Affected Devices & Communication Channels In Insider Incidents

Alex Pickering

April 2020

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.

DM20-0366

Definitions

- **Affected Device** – Any system that was damaged, used, or otherwise modified during the course of the incident.
  - Affected devices may be a target of the attack, incidentally affected by the attack, or modified after the attack for concealment.
  - A single incident can affect 1 or more devices. All incidents in the CERT Insider Threat Corpus are technical insiders, so at least 1 device will be affected.

- **Communication Channel** – Any way for an insider to communicate with other actors; this could be an insider and an outsider, the insider and a competing organization, or two insiders conspiring together.
  - The insider using a technology as a way to exfiltrate data is not a communication channel, e.g., an insider stealing organization data by emailing it to themselves is not a communication.

Taxonomy of Devices

Organization Desktop

Organization Laptop

Organization Mobile Device

Personal Computer

Personal Mobile Device

File Server

Web Server

Database Server

Printer/Copier/Fax Machine

Other

Unknown

Taxonomy of Communication Channels

Organization Email

Organization Phone

Personal Phone

Instant Messaging

Unknown Phone

Online Forum

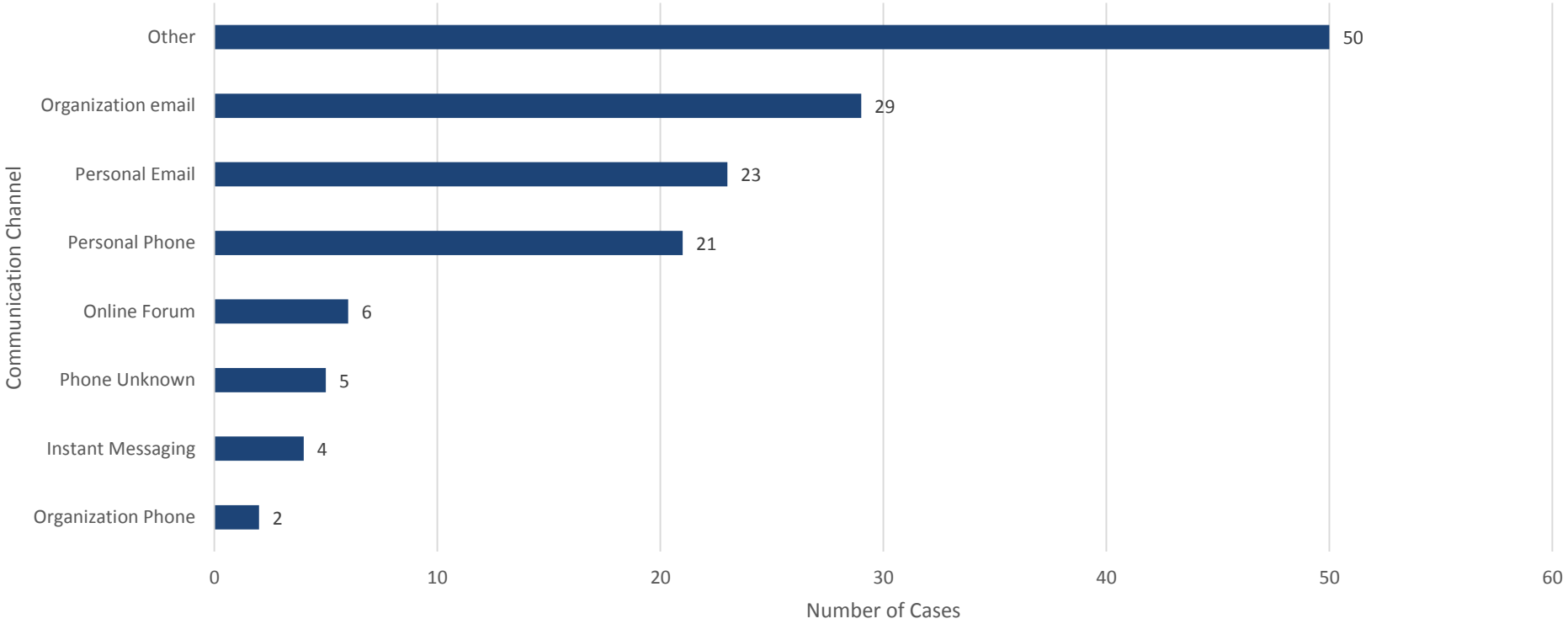
Other

Unknown

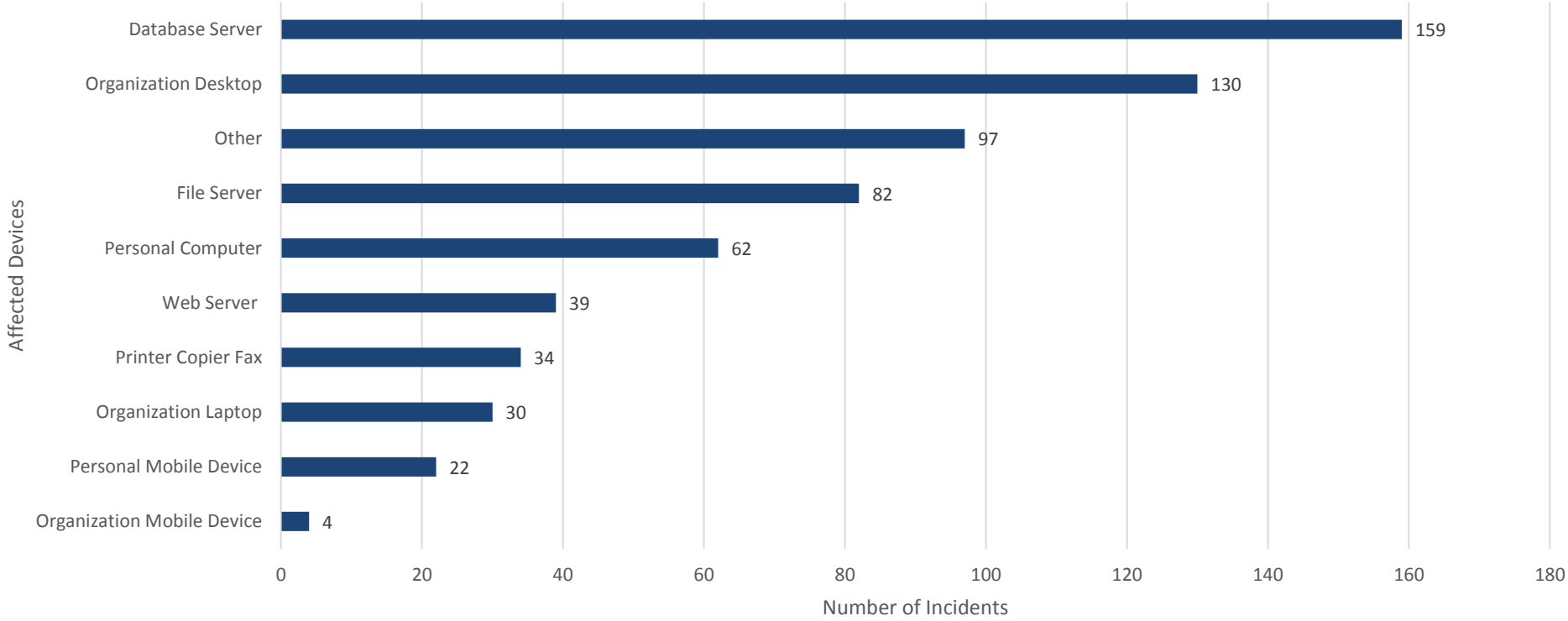
Affected Devices & Communication Channels In Insider Incidents

Summary Statistics

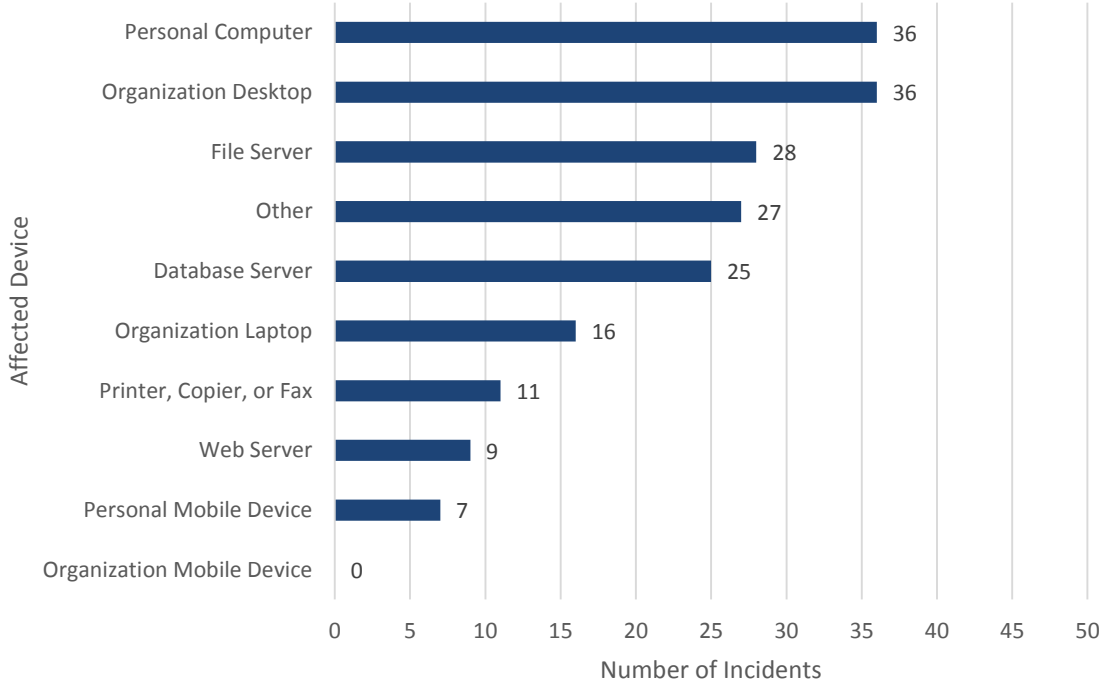
Communication Channels



Affected Devices

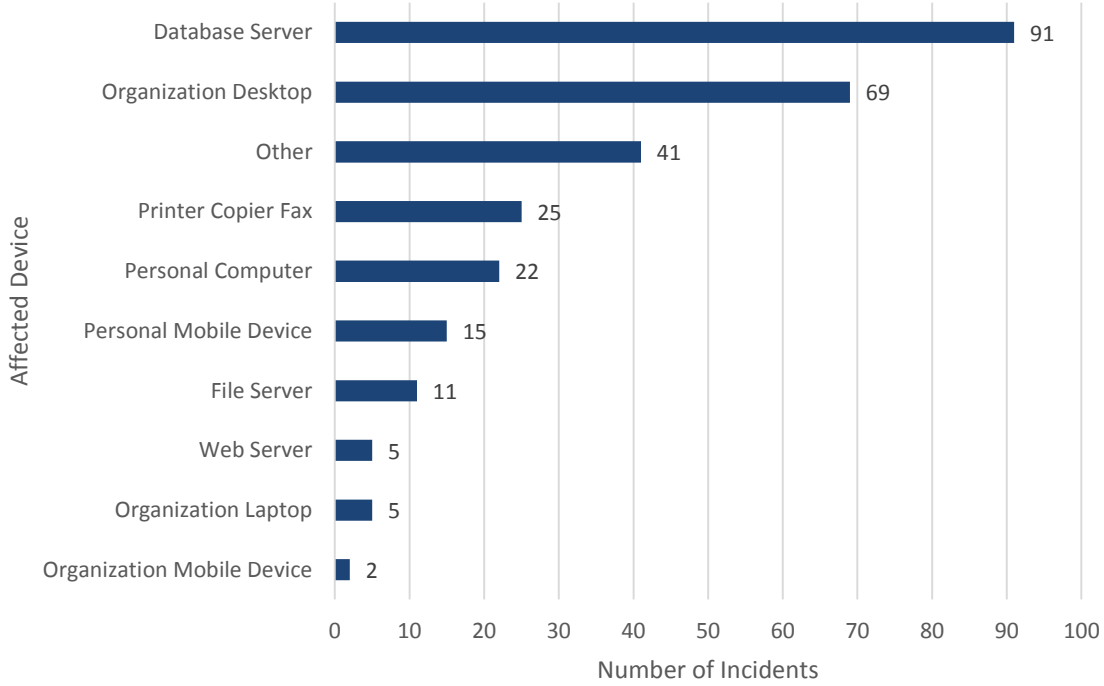


Affected Devices in Theft of IP Cases



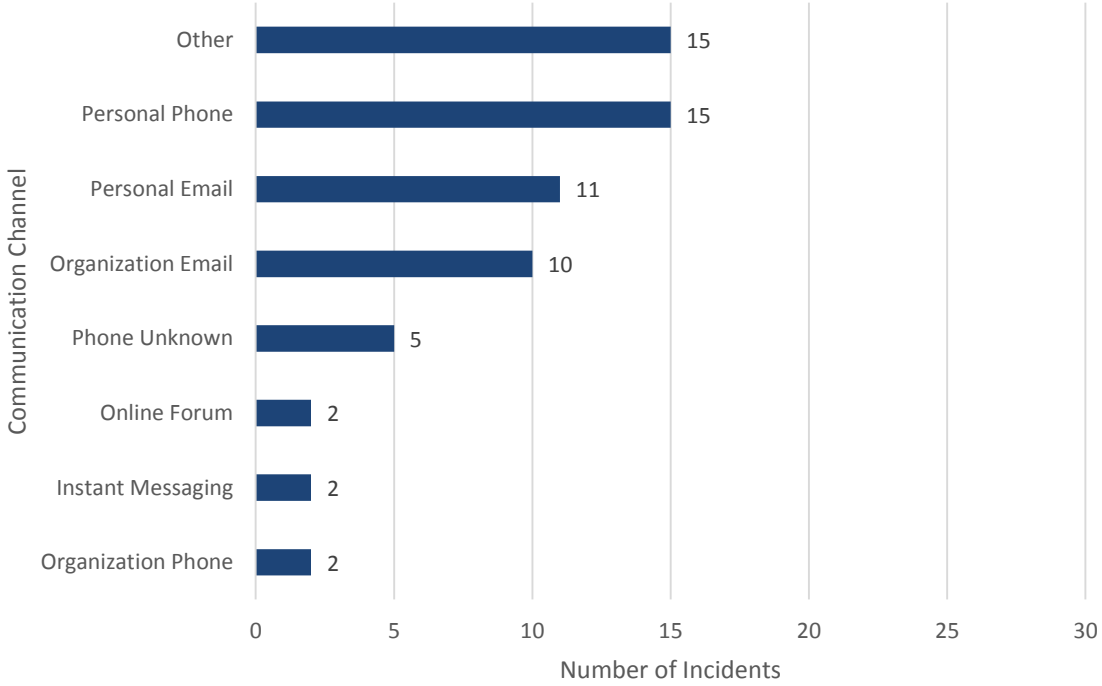
The most commonly affected devices in incidents where an insider stole an organization's intellectual property are the insider's personal computer and an organization owned desktop.

Affected Devices in Fraud Cases



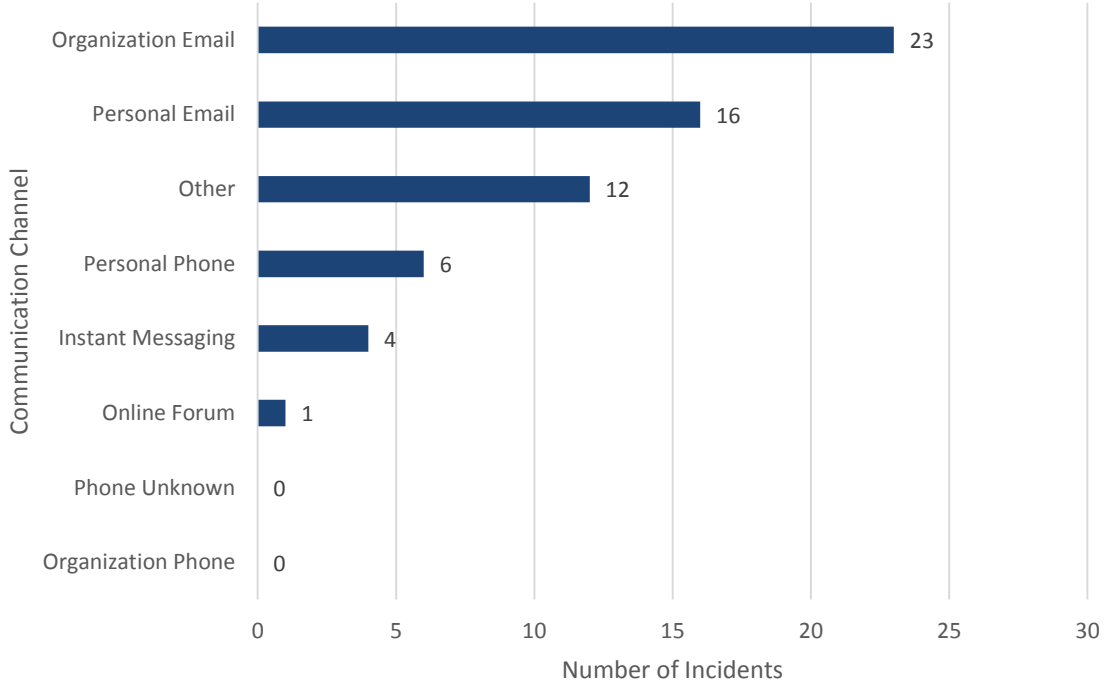
- The most commonly affected devices in incidents where one or more insiders are involved in fraud or embezzlement are databases.
- Most “Other” devices are organization owned servers that don’t fit cleanly into our taxonomy.
- These include authentication servers, Point of Sale (PoS) systems, and SCADA controllers.

Communication Channels in Fraud Cases



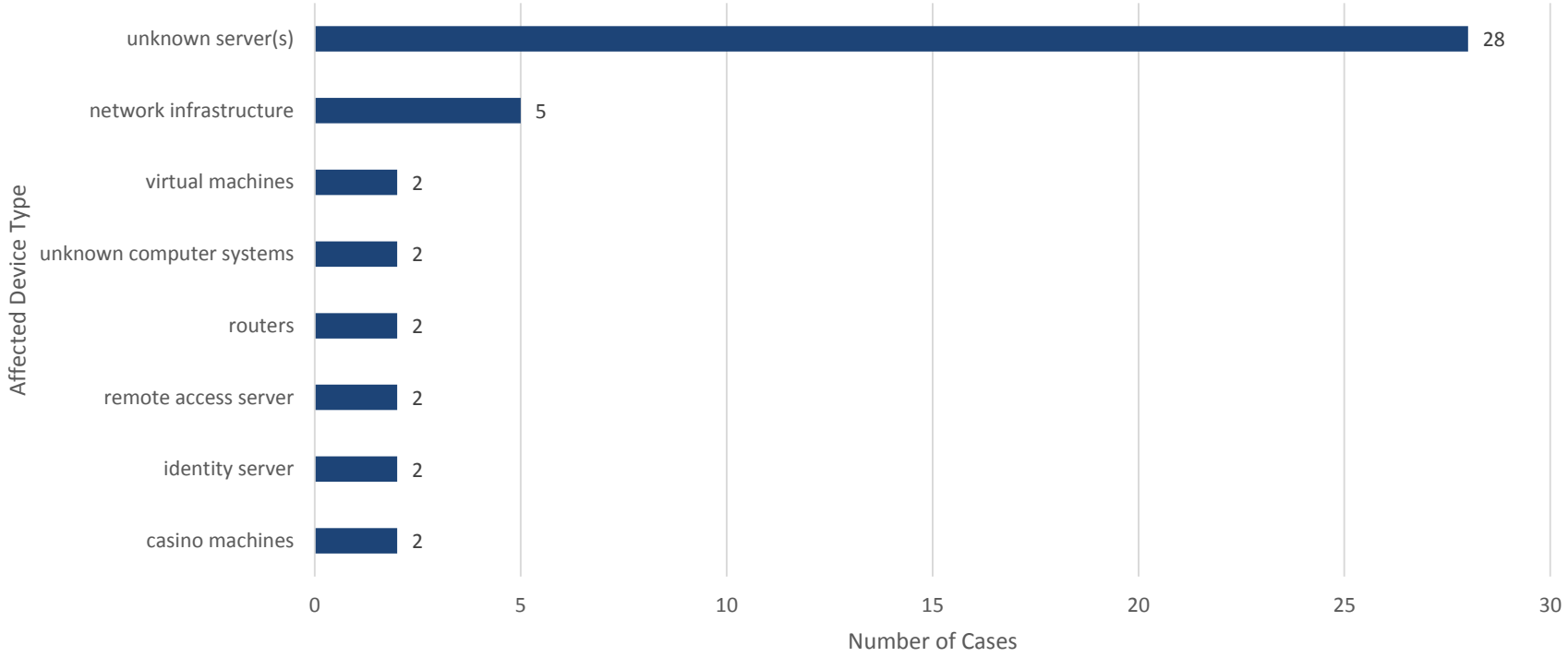
- Some insiders conspire together to bypass organizational controls, increase profits, or conceal activity.
- When they do, fraudsters have a greater average number of communication channels than any other case type.

Communication Channels in Theft of IP Cases

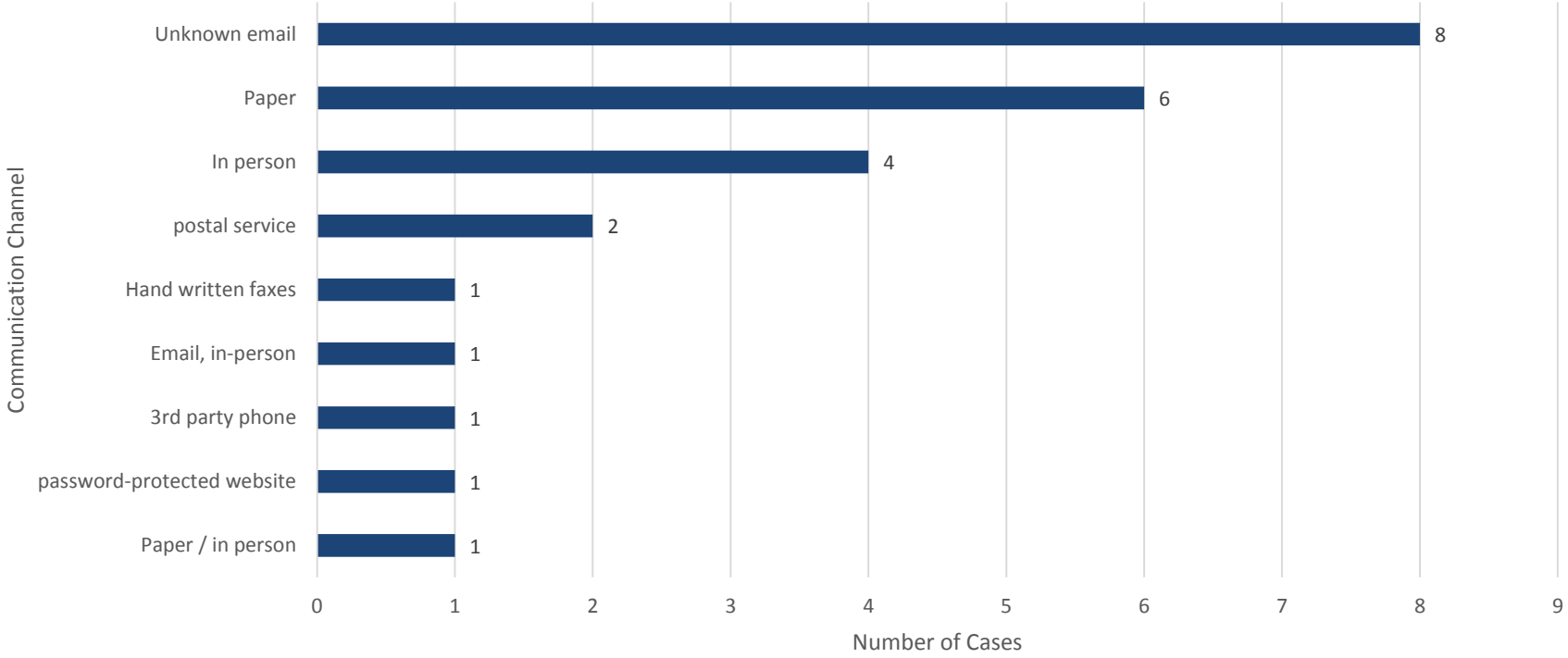


- Insiders engaged in theft of intellectual property tend to use email, either the organization's or their own, to talk to each other.
- The most common sub-category for "Other" communication channels for IP theft is "Unknown Email"

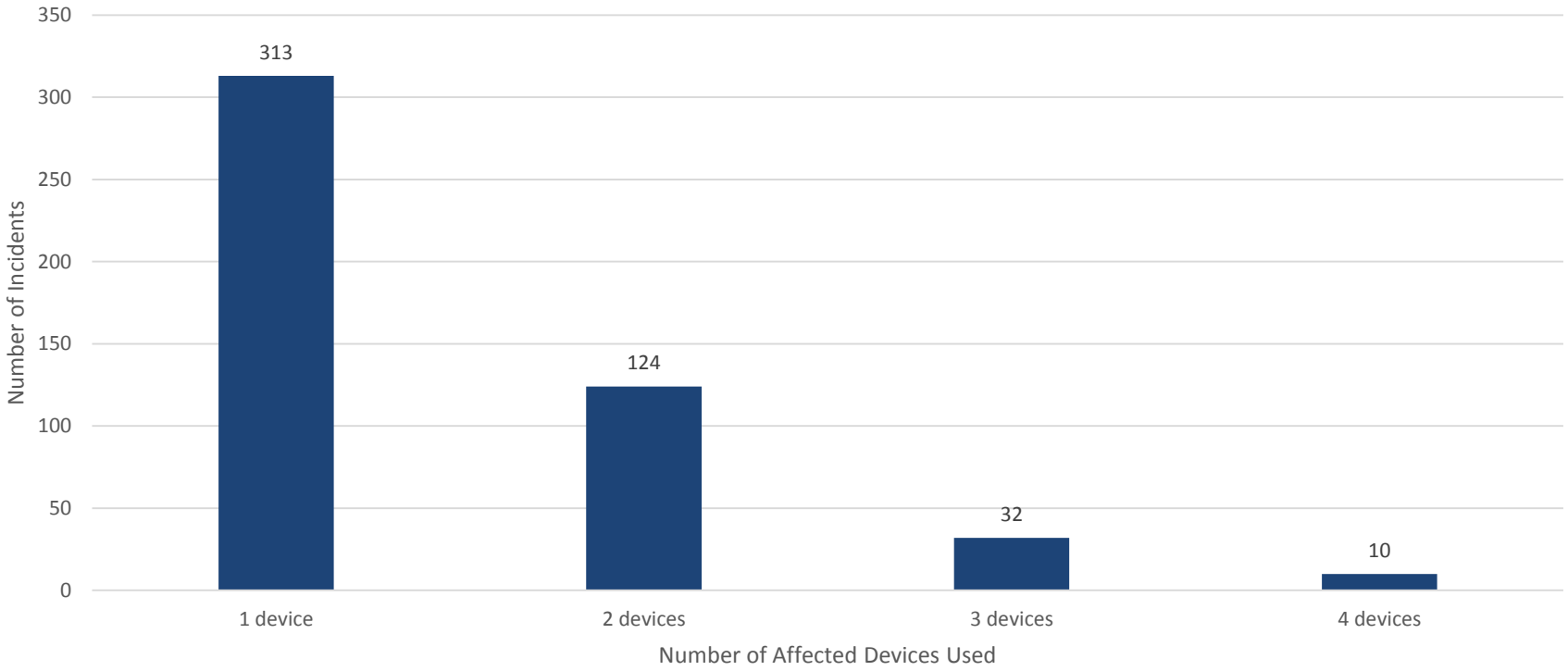
Top 10 “Other” Affected Devices



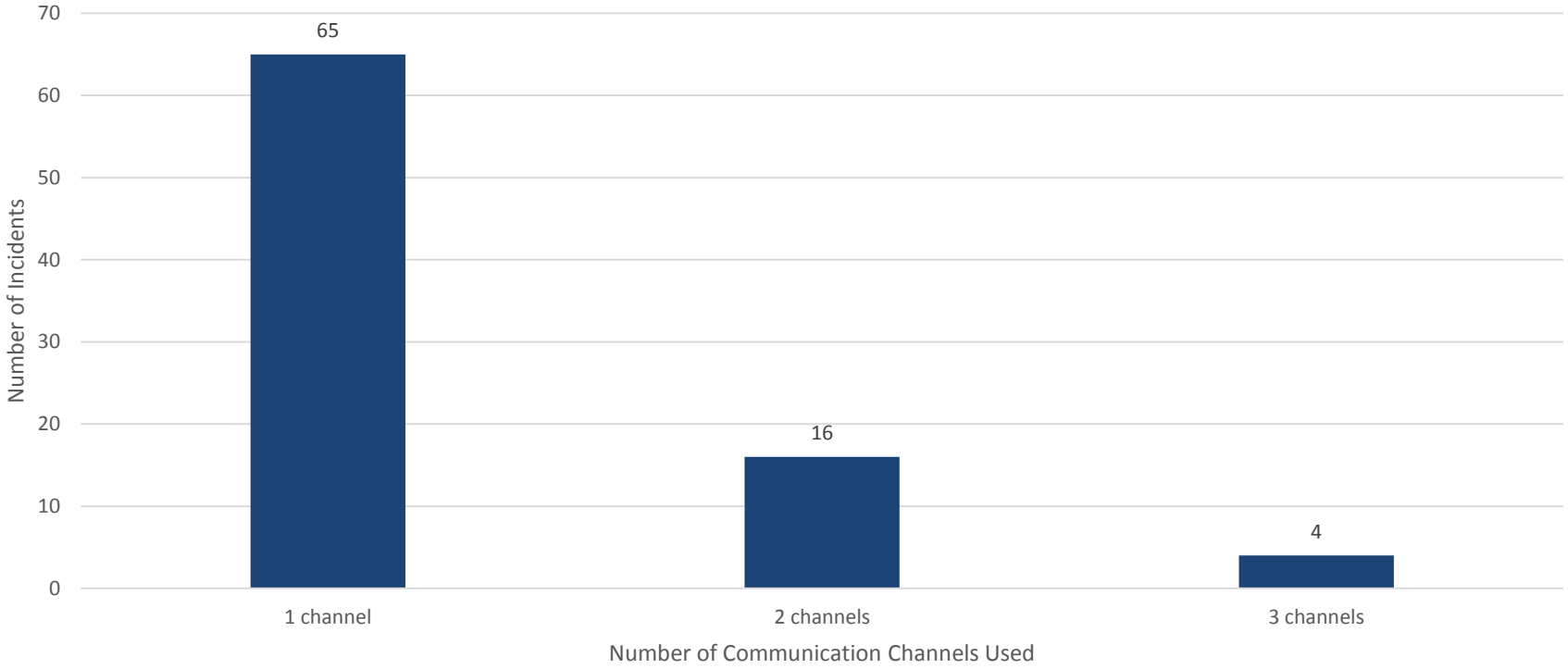
Most Common “Other” Communication Channels



Number of Affected Devices in an Incident



Number of Communication Channels in an Incident



Wrap-Up

Analytic Value

In the future, we can correlate this data with other features in our incident corpus, including:

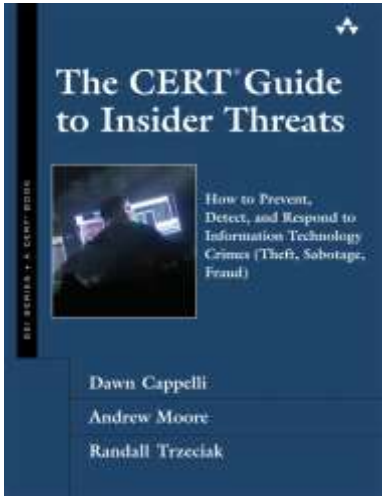
- The cost of an incident to an organization.
- What actions an insider took on the course of an incident.
- What devices are intentionally targeted by insiders, and what devices are not targeted, but affected.
- Which devices present more risk with BYOD policies.
- What devices are useful to look at after an incident has been identified.

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