ALISTAIR EWING, *Managing Consultant at Trustwave DFIR UK*
https://www.trustwave.com

As the managing consultant in the DFIR Department at Trustwave, Alistair specialises in high-level digital forensics and incident response, making a significant impact on organisations' security. With 13 years of experience and certifications in various computer forensics disciplines, he excels in security breach analysis, data loss prevention, and providing court-admissible digital evidence. His expertise extends to eDiscovery, where he utilises advanced tools like Velociraptor and Spy Guard to secure organisations against future cyber threats.

TIP 1. EMPHASISE BYOD RISKS

Establish a robust Bring Your Own Device (BYOD) policy that clearly delineates security protocols for using personal devices for work. This policy should mandate antivirus software, encryption, and secure connections. Ideally, limit usage to corporate machines and mobiles. This is particularly crucial for small businesses, where personal devices are often used for work, to ensure comprehensive security.

TIP 2. DEPLOY A MAIL SCANNER

Integrate a robust mail scanning solution to filter out spam, phishing attempts, and malware from incoming emails. This reduces the risk of security breaches via email. Products like MailMarshal by Trustwave thwart 99% of phishing and dangerous emails compared to Microsoft's detection.

TIP 3. DEVELOP AN INCIDENT RESPONSE PLAN

Develop a detailed cybersecurity incident response plan. This plan should outline the steps to take when a security breach occurs, including how to contain it, notify affected parties, and prevent future incidents. This will lessen the time, impact, and loss following an attack.

TIP 4. EARLY DETECTION OF DATA BREACHES

Small businesses can be alerted early if their data, such as stolen customer information or proprietary business data, appears on the dark web. This early warning system allows them to act swiftly to mitigate damage. This proactive approach strengthens an organisation's security posture and supports compliance with data protection regulations by demonstrating due diligence in monitoring and protecting against external threats. Alerts can be set up so no manual check is required daily. Small businesses often work with suppliers and partners, which can introduce additional risks. Dark web monitoring can reveal if these third parties are compromised, potentially affecting their security.

TIP 5. ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

Multi-factor authentication is required to access business networks and sensitive data. This adds an extra layer of security beyond just passwords.

TIP 6. IMPLEMENT A VPN

Secure remote connections with a dedicated Virtual Private Network (VPN). This helps encrypt internet traffic, protecting sensitive data from interception. A dedicated IP will make business VPN traffic easier to identify, and bad actors will attempt to stand out in detection rules. Additionally, IP addresses of unwanted domain names as addresses that are not routable on the public internet provide another layer of security.

TIP 7. PERFORM REGULAR BACKUPS

Regularly back up data and ensure backups are stored securely offsite or in the cloud. Even a 2TB disk with the 'crown jewels' saved weekly, offline, can hasten recovery following a Ransomware attack or data loss. This helps quickly restore data in case of a ransomware attack or data loss.

TIP 8. RESOURCE ALLOCATION

Small businesses can allocate their limited security resources more effectively by better understanding the most pressing threats. Instead of spreading resources too thinly, they can focus on the most critical areas of vulnerability.

TIP 9. EMPOWER EMPLOYEES WITH SECURITY PRACTICE

Your employees are the first line of defence in maintaining cybersecurity. Regular training on cybersecurity best practices, such as identifying phishing emails, creating secure passwords, and practising safe internet usage, is vital. Consider implementing simulated phishing emails to test their vigilance. This underscores the importance of employee awareness and its significant role in cybersecurity.

TIP 10. LEVERAGE MANAGED SECURITY SERVICES

Consider outsourcing your cybersecurity efforts to managed security service providers. They offer comprehensive security measures, continuous monitoring, and rapid response to threats, all at a scalable cost. For smaller firms, contractors can provide constant monitoring and alerts. This underscores the value and cost-effectiveness of this approach for small businesses.