Grow your Business Securely

GROW YOUR BUSINESS

The rise of nation state hackers fuelled by geopolitical tensions, ever-increasing sophistication of cyber attacks by advanced persistent threats and regularity of scams, ransomware attacks and business email comprise of threats that present real dangers for all businesses today.

Growing businesses need to be cognisant of changing processes and activities creating new vulnerabilities for hackers to exploit. This can occur when business models change. The movement towards working from home, is exposing many organisations to new threats.

For example, its common for payment processes to require approval by another person, known as a separation of duty control. This is typically a handwritten signature on a piece of paper. But can be a tendency to skip some process steps in times of crisis, or major change, with a variety of excuses, whether valid or not. This could result in signatures being replaced by an email, which may be a lot easier to forge.

Physical signatures may not be possible when all staff in a team are working from home, but other options are available. Some accounting and ERP systems provide in-built approvals systems.

Advanced cybersecurity mechanisms can also protect against the likelihood of a hackers being able to infiltrate email systems. Digital signatures and encrypted emails also present other opportunities to address this threat.

Cloud Computing

Most organisations today, have moved many IT workloads to the cloud. However, not all clouds are the same. And not all cloud cybersecurity is the same. Clouds generally offer greater potential to secure information and identities better than traditional on-premise IT environments, but there is a wide spectrum of how this actually occurs in practice.

Additionally, although most cloud platforms provide many layers of security, it is often up to individual organisations or the technology companies that support them, to decide to implement the security features available. Some features require licences and therefore costs; some have significant impact on users.

A detailed understanding of layered protection often eludes directors, managers and in fact, most IT staff.

It is very rare to find IT resources who have trained formally in the art and science of cybersecurity. And rarer still, to find those individuals with an excellent understanding of data privacy, data rights and legal obligations around privacy legislation and regulation.

Another issue for many, is that the move to the cloud is in progress – meaning that all the traditional on-premise vulnerabilities still exist until the digital transformation is complete. And there is still resistance from some, under

the fallacy that they can protect their information better than the large global IT vendors who in some cases spend over a billion dollars a year on cybersecurity.

A strategy for agility and resilience

Growing organisations need to balance agility with resilience. Both are critically important but can be at odds with each other as the relentless search for productivity, efficiency and profits can dominate strategic plans and objectives.

Building in a strong culture of security and privacy awareness, is crucial to building organisational resilience whilst being agile enough to take calculated risks as opportunities present themselves.

The following suggestions are made for consideration:

- Continually work on improving the digital literacy at all levels of the organisation – from the board to the front-line workers
- Recognise that cybersecurity and data privacy are not traditional skill-sets of IT professionals, and seek expert advice appropriately
- Understand that cybersecurity is not just for large organisations. Many small businesses and charities have been devastated by cyber attacks and need to continually address these risks.
- Realise that adequate protection isn't an expensive exercise, but one that requires starting a never-ending journey of layering security
- For each new project or change to business operations, pause and consider cyber risks and privacy risks, ideally documented in an impact assessment

> *If you aren't moving forward, you're being left behind. Take the opportunity to strengthen your defences before the next attack.*

And realise that investing in user awareness, attack simulations and your response and recovery post-breach are all as important as the cybersecurity systems put in place to deter and defend in the first place.

Business Central Security Features

The cloud accounting and ERP system from Microsoft, Dynamics Business Central, is part of an integrated solution within the Microsoft 365, Dynamics 365 and Azure cloud platforms.

Built on the Microsoft Cloud Framework, it provides a solid foundation for protecting identities, systems and data from exfiltration, deletion and modification.

Automated database backups occur throughout the day. These can be exported and stored in a variety of locations to ensure permanent records can be kept to address operational and legislative requirements.

User and security management is baked into the fabric of the Microsoft Cloud, using Azure Active Directory to centrally store all user accounts. These can be protected via multi-factor authentication, conditional access policies and other cybersecurity techniques to ensure only valid users have access to confidential, personal and sensitive information.

Business Central can be used to implement an organisation's delegation of authority policy, by not just limiting the functions available within the application, but also by considering the details of individual transactions, such as limits on purchase orders or sales invoices where a financial amount is exceeded and additional approval is required.

Audit trails can be configured to record every new record added, change of information and deletion of data. This may be designed for example, to identify any time that a creditor bank account number is changed. This event can trigger an approvals process, send an alert or otherwise simply record the activity for later analysis.

As part of the Microsoft Cloud Framework, Business Central is a fully-functioning, integrated suite of ERP modules designed for small, medium and enterprise customers with complex needs.