PAUL MAXWELL *Founder, Stratia Cyber*
LinkedIn:www.linkedin.com/in/paul-maxwell-2289b0/

Paul is a distinguished cybersecurity leader with extensive experience spanning over two decades, primarily with Stratia Cyber, where he has spearheaded significant security transformations. He has delivered comprehensive risk management frameworks and robust cybersecurity solutions across various sectors, including finance, healthcare, and government. Known for his strategic implementation of cyber strategy, Paul has significantly enhanced organisational resilience and compliance for numerous high-profile clients.

TIP 1. IDENTIFY YOUR KEY ASSETS

If you don't know what is important, how can you protect it? Identify, and prioritise your most critical assets, such as sensitive customer data, intellectual property, or financial systems. Understanding which assets are vital to your organisation helps in focusing your security efforts and resources more efficiently. This process involves regularly reviewing what data or systems would most impact your business if compromised.

TIP 2. APPLY MINIMUM SECURITY CONTROLS

Establish a baseline set of security measures for all systems, but especially for those handling your key assets. These controls should include robust access management, encryption, regular security assessments, and physical security measures. The goal is to create a security floor, below which your systems and data are never unprotected.

TIP 3. CONDUCT REGULAR RISK ASSESSMENTS

Things change; make sure to regularly evaluate your cybersecurity stance through risk assessments to identify vulnerabilities that could be exploited by attackers. This proactive approach allows you to adjust your security strategies based on evolving threats and business needs, thus staying ahead of potential risks.

TIP 4. PROMOTE A CULTURE OF SECURITY

Cultivating a security-aware culture is crucial. Encourage employees to take an active role in cybersecurity by providing continuous education on the latest threats and best practices. This cultural shift helps prevent breaches by ensuring that all team members are vigilant and knowledgeable about potential security threats.

TIP 5. IMPLEMENT MULTI-FACTOR AUTHENTICATION (MFA)

Multi-factor authentication adds layers of security by requiring additional verification to prove identity on top of a password. This could include something you know (a password), something you have (a security token), or something you are (biometric verification). MFA significantly reduces the risk of unauthorised access caused by stolen credentials.

TIP 6. KEEP SOFTWARE AND SYSTEMS UPDATED

Attackers often exploit vulnerabilities in outdated software. Ensuring that all software, operating systems, and applications are up to date with the latest patches is essential. Automate updates where possible to maintain protection against the latest security threats without manual intervention.

TIP 7. BACKUP DATA REGULARLY

Implement a robust data backup strategy that includes regular and systematic backups of important data. Store backups in a secure, offsite location and test them regularly to ensure that they can be restored quickly. This practice helps mitigate the impact of data loss or corruption from cyber-attacks, hardware failures, or natural disasters.

TIP 8. USE ENCRYPTION

Employ strong encryption protocols to protect data at rest and in transit from unauthorised access or theft. Encryption acts as a last line of defence by making compromised data unreadable and unusable without the decryption key. This is particularly important for sensitive information that, if exposed, could harm your business or clients.

TIP 9. DEVELOP AND TEST AN INCIDENT RESPONSE PLAN

Prepare for potential cybersecurity incidents by developing a comprehensive incident response plan. Outline clear procedures and responsibilities for responding to cyber threats and breaches. Regularly test and refine this plan with tabletop exercises and real-world simulations to ensure that your team can execute quickly and effectively under pressure.

TIP 10. MANAGE THIRD PARTY RISKS

Continuously evaluate and manage the security practices of third-party vendors that access or process your data. Implement strict contractual obligations and regular security audits to ensure third parties comply with your cybersecurity standards. This is crucial, as third-party breaches can significantly impact your data security and business continuity.