CERT© Insider Threat Incident Corpus Case Study – Parent & Subsidiary Organizations

April 2020

Nick Miller

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

DM20-0342

Overview

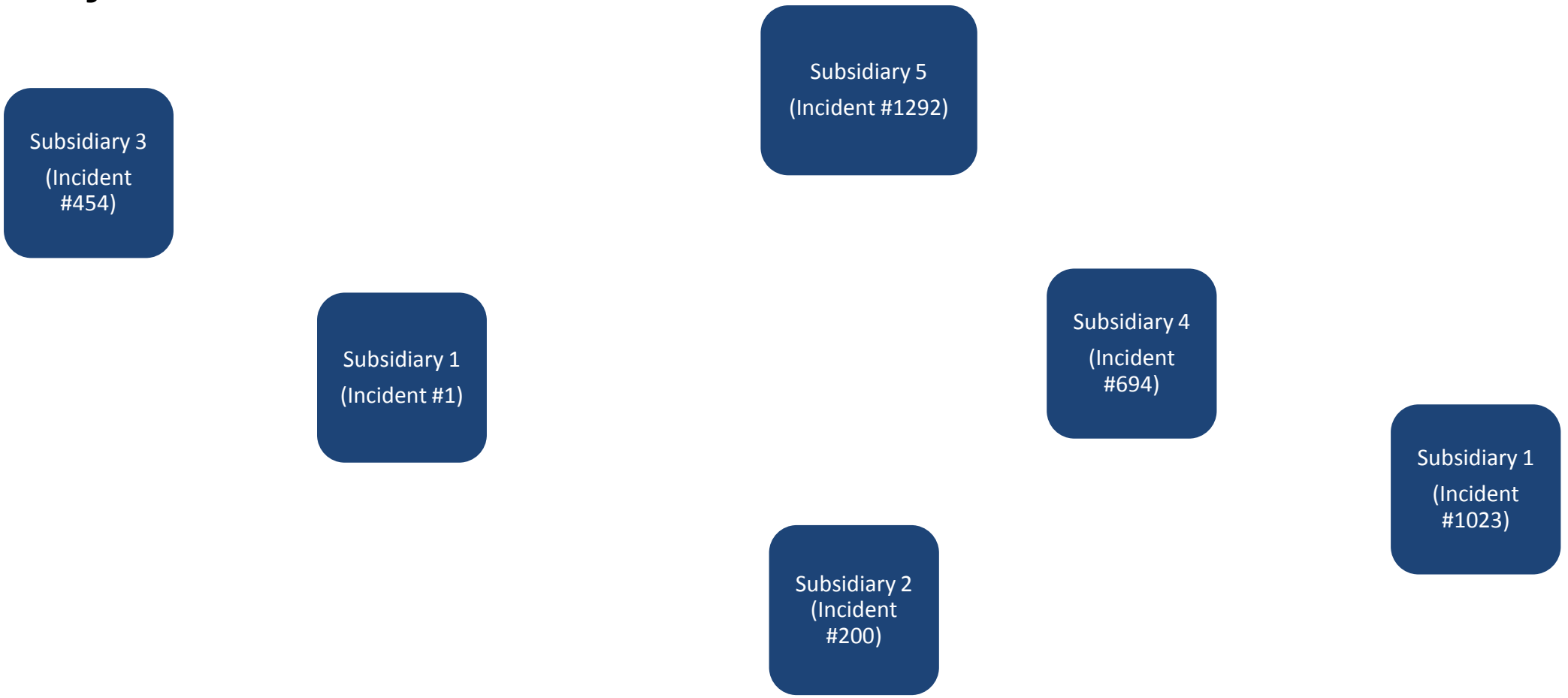
Project Basis

Summary Statistics

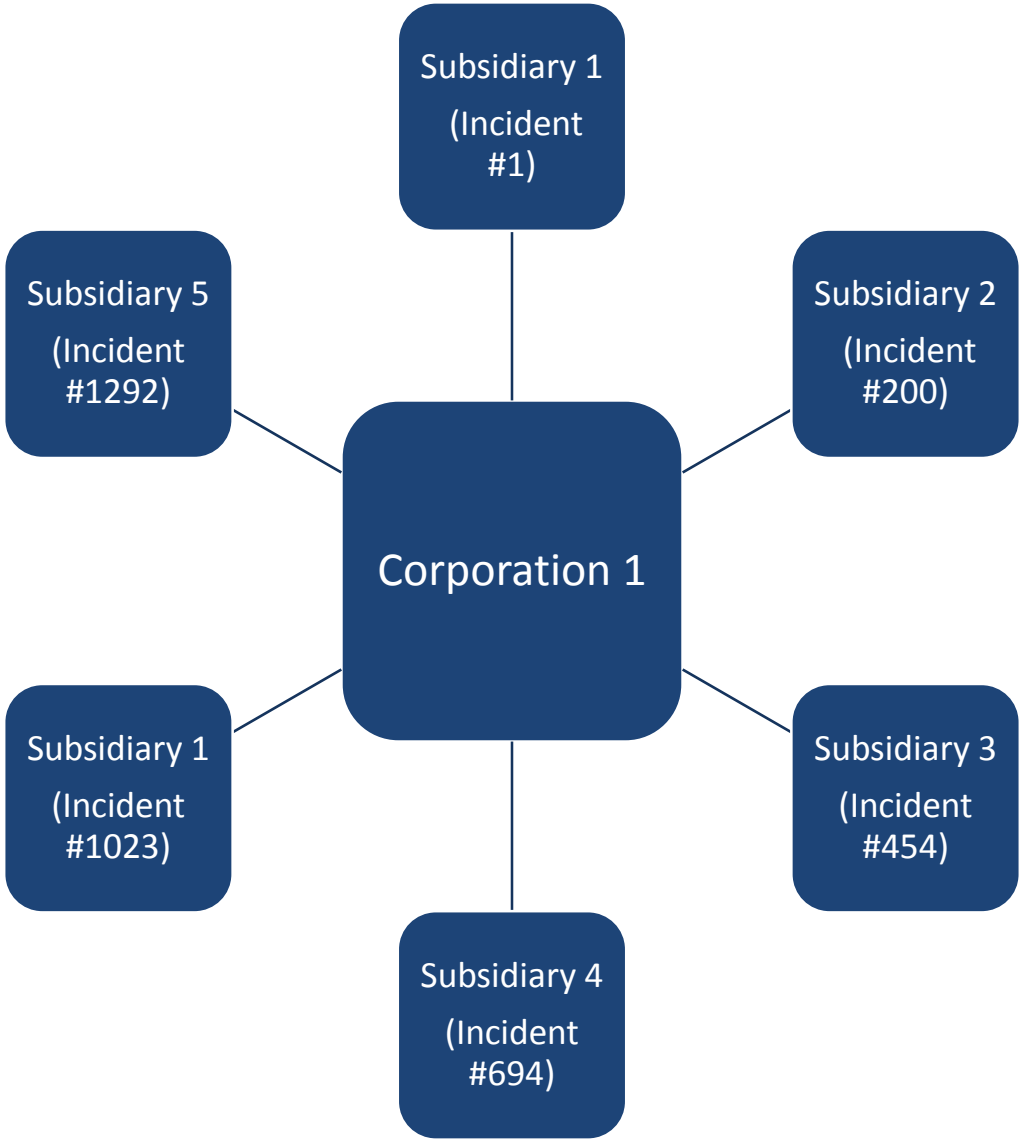
Case Studies

Wrap-Up

Project Basis



Project Basis

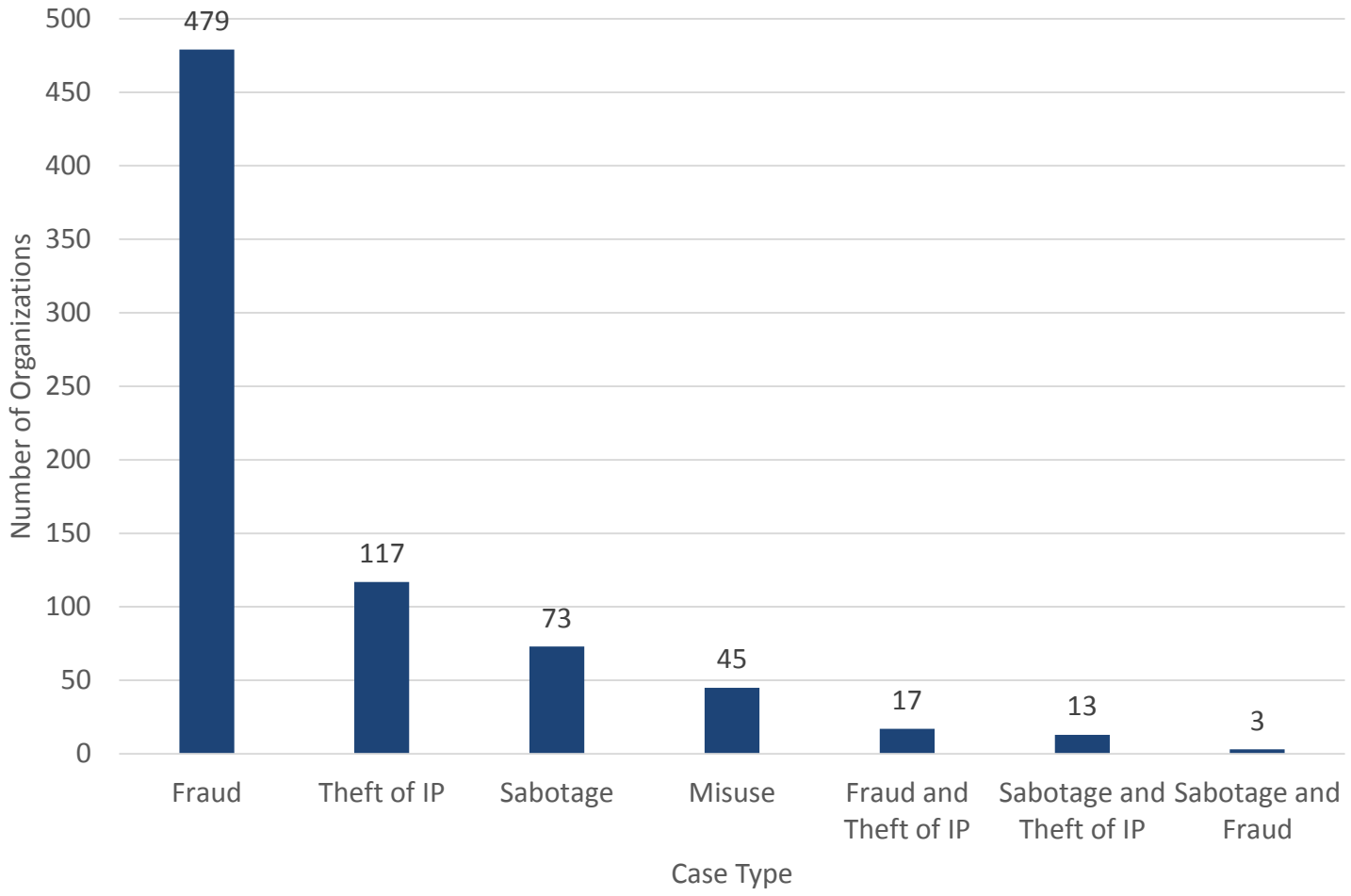


CERT© Insider Threat Incident Corpus Case Study – Parent & Subsidiary Organizations

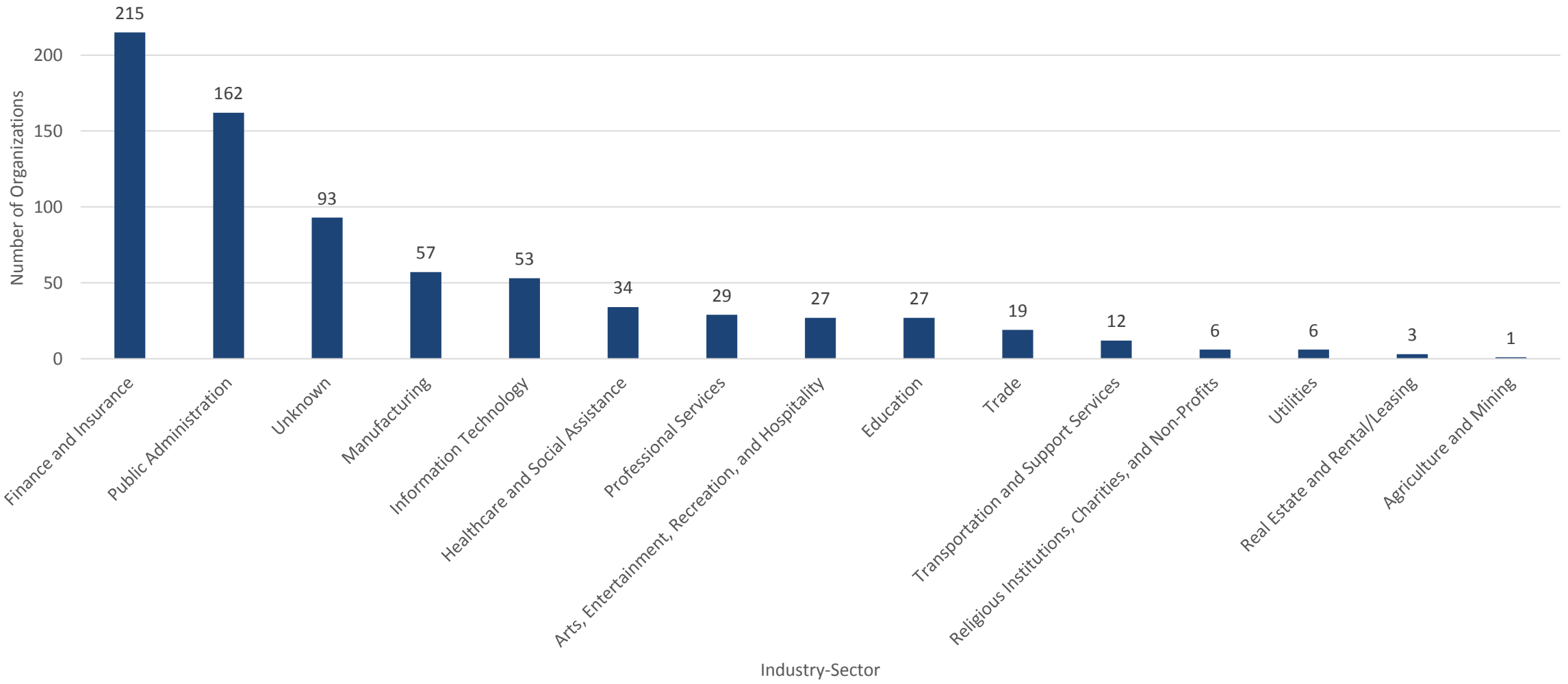
Summary Statistics

Parent Organizations – Quick Facts & Case Type

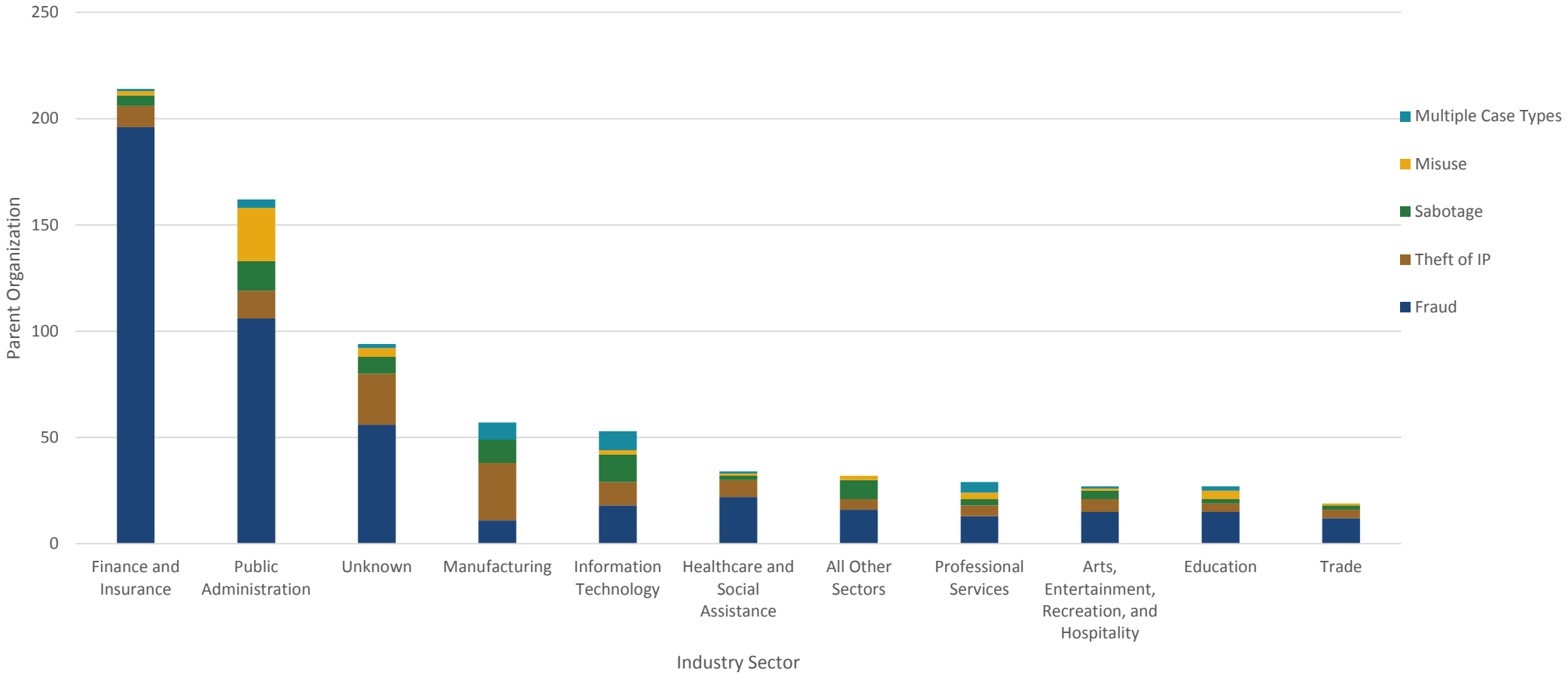
- 748 total organizations with parent organization
- 518 incidents with parent organization/agency
- 119 incidents with more than one organization with a parent



Parent Organizations by Industry-Sector



Parent Organizations by Industry-Sector and Case Type



CERT© Insider Threat Incident Corpus Case Study – Parent & Subsidiary Organizations

Case Studies

Corporation B Case Study – Five Subsidiaries and Five Incidents

- **Subsidiary 1 (California)**
  - A full time software programmer, without authorization, accessed source code, and copied it, which deleted files.
- **Subsidiary 2 (Florida)**
  - An IT worker, working in the network support department, stole backup tapes of important voice recordings.
- **Subsidiary 3 (Georgia)**
  - A network engineer submitted hundred of fraudulent service requests on behalf of the victim organization, allowing the insider to sell all of the non-used parts delivered by the service requests.
- **Subsidiary 4 (Alabama)**
  - Insider worked as a network technician, who sold multiple customer records to an undercover private investigator.
- **Subsidiary 5 (Virginia)**
  - An HR administrator changed job roles within the organization, and was able to exploit this access to modify records of recently terminated employees to indicate that they had been re-hired at a higher rate.

State Council of the People's Republic of China (Beneficiary)

- **Subsidiary 1 [Telecommunications]**
  - Subsidiary 1 provided over a million dollars in funding for a joint venture with insider, who stole trade secrets from their current employer.
- **Subsidiary 2 [Agriculture and Mining]**
  - While being trained at the victim organization as a software developer, insider stole software and source code for Subsidiary 2.
- **Subsidiary 3 [Aerospace, Auto, Marine, and Machinery]**
  - Insider stole trade secrets from victim organization, and Subsidiary 3 hired insider because of the stolen trade secrets.
- **Subsidiary 4 [Chinese Government Agency]**
  - Insider, as a foreign national, used their access to direct their trade secrets to the Chinese-run government agency.
- **Subsidiary 5 [Electronic Manufacturer]**
  - Send trade secrets from foreign national.
- **Subsidiary 6 [Aerospace, Auto, Marine, and Machinery]**
  - A naturalized citizen, recruited former employees of victim organization to retrieve property related to a coveted chemical process.
- **Subsidiary 7 [Chinese Government Agency]**
  - After being hired as a software developer, insider gained access and used access to benefit Subsidiary 7.
- **Subsidiary 8 [Aerospace, Auto, Marine, and Machinery]**
  - Insider sent Subsidiary 8 a set of trade secrets in order to obtain employment.

CERT© Insider Threat Incident Corpus Case Study – Parent & Subsidiary Organizations

Wrap-Up

Analytic Value

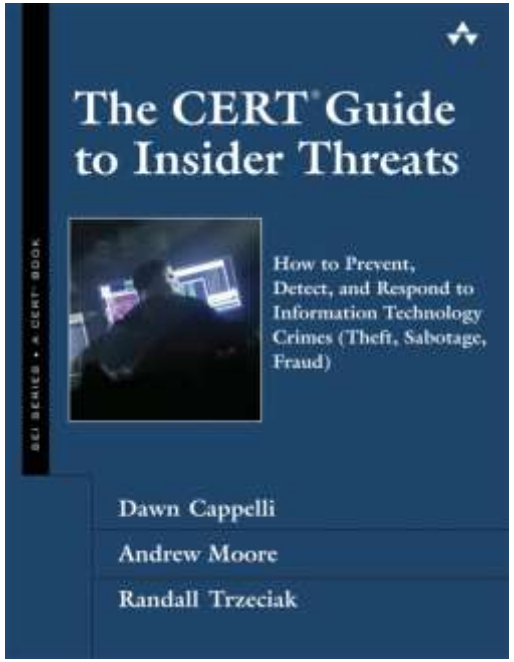
- Potential to see how the organizations spread their subsidiaries across state lines.
- Determine if an organization is represented in the CERT Insider Threat Incident Corpus more frequently because it is a larger organization, more distributed across the US, or a conglomerate
  - Benchmarking value: Help such organizations refine the probability of an incident
- Cross-comparison of specific organizations within a sector
  - Benchmarking value: Help an organization establish insider threat risk management performance compared to peers
  - Actionable intelligence: Determine if there are factors associated with organizations that are more represented in the Corpus within a sector compared to those with more infrequent incidents, albeit with some caveats (i.e., other organizations under-prosecuting or failing to detect incidents)
- Cross-comparison of sectors
  - Benchmarking value: Do some industry sectors have a higher baseline of a particular threat vector?
  - Actionable intelligence: Help an organization determine the potential insider threat risk associated with acquisitions within a sector

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.



For More Information

Software Engineering Institute (SEI)

National Insider Threat Center	http://www.cert.org/insider-threat/
National Insider Threat Center Email	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

Open Source Insider Threat (OSIT)

Data Analytics Special Interest Group (DA SIG)

Energy Special Interest Group

Financial Services Special Interest Group

osit-forum-support@cert.org

Privacy Special Interest Group

privacy-sig-owner@cert.org