ADAM BENNETT, *CEO Red Piranha*
LinkedIn: https://www.linkedin.com/in/adambennettwa/
Company page:www.linkedin.com/company/redpiranha
Website: www.redpiranha.net

TIP 1: DEVELOP A CYBERSECURITY STRATEGY PRIOR TO IMPLEMENTATION.

The first step begins with planning and preparation; as with implementing any new management system across your organisation, executing a new cybersecurity strategy will significantly impact all departments. It's essential to understand your organisation's operating model, conduct a security risk assessment across your organisation to understand your attack surface, evaluate your technology stack and vendors, select a security framework based upon your maturity and address any risks from the top down.

TIP 2. EDUCATE YOUR TEAM ON YOUR CYBERSECURITY STRATEGY

Your employees are your strongest and your weakest link in relation to your organisations' cybersecurity defence. It's vital that your team not only knows your cybersecurity strategy but understands how the protections work and why they are in place. The threats they are protecting the businesses' data and themselves from can be minimised by making your team agents of change and champions of cyber security. Routinely holding phishing exercises to test their knowledge and make sure that they know what to look out for will reduce risk in an organisation.

TIP 3. MAINTAIN UP TO DATE PATCHES AND UPDATES

Never underestimate the importance of keeping up to date patches across all devices, software applications, network equipment etc., that connects or runs on your corporate network. Implementing a strategic approach to your patch management, detailing your organisational processes, inventory of your systems and schedule patch updates reduces system downtime and ensures a robust security environment.

TIP 4. DESIGN YOUR NETWORK SECURELY

Secure your environment, and design your network, so only the correct employees and devices have access to the systems and data required to complete their work. Look to break down access controls in line with your organisation's structure, ensuring that departments can only access the necessary systems. Additionally, consider restricting cross-device communications and locking server access.

TIP 5. RESTRICT ADMINISTRATION PRIVILEGES

Not everyone within your business needs or requires access to administrative privileges. Restricting access is one of the most effective methods to ensure the security of your environment from cyber threats.

TIP 6. REVIEW YOUR ENDPOINT CONTROLS

My following recommendation is to review your endpoint controls and how both your organisations' devices and third-party devices connect to your assets and how they communicate, locking down acceptable use of the software. Taking into consideration how and what software your team needs to use and restrict their access to everything else.

TIP 7. REGULAR SCHEDULE VULNERABILITY SCANS AND PENETRATION TESTING

Identify your attack vectors and quickly flag weaknesses within your environment by running regular vulnerability scans identifying potential weaknesses within your network devices, and promptly patching them. Additionally, if you're developing software, it's important that you follow up on your regular vulnerability scans by investing in regular penetration testing, reducing your cyber risk and deciding which security controls are best suited for your business.

TIP 8. IMPLEMENT MANAGED THREAT DETECTION AND RESPONSE

Continuous monitoring of your business's network activity is vital to detect data breaches, cyber threats, and other system vulnerabilities. Protecting your data and assets via security monitoring is resourced by highly skilled professionals who can promptly access, investigate, and respond to questionable incidents across your network shutting it down quickly. This reduces the risk and loss that can be attributed to any malicious activity, early detection is the key to the prevention of a full-blown event.

TIP 9. FAIL TO PLAN, PLAN TO FAIL.

Have a detailed plan and the tools in place to respond to unauthorized access to your systems, outlining essential procedures, policies, and contacts to quickly identify and address detection of unapproved access to your network. Having systems in place that allow experienced teams to access and carry out investigations efficiently and quickly will reduce the cost of dealing with an incident. It is no longer if but when.

TIP 10. MAINTAIN REGULAR BACKUP SYSTEM

Having a solid backup policy is the difference between your business surviving and failing a cyberattack. It's highly recommended that you implement a disaster recovery plan in case of a data breach, which includes:

- Regularly backing up your systems
- Testing of your backup systems
- Hosting your backups in a secure location.