Snapshot of INSIDER THREATS Within The Healthcare Sector

As we know, Insider Threat affects both the public and private organisations. Insider threats are one of the biggest security challenges that the Healthcare industry faces. In fact, in a recent Forbes article, it indicated that 58% of healthcare systems breach attempts involve inside actors, which makes this the leading industry for insider threats today.

One of the most compelling insights is how quickly healthcare is becoming a digitally driven business with strong growth potential. However, what's holding its growth

back, is how porous healthcare digital security is. Not to mention the sheer confidential, sensitive and highly valuable information that these organisations possess, makes it easy for a clumsy or a malicious insider to compromise security and potentially cause massive harm.

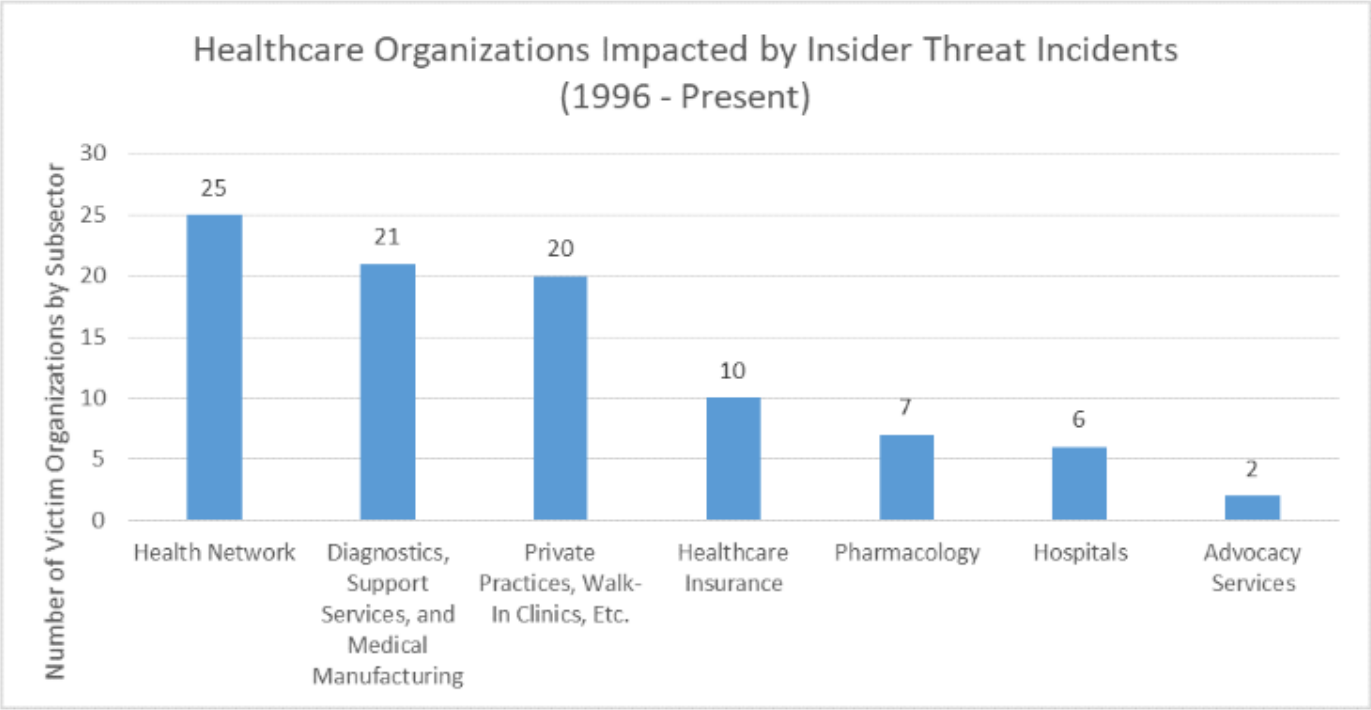
Forbes went on to say that around 66% of internal and external actors are abusing privileged access credentials to access databases and exfiltrate proprietary information.

Insider Threat Example

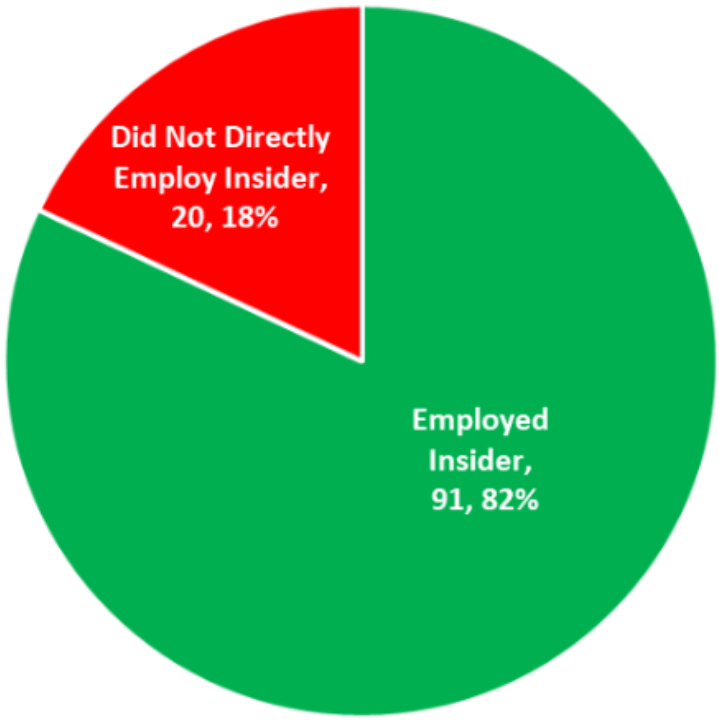
A former Dallas Hospital guard built a botnet, using the hospital network, to attack rival hacking groups. The individual was eventually caught after he filmed himself staging an "infiltration" of the hospital network and then posted it on YouTube for public viewing. The video clearly shows the individual using a specific key to "infiltrate" the hospital, which revealed his identity as Jesse McGraw, a night security guard of the building. The investigation revealed that McGraw had downloaded malware on dozens of machines, including nursing stations with patient records. Additionally, he installed a backdoor in the HVAC unit, which, if failed, would have caused damage to drugs and medicines and affected hospital patients during the hot Texas summer. McGraw pled guilty to computer tampering charges and is serving a 9-year sentence in addition to paying $31,000 in fines.

Overview of Insider Threats Within The Healthcare Sector

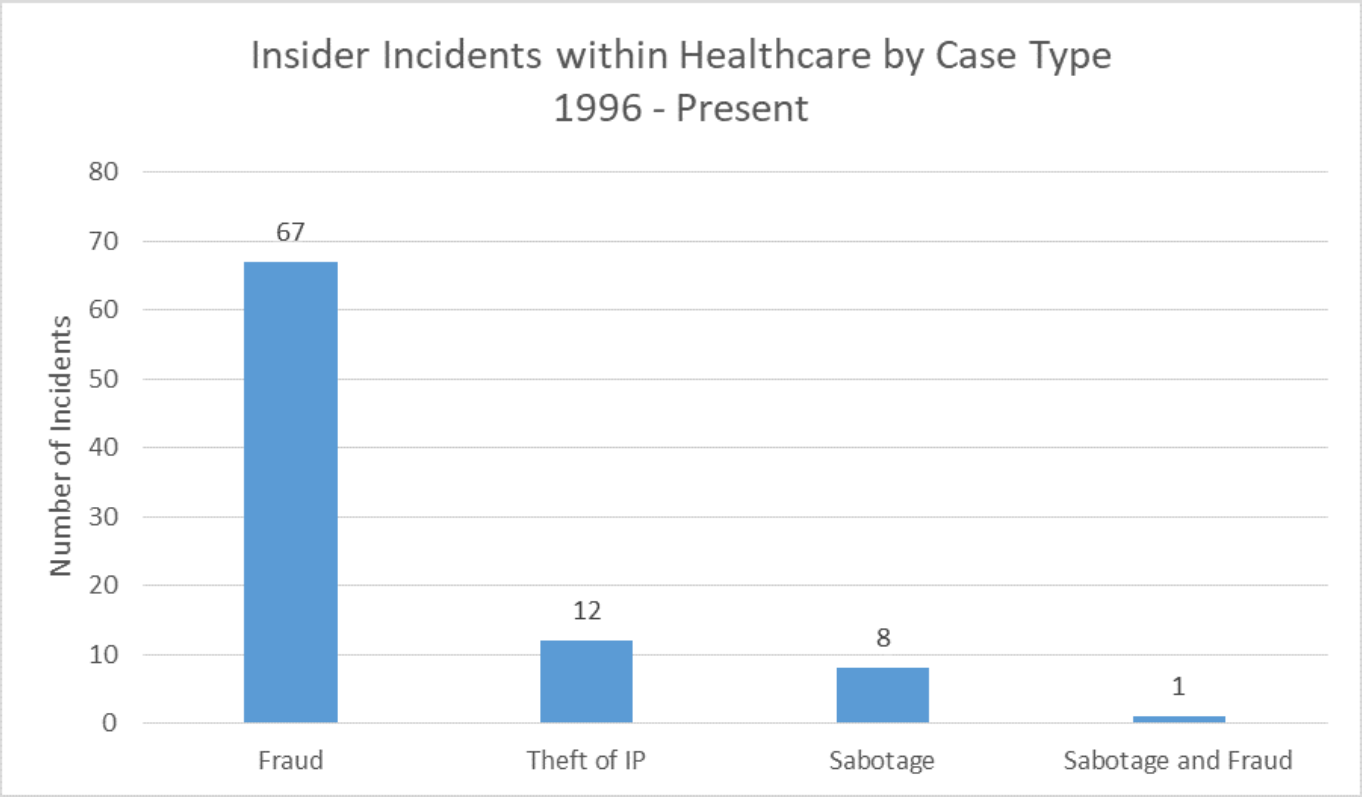
The CERT Insider Threat Centre (NITC) contains over 2,000 insider threat incidents which is used as a foundation for their empirical research and analysis in this article. In total, CERT identified 88 malicious insider incidents mapped to 91 healthcare organisations that were directly victimised in the attack. Of the victim organisations, Health Network make up the largest subsector. These are the networks of hospitals and medical centres that are dedicated in bringing healthcare to specific regions.



Interestingly, 20 victim organisations indirectly employed the insider in some sort of trusted business partner relationship or non-regular full-time employment (e.g. contractors).



As the chart below shows that Fraud is the most frequent insider threat incident type accounting for about 76% of all incidents. Within these fraud cases, we generally see individuals with access to patient payment records taking advantage of their access to customer/patient data to create fraudulent assets such as credit cards in order to make a profit.



Insider Fraud Incidents

- **Who?**
  - 64.3% of the healthcare fraudsters began their malicious activities within their first five year of working for the organisation;
  - 72.8% misused their authorised access (e.g. Privilege account or PII data access);
- **What?**
  - Around 52.7% of fraud incidents within the healthcare sector involved the theft of customer data;
  - Around 37.5% of incidents directly targeted financial assets;
  - Around 94.9% of personal identifiable information (PII) that was stolen, was customer data;

- **When?**
  - For incidents where attack was known, around 70% involved insider activity during business hours. The other 30% of incidents took place both during work hours and outside work hours;
- **Where?**
  - Around 72.7% of incidents took place on site when attack location was known;
  - Around 23.6% involved both onsite and remote activity;
- **How?**
  - Most incidents used rudimentary techniques.
    - 25.8% of insider incidents either received and/or
    - 24.2 transferred funds and/or abused privileges;
  - Around 36.4% the insider tried to conceal their activity in some manner such as modifying the log files, using a compromised account or creating an alias;
- **Why?**
  - Around 84.8% committed insider Fraud because their motivation was financial gain.

Suggested Mitigation Strategies

Healthcare information security should be the outmost importance for the organisation. Although identity theft is the most common misuse of patient data, patients can face severe, permanent consequences from medical record misuse, alteration, or destruction.

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

- 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.

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

References

- Forbes Article - 58% Of All Healthcare Breaches Are Initiated By Insiders