Security And The End User

More than ever, user education, predominantly through the use of global electronic communications policies, is becoming central to securing company networks and avoiding cyber-attacks. Ultimately, organisations that want to leverage BYOD without risking security breaches must ensure that users take personal responsibility for how their behaviour can impact a company's network.

HR and IT must collaborate in order to set out clear and well-publicised rules while using training sessions to educate users on the consequences of non-compliance. In addition, conducting internal IT security policy quizzes or tests for employees will encourage users to learn policy violations and their potential impact on the business. Organisations can also consider registering employees for free daily online security tips, like these from the SANS Institute.

Communications policies should aim to outline what is expected of employees and what they can do to protect corporate networks and devices from malicious attacks. The simple and often common-sense measures that employees can take to help keep data secure are often the most effective. This includes the immediate reporting of lost devices, working closely with the company's IT team, refraining from installing apps from unknown sources and not putting off security updates.

HR should work together with IT to encourage employees to have different passwords for various sites, while ensuring that the password itself is strong, with a combination of numerals, letters and special characters. If employees are using a public computer, it is imperative that they log out when finished and not share passwords with others both internally and externally or leave them anywhere easily accessible.

Public or unsafe Wi-Fi networks can also pose a serious security risk to organisations, particularly if employees are travelling abroad. When processing financial transactions and sharing sensitive information it's safer to use a protected private network (wired or wireless).

We tend not to exercise the same amount of caution while sharing information on social media as we do with other forms of peer-to-peer communication. It is essential that employees are aware of what information they are sharing over social media. It's not only friends and professional connections that are privy to your information. There can be cyber-criminals snooping around, and listening in on your conversations and social messages.

Untrusted, potentially malicious sites will often appear genuine, but in reality can mislead employees to disclose personal, financial and secure information (such as username password, bank account number or credit card PIN). Phishing is becoming increasingly common on the Web. Employees should only enter passwords on websites when they know it is a trusted source and never by following a link in an email or chat message.

Additionally, by checking that websites have the closed padlock symbol on the address bar, employees help ensure that the right encryptions are in place to secure data integrity. If sites appear fishy, users should come out of them immediately and inform HR and IT to ensure credentials have not been compromised.

Companies must also be cognizant of data theft from within the organisation, often caused by the ease of access to data. USB Data Theft has been the simplest form of insider data theft because, all it takes is to plug in a flash drive and copy sensitive or confidential information.

Over the past few years, we have seen so many organisations tracking down the loss of sensitive and confidential information to have happened owing to usage of USB drives and other mass storage media. Making sure that your employee signs a privacy agreement alone is not a strong deterrent. Typically, it could be a disgruntled employee that decides to just copy sensitive information and tries to leak it externally or may be a case where an employee's unsuspecting USB device has a malware in it which can automatically trigger a script or code to install or run on your system and steal data.

Transmitting sensitive files online using online file sharing tools has also become common practice with the advent of cloud-based solutions like Dropbox and Google drive. So when an employee tries to share files or transfer files through insecure channels, there are chances that sensitive corporate data can be easily accessed by third parties especially when data is stored in the public cloud.

A concerted plan to curb employee data theft should incorporate admin, human resources, IT and top-level management. There are steps that a watchful and well-equipped IT department can take to pre-empt data theft, with network data providing valuable insights into employee behaviour. With the help of a reliable security and management tools, organisations can build rules to restrict unauthorised access and be notified about violations. You can also build an authorised group with limited people and ensure that they are the only ones with privileged access to business critical data.

Security education is part of smart security preparation. Better awareness and preparedness will help avoid many commonplace security lapses, ultimately better protecting an organisation's intellectual property and corporate data.

Don Thomas Jacob, Head Geek, SolarWinds.

Don Thomas Jacob has worked in a variety of tech roles including tech support engineer, product blogger, product evangelist, and tech marketing lead. His experience and interests lie in network performance monitoring, security analytics, packet inspection solutions, flow-based technologies like NetFlow, sFlow and IPFIX, and technologies such as QoS, NBAR, IPSLA, and Cisco Medianet and MediaTrace. Don follows tech blogs like Wired.com, TechCrunch, and ARS Technica, and struggles to decide whether Neo, Yoda, or Darth Vader rules the sci-fi universe. For further information visit www.solarwinds.com