Cybersecurity strategies to reduce risk and potential reputational harm

FLOW ENTERPRISE

The growing pace and sophistication of cybercrime incidents across the world have made it imperative for businesses of all sizes to reassess their security strategy and infrastructure. The rate of cybercrime is increasing with each passing year and impacts more than 80% of companies worldwide. This is particularly concerning since digital transformation has accelerated for businesses from all industry verticals in the post-COVID world.

Cybercrime can bring any business, even large organisations, to its knees because of financial loss leading to a massive erosion of its market capitalization and profits. According to recent research by Ponemon Institute, the average cost of a data breach is $4.35 million in 2022, up from $4.24 million in 2021.

Cyber incidents are not just about financial loss but can potentially lead to loss of reputation, which is challenging to rebuild and also impacts future growth. Reputational harm means that the organisation will end up spending significantly to retain the existing clients and employees even as it becomes tough for them to attract new customers. Further, the loss related to cybercrime can have a wide-ranging and long-term impact. Not only does it lead to a loss in revenue because of system downtime, but it also demands more effort and investment to acquire new business. That's not all! A cybercrime incident can potentially lead to regulatory and legal action against the organisation, thus putting the onus of data protection on the company.

Take the recent case of the UK's TalkTalk, a telecom firm, which revealed that cybercrime had compromised the personal information of its 150,000 users. In the short term, the company lost 100,000 customers and a third of its value. This kind of reputational damage can take a long time to repair and in some instances, the company may not be able to recover from the damage.

Another high-profile example is that of Capital One, which recently suffered a data breach of 100 million customers in the US and Canada. The banking group revealed that the financial impact on its business would be in the range of $100-$150 million. Further, the company's share price dropped by 6% immediately after the data breach was revealed.

The loss of reputation is hard to measure though it is significant as organisations now derive tremendous value from intangible assets like brand equity, intellectual property and goodwill in the industry. This makes businesses more vulnerable to reputational damage.

Protecting your “house”

Considering the substantial short-term and long-term impact of a cybercrime incident, it is crucial for organisations to adopt a holistic approach to safeguarding their digital infrastructure and assets, like user data. This is all the more critical since there has been an increase in the use of technology to manage their operations, making them more vulnerable to cyberattacks.

What adds to the challenge of ensuring cyber security is that organisations must protect their IT infrastructure on several fronts simultaneously, much like we adopt several measures to protect our houses. From placing a fence around your house to putting a lock on the main door to moving valuables to the bank locker, we take several steps to protect our valuables.

However, most of these measures are centred around securing the perimeter and the premise's main entrance and exit points. Unfortunately, this strategy in preventing cybercrime is counterproductive now as enterprises increasingly use the cloud to improve productivity and operational efficiency. Further, trends like Bring Your Own Device (BYOD) and remote working mean that a comprehensive approach to security is required.

An organisation's security team needs to continuously undertake gap assessment of their current infrastructure to ensure that it is in place to address any cyber threat.
A comprehensive analysis of the infrastructure, including network, endpoint security, identity management, and application security, will better equip the team to manage risk and new evolving threats effectively.

All this demands proven expertise in cyber security and managing networks. Flow Enterprise comes with a range of solutions, including Secured Enterprise Edge, Secured Enterprise Core, Secured Enterprise Application and Secure Enterprise Complete, to provide end-to-end security to help businesses protect their IT infrastructure. While Secure Enterprise Edge secures endpoints, Secure Enterprise Core is a solution for next-generation, highly available applications. Secured Enterprise Application ensures the safety of apps at all touchpoints. On the other hand, Secure Enterprise Complete is an enterprise-wide solution to help businesses strengthen their defences and proactively respond to emerging threats. The comprehensive range of solutions is designed to help organisations minimise their overall security risks, reduce downtime, and protect their digital assets.

Wrapping up

The exhaustive financial and reputational damage a cyber incident can inflict on an organisation implies that businesses of all sizes must regularly assess their cyber risk and proactively manage their defences. In addition, they must take steps to mitigate the impact of a cyberattack to ensure their reputation is not negatively affected. Partnering with Flow Enterprise allows organisations to leverage industry-leading security solutions to safeguard their infrastructure and protect their reputation.

At Flow Enterprise, we partner with technology stakeholders to accelerate and support enterprises and governments in cyber security, cloud and datacentre, unified communications and connectivity & networking. Our comprehensive suite of streamlined, scalable, and secure IT solutions is designed to enable effective digital transformation. We are proud to operate the largest and best-performing network in the Pan-Caribbean region, providing a solid foundation for your success.

