Cybersecurity strategies to reduce risk and potential reputational harm

According to Fortinet's State of Operational Technology and Cybersecurity Report, 93%[1] of organisations experienced cybercrime intrusions in 2022. It is therefore more important than ever for businesses of all sizes to reassess their security strategy and infrastructure. This is particularly critical given that, in the post-COVID era, digital transformation has accelerated for organisations across all industry sectors.

Cybercrime can bring any business, even large organisations, to its knees because of:

1. **Financial loss,** leading to a massive erosion of its market capitalisation and profits because of system downtime, and it also demands more effort and investment to acquire new business going forward. According to recent research by the Ponemon Institute, the average cost of a data was $4.45 million in 2023, up from $4.35 million in 2022[2].

2. **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.

3. **Regulatory and legal action** against the organisation, thus putting the onus of data protection on the company.

Take the infamous case of the UK's TalkTalk, a telecommunications 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[3]. 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 notoriously suffered a data breach 100 million customers in the US and Canada. The banking group revealed that the company's share price dropped by 6% immediately after the data breach was revealed[4]. The total financial impact on its business would be in the range of $100–$150 million[5].

The drop in the company's share price and the loss of customers are indicators of the loss of reputation. Reputation is significant for organisations as it has a tremendous value for intangible assets like brand equity, intellectual property, and goodwill in the industry. This instils the importance of planning a cybersecurity strategy.

[1] Fortinet's State of Operational Technology and Cybersecurity Report

[2] Ponemon Institute - Cost of a Data Breach Report 2023

[3] Reuters - TalkTalk lost more than 100,000 customers after cyber attack

[4] WSJ - Capital One Shares Fall Nearly 6% After Breach

[5] Reuters - Capital One says information of over 100 million individuals in U.S., Canada hacked

Protecting your 'home'

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 business operations, making them more vulnerable to cyberattacks.

An additional task of ensuring cybersecurity is that organisations must protect their IT infrastructure on several fronts simultaneously, much like we adopt several measures to protect our homes. 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 premises' main entrance and exit points. Unfortunately, adopting this strategy solely to prevent cybercrime is counterproductive 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 and nuanced approach to security is required.

An organisation's security team needs to continuously undertake a gap assessment, a comprehensive analysis of the infrastructure, including network, endpoint security, identity management, and application security of their current infrastructure to understand their readiness to address any cyberthreat. Thus, the team will be equipped to manage risk and new evolving threats effectively.

Choosing the right cybersecurity approach

The exhaustive financial and reputational damage a cybersecurity incident can inflict on an organisation means that businesses of all sizes must regularly assess their cybersecurity risk and proactively manage their defences. Should an incident arise, they need to take steps to mitigate the impact of a cyberattack to ensure their reputation is not negatively affected. Partnering with C&W Business allows organisations to leverage industry-leading security solutions to safeguard their infrastructure and protect their reputations.

C&W Business comes with a range of solutions, designed to help organisations minimise their overall security risks, reduce downtime, and protect their digital assets.

- Secured Enterprise Edge
- Secured Enterprise Application
- Secured Enterprise Core
- Secure Enterprise Consultancy Services

We are here to ensure end-to-end security to protect and strengthen your business's defences and proactively respond to emerging threats.

At **C&W Business,** we're your catalyst for transformative success.
From Cybersecurity to Cloud, Data Centres, Unified Communications, and Connectivity, our streamlined solutions ensure scalability and security. With the Pan-Caribbean region's largest and most reliable network.