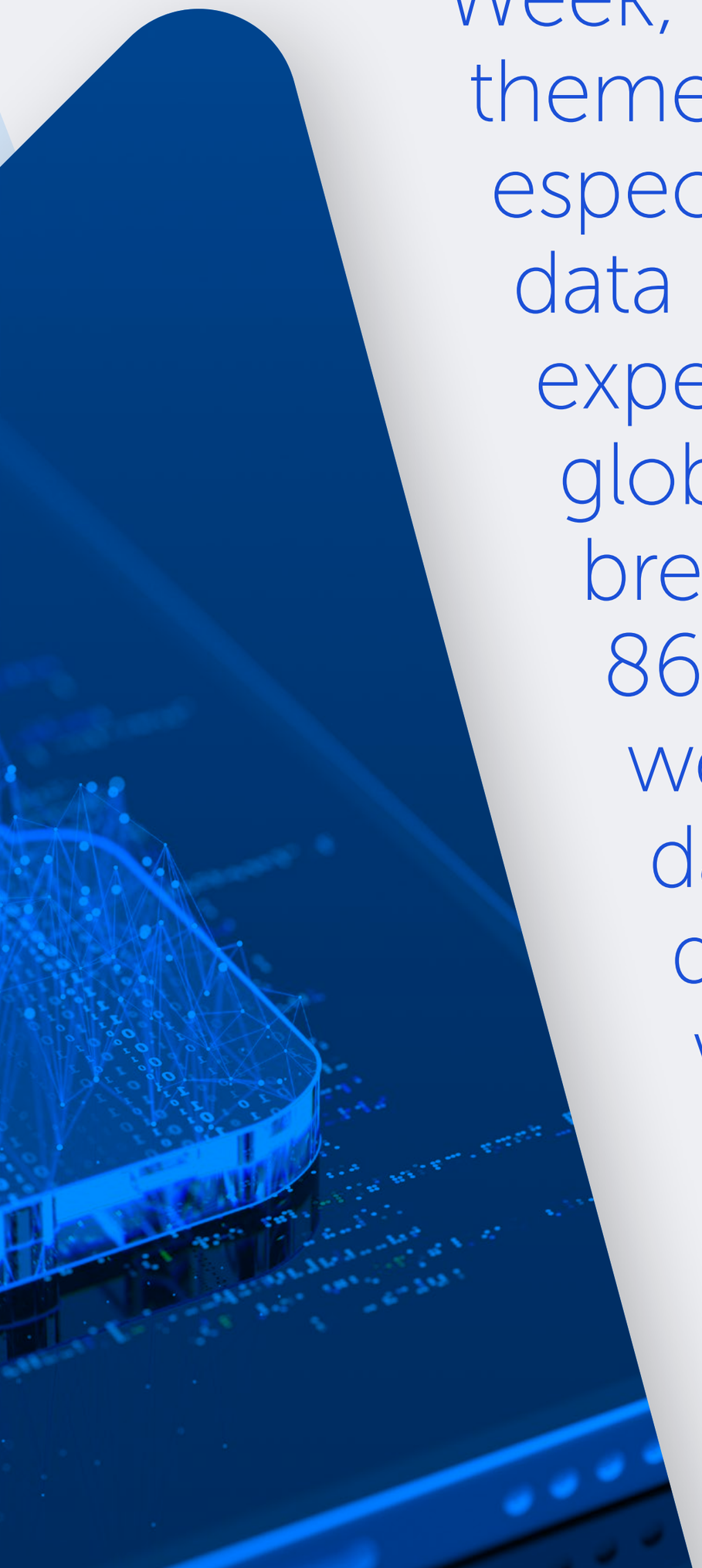
Protect your data:

Essential steps to take after a data breach



As we celebrate Data Privacy Week, it's crucial to remember the theme: take control of your data, especially with the increase in data breaches which are being experienced worldwide. The global average cost of a data breach is USD 4.44 million and 86% of organisations' operations were disrupted as a result of a data breach. It is no longer a question of if an organisation will experience a data breach; it is when this will happen.

Here's what you need to do as an organisation when you experience a cybersecurity incident which has resulted in a data breach.

Notify your cyber insurance provider (if you have one).

Your cyber insurance provider might require you to use specific lawyers or security experts. Stay in close contact with them to make sure you follow your policy and keep your coverage.

Appoint external legal counsel as soon as possible.

Hiring a lawyer early helps protect your communications under legal privilege, which may limit what information needs to be made public. An experienced lawyer can guide you through the process and help you meet your legal duties.

Engage cybersecurity specialists through external legal counsel to investigate the incident.

Security experts can help you get your systems back online. They will find out how the breach happened and provide a confidential, legally privileged report on the incident.

Preserve all evidence and contain the breach.

Keeping all evidence is crucial for defending your business against any legal claims. You also need to contain the breach quickly to minimize damage to your business.

Consider legal advice and consult with your cyber insurance provider before paying any ransom.

Your insurance policy might restrict or prohibit ransom payments, so check with your provider first. Your lawyers can also offer experienced advice on how to handle ransom demands.

Get legal advice to reduce liability and penalties.

Your legal advisors will orchestrate a strategic response to minimise legal, financial, and reputational harm. They will act as your central coordinator, managing everything from regulatory compliance and notifications to evidence preservation and potential litigation.

Assess any regulatory notification requirements.

In South Africa, you generally must notify the Information Regulator within 72 hours of discovering a breach. Depending on your industry, other notifications may be required. For example, insurance companies must notify the FSCA/PA within 24 hours. Incidents that are criminal in nature should be reported to the South African Police Services in terms of the Cybercrimes Act No. 19 of 2020.

Prepare internal and external communications.

Carefully plan all communications with the public and your employees.

Keep a detailed record of all steps taken.

These records might be needed for any investigations that follow the incident.

Review the incident to improve security.

It’s essential to assess your response plan and security measures. This helps prevent future incidents and improves how you handle them if they occur.

Click on the link to access the **Data Privacy Guide**