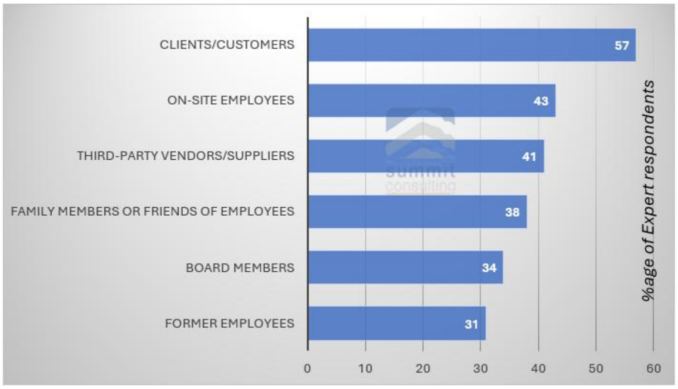
## 1.1 The target of data breaches

During one of our board-level presentations in August 2024, a financial institutions Director asked, "You are the experts. How do the attackers identify their targets and exploit them?" The truth is that cybercriminals are highly organized. They take time to study their target and find the most effective way to strike. Our research shows that clients and customers are often at the top of the target list by hackers. This highlights the fact that vulnerabilities in a company's network can easily spread beyond its direct control. It also points to the need for businesses to recognize that some employees, due to their job roles, visibility, or access to sensitive data, are more likely to be targeted by attackers than others.

A high-profile employee is more likely to be targeted by advanced malware attacks, while someone with access to the CEO may face phishing attacks that impersonate the CEO or other executives. Assessing an employee's vulnerability involves looking at several factors: the cloud apps they use, the number and type of devices they have, their level of access to sensitive information, their interests and how often they are targeted, and whether they follow good digital security practices. These factors help determine how exposed an employee might be to cyber threats.

*Figure 1: Customers remain a top target. Companies need to understand the degree to which some employees, because of their visibility, work routine or level of data privilege may be more vulnerable to attacks than others*



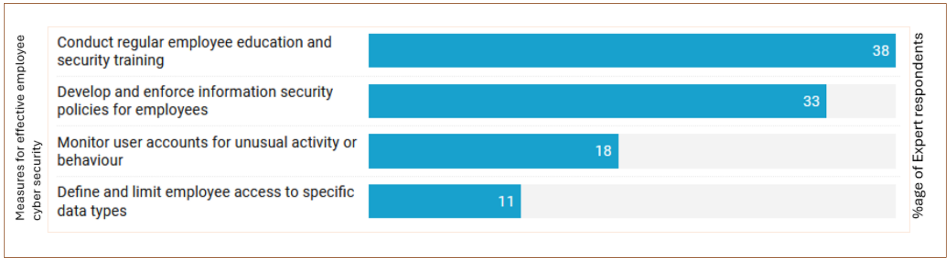
## 1.2 Addressing data breaches

Reducing the risk of a major data breach is now a top priority for most companies in Uganda, as cybersecurity has become a key topic in boardrooms and among regulators and industry leaders. This is a positive step, with strong support from the board and executives for efforts to manage cybersecurity risks. Boards must be regularly informed about these risks to stay ahead of potential threats.

How are companies tackling data breaches?

Many start by centralizing their cybersecurity efforts to build a culture of security that includes every employee, every department, and all business operations. This approach ensures that everyone understands the role they play in protecting the company’s networks and sensitive data.

*Figure 2: Ongoing staff training empowers your staff to be responsible when it comes to cybersecurity management starting at the personal level*



For cybersecurity education and training to be effective, it must actively involve employees at every level. It's not just about providing information-it's about raising awareness and giving employees the tools to understand and manage their security risks. This requires regular engagement, such as monthly check-ins with each department, to monitor and reinforce key practices. For example, tracking employee behaviors like whether they are using the correct authentication methods when logging in ensures that everyone is following the necessary security protocols. By staying engaged, organizations can foster a culture of continuous vigilance and responsibility.