You are the strongest link

Description

One of the leading cyber threats to companies today is vulnerabilities in the supply chain, but if we all remain vigilant, there can be no weak link in our chain for criminals to exploit.

Our industry relies on our supply chain – a complex network of third-party vendors, software providers, and data-sharing platforms – that we use to offer our clients the best products and services.

But this means we can be vulnerable to cybercrime somewhere along the way. In addition, the rapid advancement of technology and the proliferation of connected devices mean we must take extra care to keep our company safe.

If our supply chain is breached, it can have severe consequences for AfroCentric, including financial losses through ransomware attacks and fraud, and reputational damage through loss of trust from our clients and stakeholders.

To avoid this, we invest in advanced threat protection measures; ensure that we remain compliant with industry regulations and standards for data protection; and foster a culture of cybersecurity awareness.

Where the risk lies

- Third-party risks: Weak security measures among vendors can expose sensitive data.
- Phishing attacks: Employees targeted with fraudulent emails can inadvertently grant access to malicious cybercriminals.
- Outdated systems: Unpatched software and legacy systems are prime targets for exploitation.
- Insider threats: Both intentional and accidental breaches by employees can compromise our data integrity.

Keep our chain strong

Employees are the first line of defence against cyber threats and we encourage you all to help us keep our company's supply chain safe and strong.

- Recognise phishing attempts: Be cautious of unsolicited emails, especially those requesting sensitive information or containing suspicious links.
- Follow data handling protocols: Ensure that sensitive information is stored and shared securely in line with our company protocols.
- Update passwords regularly: Use strong, unique passwords and enable multi-factor authentication.
- Participate in training: Stay informed about the latest cybersecurity threats and best practices, and complete all your mandatory training on KnowBe4.
- Report potential threats: Immediately notify the IT department of any suspicious activity or potential breaches. You can also report any suspicious emails using the Phish Alert Button (PAB) on your MS Outlook.
- By staying vigilant and proactive, we can protect the sensitive data that our clients entrust us with and maintain our stellar reputation in the industry.

Category

1. Our Knowledge