OVERVIEW

A Breach in Trust

Malicious insider data breaches occur when trusted affiliates abuse their permissions to steal from an organization they are a part of. This is a separate category of incident because threat modeling assumes that the internal actor will circumvent different layered controls to achieve their objectives.

A recent study conducted by the Ponemon Institute found that approximately one quarter of insider incidents were considered "criminal and malicious" but the average number of such incidents per company was on the rise: from 3 per company in FY2016, to 5.4 in FY2019. For reference, the rates for insider incidents due to negligence were approximately triple these frequencies, and also on the rise.

One example of a malicious insider data breach occurred in 2019 at the Desjardins Group, a Canadian financial institution. An employee allegedly collected internal records on over 2.7 million individuals and shared them with a third-party. The employee did so by gaining the trust of his colleagues and abusing that trust to get around controls. This also points to the levels of data third-party providers can have, that internal employees may not.

BEST PRACTICE

Malicious Insider Resulting in Data Breach

Resilience's Cyber Meteorology Framework models cyber risk trends and helps companies stay up-to-date with current best practices and mitigation guidance. Resilience's model for a data breach caused by a malicious insider recommend that organizations do the following to prevent and mitigate these attacks:

- Maintain appropriate permissions for enterprise network users, develop procedures to periodically audit and revoke permissions as necessary
- Employ user behavior analytics (UBA), endpoint detection and response (EDR), and network monitoring software
- Conduct periodic Cybersecurity awareness training, including that of insider threats

INSURANCE

Breach of Privacy

Disgruntled and enticed insiders are a constant threat for any business. Insurance should provide coverage for cyber events if they begin from attacks or are caused by malicious insiders. Ask your broker to

learn more.

Example Claim

Criminals have used social media to target people who might be enticed to commit fraud on their behalf. HR, payroll, technical, financial administrative, call center employees all have regular access to money or sensitive data. Professionals who are passed up for a promotion, given a negative review, or are terminated may retaliate on the way out by shutting down protections, leaving back doors, or otherwise creating vulnerabilities.