Snapshot of Insider Threats Within Finance And Insurance Sector

As we know, Insider Threat affects both the public and private organisations. Insider threats are one of the biggest security challenges that Financial and Insurance entities face.

The sheer confidential, sensitive and highly valuable information that such organisation possess, makes it easy for a clumsy or a malicious insider to compromise security and potentially cause massive harm.

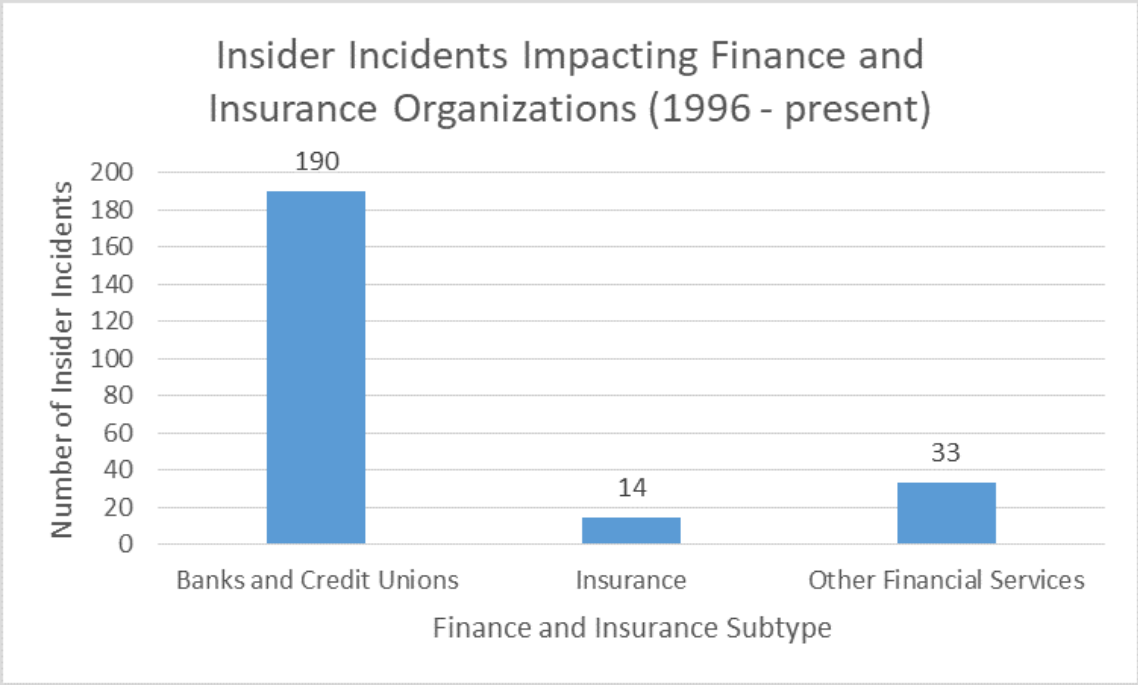
Here are some examples:

- **AMP** – In February 2019, a Chinese contractor for financial services giant AMP was caught stealing confidential data of 20 of its customers;
- **Société General** - One of the largest banks in Europe, was compromised via a rogue employee that had executed a series of "elaborate, fictitious transactions" that cost the company more than $7 billion, the biggest loss ever recorded in the financial industry by a single trader;

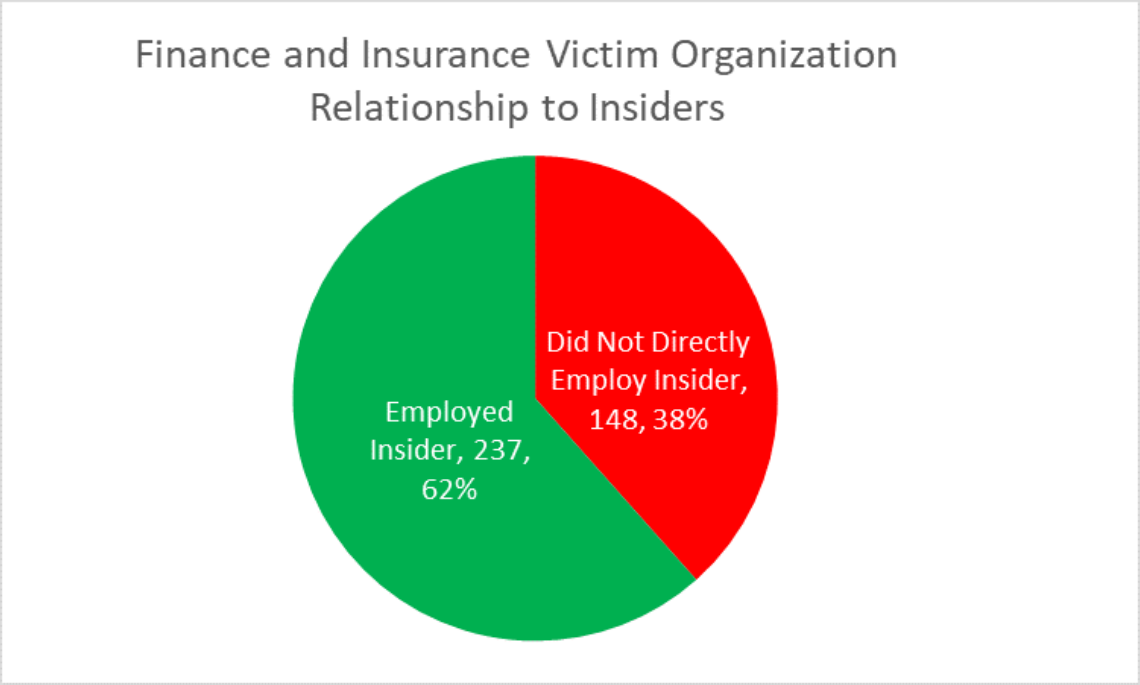
- **Sage** – In August 2016, Sage a UK company of accounting and payroll software was on the receiving end of a data theft between 200 and 300 business clients;
- **Wells Fargo** - In September 2016, federal bank regulators imposed a fine of $185 million on Wells Fargo for allegedly creating millions of accounts on behalf of customers. As a result, millions of Wells Fargo customers had credit card, checking, and other accounts without even knowing about them. The episode led to the firing of more than 5,000 bank employees, and then-CEO John Stumpf ended up giving up substantial portions of his pay and leaving the company in October; And
- **Enron & Arthur Anderson** - Enron Corp reached dramatic heights, only to face a dizzying fall. The executives of Enron defrauded the company by hiding its mountains of debt and toxic assets. Arthur Anderson, as one of the five largest accounting firms in the United States offered a stamp of approval, signing off on the corporate report for years. Its collapse affected thousands of employees and shook Wall Street to its core.

Overview of Insider Threats Within The Financial And Insurance 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 237 non-espionage insider incidents where a Finance and Insurance organisation were both the victim organisation and the direct employer.

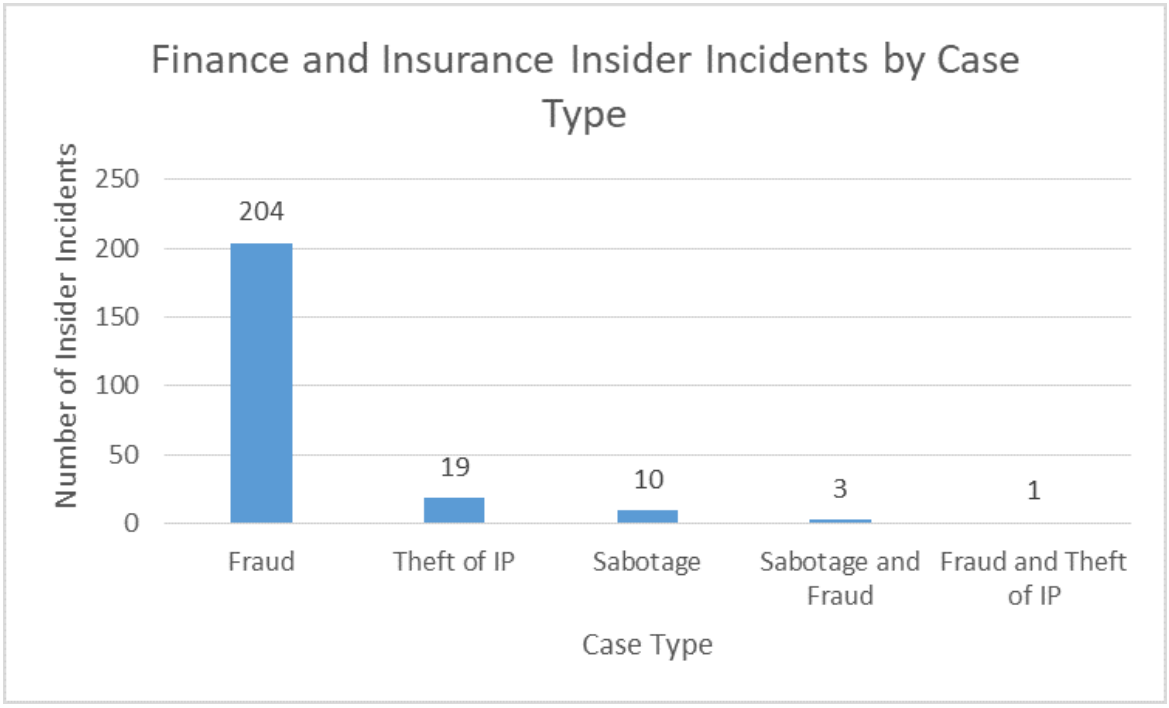


However, there were 148 additional incidents where a Finance and Insurance organisation was impacted by a Trusted Business Partner or an insider at another organisation.



What's interesting is that Insider threat incidents in the Financial & Insurance sector had a great deal of collusion with outsiders.

As the chart below shows that Fraud is the most frequent insider threat incident type followed by Theft of Intellectual Property and IT Sabotage. Nearly all (87.8%) of the insider incidents impacting Finance and Insurance organisations involved Fraud.



Insider Fraud Incidents

- **Who?**
    - 49.5% of insiders that worked with the organisation for 5 years or more;
    - Around 97.1% of insiders were full time employees;
    - Around 93.4% were current employees;
    - 50% had an authorised account;
    - Around 26.4% had privilege access;
    - The most common role was management 32.8%, followed by cashier (13.8%), executive (12.6%) and other non-technical (29.9%);
- **What?**
    - Around 40.7% of the insider targets were related to money in an electrical form; Around 5.4% targeted money in physical form;
    - In addition, 5.4% of insiders targeted electronic customer data which in turn can be used to commit identity theft;
- **When?**
    - For incidents where attack was known, around 98.3% involved insider activity during business hours. Around 31.8% of incidents also involved outside work hours;
- **Where?**
    - Around 99.5% of incidents took place on site when attack location was known;
    - In addition, 27% of incidents involved remote access;
- **How?**
    - Around 32.8% of insiders created or used a fraudulent asset to commit their attack and 25% of insiders created or used an alias over the course of their fraud scheme;
    - 24.5% of insiders made a fraudulent purchase;
    - 20.6% of insiders also abused privilege access and 20.1% falsified information;

    - 16.2% modified critical data;

- **Why?**
    - Around 97.8% committed insider Fraud because their motivation was financial gain. Insiders were also motivated by gambling addiction (2.2%, family pressure (1.6%), competitive business advantage (1.1%), or a desire for recognition (1.1%)

Further Analysis

Insiders committing Fraud in Finance and Insurance sector tended to be more tenured employees and many were in management position. These insiders also had privileged access to information systems and customer personally identifiable information (PII) commensurate with that level of experience or role.

These insiders exploited vulnerabilities in processes they were familiar with to access money or customer data. Nearly all of the insiders were motivated purely by financial gain.

The median financial impact according to CERT was between $98,137 and $268,403.

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 Organisation?

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 user risk within your organisation.

CommsNet Group **Internal User Risk Assessment will** help you to bring forwards unique visibility into your organisation user activities and associated risky behaviour than any other assessment. You may be surprised what you may find out about your organisation – Anything from theft of confidential and proprietary data to use of hacking tools and pirated applications.

To get started, reach out to us on info@commsnet.com.au OR give us a call at: +61 26282-5554

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.

Insider Threat Workshop

Interested in attending an Insider Threat workshop? If so, register your details at CommsNet Group Insider-Threat-Workshop, so that we can let you know when our next scheduled course will take place.

For more information regarding Insider Threats, you can reach us at

- Email: info@commsnet.com.au OR
- Phone: +61 26282-5554.