Deploying Enterprise-Grade Security – The Rule of Five

Small and medium enterprises deal with the challenge of minimising their business risks without creating an adverse impact on productivity and the ease of accessing systems. IT security policies need to be implemented in a way that they allow the workforce to meet its goals in any location or from any device without the bother of an excessively complicated user experience. Along with this, it is also important to secure the business applications against cyber threats and to ensure compliance in order to avoid data theft. Implementing some fundamental rules can help in this regard.

The security of business collateral is a lot more than just password management. It has to be detailed at every level. In the era of cloud storage and BYOD trends, implementing the business data security policies is even more challenging. While IT administrators have to focus on the security of enterprise data, the non-technical employees only worry about completing their routine tasks within stringent deadlines.

Today, conventional methods such as creating a boundary around business data and using open-source firewalls, VPNs, gateways and confining employee activities to company-owned computers connected to LAN no longer work.

This does not imply that the value of those tools is diluted. They still play a prime role in securing business data regardless of whether employees use personal or company-issued devices. However, these basic security elements now need to help in identifying and applying controls that are targeted towards end-users rather than towards specific devices. It calls for a more balanced approach to the deployment of security at the points where the business data is being accessed both within and outside the boundaries of the trusted IT environment.

A few rules can be deployed to mitigate risks while also ensuring that enterprise security policies do not hinder the employees from fulfilling their daily duties within the assigned deadlines.

Here are five such rules:

1) Continually Review Your Security Policies – New security threats continue to emerge every day and it is impractical to believe that your company directors and IT administrators can simply sit down to draft a series of policies which will work both in the present and in the near future. It is critical to develop formal rules for identity and access, network security, application security, data security and audits. Along with this, you should also have the flexibility to maintain and amend the policies as necessary. Keep evolving your security policies so that they stay relevant and effective in protecting the business data against all kinds of new threats. Also invest periodically in upgraded software and hardware to secure mission-critical systems.

2) Test IT Policies for Clarity and Efficacy – Before a new security policy is rolled out across the organisation, it is advisable to test it on a small team of employees. This way, the IT administrators can check their reactions and see how effective it is in managing the workplace scenarios. It is also important to determine if any of the new policies interfere with critical business functions and prevent the workers from accessing information/data that is vital to fulfilling their assigned tasks.

Such test runs help in discovering issues that managers may have never thought of. The success and loopholes in policy enforcement when employees work from remote locations or use their own devices can also be unearthed through the tests.

3) Engage with and Train Workers Across All Levels of the Organisation – IT policies have to be espoused and supported by the entire organisation – from the junior executives to the C-level officers. The security teams must engage with the members of different teams to ensure that their needs are met. Comprehensive training must be organised to explain the policies, the protocols of using company resources and the consequences of non-compliance with the rules.

4) Check for Vulnerabilities, Manage Patches and Back up Regularly – Network administrators must detect any weaknesses in the company's technology infrastructure before the cyber thieves can. There should be a routine to check the security of the network across the organisation and its branches. The enterprise should also have a code to purge the system of any vulnerability. How and when the security patches will be deployed should be clearly defined in the data security policies.

Another way to ensure that enterprise data is stored safely is to schedule regular backups in the cloud or on external hard drives. Complete backups for servers on a weekly basis and more frequent incremental backups are recommended for most enterprises.

5) Monitor and Control User Accounts – Companies need to keep a track of all employees who can access the critical business information. Often, the sources of data compromises are legit but inactive user accounts. This is commonly the case when employees resign or are laid off but their accounts are not deactivated. A disgruntled ex-employee can misuse the company's data and this can be detrimental to business interests. IT policies should require the administrators to check and regulate user accounts diligently for preventing illegal activities.

These rules are important because enterprise-grade security is a vital area of concern for any business. When you look at all the information that you manage in virtual storehouses – including company financial records and customers' information – it is simple to understand how any breach could result in serious consequences for the organisation.

Enterprises today need comprehensive security measures irrespective of how their employees work – from any location, on any device and with any method of information access. With investment in tailored security products for business continuity, mobile device administration, firewall, intrusion prevention, anti-malware and anti-spam software, organisations can ensure both security and desired productivity levels in their work environments.