Evolving SMB cyber resilience for the NEXT NORMAL

CYBER SECURITY MONTH
OCTOBER 2023

Evolving SMB cyber resilience for the NEXT NORMAL

CYBER SECURITY MONTH
OCTOBER 2023

Evolving SMB cyber resilience for the NEXT NORMAL

CYBER SECURITY MONTH
OCTOBER 2023

Trends like AI, cloud, and work-from-home create new challenges and opportunities for SMB companies.

CYBER RESILIENCE MUST EVOLVE TO KEEP UP AND KEEP COMPANIES SAFE.

Statistics show that cyber threats are evolving, becoming more sophisticated, stealthy, and powerful.

Data breaches illustrate how their effects on businesses are wide-ranging. According to IBM's Cost of Data Breach 2022 report, a data breach costs companies an average of US$4.35 million. In some cases, the total is much higher.

T-Mobile paid US$ 350 million to customers over a data breach. Slack, Twitter, Uber, TransUnion, Credit Suisse, and Samsung are just a few other enterprises targeted by cyberattacks during the last 12 months – and cyber threats include much more than data breaches.

Small to mid-sized businesses (SMBs) are likely more exposed to attacks. One reason is that smaller organisations likely have fewer in-house cyber resources and less budget than large enterprises.

To navigate the changing threat landscape, companies must develop their approach to cyber resilience. The starting point is to recognise and accept total prevention of cyber risks is not possible. Cyber impacts can occur, and companies should work proactively to minimise the potential for breaches and the effects of successful attacks. This is at the core of improving cyber defence capabilities and confidently managing cyber risk.

> "For 83% of companies, it's not if a data breach will happen, but when," the IBM Cost of Data Breach 2022 report says.

Cyber resilience keeps companies operating

The National Institute of Standards and Technology (NIST) defines cyber resiliency as:

“The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”

In other words, cyber resilience is a set of risk mitigation strategies and initiatives to help define and achieve specific objectives and protect an organisation’s digital assets and systems. It covers a broad range of areas, including everything from IT hygiene to a company’s board’s ability to deal with cyberattacks.

The core objective of cyber resilience initiatives is straightforward: to enable a company to carry on normal business operations to the greatest degree possible. While maintaining high-quality operations is, of course, optimal, it is not always possible.

Cyber threats create risks to operations as well as other areas. A company's reputation and relationship with customers, clients, revenues, and bottom line can be at stake.

Cyber resilience is a central tool to mitigate risks and protect short- and long-term revenues and profitability

New technology requires updates to cyber resilience

Companies’ IT environments are changing due to the likes of generative AI, cloud, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), and work-from-home (WFH). The changes enable companies to increase efficiency, productivity, and innovation. However, the changes can also open new attack paths for hackers and cybercriminals.

Ransomware attacks that interrupt or even temporarily terminate business operations provide an excellent example of this trend. The attack frequency has multiplied, costing companies and organisations $20 billion in 2021, a figure expected to rise to $265 billion by 2031. In 2021, 37 per cent of all businesses and organisations were hit by ransomware. The ones breached saw average costs of $1.85 million.

Among the most prominent supply chain attacks was SolarWinds' cyberattack, which went undetected for months, exposing businesses' supply chain vulnerabilities. Hackers breached SolarWinds and injected malicious code into software updates sent to its clients, affecting major organisations like Microsoft, Deloitte, and Intel. This breach highlighted the need for proactive cybersecurity and supply chain vigilance. Many affected companies didn't realise SolarWinds was a critical supplier until it was too late. To ensure business resilience against unforeseen threats with far-reaching consequences, comprehensive supply chain security is critical.

Companies’ IT environments, and the effects of the trends mentioned above, are still evolving. This is why talking about the "next normal" is more beneficial than the "new normal."

However, it is already clear that there are knock-on effects on cyber resilience.

The attack frequency has multiplied, costing companies and organisations $20 billion in 2021, a figure expected to rise to $265 billion by 2031.

What are your crown jewels?

One of the first cyber resilience steps is identifying your crown jewels. They are the systems, information, data, and infrastructure critical for operational efficiency, revenue, and profits.

What constitutes crown jewels and what defences to deploy around them depends on your company and industry. For example, an online commerce site is a crown jewel for most consumer businesses, making protection against ransomware and Distributed Denial of Service (DDoS) attacks a core priority. For a manufacturing company, production equipment is vital, making defences against outside hackers and third-party vulnerabilities extra relevant.

Two tools help guide risk mitigation efforts in this space: risk assessment and risk evaluation.

Risk assessment covers finding all types of risks. Risk analysis is a subset of risk assessment that determines the severity of each risk. Risk is derived by two main “compasses”:

1. A business impact compass: How each risk will impact business operations
2. An intelligence compass: The threat landscape and level facing an organisation at any given time.

Cyber resilience efforts are prioritised by risk, and therefore combining the two compasses provides direction for an organisation’s cyber efforts.

Cyber resilience frameworks and associated action plans overlap existing plans for areas such as mitigating the breakdown of critical production equipment, severe disruptions to supply chains, etc.

In other words, cyber is rarely a stand-alone risk but is interconnected with general business operations and should be incorporated as such throughout risk frameworks and strategies.

Updating your view on cyber resilience

So, what does the evolving situation mean for cyber resilience, and how do companies best protect their cyber assets?

For one, it may raise questions about how up-to-date companies' cyber resilience efforts are and how cyber resilience is handled within their organisation. Companies must closely examine their structure, organisation, roles, responsibilities, assets, and action plans to keep up with the evolving digital threat landscape. An exact evaluation of cyber resilience levels will help clarify organisational resilience, which plays a significant role in business planning and strategy processes.

Companies may also need to consider ongoing technological trends when updating or expanding cyber resilience frameworks. For example, hybrid cloud environments and applications result in increased interconnectedness or undertaking cloud migration initiatives can heighten security complexity.

Cyber resilience initiatives should also consider the positives and negatives of each of its many components. For example, work-from-home initiatives complicate the security landscape but also spread the cyber footprint, thereby increasing resistance to distributed denial of service (DDOS) attacks.

A further consideration is whether the organisation has all the required resources and skills available in-house. Often, this will not be the case. In such cases, outsourcing all or parts of cyber resilience provides optimal access to the skills and experience necessary to optimally mitigate cyber risks.

Companies may need to consider ongoing technological trends when updating or expanding cyber resilience frameworks.

Cyber resilience for companies in the "next normal"

The above has laid out how companies inhabit an increasingly complex cyber landscape. Cyber resilience, including the previously mentioned compasses, provides a framework for safely navigating that landscape.

However, many companies, especially in the SMB segment, may need external support to optimise cyber resilience.

Collaboration is often vital, as cyber resilience and risk mitigation expertise may only be available in some places. Simultaneously, there will still be areas where technical insights and expertise are needed to create the best results. Here, advisors can draw on their organisations' knowledge and experience.

Companies and their advisors can collaborate on updating resilience strategies and initiatives and increase focus on protecting its crown jewels and continual, optimal operations managing cyber resilience risks.

Across the spectrum, BDO stands out with cybersecurity services tailored to meet the needs of mid-market companies looking to update cyber resilience to meet the challenges and exploit the opportunities created by the "next normal.".

Areas covered by cyber resilience frameworks

THREAT IDENTIFICATION

Clear insight into how threats are detected and identified across IT infrastructure and applications.

RISK MITIGATION AND MANAGEMENT

Identifying crown jewels and defining what actions to take to mitigate and manage cyber-related risks.

CONTROL MATURITY

Ensuring that cyber risk mitigation controls are mature and developed enough to match the evolving threat landscape and the overall cyber resilience / cyber security strategy.

BUSINESS CONTINUITY

Defining strategies and initiatives help ensure that a business stays in an operational state.

INCIDENT RESPONSE AND CRISIS MANAGEMENT

Clear plans for actions taken in case of an attack, including if the attack happens outside of office hours and how management will support crisis management activities.

INTERNAL COMMUNICATION

Deciding what will be communicated to whom and when concerning an attack and any actions taken as a consequence of the attack.

AUTHORITY

Clarifying who has the control and rights to make decisions and developing a clear chain of command.

TRAINING AND SIMULATION

To optimise cyber resilience, employees and management should also be trained for different scenarios and develop plans for responding to them.

BDO - your partner for cyber resilience and cybersecurity

BDO assists companies and organisations with increasing cyber resilience across their operations. We are a one-stop shop for cyber-related services and consultation. We also assist companies with developing all aspects of cyber resilience.

BDO is also a leading provider of post-breach capabilities. Often, the full cycle of a cyberattack that leads to a breach involves post-breach evidence gathering, damage evaluation and insurance claims. Contact us to hear how we can assist your company.

FOR MORE INFORMATION:

OPHIR ZILBIGER
Global Cyber Leader, BDO
+972-52-6755544
OphirZ@bdo.co.il

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad statements only. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication. No entity of the BDO network, its partners, employees and agents accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

'BDO', 'we', 'us', and 'our' refer to one or more of BDO International Limited, its network of independent member firms ('the BDO network'), and their related entities. The BDO network (referred to as the 'BDO network') is an international network of independent public accounting, tax and advisory firms which are members of BDO International Limited and perform professional services under the name and style of BDO (hereafter: 'BDO member firms'). BDO International Limited is a UK company limited by guarantee. It is the governing entity of the BDO network.

Service provision within the BDO network is coordinated by Brussels Worldwide Services BV, a limited liability company incorporated in Belgium.

Each of BDO International Limited, Brussels Worldwide Services BV and the BDO member firms is a separate legal entity and has no liability for another entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BV and/or the BDO member firms. Neither BDO International Limited nor any other central entities of the BDO network provide services to clients.

BDO is the brand name for the BDO network and for each of the BDO member firms.

www.bdo.global