Cyber Security for IT Managers Checklist

☑ ACTIVITY

□ Address findings from a company risk register

Many businesses maintain a risk register, typically focusing on business risks without considering technical aspects. However, it's important to recognise potential business risks stemming from technical origins.

Begin by understanding how technical issues may contribute to business risks and prioritise securing these areas. Identify business risks that could benefit from inclusion in the register, which may also enhance the Senior Leadership Team's comprehension of the situation and potentially lead to budget allocation if security and technical shortcomings pose a clearly-defined risk to the business.

□ Admin alerts

Where permissible, set up admin alerting for new admins created in products and on devices. For example, Google Workspace and other business management tools have options for you to enable alerting when new admin accounts are created or attempted.

□ Automation such as Web Application Firewall (WAF)

Ensure websites and outward-facing assets are positioned behind a web application firewall. Services such as Godaddy, Wix and WordPress have tickbox options or plugins that are relatively inexpensive.

□ Don't use proprietary software and apps if you don't need to!

Where it can be avoided, don't use proprietary software. Custom-built software requires long-term investment and management, which is costly and can leave the business in a vulnerable position if the resource maintaining it leaves the business or fails to document properly. Off-the-shelf products offer a lower-risk alternative.

□ Enhanced spam filtering

Modern email clients have enhanced spam filtering, which is usually free. It's just a case of going into settings and turning on extra security settings.

□ Internal auditing/asset register creation

Conducting an internal audit to assess existing systems provides an excellent foundation for establishing a hardware and software asset register. Once compiled, prioritise these assets based on their criticality to the business. For instance, internal payroll software may be considered a critical asset, warranting immediate implementation of measures such as Multi-Factor Authentication (MFA) and account audits ahead of addressing end-user laptops.

□ JML Process (Joiners, Movers and Leavers)

If a procedure for Joiners, Movers, and Leavers (JML) is not in place, establish one. Ensure that new employees receive only the necessary access for their responsibilities. Restructure access for employees transitioning to different roles or departments, and promptly revoke access for departing personnel.

Implementing a defined process, with designated responsible parties such as managers or the service desk, is cost-effective and enhances the alignment of the business's access footprint with the current workforce and their needs.

□ Multi-Factor Authentication (MFA)

Most, if not all, tools can enable Multi-Factor Authentication (MFA), and it's usually free to do so. Consider conducting a mini audit of the tools critical to the business, such as social media management tools, HR systems, accounting systems, food ordering systems, etc. Prioritise these tools in order of importance to the business and ensure that all of them have mandatory 2FA/MFA switched on for all users.

□ Password managers

Password managers do incur a charge, but they can be relatively inexpensive, and it's money well spent. A good password manager enforces strong passwords, promotes the use of unique passwords and means your employees don't have to remember all of their passwords; they have to remember the one to enter the password manager. These days, some browsers (such as Chrome and Firefox) come with browser-based password managers. These cannot be centrally managed, however, so a product with a management console is highly recommended.

Consider your appetite as a business for enforcing the use of password managers and strong passwords across all tools and systems.

Cyber Security for IT Managers Checklist

☑ ACTIVITY

□ Remote access solutions

Be sure to limit remote access to only what is 100% necessary, keep a record of it and ensure secure protocols are in use; for example, remote SFTP in favour of FTP.

□ Secure build standards

Many companies adhere to a standard configuration for laptops, servers, and cloud instances, yet these standards are frequently poorly documented. Review your standard build and identify security measures such as host-based firewalls and sudoers file editing. Consolidate these security implementations into a standard build sheet, which must be followed before systems are deployed to users or integrated into the network.

□ Security standards

Set some security standards as a basis for the business and seek support from the Senior Leadership Team to enforce the standards. Consider the CIS controls, specifically control group (1), as a starting point for an SME with little to no cyber security investment in place.

□ Understand what technology you already have and make use of pre-existing security settings on tools (e.g. HR and marketing systems)

While crafting a comprehensive asset register, compile a list of Software as a Service (SaaS) products and internally managed items utilised within the business. Many of these possess security features that can be activated with time and perseverance, and most offer well-documented guidance.

For instance, recognising the presence of a LinkedIn page should prompt you to implement security measures within LinkedIn. Avoid focusing solely on technical products and systems exclusive to the tech team.

□ Understand your external attack surface

When producing an asset register, be sure to pay close attention to externally facing assets such as websites, captive portals and accessible servers. This will help you understand what you have and where, as well as how widespread your attack surface is.

□ Vulnerability and patch management process

Ensure you have implemented a process to identify missing patches and perform updates. Consider implementing automated updates if your company policy permits and if it is reasonable for your organisation to do so.

NOTES