Cyber-risks & Liabilities

Courtesy of The Risk Hub Ltd

Managing Cyber-risks in a Down Economy

During a recession, businesses usually experience decreased sales and profit margins stemming from changing consumer behaviours, prompting them to reduce spending to avoid issues such as bankruptcy. Furthermore, a down economy can also create heightened cyber-security risks. After all, cyber-criminals have historically capitalised on social and economic crises by leveraging public uncertainty to launch additional attacks, as evidenced by rising cost-of-living scams and numerous cyber-losses throughout the COVID-19 pandemic.

As such, it's crucial for businesses to understand the cyber-exposures that may result from a recession and adjust their operations accordingly. This article outlines cyber-security concerns for businesses to keep in mind amid a down economy and provides risk management strategies to mitigate such issues.

Cyber-exposures in a Down Economy

An economic downturn could pose a variety of cyber-risks for businesses of all sizes and sectors, including:

- **Limited IT spending abilities—**In preparation for a recession, businesses may implement strategies to decrease their spending and scale back certain operational costs. This could entail cutting IT expenses and, in turn, reducing available cyber-security resources. While making difficult financial adjustments is common during a down economy, limiting IT spending may leave businesses unable to purchase new technology, conduct critical software updates and invest in advanced security solutions to address the latest cyber-threats. Consequently, companies' digital defences will likely degrade, making them increasingly vulnerable to cyber-incidents and associated losses.

- **Elevated skills shortages—**Labour shortages have impacted the vast majority of businesses in recent years. Such shortages have contributed to widening cyber-security skills gaps within many workplaces. In the lead-up to an economic downturn, businesses may implement hiring freezes or conduct staff redundancies, which theoretically could help decrease these skills gaps by allowing the talent pool to catch up with the demand for labour. However, shrinking workforces paired with rapidly evolving digital threats will likely only exacerbate demand for cyber-security talent and compound skills gaps. Further, companies that limit or cut their cyber-training programmes as a cost-saving measure could encounter even larger skills gaps among their existing employees. As cyber-criminals become aware of companies' staffing changes, they may exploit these skills gaps by deploying additional attacks.

- **Increased insider threats—**Poor economic conditions affect both businesses and individuals. This means a recession could place some individuals in troubling financial situations, potentially pushing them to engage in activities they otherwise wouldn't to help increase their incomes—namely, employee-orchestrated cyber-incidents. These crimes may involve sharing confidential company data, distributing workplace login credentials or providing digital access to essential business assets in exchange for payment, all of which could result in costly cyber-losses for impacted employers.

- **Compounded cyber-crime concerns—**Apart from increasing insider threats, a down economy could also exacerbate existing cyber-crime concerns resulting from external attackers. It's certainly possible that history could repeat itself amid a future recession, taking already surging cyber-incident frequency and severity to new highs.

- **Heightened nation-state exposures—**When a country enters a recession, other nations may attempt to exploit its economic weaknesses and further destabilise its operational frameworks by launching cyber-warfare and other digital attacks against its citizens and businesses. As a result, certain industries could be more susceptible to nation-state cyber-attacks during a down economy. Specifically, businesses in the private sector could be targeted due to their integral involvement in promoting a sufficient flow of capital. Considering cyber-warfare incidents are currently on the rise due to the ongoing Russian war in Ukraine, growing nation-state exposures could be particularly concerning for businesses.

- **Reduced innovation capabilities—**As part of their decreased spending measures, businesses may cut back or completely eliminate funding for developing and adopting new cyber-security solutions amid an economic downturn. However, cyber-criminals' attack methods will continue to advance, allowing them to exploit the shortcomings in companies' prevention and response capabilities and exacerbate losses.

Cyber-risk Management Considerations

To combat cyber-risks in a down economy, businesses can consider these best practices:

- **Have a plan.** Cyber-incident response plans can help businesses establish protocols for mitigating losses and acting swiftly amid cyber-events. Successful plans should outline potential cyber-attack scenarios, methods for maintaining key functions during these scenarios and the individuals responsible for such functions. These plans should also provide procedures for notifying relevant parties of cyber-incidents. Businesses should routinely review their plans to ensure effectiveness, making adjustments as needed.

- **Conduct training.** Employees are often the first line of defence against cyber-attacks. That's why it's important for businesses to make cyber-security training a priority. Employees should receive the following guidance during such training:

    - Avoid opening or responding to emails from unfamiliar individuals or organisations. If an email claims to be from a trusted source, verify the identity of the sender by double-checking the address.
    - Never click on suspicious links or pop-ups, whether they're in an email or on a website. Don't download attachments or software programmes from unknown sources or locations.
    - Utilise unique, complicated passwords for all workplace accounts. Never share credentials or other sensitive information online.

- **Purchase cyber-cover.** Especially during an economic downturn, it's imperative for businesses to have sufficient insurance. Companies should consider purchasing dedicated cyber-cover to ensure financial protection against cyber-losses.

Conclusion

Overall, it's evident that businesses will encounter elevated cyber-exposure in a down economy. By better understanding these risks and taking steps to mitigate them, businesses can reduce associated losses. Contact us today for more risk management guidance.