DATA SECURITY

Why The Responsibility Sits With The C-suite

Protecting Data at Board Level

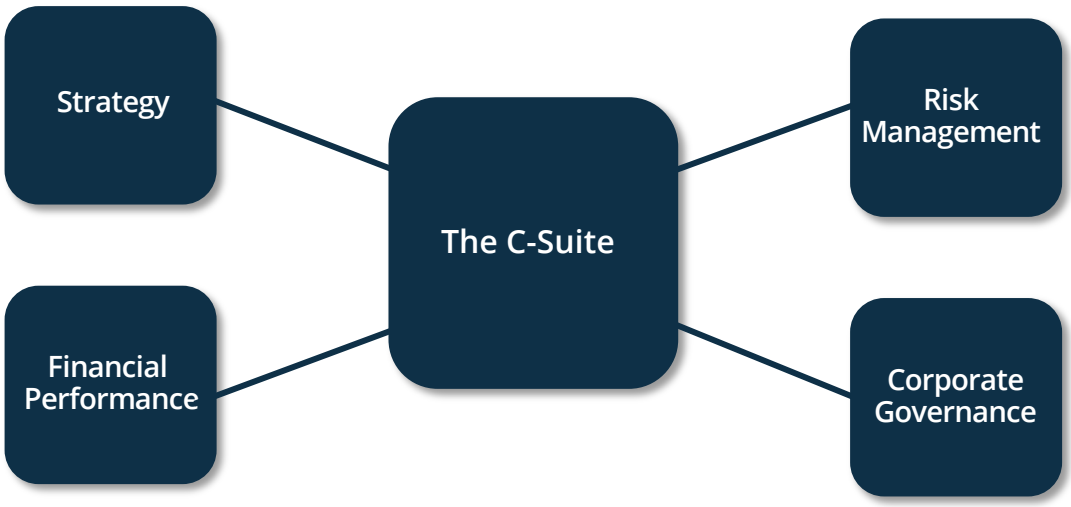
Data has become the most valuable asset for companies of all sizes. By 2023, the big data analytics market is set to reach $103 billion.

The sheer volume of data being generated and stored by businesses has increased exponentially over the past decade, leading to increased risks and vulnerabilities associated with data breaches. According to IBM, the average cost of a data breach in 2020 hit a whopping $3.86 million. This not only impacts a company's finances but also its reputation and customer trust, and can even breach regulatory compliance. Resulting in companies seeking efficient and reliable data security to protect their assets and maintain their operations.

Below, we discuss just why data security needs to be at the top of the C-Suites agenda, the importance from a network and data security perspective and the repercussions of a data breach to the C-Suite and the personal ramifications should a breach occur.

Core Responsibilities of the C-Suite

The C-Suite's responsibility sits further than just overseeing the management and operations of a company, from financial performance to strategic planning, and risk management.



According to the National Association of Corporate Directors, the core responsibilities of the C-Suite can be summarised into the following areas:

- **Strategy:** Developing and approving the company's overall strategic direction and ensuring that it aligns with the company's values and objectives.
- **Financial Performance:** Overseeing the company's financial performance, ensuring that it meets its financial goals and objectives, and maintaining accurate financial records.
- **Risk Management:** Identifying and assessing the risks associated with the company's operations and developing strategies to mitigate those risks.
- **Corporate Governance:** Ensuring that the company adheres to ethical and legal standards, including compliance with regulatory requirements and the protection of shareholder interests.

But how does the management and security of data fall into these responsibilities and why?

Why Data Security Sits at C-Suite Level

A data breach can result in financial losses, damage to the company's reputation, and even legal action, all of which can negatively affect the board's ability to fulfil its responsibilities.

Theft of customer data can have serious consequences not only for the business as a whole but for the individuals responsible for the business. In most recent cases CEOs have received suspended prison sentences and lost their jobs - highlighting just how important data protection is at the board level.

So just how is a C-Suites responsibility affected when a data breach occurs:

Strategy:
A data breach can cause serious disruptions to operations, leading to losses in productivity and revenue. Impacting the company's ability to achieve strategic objectives and in some cases cause complete revisions in strategic direction depending on the data breach's severity.

Financial Performance:
With the average data breach costing millions, significant financial losses are not only at the fee for a breach but cascade to costs of incident response, investigation and further legal fees. These are the short-term affects but in the long-term these losses can continue as businesses experience loss of revenue as productivity has been impacted as well as reductions in customer base and market valve - seriously impacting the C-Suites' financial goals.

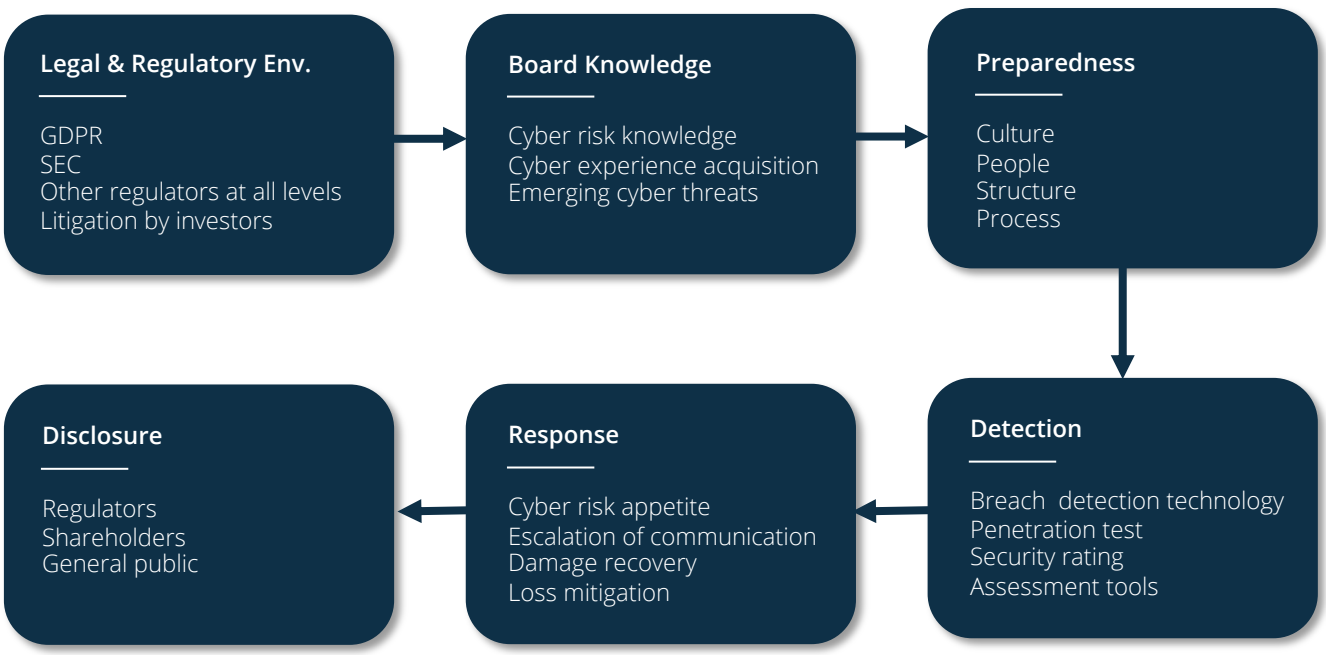
> **Neglecting to safeguard data is equivalent to failing to protect the company, its employees, and shareholder value. Therefore, it is imperative that the C-Suite must understand the significance of data security and the impact it has on their accountability.**
>
> *Paul German – CEO, Certes Networks*

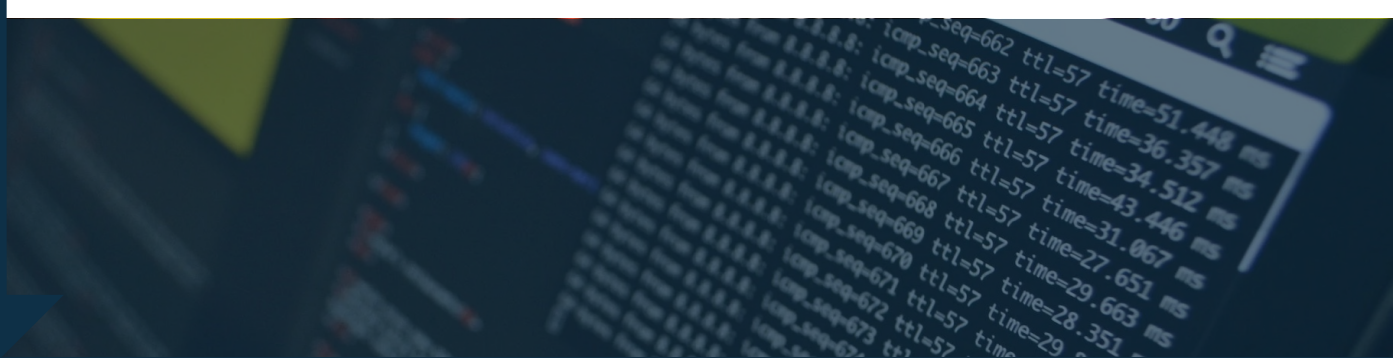
Risk Management:
A data breach exposes the company to regulatory fines and legal action. The board is responsible for identifying and mitigating risks, including the risk of data breaches, to ensure the company's continued success. Holding your data team accountable for breaches is no longer enough to keep protected. Responsibility for your data sits at the top of the funnel.

Corporate Governance:
Any media attention from legal action and regulatory fines, can hugely impact the company's reputation and shareholder value. As well as loss of customer trust and confidence equally furthers revenue instability and market value. Responsibility for ethical and legal standards sits at the C-Suite level, including the protection of customer and shareholder data.

Too many senior leaders are still relying on the network security team to safeguard data. They are not inquiring enough to identify any potential risks to the business, which can be considered reckless. Neglecting to safeguard data is equivalent to failing to protect the company, its employees, and shareholder value. Therefore, it is imperative that the C-Suite must understand the significance of data security and the impact it has on their accountability.

Board Oversight of Cyber Risks





The Solution: Data Protection Across its Entire Journey

Traditionally, when it comes to data management the C-Suite would hire a Chief Risk Manager and a team to manage its data and the responsibility would sit with them and not be classed as a wider business issue. However, CEOs are now personally liable for failing to meet regulations, making data protection a wider business issue that requires a shift in mindset.

A crucial element of data protection sits at keeping data secure across its entire journey, from the source right the way through to its destination. Encrypting the data to keep it protected.

Encrypted security measures can shield the data from unauthorised access, rendering it useless even if a hacker gains access. This means that in the event of a breach, the company will not be held liable for data stolen, fines, reputational damage, or the personal liability of the senior team.

The responsibility of implementing the appropriate security frameworks lies with senior management, who should conduct internal audits to ensure that only authorised individuals have access to the data and that it is unusable to any other unauthorised recipient. Hence, a data-driven approach is crucial for effective security measures and complete protection to the business.

> **Management should be accountable for maintaining strong cyber preparedness, detection, response and disclosure processes. The board should make cybersecurity a top priority and develop its governance framework – not sitting back but leaning in – to add the right insights and ask the right questions.**
>
> *Simon Pamplin – CTO, Certes Networks*

Contact Certes Networks

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

CERTES NETWORKS

Tel: 1 (888) 833-1142
sales@certesnetworks.com

www.certesnetworks.com