Snapshot of INSIDER THREATS Within The Information Technology Sector

As we know, Insider Threat affects both the public and private organisations. Insider threats are one of the biggest security challenges to any business especially those that are in the Information technology sector (software; web developers; telecommunications; IT providers; data processing; hosting).

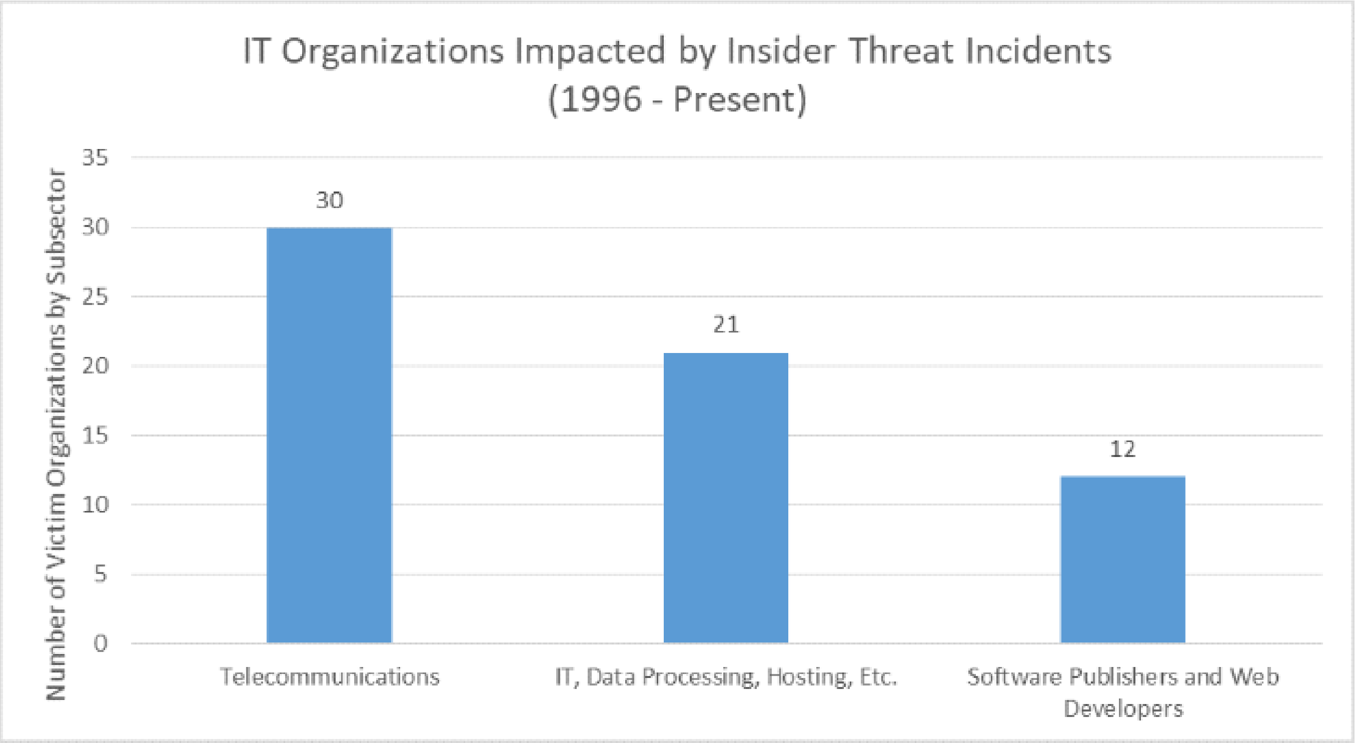
It is important to realise that this industry typically employs a great deal of technology skilled and expertise people. Predominantly, these people have higher level of system privileges, access, and technical knowhow and can easily conceal malicious activity.

Some Insider Threat Examples

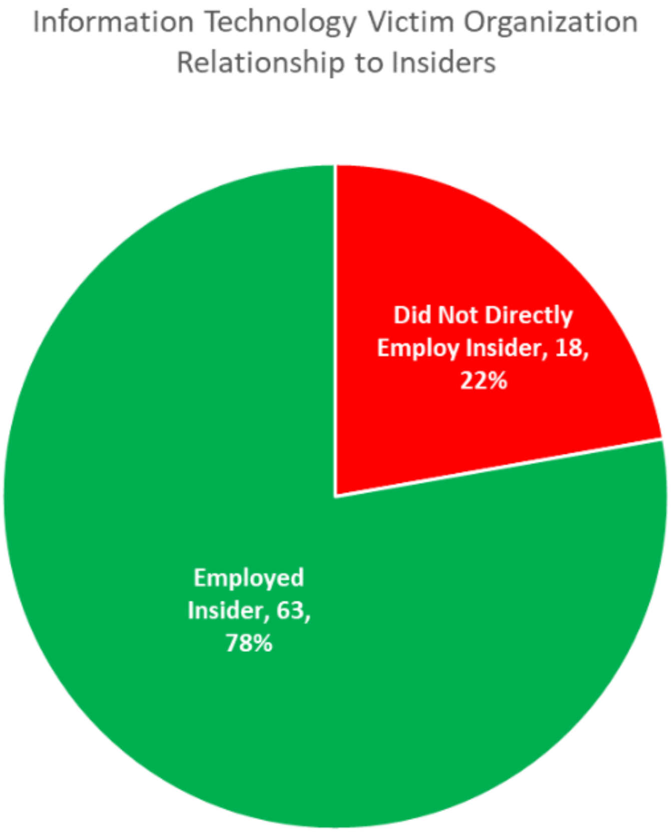
- In January 2019, a Chinese Apple employee was charged for stealing Apple's autonomous car secrets. The individual is accused of possessing confidential Apple manuals, schematics, diagrams, and photographs, including images snapped inside an Apple building, and "an assembly drawing of an Apple-designed wiring harness for an autonomous vehicle;
- In May 2016, Telstra (Australian largest telecommunication provider) sacks The Chief Technology Officer (CTO) after they discovered that he faked his resume and plagiarised material in presentations. He worked for Telstra for nearly two years;
- In 2014, AT&T had to pay a hefty fine of $25 million as some of its employees that were based in Mexico, Columbia and the Philippines accessed personally identifiable information from its 278,000 customer accounts without authorisation and then provided it to third parties;
- In September 2013, Vodafone Germany confirms insider theft of two million of its customer data. According to Vodafone, this attack was highly complex and conducted with inside knowledge of their most secure internal systems.

Overview of Insider Threats Within The Information Technology Sector

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 60 incidents in Information Technology, with 63 victim organisations came from the Telecommunications organisations that accounted for majority of insider threats.



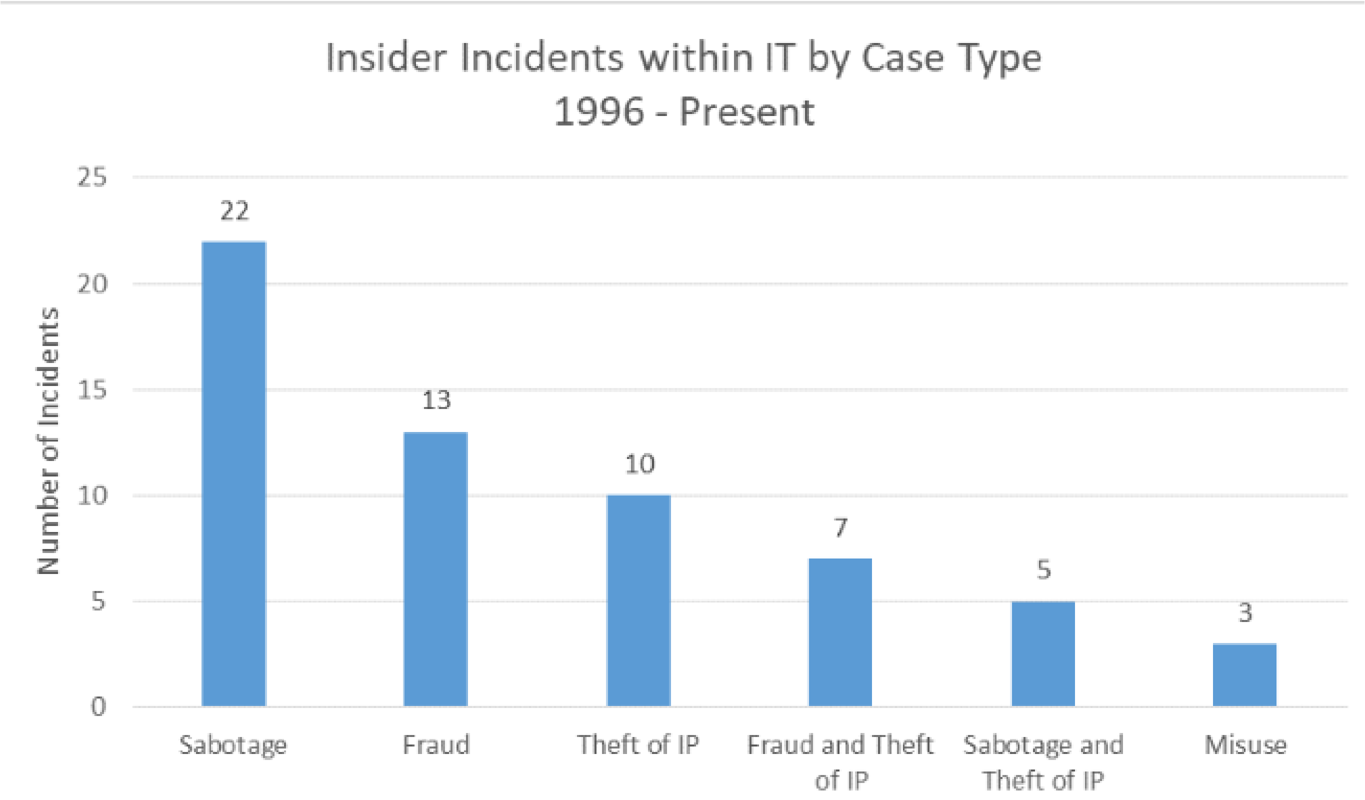
Of the 60 IT insider incidents, CERT identified 81 organisations impacted by those incidents, of which 63 (78%) organisations were both the direct victim and the direct employer of the insider.



The remaining 18 (22%) organisations involved trusted business partner relationships in which an insider was a contractor or had non-regular full-time employment with the victim organisation,

As the chart below shows that Sabotage is the most frequent insider threat incident type accounting for about 36.676% of all incidents followed closely by Fraud (21.67%) and Theft of IP (16.67%).

Cases for Insider Sabotage are crimes that are typically committed by technically sophisticated people such as system administrators, developers, and programmers that use the same type of online actions that typically are being used by those same employees or contractors in the course of their normal activity.



Insider Sabotage Incidents

- **Who?**
    - 80% of insiders were full time employees while employed at the victim organisation;
    - 20% of insiders were former employees who still had access and 15% of them had administrator or root privileges;
    - Most insiders occupied system administrator positions (31.8%)
- **What?**
    - More than 60.7% of the targets in sabotage incidents were network or systems;
    - Around 10.7% insiders deleted, modified, copied or hid customer data;
- **When?**
    - For the attacks that were known, 50% of incidents involve malicious activity taking place only outside of work hours;
- **Where?**
    - Insider sabotage were primarily committing using some type of remote access (81%);
- **How?**
    - Since most of the insiders have technical knowledge, some insider sabotage backups (17.6%), created an unauthorised account (17.6%), used a keystroke logger (5.9%);
    - Interestingly, almost 30% of insiders abused their privileges access or modified critical data;
- **Why?**
    - The motive for the insider to commit insider sabotage within the information technology sector is usually seeking revenge;

Suggested Mitigation Strategies

Recall that the majority if insiders that commit insider sabotage held technical positions such as system administrators, DBA, programmers or developers. They have the technical ability and access to perform actions that ordinary users cannot. They can usually conceal their actions, since their privilege access typically provides them the ability to log in as other users, to modify, falsify audit logs and monitor reports.

To better protect your organisations from insider threats incidents, here are some best practices that I suggest that you adopt:

- Mitigation protection starts with better screening and identification of employees at hiring, including discussions with prior employers regarding the individual's competence and approach to dealing with work;
- Clearly communicate and consistently enforce responsibilities and constraints of your employees and consequences for violations. When employees see inconsistent enforcement, it quikcly leads to animosity within the workplace;
- Often the sign of a disgruntled employees is the onset of concerning behaviour within the workplace. Supervisors and managers must recognise and respond to inappropriate concerning behaviours;
- Management and executives should focus on identifying their highest-priority assets and implementing prioritised alerting when changes to those assets occur;
- Utilise user activity monitoring solutions to identify online user activities that can be used to detect unauthorised activities;
- Pay careful attention to when events such as demotions or terminations may cause increase disgruntlement, so organisations should follow a careful and consistent approach;
- Effective backup and recovery processes needs to be in place and operational. Any compromise, business operations can be sustained with minimal interruptions; Apply the 2-person rule for protecting the backup process and physical media so that one person cannot take action without the knowledge and approval of another employee;
- Encourage employees to recognise and report on suspicious behaviour including outside facilitations;
- Develop an employee assistance program that includes financial counselling.

Insider Threat Book

Have you read our latest Insider Threat Book titled "***Protecting Your Business From Insider Threats in 7 Effective Steps***?" If you haven't, you can download the Insider Threat eBook at CommsNet Group website, 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.

Other Insider Threat Industry Articles

- Snapshot Of Insider Threats Within The Finance Sector
- Snapshot Of Insider Threats Within The Government
- Snapshot of Insider Threats Within The healthcare Sector