CHANI SIMMS *BSc (Hons), FBCS, CHFI, ISO 27001 Lead Implementor, CIS LA*
LinkedIn: https://www.linkedin.com/in/chani-simms/
LinkedIn: https://www.linkedin.com/company/meta-defence-labs-ltd/?viewAsMember=true
Website: https://www.metadefencelabs.com/

Chani is an Award-winning Cybersecurity Leader. Managing Director of Meta Defence Labs and Founder of SHe CISO Exec. Platform . She is a TEDx speaker and one of the 50 Most Influential Women in Cybersecurity.

1. IDENTIFY YOUR CROWN JEWELS

Asset Identification: Understand what your most critical assets are - your "crown jewels." These are the assets that, if compromised, could have the most significant impact on your business. Identifying and prioritising the protection of these assets is the first step in building a robust cybersecurity strategy. Ensure these assets are given the highest level of protection and regularly review their security status.

2. LEADERSHIP COMMITMENT & STRATEGY

Leadership Engagement: Secure a strong commitment from senior management to support and prioritise cybersecurity initiatives. Develop a clear and comprehensive cybersecurity strategy that aligns with business objectives. Leadership should foster a culture where cybersecurity is a shared responsibility across all levels of the organisation. Regularly communicate the importance of cybersecurity and ensure that it is integrated into all business processes.

3. EDUCATE YOUR EMPLOYEES

Human Firewall: Regularly educate and test your staff on recognising phishing scams and other social engineering attacks. Use real-world examples and simulated attacks to keep their awareness sharp. Implement continuous awareness campaigns and provide ongoing training to ensure that employees are vigilant and capable of identifying potential threats. Encourage a reporting culture where employees feel comfortable reporting suspicious activities.

4. SECURE CONFIGURATION

Best Practices: Configure all devices and applications securely by disabling unnecessary features and services, changing default passwords, and applying security patches promptly. Enable Multi-Factor Authentication (MFA) for all user accounts, especially for those with administrative access, to add an essential layer of security beyond just passwords. Regularly review and update configurations to ensure they adhere to best security practices.

5. CONDUCT REGULAR VULNERABILITY SCANS

Proactive Defense: Regularly scan your IT infrastructure for vulnerabilities and address them promptly. Use automated tools to identify and mitigate potential security weaknesses. Perform both internal and external vulnerability assessments to ensure comprehensive coverage. Prioritise the remediation of critical and high-risk vulnerabilities to reduce your attack surface.

6. MANAGE ACCESS CONTROLS

Limit Permissions: Restrict access to sensitive data and systems to only those employees who need it for their roles. Implement the principle of least privilege and regularly review access controls to prevent unauthorised access. Use role-based access control (RBAC) to ensure that permissions are granted based on job responsibilities. Remove or disable access for employees who no longer need it.

7. MAINTAIN UP-TO-DATE SOFTWARE

Patch Management: Ensure that all software, including operating systems and applications, are kept up to date with the latest security patches to protect against known vulnerabilities. Establish a regular patch management schedule and automate updates where possible. Monitor for new vulnerabilities and apply patches promptly to minimise exposure to threats. Try patching 'critical' and 'High' vulnerabilities sooner, maybe within 7 to 14 days of relese. You can only do this effectively if you are conducting regular vulnerability scans to identify the issues.

8. DOCUMENT YOUR SECURITY POLICIES

Due Diligence: Maintain detailed records of your cybersecurity policies, procedures, and practices. This documentation demonstrates your commitment to data protection and helps maintain compliance with regulations. Ensure policies are clear, accessible, and regularly updated to reflect changes in the threat landscape and business operations. Include incident response plans, data protection policies, and employee training records. Have people accountable.

9. IMPLEMENT STRONG DATA BACKUP PRACTICES

Data Recovery: Regularly back up your data and ensure that backups are stored securely. This helps you recover quickly from data loss incidents, such as ransomware attacks. Implement the 3-2-1 backup strategy: keep three copies of your data, store two copies on different media, and one copy offsite. Test your backups regularly to ensure they can be restored successfully.

10. ENGAGE IN REGULAR SECURITY AUDITS

Continuous Improvement: Conduct regular security audits to identify and address potential security gaps. Use frameworks like Cyber Essentials, ISO 27001, NIST to guide your audits and ensure that your security measures are effective. Regularly review and update your security controls based on audit findings and evolving threats. Consider third-party independent audits for an unbiased assessment of your cybersecurity posture.