Insider Risk in Telecommunications

"People leverage their cellphones like they're magic. They don't think about the fact that there's this whole infrastructure that makes it work ... and that infrastructure is not something that you can take for granted." Adam Meyers, CrowdStrike's senior vice president of intelligence

Why are telecommunication companies affected by insider risk?

Because they have extensive information on their customers, including personal and even financial data as well as online behaviour information based on communication patterns.

Telecom insiders are often cellular and internet service provider employees. In many cases, insiders are used to deliver subscriber and company data. Such insiders can remotely reroute, intercept, and manipulate incoming calls and messages of customers. This increases the probability for a wide array of insider acts such as SIM card duplication/illegal reissuing, network mapping and man-in-the-middle attacks.

External actors are increasingly attracted to insiders for a variety of reasons:

- Employees in the telephony and internet industries are the most affected by human errors
- Employees already have authorised access to critical telecom data and networks
- Employees know how the company's network device function and can easily identify vulnerabilities
- Employees may know about security measures and how to circumvent them

Sign post Six
WHERE PSYCHOLOGY MEETS TECHNOLOGY

26%

of insider incidents are caused by

intentional insiders

who have/had authorised access to sensitive company information and intentionally exceed or misuses that access in a manner that negatively affects the organisation.

56%

of insider incidents are caused by

unintentional insiders

who have/had authorised access to sensitive company information and accidentally affected the organisation in a negative way, possibly by being tricked by an outsider's use of social engineering.

Impact

Companies can face costs* up to

$121k for unintentional insider incidents,

$2.5M for intentional insider incidents and

$3.4M for social engineering attacks.

***Reputational damage, business disruption or decreased trust of investors** are additional consequences that companies have to carry.

A holistic approach

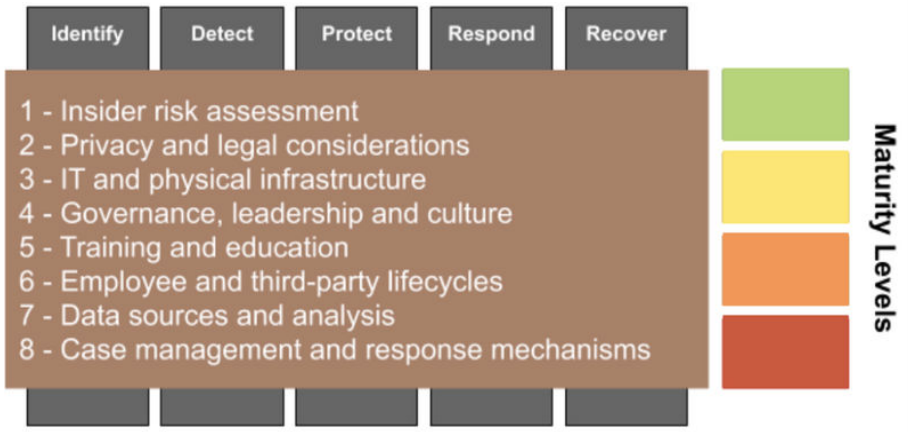
Insider risk is about people. Historically, organisations have mainly focused on external security mechanisms such as (fire)walls, intrusion detection systems, and (electronic) building access systems. However, while organisations have made external attacks less likely to occur, attackers have continuously been taking the path of the least resistance by increasingly using insiders.

Prevention is key.

Technical cybersecurity solutions often detect anomalies when it is already too late. It takes companies an average of nearly 85 days to contain an insider incident. The costs for countermeasures are rising. It's becoming increasingly hard for organisations to get critical data back or prevent its distribution. Companies should move from short-term response to long-term integration of prevention and detection measures.

Tools alone cannot provide a solution. Insider risk management requires a holistic approach.

Signpost Six supports organisations in assessing the risks, closing countermeasure gaps and delivering communications and training as part of the insider risk management journey within your organisation, while also keeping a focus on the duty of care for your personnel.



SIM SWAP Fraud

Former Verizon employee, Stephen DeFiore, accepted multiple bribes in order to perform SIM swaps. A co-conspirator sent DeFiore customers phone numbers, four-digit PINs, and SIM card numbers to which numbers were to be swapped. DeFiore received approximately $2,325 in a series of twelve payments. A SIM Swap scam is a cellular phone account takeover fraud with the intention of routing a victim's incoming calls and text messages to a different phone. Once this swap is made, a victim's personal accounts, including email accounts, bank accounts, and cryptocurrency accounts become easily accessible.

verizon

AT&T 7-year Scheme

In 2019, Muhammad Fahd was accused of bribing AT&T call-center employees by persuading them to install malware and unauthorised hardware as part of a scheme to fraudulently unlock around 2 million cell phones. The scheme began back in 2012, when he conspired to recruit employees through Facebook. AT&T insiders are believed to have received more than $1 million in bribes and the overall scheme resulted in more than $200M of losses.

AT&T

Signpost Six
WHERE PSYCHOLOGY MEETS TECHNOLOGY

Signpost Six
Koninginnegracht 62
2514 AG The Hague
The Netherlands
+31 70 22 11 940

www.signpostsix.com
info@signpostsix.com
Signpost Six
@SignpostSix