The ROI of Doing Nothing

Addressing Data Protection and Personal Liability

The average data breach is estimated to cost $10 million, but the personal cost to senior management can last a lifetime. With news that a Finnish CEO has received a suspended prison sentence following the theft of customer data, C-suites globally need to recognise their personal liability. Data protection is a corporate essential – not just a tech issue that can be handed off to the network security team.

Every single company handles personally identifiable information (PII), from employee records to customer credit card data. This information is increasingly flowing across the world, between cloud servers, emails, laptops and supplier systems – and it is being stolen, again and again because companies are focused on protecting the infrastructure, not safeguarding the data. The cost, to customers, employees, the business and shareholders continues to rise.

The C-suite needs to recognise two key points. Firstly, protecting data is a management responsibility. Secondly, network security alone is not enough. To safeguard the business will require an additional layer of data security. With the risks – and consequences - of breaches continuing to rise, Simon Pamplin, CTO at Certes Networks explains why doing nothing is the most expensive option, personally and professionally.

Personal Liability

Data security has become personal. Not only are companies now liable for the protection of all personally identifiable information (PII) but the C-suite is personally liable for any failures to protect that information. And regulators are becoming increasingly serious about enforcing that liability. In Finland, the CEO of a psychotherapy company has been deemed personally liable for the breach of highly sensitive customer data. Not only did he receive a three-month suspended sentence but he also lost his job. And, in the furore surrounding this breach, the business filed for bankruptcy.

Criminal negligence is a board level issue. From export legislation to ensuring employee health and safety – especially in high-risk occupations – the C-suite is familiar with the concept of personal liability and the risk of a prison sentence. Until recently, however, while regulators globally have had the option to take personal action as a result of a data breach, it has been a threat rather than a reality.

Any C-suite that oversees the loss of PII is in trouble. To the eye-watering regulatory fines, companies are now adding civil lawsuit costs that can more than treble the overall costs. T-Mobile's data breach in 2022 cost the company $350 million – and that's just in customer pay outs. With the additional risk of jail terms, the personal and financial costs of this endemic failure to safeguard data are devastating. Yet how many C-suites can be confident that the current data security posture is adequately robust to avoid such a fate?

Consequences of a data breach

Financial Damage

Reputation Damage

Legal Action

Operational Downtime

Personal Liability

Ask the Question

Too many senior leaders are still relying on the network security team to safeguard data – and failing to ask the right questions to determine whether or not the business is at risk. This is negligent. Failure to safeguard data is both a failure to protect the business – and its employees – and a failure to protect shareholder value.

There is a fundamental misunderstanding of roles and responsibilities. Network security teams are tasked with safeguarding the infrastructure; they have no control over or understanding of the value of data passing across that infrastructure. Moreover, corporate data is no longer contained within a company's physical infrastructure, in its data centres. It is in the cloud, in emails, on laptops, in suppliers' systems, in customers' systems. This is why the regulation is very clearly focused not on the infrastructure but on the data. A security breach only leads to a contravention of the specific local regulation if the PII is visible to – and hence available to use and misuse by – a bad actor.

This is why asking a network security officer if the data is secure is passing the buck, leaving the business at serious risk and compromising the personal and professional future of the C-suite. The question boards need to ask is: "When (not if) our systems are breached can the data be read and/ or used?".

Lost in Translation

It is too easy to assume the network security and IT teams are complying with the processes, governance and framework laid out by the Chief Data Officer or Chief Compliance Officer. Frequently, the individuals tasked with implementation do not understand the implications of their technical decisions, embarking upon workarounds that fundamentally compromise the organisation's regulatory compliance. The C-suite only discovers that key steps haven't been followed and the extent of the corporate – and personally liability – when a breach occurs.

For example, the US Criminal Justice Information Services (CJIS) security policy demands any criminal justice information moving across an environment from one location to another has to be secured with FIPS140-2 certified encryption. Irrespective of whether the agency owns the infrastructure the data is travelling across or the quantity of information, it has to be secured. Yet multiple agencies have failed their audit because they believed that securing the perimeter with a firewall was adequate to secure that data. It wasn't.

GDPR requirements lead to similar misunderstandings. Under the regulation, any business handling PII has to ensure there is justification for handling the data and that data is rendered unintelligible to anyone who isn't authorised. The network security response to that requirement is to secure the network using a firewall – but that does not safeguard the data. If a breach occurs (and more than 4,100 publicly disclosed data breaches occurred in 2022, equating to approximately 22 billion records being exposed) the integrity of the data will be compromised. The business is contravening the regulation. Misinterpretation is leaving businesses exposed and the C-suite personally liable.

Data Protection

Protecting the perimeter through powerful firewalls, LAN segmentation and strong user authentication and access tools is, of course, essential – there is no point in leaving the door wide open. But to meet regulatory demands requires an additional layer of security that focuses specifically on protecting the data, not just the infrastructure.

Wrapping security around the data – for example by using encryption and limiting access to the encryption keys used to only the data owner – means that if a bad actor is able to gain access to the systems, the data is not usable. As a result, even while a business will still have to inform the regulator that a security breach has occurred because the bad actors have been unable to see – and hence use – any data, there is no liability. The business doesn't have to inform data subjects. There is no fine, no reputational damage and no compromise to the personal liberty of the C-suite.

> **The onus is on the senior management team to ensure the right frameworks are in place. Internal audits must rigorously check that data can only be read by authorised individuals and, critically, that information is completely unusable by anyone other than the intended recipient. And that can only be achieved with a data-focused approach to security.**
>
> *Simon Paplin - CTO, Certes Networks*

Conclusion

Data protection is a serious business problem – not a technology issue. And the responsibility for mitigating this ever-escalating corporate risk lies directly with the C-suite. And when compared to the cost of failing to secure data and the associated personal liability,
can any C-suite afford to do nothing?

Contact Certes Networks
300 Corporate Center Drive, Suite 140
Pittsburgh, PA15108

CERTES

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

www.certesnetworks.com