Courtesy of
SCS Agency Inc

Managing Cyber Risks in a Down Economy

To help minimize growing inflation concerns that have spanned across industry lines over the past few years, the Federal Reserve (Fed) has steadily been hiking up interest rates. Economic experts predict the Fed's efforts will eventually pay off in 2023, with inflation issues subsiding throughout the year. Yet, some experts have forecasted that rising interest rates will ultimately cause a recession—a prolonged and pervasive reduction in economic activity—in the near future.

During a recession, businesses usually experience decreased sales and profit margins stemming from changing consumer behaviors, prompting them to reduce spending to avoid issues such as bankruptcy. Furthermore, a down economy can also create heightened cybersecurity risks. After all, cybercriminals have historically capitalized on social and economic crises by leveraging public uncertainty to launch additional attacks, as evidenced by rising health care scams and related 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 cybersecurity 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 cybersecurity 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 cyberthreats. Consequently, companies' digital defenses will likely degrade, making them increasingly vulnerable to cyber incidents and associated losses.
- **Elevated skills shortages**—Labor shortages have impacted the vast majority of businesses in recent years. Such shortages have contributed to widening cybersecurity skills gaps within many workplaces. Leading up to an economic downturn, businesses may implement hiring freezes or conduct staff layoffs, which theoretically could help decrease these skills gaps by allowing the talent pool to catch up with the demand for labor. However, shrinking workforces paired with rapidly evolving digital threats will likely only exacerbate demand for cybersecurity talent and compound skills gaps. Further, companies that limit or cut their cyber training programs as a cost-saving measure could encounter even larger skills gaps among their existing employees. As cybercriminals 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. A recent survey conducted by security company Palo Alto Networks confirmed that economic hardship can potentially lure a significant proportion of individuals

into committing cybercrimes against their employers, thus driving up insider threats within businesses. 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 cybercrime concerns**—Apart from increasing insider threats, a down economy could also exacerbate existing cybercrime concerns resulting from external attackers. According to FBI data, cybercrime increased by 22.3% during the last major U.S. economic downturn—known as the Great Recession—which took place between 2007 and 2009. 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 destabilize its operational frameworks by launching cyberwarfare and other digital attacks against its citizens and businesses. As a result, several U.S. industries could be more susceptible to nation-state cyberattacks 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; similarly, those in the public sector could be attacked due to their contributions to vital infrastructures. Considering cyberwarfare incidents are currently on the rise due to the ongoing Russia-Ukraine conflict, growing nation-state exposures could be particularly concerning for many businesses.
- **Reduced innovation capabilities**—As part of their decreased spending measures, businesses may cut back or completely eliminate funding for developing and adopting new cybersecurity solutions amid an economic downturn. However, cybercriminals' 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 cyberattack 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 defense against cyberattacks. That's why it's important for businesses to make cybersecurity training a priority. Employees should receive the following guidance during such training:
    - Avoid opening or responding to emails from unfamiliar individuals or organizations. If an email claims to be from a trusted source, verify their identity 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 programs from unknown sources or locations.
    - Utilize unique, complicated passwords for all workplace accounts. Never share credentials or other sensitive information online.
- **Purchase cyber coverage.** Especially during an economic downturn, it's imperative for businesses to have sufficient insurance. Companies should consider purchasing dedicated cyber coverage 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.