Got something to say?
If you have any comments to make on this issue, please e-mail: david.ndichu@itp.com

Ram Vaidyanathan

Cyber-crime in an age of collaboration

> To fight data breaches and defend their business, organisations must protect all entry points."
>
> **Ram Vaidyanathan, IT evangelist at ManageEngine**

Collaboration, the cornerstone of many a successful organisations, often comes with a risk. This is because these tools can provide new points of entry for hackers looking to cause damage, a risk that will only grow as employees use collaboration tools to maximise their company's productivity.

Cyber-crime costs the global economy as much as USD 450 billion each year. And, the median cost of cyber-crime has increased by nearly 200% in the last five years.

Meanwhile, collaboration has become the cornerstone of successful organisations. But collaboration often comes with a risk. The number of cyber-attacks will grow as employees increasingly use collaboration tools to maximise their company's productivity. This is because these tools can provide new points of entry for hackers looking to cause damage.

Here are three ways in which an organisation's security can be compromised due to increased collaboration.

A wolf in sheep's clothing

Companies collaborate ith suppliers, vendors and customers in the cloud every day. Consider this scenario: A supply chain executive receives an automated weekly email with an MS Excel file from their logistics partner, giving the estimated time of arrival for products. A cyber-criminal somehow discovers this practice. The criminal then impersonates the logistics partner by using a similar email address. The executive doesn't notice and downloads the attachment—an executable (.exe) file masked as a MS Excel file. When the executive opens the file, a wolf in sheep's clothing enters the company's network to steal trade secrets, financial data, and customer information. This modus operandi, called spear phishing, is popular globally. By some estimates, 91 percent of all attacks begin with spear phishing (Wired.com).

A betrayal

With the advent of bring your own device (BYOD), collaboration has become fairly common. Employees can now access work files while away from the office and increase their productivity. On the other hand, disgruntled employees can easily expose information or even sabotage company files. What if an employee who is about to join a competitor were to print customer contact details from a remote location? And what if this employee took this information to the new workplace? This betrayal could lead to the company losing its competitive edge.

A foreign adversary

Even governments are not immune to cyber-attacks from foreign state-sponsored adversaries. Government employees may visit certain websites frequently to collaborate with employees from other departments or with their citizens. Malware placed on these sites could exploit vulnerable end points and compromise the devices of any visitors. Malware can also morph into more serious advanced persistent threats (APTs) that can lurk in the victim's system for a long time. This way, these adversaries could secretly keep a tab on issues of national security and international policy. When governments can face such threats, businesses are all the more at risk.

To fight data breaches and defend their business, organisations must protect all entry points.