



Insider Incidents in the Food and Beverage Industry

Insights into the CERT National Insider Threat Center (NITC) 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.

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

DM19-0642

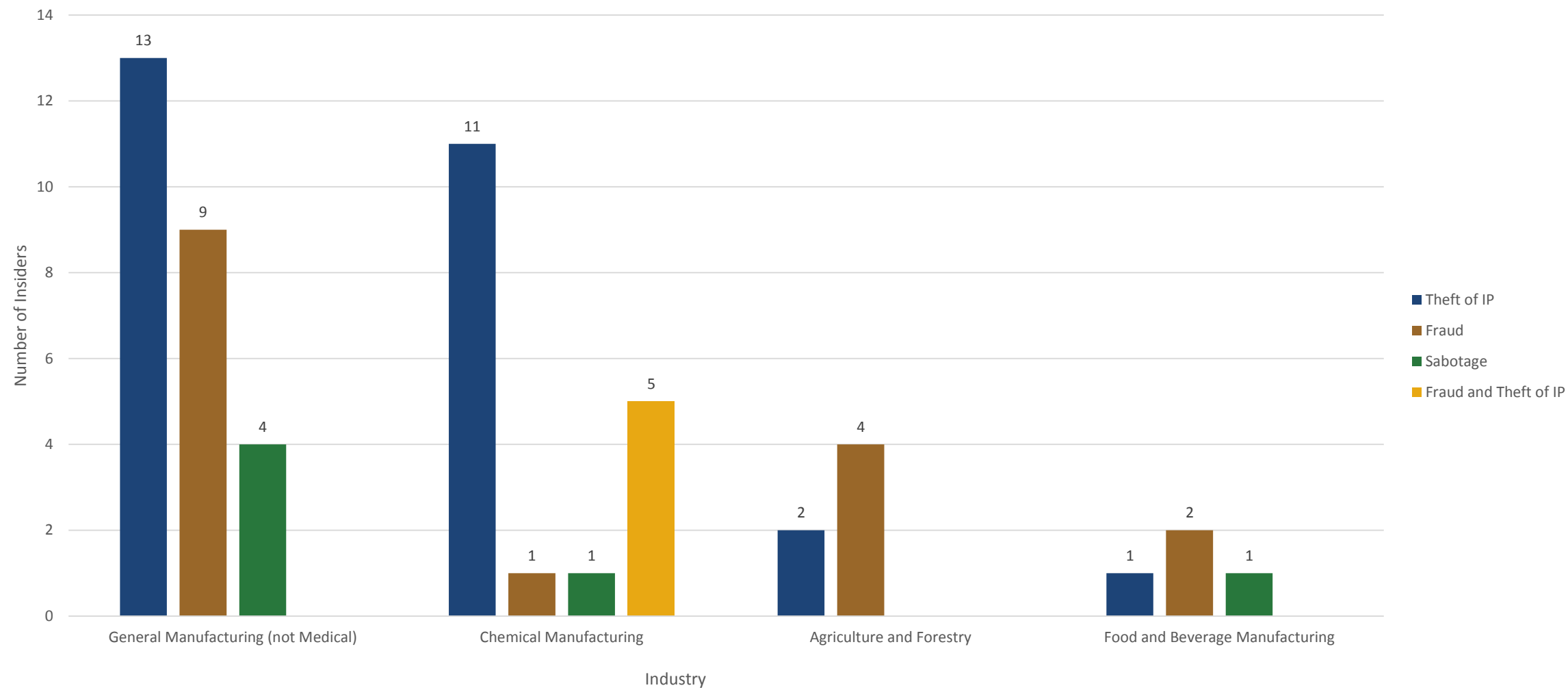
A Note about the Cases

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

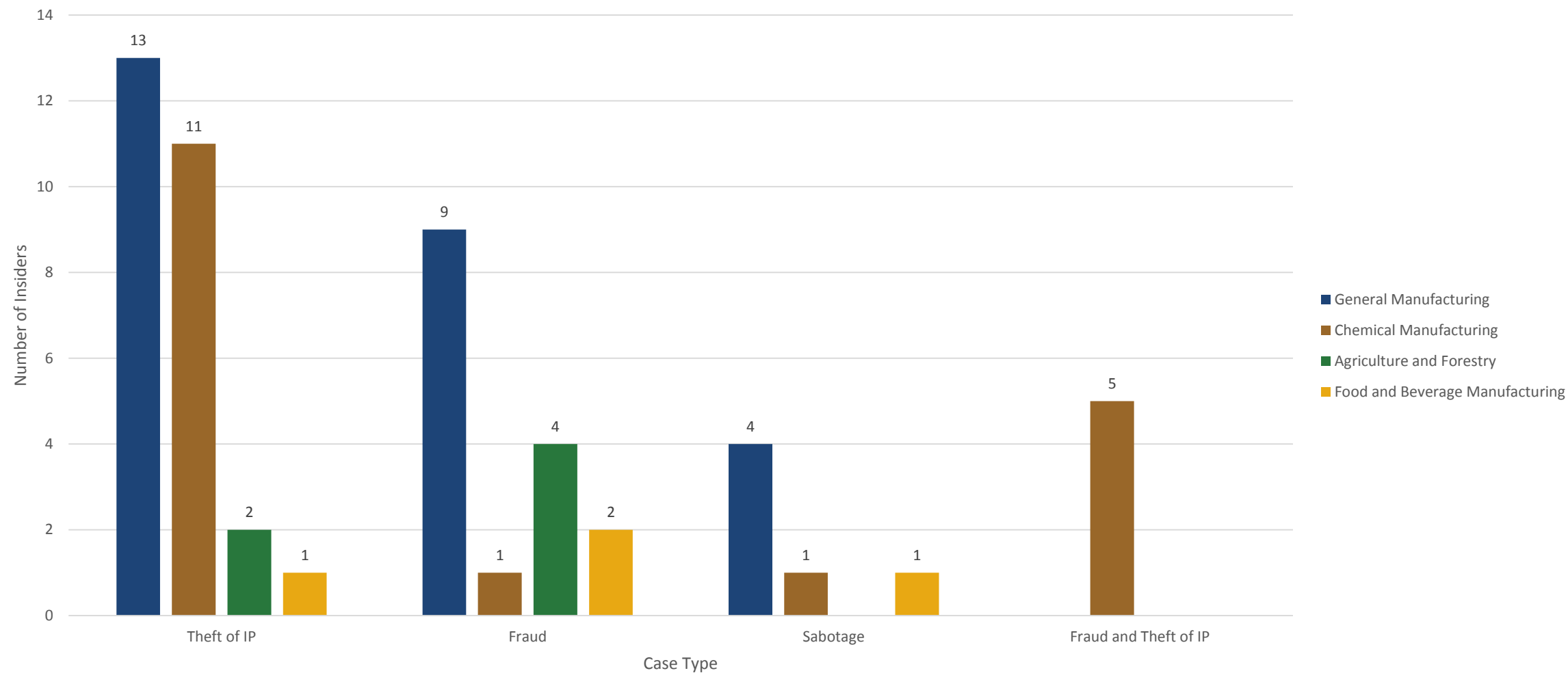
- Domestic incidents with publicly available information that were not dismissed or otherwise settled out of court
 - These incidents primarily took place in federal criminal courts
- Malicious insiders
- Cases identified as Fraud, Sabotage, Theft of IP, or Misuse
- Victim organizations identified as Agriculture and Forestry, Food and Beverage Manufacturing, Chemical Manufacturing, and General Manufacturing (not Medical).

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.

Industry by Case Type



Case Type by Industry



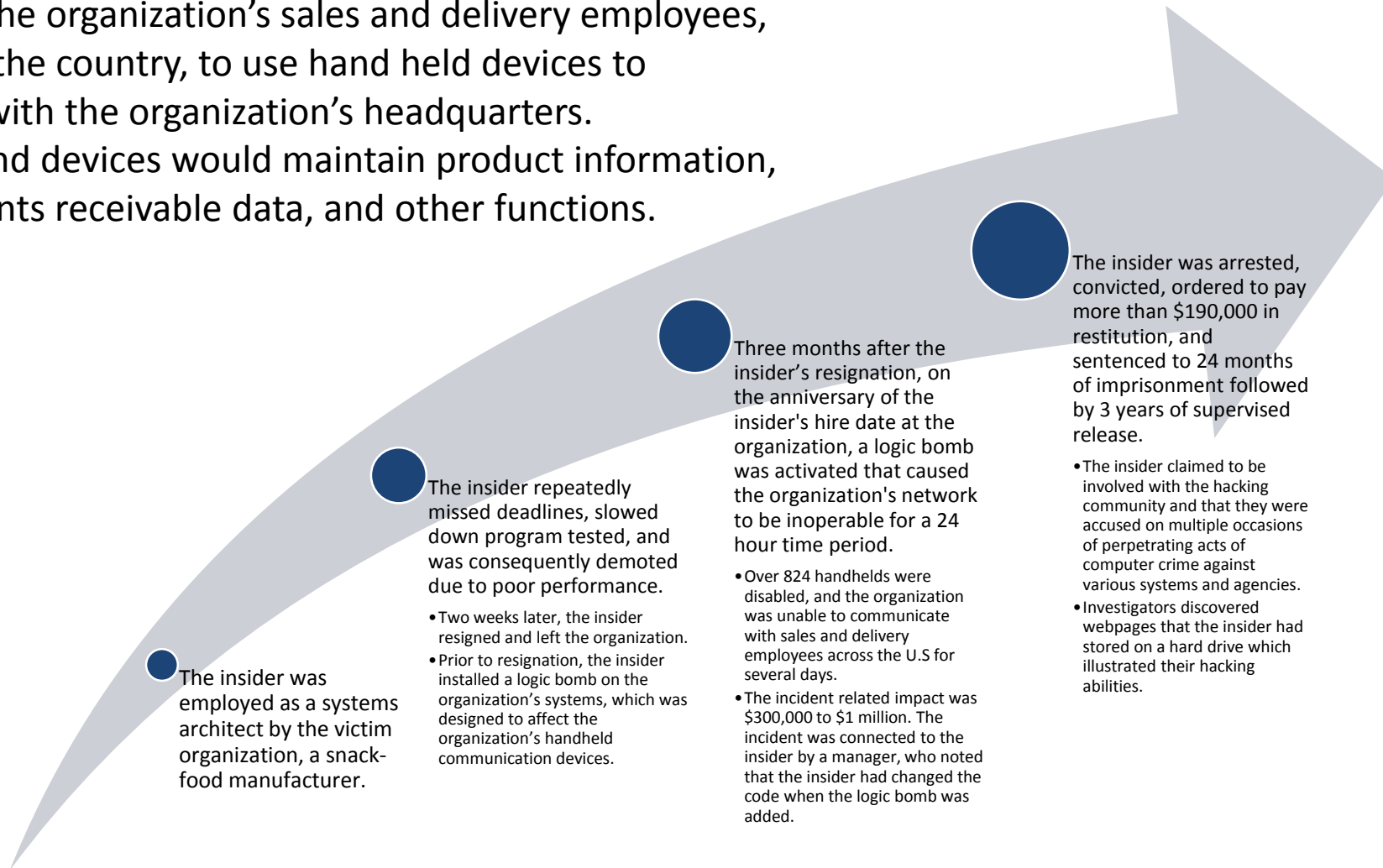


Insider Incidents in the Food and Beverage Industry

Case Examples

IT Sabotage

The insider was hired to develop a computer program that would enable the organization's sales and delivery employees, located across the country, to use hand held devices to communicate with the organization's headquarters. The program and devices would maintain product information, receipts, accounts receivable data, and other functions.



Fraud

The insider was a full-time accounting official for the victim organization, an agriculture and food company. Over the course of about 10 years, the insider stole \$3.1 million from the victim organization and caused over \$25 million in additional losses. The insider stole hundreds of customer payments sent to the victim organization, totaling at least \$3.1 million. The insider deposited the payments into their personal bank accounts. The insider also created fraudulent invoices and mailed them to the victim organization's customers, directing them to send payment directly to the insider, thereby bypassing the victim organization's corporate controls. To hide their activities, the insider made false entries into the victim organization's accounting software. The insider was sentenced to 60 months in prison and 2 years of supervised release. The insider was also ordered to pay \$3.6 million in restitution, which reflected their embezzlement and falsified tax returns that they submitted over the course of the scheme.

Fraud

The insider was a sales executive for the victim organization, a food and beverage manufacturer. The insider was required to manage a portion of the promotional activities for the victim organization's products. Over the course of about 10 years, the insider submitted more than \$1.7 million worth of fraudulent invoices. The insider incorporated a business in their spouse's name. Through this business, the insider submitted to the victim organization more than 200 fraudulent invoices totaling \$1.7 million for services such as promotional signs and banners, delivery of sample products to retail stores, and the offering of discount prices to retail stores. None of the services billed to and paid for by the victim organization were actually provided. Additionally, the insider admitted that they failed to declare any of the income they derived through their business on the joint federal tax filings they filed with their spouse. The insider was charged, pled guilty, and sentenced to 33 months in prison, 2 years of supervised release, and over \$2 million in restitution.

Theft of IP

The insider was employed as an executive administrative assistant to a top executive in the victim organization, a beverage manufacturer. The insider's proximity to the executive granted them access to the organization's trade secret information, including confidential and proprietary documents, and product samples that had not been publicly released.

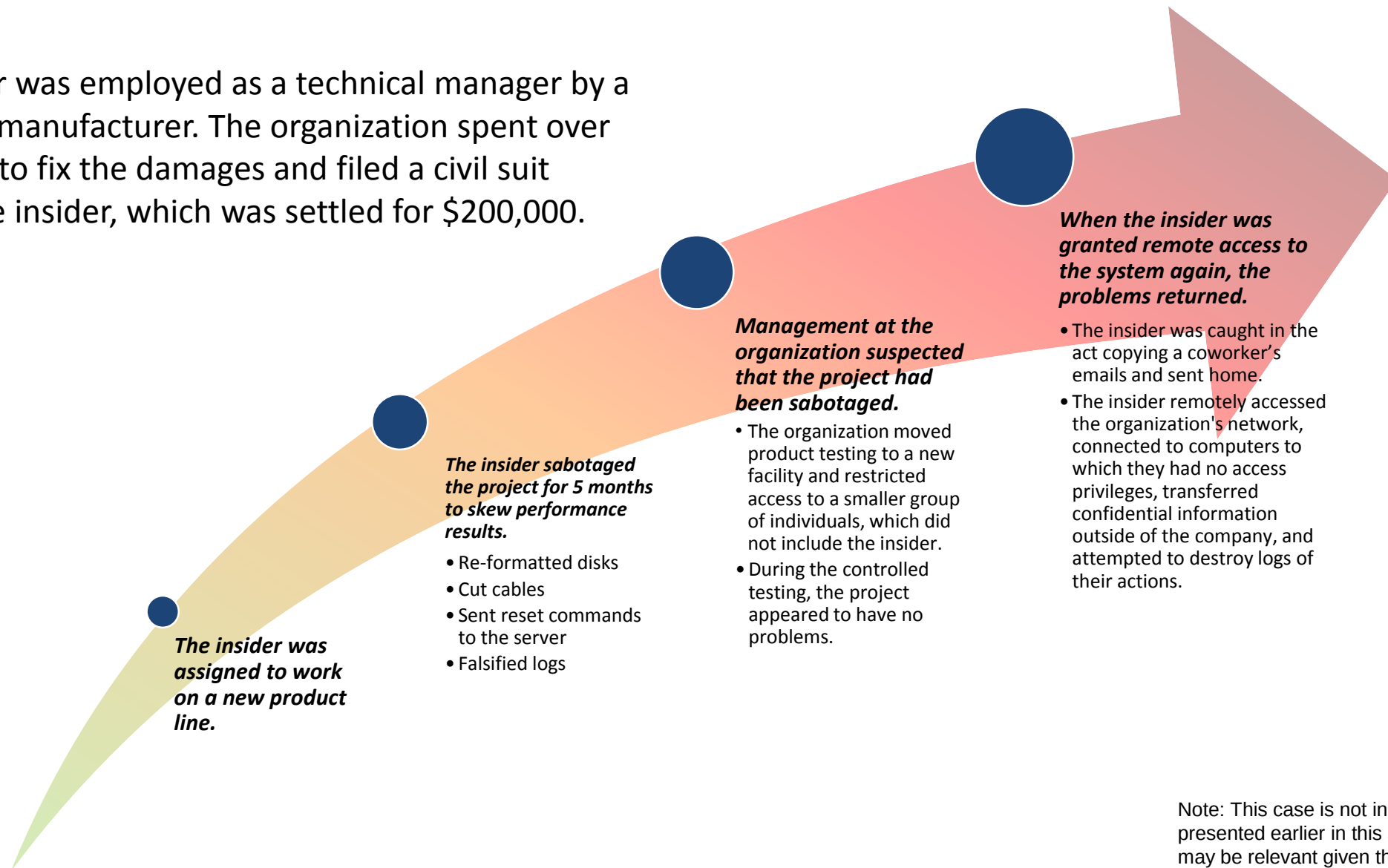
Over the course of two months, the insider exfiltrated data by:

- Placing trade secret documents and a product sample into their bag
- Copying or printing documents (including email communications) and stealing others
- Fax

The insider was convicted, ordered to pay \$40,000 restitution, and sentenced to 8 years imprisonment followed by 3 years of supervised release. The insider's substantial credit card debt, which was equal to their yearly salary, likely motivated them to perpetrate the incident. The insider had violated employment and confidentiality agreements.

IT Sabotage

The insider was employed as a technical manager by a computer manufacturer. The organization spent over \$1 million to fix the damages and filed a civil suit against the insider, which was settled for \$200,000.



Note: This case is not included in the statistics presented earlier in this slide deck, but the scenario may be relevant given the context.

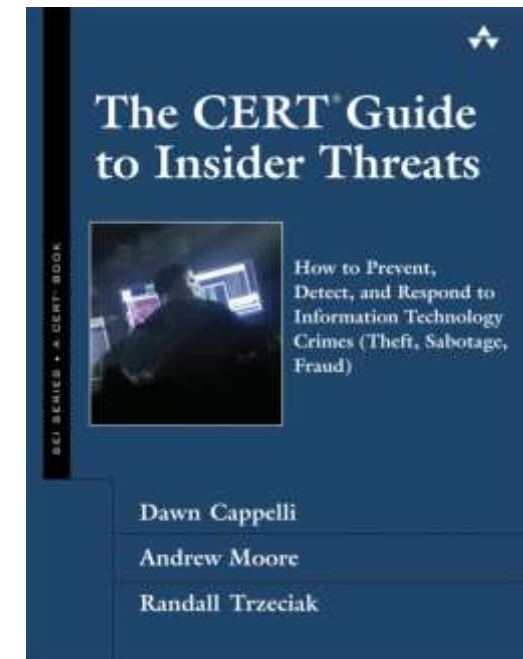


Insider Incidents in the Food and Beverage Industry

Additional Resources

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 on Insider Threat

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

Sarah Miller

Insider Threat Researcher

CERT National Insider Threat Center

Email: semiller@cert.org

Software Engineering Institute

Carnegie Mellon University

4500 Fifth Avenue

Pittsburgh, PA 15213-3890

