Somerville

Business Security Meets Business Continuity: Important Considerations for Your Planning

Digital transformation across all sectors and industries has accelerated, as businesses of all sizes are increasingly moving workloads, data, applications, and services to the cloud. The application of the Internet of Things is expanding, artificial intelligence and machine learning are being leveraged to solve hard to answer problems.

Besides the obvious benefits these technologies bring, new risks emerge threatening the success and effectiveness of digital-first strategies. Ransomware has become one of the greatest cyberthreats facing organisations. The sophistication and adaptability of ransomware and other cyber threats today require an agile, layered defence.

Without a holistic way to manage cybersecurity risk, it would be easy to focus all your efforts into preventive defences, such as firewalls or access management while neglecting the processes and tools that are mandatory to effectively respond to, and recover from, a successful attack.

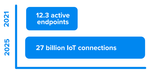
The state of the threat landscape

Globally

89% of businesses have embraced a multi-cloud strategy[1]

66% of organisations were hit by ransomware in 2021, a 78% increase from 2020[2]

1 month Once access has been purchased from Initial Access Brokers, it takes up to a month for a ransomware attack to take place[3]



2021: 12.3 active endpoints

2025: 27 billion IoT connections

By 2025, there will likely be over 27 billion IoT connections, up from 12.3 active endpoints in 2021[4]

Company Average: 254 SaaS apps

Enterprise Average: 364 SaaS apps

The average company has a **whopping 254 SaaS apps**, with enterprises averaging 364 apps[5]

In Australia

55% of security incidents are attributed to compromised credentials[6]

23% of all cyber security incidents are Ransomware attacks

55% of all data breaches were sourced on malicious or criminal activities

41% of all data breaches happened because of human error

The sectors most affected by data breaches were healthcare, finance and legal

The importance of MFA in preventing ransomware attacks

According to industry research, users who enable MFA are up to 99 percent less likely to have an account compromised[7]

When implemented correctly, multi-factor authentication can make it significantly more difficult for an adversary to steal legitimate credentials to facilitate further malicious activities on a network[8]

Why does MFA adoption lag?

Only 52% of APAC businesses have adopted MFA[9]

Biases

Hurt user experience

Difficulty justifying the cost

The importance of a business continuity and recovery plan

Security controls eventually fail, especially as adversaries are becoming more innovative and sophisticated. Data breaches can become very costly for every business.

$4.24 million the average cost of a data breach[10]

$4.62 million the average cost of Ransomware attacks

$4.87 million the average cost of data breaches that took longer than 200 days to identify and contain

of the overall average cost is 'lost business'

Planning for business continuity and recovery

Identify – environment and risks
Protect – controls to protect your environment
Detect – time is essential to mitigate impact
Respond – mitigate the attack to reduce impact
Recover – timely recovery

Best practices for building business continuity and recovery capabilities

- Scalable solution to protect all workloads wherever they are
- Verified backups – follow the 3-2-1-1-0 rule
- Protect your backups with best cyber hygiene controls
- Timely and fast data recovery
- And last but not least: Immutable backups

Conclusion

In today's changing and evolving threat landscape, multi-factor authentication is your ally to help you prevent the most disruptive attacks. As MFA is quickly becoming a mandate across all jurisdictions, **now is the time to secure the future of your business**. However, your defenses should not stop at deploying MFA. You should supplement MFA with other controls, such as good and working backups, that will allow you to recovery fast and effectively in the event of a cyber incident. If you feel overwhelmed by all these controls, hiring an experienced managed services provider, like Somerville, will help you build a resilient organisation.

References:
1. Flexera 2. SOPHOS 3. KELA 4. IOT ANALYTICS 5. Productiv
6. OAIC 7. 8. ACSC 9. THALES 10. IBM

To learn more about how Somerville has helped other organisations become resilient, contact us today