Does Higher Collaboration Mean Lower Security – An Analysis

Improvements in employee productivity are vital to the growth and success of any business. A number of digital tools are now available for effective collaboration, which enable remote team members to be more efficient and productive. However, as employees collaborate with their colleagues to share data and insights, it is also necessary to ensure that such teamwork does not allow the leakage of confidential details to unauthorised people and hackers.

As businesses take on versatile technology tools for smoother collaboration between their employees and with customers, the security and data privacy concerns are also mounting. Surveys show that security remains a key focus for organisations that invest in IT frameworks, and this is particularly serious for collaboration apps that can contain critical business information – their customer details and the new innovative ideas they are contemplating.

The corporate world has been increasingly talking about the advantages of collaboration tools, and the IT companies designing them emphasise how they contribute to more organic and productive teamwork on projects.

Collaboration tools cover several solutions. These may be video conferencing, Voice over Internet Protocol (VoIP), instant messaging apps and document sharing. It is, however, also necessary to be wary of the security threats associated with these tools. Document sharing platforms, remote support applications and virtual events carry potential risks. An organisation using these tools must have the processes to evaluate vulnerabilities and implement viable solutions when it prepares its kit of collaboration tools.

Here is a closer analysis of the security concerns with these systems and procedures that can be used to circumvent them:

**Authorised users may access sensitive information not relevant to their process**

Different employees in your company may have their specific levels of access to the collaboration platforms. With these systems, data can stay inside partitions. As an example, different departmental projects and processes may have their own distinct areas, which only the team members can access.

To avoid compromise on any user’s information, check how flexible the collaboration tool’s points of user access are, and determine the possible risks at any level. The solution here is to let administrators set up strict controls around the information that each user can see and set alerts whenever anyone tries to delve into information that he or she is not allowed to check. There should also be an ability to terminate the access rights (including all authorised users) for any account that has been compromised.

**Breach of login credentials**
Do your team members still use words like ‘password01’ for their logins? Collaboration tools usually have a username and password login structure. If these get hacked for an employee, his/her access can instantly give unauthorised people a direct route to financial details, confidential company information and customer data.

A business can tone down these concerns with strict password rules – such as a combination of upper and lowercase letters, numeric and special characters and a certain length. It should also be a mandate to change the password frequently – preferably every quarter. Another strategy is to use device-based OTP recovery of passwords rather than going for security questions that can be decoded by social engineering.

**Threats from the Internet**

If collaboration tools are used from the public Internet, the user’s login credentials and data are exposed to numerous threats such as malware and unauthorised tracking.

The antidote here is to let the employees (accessing collaboration tools) use an application that gives them access to confidential information only through safe VPN connectivity.

**Summary/minutes of meeting settings**

Even if you have a very secure collaboration system, but you also send regular summaries or minutes of online meetings to employees and vendors through an email service, there are chances that you are unknowingly exposing protected information. There could be weaknesses in your email setup, and when workstations are unlocked, the summaries can be read by people who were not even in the mail list.

Instead of using email for this purpose, it is advisable to choose collaboration tools offering ‘recent activities’ synopsis within the platform. These can be conveniently accessed when the authorised users log into the security setup.

**URL-related problems**

Cyber criminals can also get access to business data by following basic protocols for web-based applications. As an example, businessname.appname.com or .co.in may lead to the personalised section of a company on a web-based app. Certain collaboration tools can also pull metadata from the software into the URLs, and this can inadvertently expose confidential information.

It is, therefore, good to select a collaboration tool that gives the business IT team flexibility to manage security settings and establish a URL structure that is tailored and secure.

While businesses understand the benefits of digital collaboration tools, it is also imperative for them to choose secure solutions that are well encrypted and adhere to the compliance laws in their industry. The IT administrators must be aware of any security threats associated with these tools and have policies to address them.
In rolling out best practices and carefully choosing your vendors in this regard, you will realise long-term ROI on efforts for secure collaboration.