1.

**Indicators of Intentional Breach (Malicious Insider):**

* **Unusual Behavior from Privileged Accounts**: Anomalies in the behavior of a privileged user account can indicate a malicious attempt to gain a foothold into a company's network.
* **Unauthorized Access Attempts:** These include insiders trying to access servers and data which are not related to their job functions, logging in at abnormal times or from unusual locations, or logging in from multiple locations in a short time frame.
* **Data Theft and Unauthorized Data Transmission:** This could involve insiders uploading large files to personal cloud applications, downloading large files to external storage devices, or sending large numbers of email messages with attachments outside the company.
* **Economic Espionage**: Stealing sensitive information to sell to a competitor or to harm the organization in other ways.
* **Conflict with Other Employees:** Constant conflict with other employees might indicate a disgruntled employee who could potentially engage in malicious activities.

**Indicators of Accidental Breach (Unintentional Insider):**

* **Human Error:** This encompasses mistakes made due to lack of knowledge or awareness, such as sharing sensitive information inadvertently.
* **Phishing:** Falling victim to phishing attacks, wherein the employee might unintentionally give away sensitive information or credentials.
* **Bad Judgement:** Making decisions that unknowingly put the organization's data at risk, such as using weak passwords or ignoring security protocols.
* **Malware Infection:** Unintentional downloading of malware through actions such as clicking on malicious ads (malvertising) or falling for scareware.
* **Unintentional Data Sharing:** Sharing sensitive data with unauthorized individuals due to lack of understanding of the security protocols.
* **Stolen Credentials:** Using credentials that are unknowingly compromised, leading to unauthorized access to the systems.

Thus, in detecting intentional breaches, we would expect to find evidence of unauthorized access, data theft, configuration changes, and possibly economic espionage. In the case of accidental breaches, we would expect to see evidence of human error, phishing incidents, and malware infections, among others.

Reference:

Eric Hahn (2023, September 7) What Is an Insider Threat? Definition & Examples. <https://www.proofpoint.com/us/threat-reference/insider-threat>

2.

The issue of spying on people through social media is very complicated. In some situations, like when a company is checking if someone is lying about a work injury, it might be considered okay. But, this kind of spying can easily go too far, invading people's privacy and making them feel unsafe. It's important to have clear rules about what is and isn't allowed to protect people's privacy, while also preventing dishonesty and fraud. It's also good to teach people about how their information can be used or misused on social media, so they can protect themselves better.

Reference:

Gerber & Holder Workers’ Compensation Attorneys. (2023, June 27). Workers’ Comp Surveillance Tactics: How to Protect Yourself. <https://www.gerberholderlaw.com/atlanta-workers-compensation/workers-comp-surveillance/>

Response 1:

Your discussion presents an in-depth analysis of data breaches focusing on intentional and Unintentional breaches, indicators of purposeful breaches, and the challenges of proving intent. The information is given clearly, describes the characteristics and potential consequences of each type of breach based on data and statistics from IBM's 2021 research. It also tells the complexities involved in identifying and proving the intent behind data breaches, emphasizing the necessity of meticulous investigation and legal scrutiny.

The second part of the discussion addresses the ethical dilemmas associated with social media investigations, considering both corporate responsibility and individual privacy. The discussion wisely calls for a balance between safeguarding privacy and ensuring accountability, highlighting the importance of consent and transparency in investigations.

Overall, the discussion is insightful and well-articulated, offering a comprehensive overview of the topic at hand. It serves as a good starting point for further exploration and discussion on data breaches and the ethical implications of social media investigations.

Ref:

Indeed Editorial Team. (March, 10,2023). 20 Examples of Conflict of Interest in the Workplace. Indeed.com. <https://www.indeed.com/career-advice/career-development/examples-of-conflict-of-interest>