Snapshot of Insider Threats Within Government

As we know, Insider Threat affects both the public and private organisations. Insider threats are one of the biggest security challenges that Government face. The sheer complexity of Government infrastructure and the important and sensitive value of the information Government possess, makes it easy for a clumsy or a malicious insider to compromise security and potentially cause serious damage.

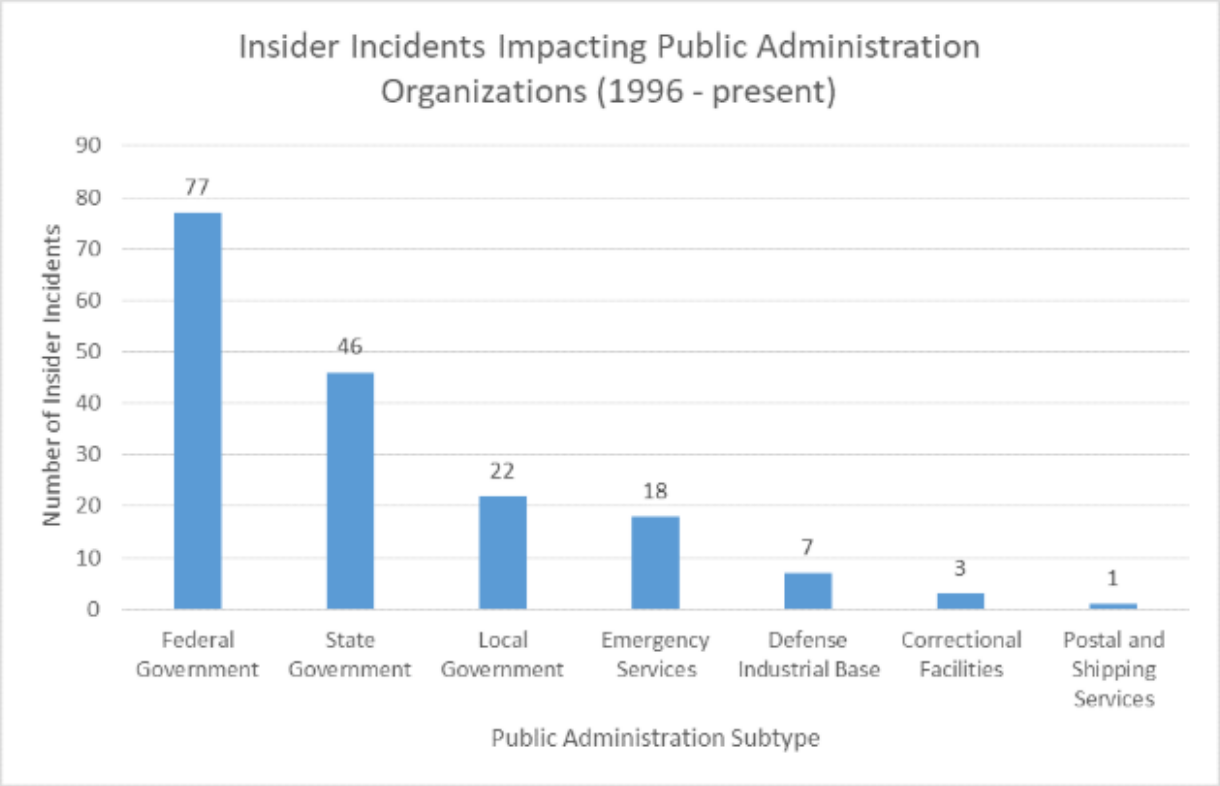
In fact, some of the biggest insider threat incidents took place within Government.

- **Chelsea Elizabeth Manning** (Bradley Edwards Manning) in 2009 and 2010 leaked hundreds of thousands of documents, many of them classified—to WikiLeaks. She was charged with 22 offenses, including aiding the enemy;
- **Edward Snowden**, a former contractor for the CIA was charged in June 2013 by the US Department of Justice of two counts of violating the Espionage Act of 1917 and

theft of Government property. It was estimated that he had copied, stolen, or downloaded around 1.7 million NSA documents according to the Department of Defense;

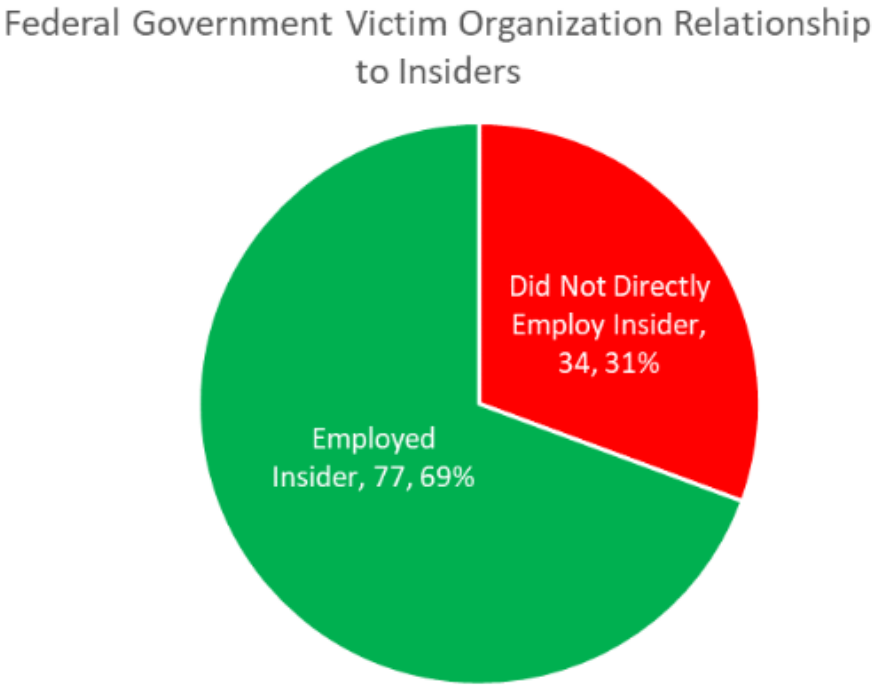
- **Office of Personnel Management** (OPM) breach in June 2015, compromised 21.5 million Government records;
- **Ex NSA worker (Harold Martin III)** was charged in august 2016 for stealing 50 terabytes worth of data during a period of two decades;
- **In Australia, in 2014–15 an Australian Bureau of Statistics (ABS)** officer working at the Bureau's Canberra headquarters was convicted of offences relating to the unauthorised disclosure of sensitive statistical information. Over a period of nine months, the ABS officer provided an acquaintance in the banking industry with unpublished market sensitive economic data which netted approximately $7 million in illegal foreign exchange trades;

Overview of Insider Threats within Federal Government



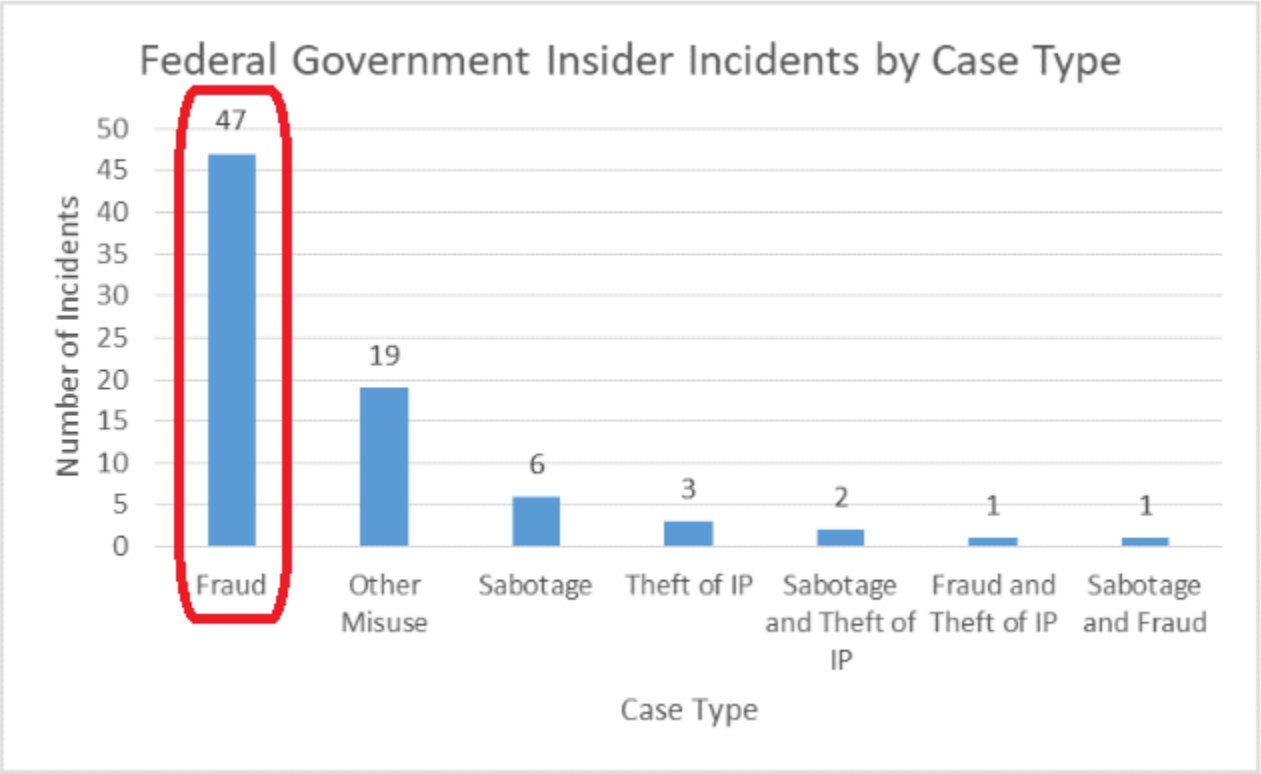
The CERT Insider Threat Centre (NITC) contains over 2,000 insider threat incidents which is used as a foundation for their empirical research and analysis in this article. In total, CERT identified 77 non-espionage insider incidents where a federal government organisation was both the victim organisation and the direct employer. However, there were 34 additional incidents where a federal organisation was impacted by an insider incident at another organisation.

By and large, these were incidents where a federal government organisation had employed a consultant or contractor.



What's interesting is that Insider incidents in the Federal Government rarely include IT Sabotage or Theft of Intellectual Property (IP). Partly because in the US, many of IT Sabotage or Theft of IP incidents are typically considered as national security espionage.

The number one most observed Insider Threat incident with Federal Government was **Fraud** followed by "**Other Misuse**".



Fraud Snapshot Analysis

Around 61% of incidents impacting federal organisations involved Fraud. It included issues of fraud, waste, and mismanagement of federal funds.

- Who?
  - 45.8% of insiders were worked with the organisation for 5 years or more;
  - 69.4% of insiders had an authorised account and data;
  - 89.5% were full time employees;
- What?
  - 52.2% of the targets in Fraud incidents were related to personally identifiable information;
- When?
  - For incidents where attack was known (27), all involved during business hours. Half of these also involved activity outside work hours. No fraud activities were determined that only took place outside of work hours;
- Where?
  - Around 97.6% of incidents took place on site when attack location was known (41);
- Why?

- Around 97.8% committed insider Fraud because their motivation was financial gain.

As mentioned, the second most observed Insider Threat incidents with Federal Government was "**Other Misuse**".

Other Misuse by insiders can be described as those incidents that involve the unauthorised use of organisational devices, networks, and resources that are not better classified as Theft of IP, IT Sabotage, or Fraud. Examples of Other Misuse include the use of organisational resources for personal benefit, to violate the privacy of other individuals (e.g. obtaining access to colleagues' emails without consent or a proper business purpose) or to commit another kind of cyber-related crime (e.g. stalking or purchasing drugs), which in turn violate organisational policies.

Further Analysis

Insiders committing Fraud in federal government tended to be in trusted positions and committed the incident during working hours. The median financial impact was between $75,712 and $317,551 and three fraud incidents had a financial impact greater than $1 million or more.

Final Thoughts

Insiders who commit fraud are usually low-level employees who use authorised access during normal business hours to either steal information or modify information for financial gain. Insider fraud crimes are often long and ongoing and is bad news for the actual organisation.

Stolen information is usually Personable Identifiable Information (PII) such as payroll or other sensitive information which is then sold to outsiders who commit the actual fraud against the organisation.

Perhaps the most notable feature of insider incidents within federal government was how prevalent incidents of Other Misuse. It is most likely, that insiders that committed Other Misuse generally did so in furtherance of an additional crime.

Suggested Mitigation Strategies

- Mitigation protection for fraud related crimes starts with better screening and identification of employees at hiring;

- Some insiders accumulate excessive privileges that enable then to carry out their crime. It is therefore important that you carefully control and audit roles;
- If possible, enforce separation of duties with all of your critical processes;
- A monitoring strategy for fraud should include monitoring access and data modification. May also include frequent random auditing on critical information fields;
- Utilise user activity monitoring solutions to identify online user activities that can be used to detect fraudulent activities;
- Encourage employees to recognise and report on suspicious behaviour including outside facilitations;
- Develop an employee assistance program that includes financial counselling.

How Prevalent Is Insider Threat Within Your Agency?

Every organisation that provides their employees with decision-making authorities gives their employees the power to make decisions that could potentially undermine itself.

Should you trust your colleagues? You hired them! Do you hire trustworthy employees? Probably not!

So, what's missing? What is missing are the number of instances that an employee breaks your organisation trust without your realising it. What is missing is the visibility and understanding of what such employees can potentially do that places your organisation at risk and you are completely blind.

What is within arm's reach of every organisation is bringing the threat down to a manageable level. But to do this, you need to Identify where you currently sit and the level of vulnerability within your organisation.

CommsNet Group **Insider Threat Vulnerability Assessment** helps you to Identify vulnerabilities within your key business systems and process to determine how well prepared you are to prevent, detect, and respond to insider threats. It is there to assist you in reducing exposure to damage from potential insider threats. To find out more, get in touch with CommsNet Group.

Contact Us

if you need some more resource material, download the Insider Threat eBook by CommsNet Group, completely free of charge. For more information, you can also send them an email at: info@commsnet.com.au OR give us a call at: +61 26282-5554.