1.1 Dealing with data breaches

Data breaches are increasingly damaging businesses globally, with significant consequences for financial institutions and telecom companies. A notable example is the October 2020 cyberattack, where hackers exploited 2,000 mobile SIM cards to breach the mobile payment system. This attack targeted Pegasus Technologies, MTN Uganda, Airtel Uganda, and even the Bank of Africa, resulting in UGX 10.5 billion in losses within just two days. This event highlighted the severe vulnerabilities in digital payment systems and the devastating financial impacts of cyberattacks.

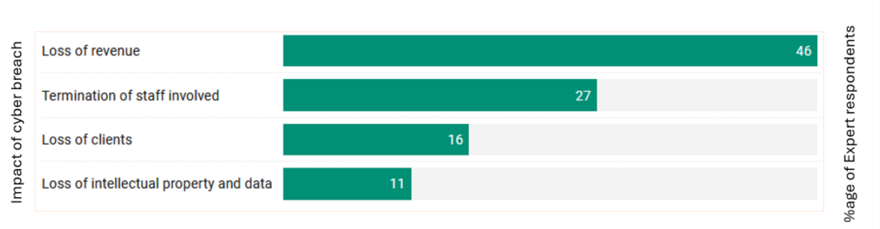
Insights from organizational leaders reveal that data breaches are widespread. Most organizations (74%) have experienced at least one data breach in the past decade. Large institutions, especially in finance and telecom, face even greater risks, with 68% reporting four or more breaches in the last five years. In contrast, smaller organizations, with fewer digital assets and smaller attack surfaces, reported significantly fewer breaches (32%). This disparity illustrates how larger institutions, like high-value targets, attract more sophisticated cybercriminals.

The impact of data breaches extends far beyond financial loss, as illustrated in the chart. Loss of revenue is the most significant repercussion, cited by 46% of respondents. Imagine a pipeline with a breach money flows out as the organization scrambles to stop the leak. Following revenue loss, termination of staff involved ranks second at 27%. This often reflects the fallout from negligence or internal lapses, showing how breaches can upend careers as well as company operations.

Loss of clients, cited by 16%, is another critical impact. Customers lose trust in companies that fail to secure their data, much like a patron abandoning a restaurant after a food safety scandal. Lastly, loss of intellectual property and data, reported by 11%, represents a long-term strategic threat. Intellectual property theft can erode competitive advantage, akin to losing the blueprints to a product that differentiates a company in the market.

Data breaches have both immediate and cascading effects. Organizations must treat cybersecurity not as a back-office function but as a core part of their business strategy. Proactive measures, including incident response plans, regular audits, and continuous employee training, are essential to mitigate these risks. Without such defenses, the consequences can spiral out of control, impacting not just the bottom line but also organizational trust and reputation.

Figure 1: Cyber attacks are more financially motivated acts leading to loss of revenue



iShield 360 experts predict that data breaches will increase, with 17% of financial institutions expected to face a major breach in the next five years. It's no surprise that companies which have already experienced one or more breaches in the past ten years are much more likely to expect another breach within the next three years, compared to those that haven't faced any breaches yet. This highlights the ongoing risk for businesses, especially in the financial sector.

Many companies in Uganda are still in the early stages of creating strong strategies to prevent and respond to data breaches, as well as reduce their impact. Not every business leader fully realizes that even a large company can be crippled by a single cyberattack. To protect themselves, organizations need to build a solid and reliable security structure to achieve true cyber resilience and be better prepared for potential threats. This also speaks to the people factor in organisations.