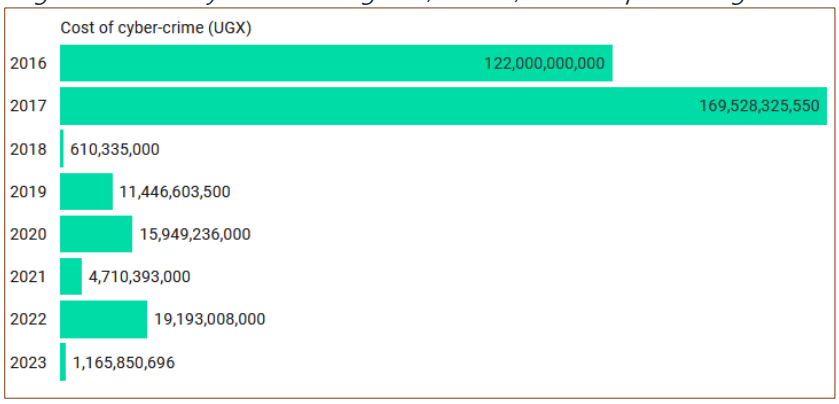
## The cost of cybercrime in Uganda

Unlike other types of crime, the majority of cybercrime incidents in Uganda and the East African Community go unreported, primarily due to the affected entities' efforts to protect their reputations. Often, victims are financial institutions entrusted with safeguarding customer deposits. They are obliged to keep customer data safe.

In 2022 and 2023, the reported annual costs of cybercrime, according to the Uganda Annual Police Report, were UGX19,193,008,000 and UGX1,165,850,696, respectively, see Figure 16.

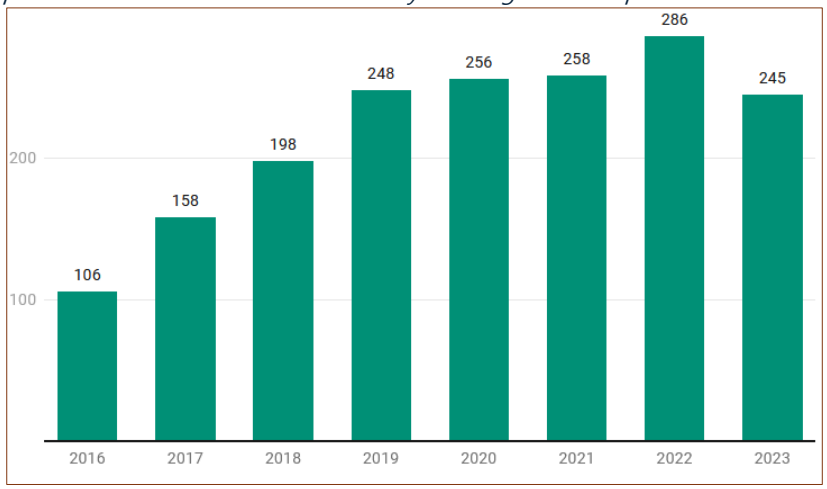
*Figure 1: Cost of cybercrime in Uganda,sSource, annual reports of Uganda Police Force.*




Over the years from 2016, the annual cost of cybercrime in Uganda has been in a steady decline according to the data from the Uganda Police Force annual reports, 2017 experienced the biggest losses. The large amount in 2017 is attributed to a suspected cyber-attack at one of the leading banks in Uganda, affecting many ecosystem players especially aggregators and mobile money agents.

Over the years, cybercrime cases reported to the Uganda Police have been growing in numbers despite the decline in actual amounts involved.

*Figure 2: Reported cyber crimes and losses reduced drastically in 2021 and 2023. Victim organizations prefer to handle the incidents internally for image brand reputation.*

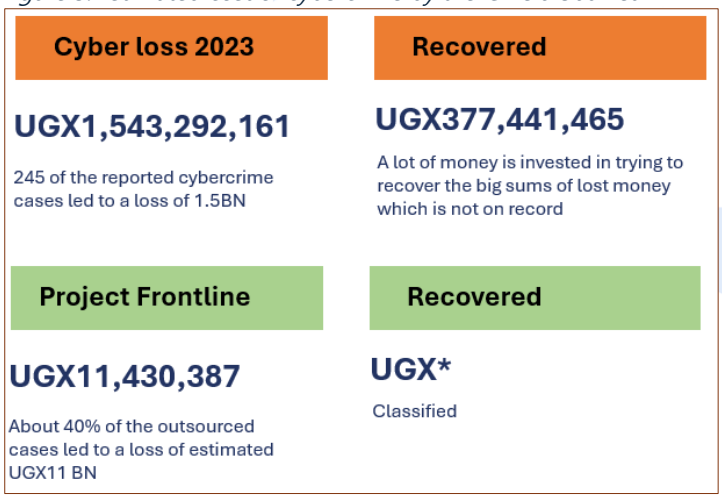


The true cost of cybercrime in Uganda remains elusive. While the Uganda Police Force's 2023 annual report recorded cyber losses of UGX 1.5 billion from 245 reported cases, the iShield 360 Team's findings paint a far graver picture. Our analysis puts losses at UGX 11 billion, highlighting a substantial gap in reported and actual impacts. These are actual cases that have been handled in our

This discrepancy underscores the hidden nature of cybercrime and the difficulty in capturing its full financial toll. The rise in the number of reported incidents signals growing awareness among victims but also points to a larger issue: the increasing sophistication and frequency of cyberattacks targeting organizations across sectors. Interestingly, while reported losses appear to have declined, the scale of damage in unreported or poorly documented cases continues to climb.

Organizations must take proactive measures to close this gap. Strengthening incident reporting, improving forensic readiness, and investing in robust cybersecurity frameworks are critical to understanding and mitigating the true costs of cybercrime. At iShield 360, we remain committed to helping organizations uncover and address these hidden threats, ensuring their defenses match the ever-evolving tactics of malicious actors.

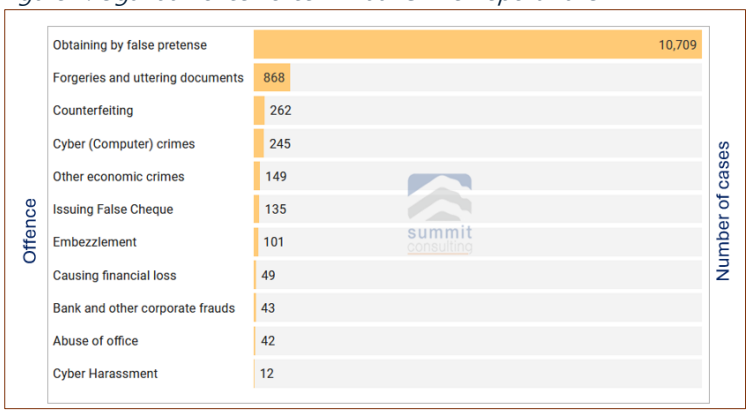
*Figure 3: Estimated cost of cybercrime by the iShield 360 Team*




The Uganda Police report provides critical insights into the state of economic and cyber-related crimes, with obtaining by false pretense topping the list at a staggering 10,709 reported cases. This crime serves as a glaring example of how deceptive practices can exploit weak systems and human vulnerabilities, much like phishing attacks in cybersecurity, where attackers manipulate trust to steal sensitive information.

Following this, forgeries and uttering documents account for 868 cases, a crime that mirrors the cyber realm's struggles with identity theft and counterfeit digital credentials. Forged documents in the physical world are analogous to falsified digital certificates or hacked credentials, which can provide malicious actors with unauthorized access to systems and resources.

*Figure 4: Uganda Police Force Annual Crime Report 2023*




Cyber (computer) crimes, with 245 reported cases, underscore the growing threats in Uganda's digital landscape. Although this number appears relatively low compared to traditional economic crimes, it highlights a critical and evolving issue: cybercriminals are capitalizing on the increasing adoption of digital technologies. Think of cyberattacks as digital termites often unnoticed until the damage becomes extensive.

Interestingly, crimes like embezzlement (101 cases) and causing financial loss (49 cases) are not just financial issues but also cybersecurity risks. For instance, insider threats often leverage weak internal controls, much like embezzlers exploit gaps in financial oversight. Weak access management, similar to leaving cash drawers unlocked, is a common entry point for insider-related cyberattacks.

Bank and other corporate frauds (43 cases) further emphasize vulnerabilities in financial institutions. These crimes often rely on exploiting lapses in transaction monitoring systems, akin to attackers bypassing firewalls and intrusion detection systems to exfiltrate sensitive data. Cyber harassment (12 cases), though fewer in number, reflects the increasing misuse of technology for personal and professional harm. It highlights the need for stronger digital literacy and enforcement mechanisms to curb such misuse.

For cybersecurity leaders, this report is a wake-up call. It underscores the importance of adopting robust preventative measures like multi-factor authentication, regular vulnerability assessments, and employee training to close the gaps that cybercriminals exploit. Just as physical security relies on vigilant guards, cybersecurity demands constant monitoring and proactive defense. The numbers may appear disparate, but they collectively point to one conclusion: Uganda's threat landscape is evolving, and organizations must prepare for an increasingly complex battlefield.

## 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.

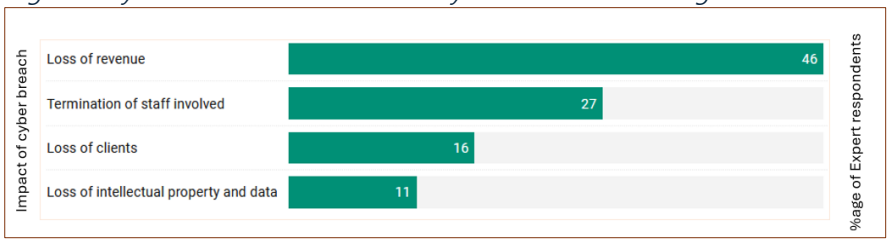
Insights from organizational leaders reveal that data breaches are widespread. Most organizations (74%) have experienced at least one data breach in the past decade. Large institutions, especially in finance and telecom, face even greater risks, with 68% reporting four or more breaches in the last five 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 5: 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.

summit