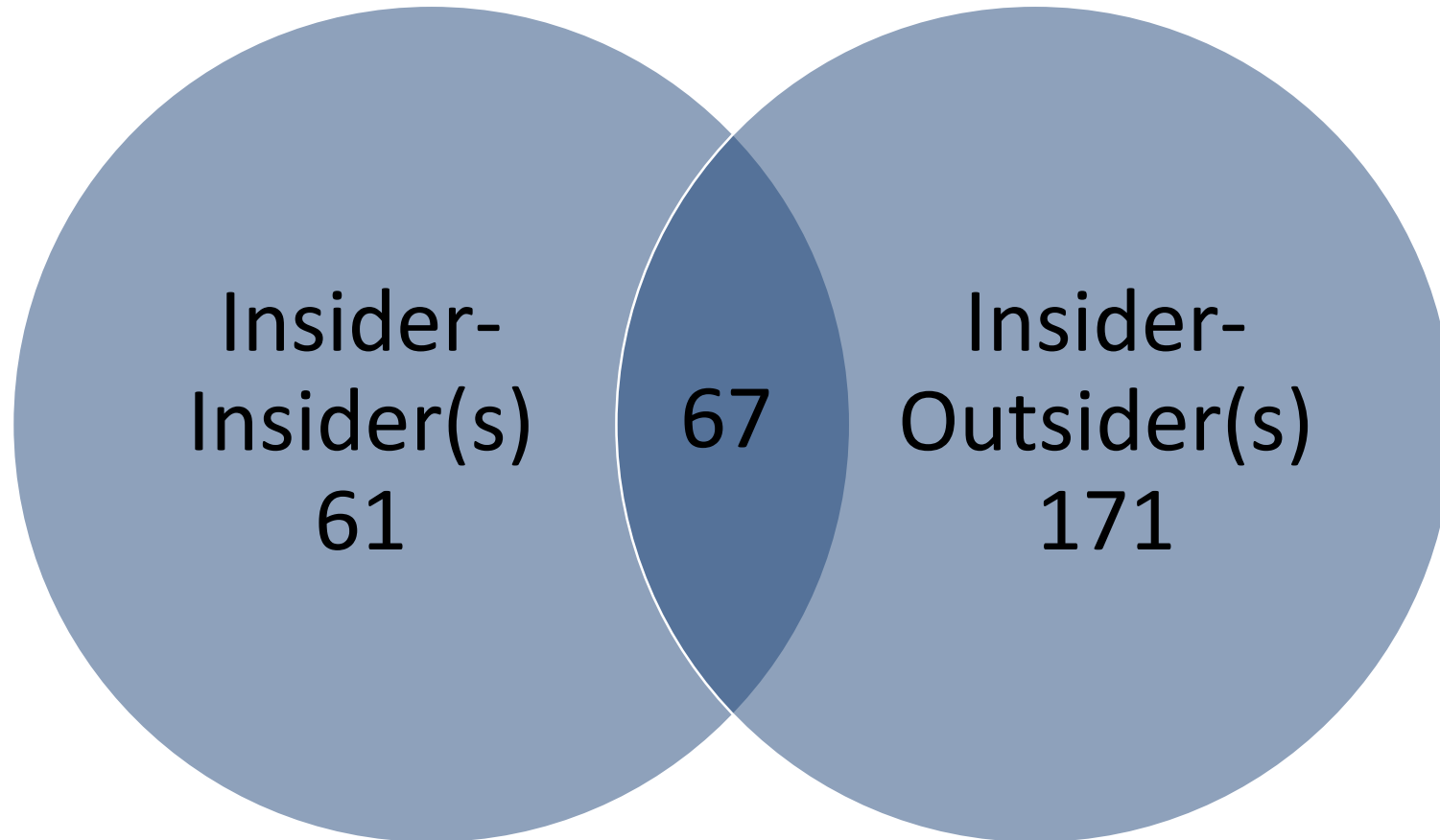
# Motive



# Collusion



# Aggregated Collusion



- 128 insiders (11.5%) colluded with one or more other insiders
- 238 insiders (21.3%) colluded with one or more outsiders
- 67 insiders (6.0%) colluded with both at least one other insider and one outsider

# Other Statistics

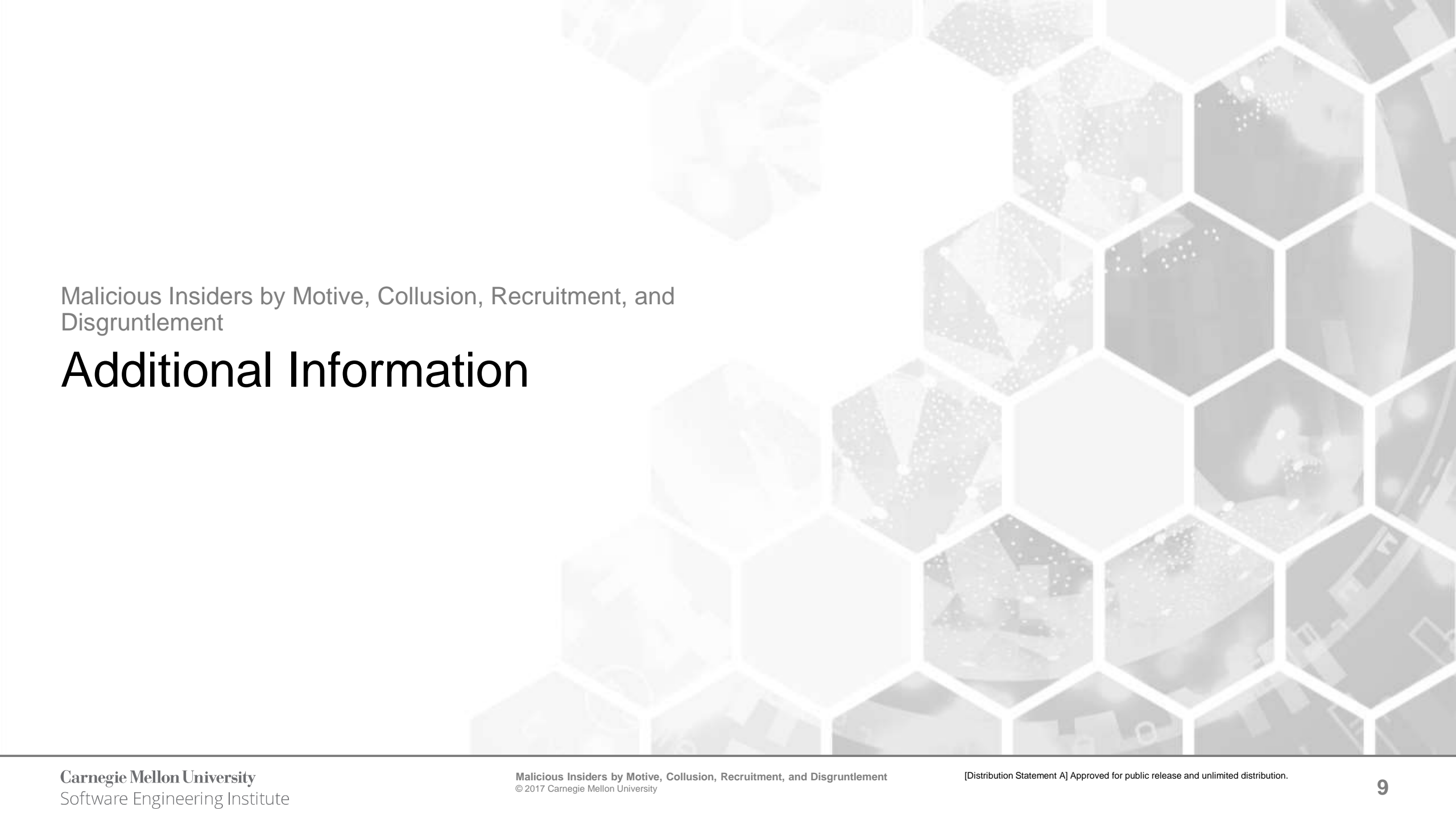
## Recruitment

- 157 insiders (14.0%) were recruited or induced by outsiders
- 29 insiders (2.4%) were recruited or induced by competitors

## Disgruntled

- 51 insiders (4.6%) showed signs of being disgruntled
- 34 of these disgruntled insiders (66.7%) committed IT Sabotage



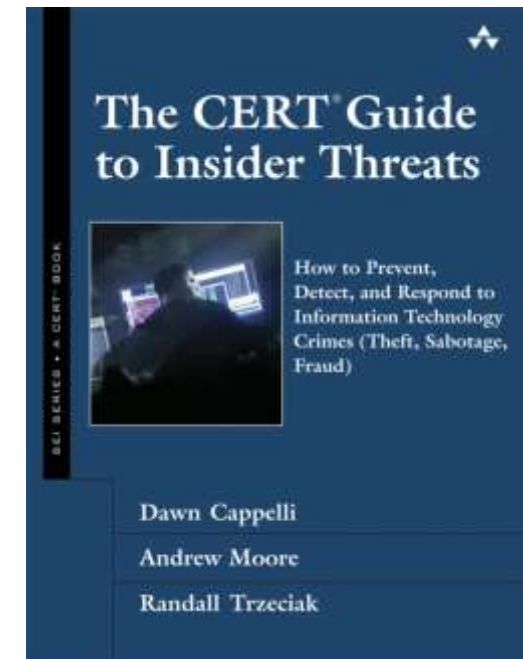


Malicious Insiders by Motive, Collusion, Recruitment, and  
Disgruntlement

# Additional Information

# NITC Publications and References

- Theis, M. C., Trzeciak, R. F., Costa, D. L., Moore, A. P., Miller, S., Cassidy, T., & (2019) Claycomb, W. R. [Common Sense Guide to Mitigating Insider Threats \(6th Ed.\)](#). Pittsburgh: Software Engineering Institute.
- Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). [The CERT® Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes \(Theft, Sabotage, Fraud\)](#). Addison-Wesley Professional.
- Moore, Andrew; Savinda, Jeff; Monaco, Elizabeth; Moyes, Jamie; Rousseau, Denise; Perl, Samuel; Cowley, Jennifer; Collins, Matthew; Cassidy, Tracy; VanHoudnos, Nathan; Buttles-Valdez, Palma; Bauer, Daniel; & Parshall, Allison. [The Critical Role of Positive Incentives for Reducing Insider Threats](#). CMU/SEI-2016-TR-014. Software Engineering Institute, Carnegie Mellon University. 2016.



# Blog Posts with Details on Motive or Collusion

- [Insiders and their Significant Others: Collusion, Motive, and Concealment](#)
- [Handling Threats from Disgruntled Employees](#)
- [The Frequency and Impact of Insider Collusion](#)
- [Insider Threats in the Federal Government](#)
- [Insider Threats in Finance and Insurance](#)
- [Insider Threats in State and Local Government](#)
- [Insider Threats in Information Technology](#)
- [Insider Threats in Healthcare](#)
- [Insider Threats in Entertainment](#)

# For More Information on Insider Threat

National Insider Threat Center

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

National Insider Threat Center Email

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

Insider Threat Blog

<http://insights.sei.cmu.edu/insider-threat/>

SEI Digital Library

<https://resources.sei.cmu.edu/library/>

# Contact Information

Sarah Miller

Insider Threat Researcher

CERT National Insider Threat Center

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

Software Engineering Institute

Carnegie Mellon University

4500 Fifth Avenue

Pittsburgh, PA 15213-3890

