OPA Report No. 2020-094
PERSEREC-RN-20-06

Why PERSEREC Did This Study

The U.S. Department of Justice (DoJ) requested that PERSEREC estimate empirically, based on research data that PERSEREC had collected on resource exfiltration by DoD insiders, the average monetary value (i.e., based on monies requested, offered or received) of exfiltrated information. An average value could then be used to estimate the typical or expected monetary value of sensitive information in situations when the specific value of one or more exfiltrated documents has not been determined.

What PERSEREC Concluded

Available data on monies offered to, received, or requested by exfiltrators were used to estimate two relevant measures (mean and median) for the average value of exfiltrated sensitive DoD information. Results indicate that, historically, the mean value of exfiltrated DoD resources is in the range of $57,516-$67,102, and the median value is in the range of $7,000-$9,000.

Research Note September 2020

Approximating the Value of Sensitive Information Exfiltrated from the U.S. Department of Defense

Eric L. Lang
Defense Personnel and Security Research Center
Office of People Analytics

What PERSEREC Found

Among 83 Department of Defense (DoD) publicly accessible exfiltration convictions between 1985-2017, 40 individuals appear to have been motivated by money. Of these 40, PERSEREC was able to find open source intelligence that referenced how much money 28 perpetrators requested, received or were offered over the course of their exfiltration efforts, which lasted several months to several years. [1]

Of the 28 perpetrators, four received no money. The remaining 24 individuals received between $200 and $636,000, with a mean value of $67,102 and a median value of $9,000.

Because it could not be determined whether the four "zero-dollar" cases involved worthless documents or, alternatively, the documents had significant value but the perpetrators negotiated ineffectively, a second analysis was performed that included the four zero-dollar cases. This fuller (more conservative) analysis of all 28 cases resulted in a mean value of $57,516 and a median value of $7,000.[2] All 28 values are listed in Appendix A.

[1] For the remaining 12 (of 40) perpetrators motivated by money, there was no open source information available on a specific monetary amount that was offered or received.

[2] When the distribution of data values in a set is "normal" (e.g., a bell-shaped curve) or similarly symmetric, the mean and median values for the set of values will be identical. However, for datasets that include one or more extreme values, the median will be less influenced than the mean by the extreme values. Because the exfiltration dataset included several extremely large monetary values, means and median averages were both calculated. Both are accurate and valid to interpret depending on the use of the information regarding "average value".

Background and Method

Estimating the value of assets is useful, for example, in developing risk-based asset protection systems, producing damage assessments, and in legal proceedings and punishments that pertain to assets that are lost, compromised or stolen.

With respect to legal proceedings that address the embezzlement or theft of Public money, property or records, 18 U.S. Code § 641 applies when the "...the value of such property in the aggregate, combining amounts from all the counts for which the defendant is convicted in a single case..." exceeds the sum of $1,000.

Resource exfiltration is a form of embezzlement or theft in that it includes cases that involve the intentional and unauthorized removal of resources from authorized locations (regardless of classification level).

Estimating the value of exfiltrated resources is difficult. Value can depend on any combination of the following (non-exhaustive) list of considerations:

1. the costs of producing the original resource,
2. the costs of replacing the resource,
3. potential financial gain by unauthorized recipients, e.g., profiting from other's intellectual property or non-public resources (hardware, software, knowledge, or documents),
4. direct and indirect financial and intangible harm caused by the resource compromise, e.g., when adversaries use unauthorized resources to undermine U.S. and allied systems, plans, personnel safety, population health, political alliances and/or public trust.

Because buyers and sellers of resources typically evaluate value considerations such as those listed above, one way to estimate resource value is to assess what purchasers have actually offered or paid for a resource. 18 U.S. Code § 641 includes this sentiment by defining "value" to mean "face, par, or market value, or cost price, either wholesale or retail, whichever is greater."

For determining the value of exfiltrated DoD resources, data are available from a PERSEREC "Resource Exfiltration" research project. A full description of this project appears in a PERSEREC 2019 Technical Report (TR-19-02[3]). The Method Section of TR-19-02 states that: Eligible cases included those perpetrators who had:

1. exfiltrated a DoD resource;
2. been arrested after November 19, 1985, the publication date of the report issued by the *Commission to Review DoD Security Policy and Practices*; and
3. been convicted or pled guilty by December 31, 2017.

These criteria resulted in 83 eligible perpetrators.

Open source intelligence (e.g., from news articles and court documents) for each case was independently reviewed and coded by two trained behavioral research scientists. This analysis identified that 40 perpetrators appeared to have been motivated by money but, of these 40, available data contained information on money received for 28 perpetrators.

[3] TR-19-02 is Open Source (non-sensitive) and available on PERSEREC's public website as well as through the Defense Technical Information Center (DTIC).

Some perpetrators offered one document, while other perpetrators offered many documents. Of these documents, some were classified, others were not.

The exfiltrated documents were all "sensitive" in the sense that all included DoD information that should not have been provided to unauthorized individuals (or even removed from an unauthorized location). Some of the documents were "Classified" (i.e., as either "Confidential," Secret," or "Top Secret"), whereas other documents had markings, such as "Sensitive but Unclassified" or "Controlled Unclassified Information". Because many of the incidents averaged here included individuals exfiltrating different mixes of Classified and Unclassified information, it was not possible to reliably specify monetary values by information Classification level, nor was it necessary given "value" was determined in a de facto "market" sense based on the amounts of monies requested, offered or received.

Limitations

Although the current analyses were designed to bolster validity by including only cases for which a crime had been committed (i.e., cases that had resulted in convictions), It is unknown whether a less rigorous but broader selection criterion, such as including certain categories of arrests, would have yielded different results.

Resulting value estimates are approximate. For example, no transformations were made to adjust upward the valuations recorded in the 1985-2017 date range into "2020 standard dollar equivalents". Additionally, it is unknown whether, as with real estate valuations, supply and demand "market" fluctuations might affect the comparison of values of exfiltrated resources between different points in time. Similarly, because there are many different kinds of sensitive documents that could be exfiltrated, the value of the documents stolen in any future incident may be substantially different than the historical values reported here. Although it is beyond the scope of this analysis to estimate the specific value of newly exfiltrated documents, basic logic would apply, e.g., if all exfiltrated documents in a new incident were Classified, their value would likely be higher (to an unknown degree) than the averages reported herein.

Finally, it is possible that some information in the open-source reporting of monetary values for exfiltrated classified documents may be different than the actual money received by perpetrators because the government office(s) providing the reported values altered the values to protect national security related sources, methods or comparably sensitive information. In such cases, logic suggests that the reported values might be lower than the actual values, e.g., in an effort to reduce the perceived incentive of other potential exfiltrators reading open-source materials.

Direct questions regarding this Research Note to:

Dr. Eric L. Lang
Director, PERSEREC
Personnel and Security Research Center (PERSEREC)
400 Gigling Rd
Seaside, CA 93955-6771
Eric.L.Lang6.civ@mail.mil

APPENDIX A:
Payments offered to, received, or requested by Convicted Exfiltrators of Sensitive DoD Information

1	$636,000.00
2	$300,000.00
3	$300,000.00
4	$77,795.00
5	$69,000.00
6	$55,000.00
7	$37,000.00
8	$32,000.00
9	$24,000.00
10	$20,000.00
11	$11,500.00
12	$11,000.00
13	$7,000.00
14	$7,000.00
15	$7,000.00
16	$5,000.00
17	$3,500.00
18	$3,000.00
19	$1,500.00
20	$1,300.00
21	$1,000.00
22	$360.00
23	$300.00
24	$200.00
25	$0.00
26	$0.00
27	$0.00
28	$0.00