DR. MUNA AL-HAWAWREH - *Lecturer in Cyber Security, Deakin university*
LinkedIn: https://www.linkedin.com/in/muna-al-hawawreh-09656010b

TIP 1. ALLOCATE A WELL-DESERVED BUDGET FOR CYBER SECURITY

When allocating your budget, prioritise cyber security as a critical investment, rather than overlooking its importance. By allocating funds for robust cyber security measures and dedicating resources to your cyber security program, you can effectively mitigate the risk of cyber attacks, protect your reputation, and earn the trust of your valued customers. Remember, a small investment in cyber security today can save you from significant losses tomorrow.

TIP 2. A COMPREHENSIVE RISK ASSESSMENT PLAN IS THE FIRST STEP

Gain a thorough understanding of your infrastructure and sensitive data through diligent risk assessment. By conducting a comprehensive evaluation, you can proactively identify potential risks, hazards and vulnerabilities within your environment that may cause harm. This knowledge will empower you to effectively implement targeted measures and safeguards to mitigate risks.

TIP 3. COMMUNICATE EXPECTATIONS CLEARLY TO YOUR EMPLOYEES

A comprehensive security policy is essential to establish clear guidelines and protocols for your employees. Ensure to be clear about expectations and consequences regarding password management, personal mobile devices, remote access, and data handling. Regularly educate your staff on best practices for cyber security and ensure they understand the potential consequences of negligent behaviour. Remember, your employees are the first line of defence against cyber threats.

TIP 4. EMBRACE A ZERO TRUST MINDSET

With zero trust, assume that no user or device can be trusted by default, regardless of their location or network. Implement strict access controls and authenticate and authorise every user and device before granting them access to resources.

TIP 5. DON'T PUT "ALL YOUR EGGS IN ONE BASKET" WHEN IT COMES TO SAFEGUARDING AGAINST CYBER ATTACKS

No one solution or measure can ensure complete protection against cyber attacks. However, you significantly enhance your defences by implementing a multi-layered security approach that goes beyond relying on a single security solution. Deploy up-to-date anti-viruses, firewalls, Virtual Private Networks (VPN), data encryption, two-factor authentication, and intrusion detection systems. Regularly update and patch your software and use shared threat intelligence to improve your security practice.

TIP 6. BACK UP YOUR DATA REGULARLY

Develop a routine of backing up your data and critical information, incorporating incremental backups on a daily basis and comprehensive server backups on a weekly, quarterly, and yearly basis. Consider utilising secure cloud storage as a backup solution for your data or portable devices like USB sticks. However, storing these devices separately in an offsite location is crucial to ensure an additional layer of protection.

TIP 7. PROVIDE TRAINING AND AWARENESS FOR EMPLOYEES

Invest in cyber security training programs to educate your employees to prevent, identify, and report cybercrime incidents such as suspicious emails, links, or activities. Make it a priority to conduct regular security awareness sessions to reinforce good cyber security practices and ensure your team remains vigilant against ever-evolving threats.

TIP 8. DEVELOP A STRATEGIC PLAN FOR MOBILE DEVICE MANAGEMENT

Managing mobile devices efficiently is essential, given their inherent security risks, especially when storing sensitive data or accessing the corporate network. It is vital to enforce password protection on users' mobile devices, guide them to rely exclusively on trusted app sources, encourage the installation of security apps like anti-virus software, and emphasise the encryption of stored data. These measures mitigate the risk of compromise in device loss or theft.

TIP 9. ESTABLISH A STRONG INCIDENT RESPONSE PLAN

Create a comprehensive plan for responding to cyber incidents, which should detail the necessary actions to be taken if such an event occurs. This plan should encompass communication protocols, containment measures, and recovery strategies to minimise any potential disruption to the company's operations. It is crucial to regularly evaluate and modify your incident response plan through testing to ensure its efficiency and effectiveness.

TIP 10. ENGAGE EXTERNAL EXPERTISE IF IT IS NEEDED

As your company scales, you might require specialised knowledge and skills beyond your internal capabilities. Consider collaborating with external security experts or consultants who can provide guidance and support in developing and maintaining an effective security program.