Three Quarters of CEOs Admit to Using Unapproved Programs and Applications, Putting Critical Data At Risk

Submitted by: Chameleon PR (and MWW)
Tuesday, 16 May 2017

At the same time, 65 percent of CIOs and 63 percent of CEOs state that losing this data would destroy their business

16 May 2017 — Today, IT decision makers (ITDMs) say that half (50 percent) of all corporate data in the enterprise is held on laptops and desktops, instead of in the data centre or centralised servers. In the U.S., this rises to as much as 60 percent. Simultaneously, the significance of this data to the productivity and security of the business is well understood at the top of the organisation — with 63 percent of CEOs stating that losing this data would destroy their business. But, awareness of the risk is doing little to change adherence to proper security practices.

CEOs are playing a game of chance with critical corporate data

Despite the known risks facing organisations today, such as data breaches, business decision makers (BDMs) and CEOs are putting critical data at jeopardy. Three quarters (75 percent) of CEOs and more than half (52 percent) of BDMs admit that they use applications/programs that are not approved by their IT department. This is despite 91 percent of CEOs and 83 percent of BDMs acknowledging that their behaviours could be considered a security risk to their organisation. These findings are revealed in Code42's CTRL-Z Study (https://www.code42.com/go/ctrl-z/). It explores, in detail, the pressures faced by CIOs, Chief Information Security Officers (CISOs) and ITDMs, and compares their responses to the views of CEOs and BDMs who control the majority of the data outside the four walls of the enterprise. The Study, which takes into account the views of 800 IT decision makers — including CIOs, CISOs and CSOs — and 400 BDMs — including CEOs — within the U.S., U.K. and Germany, highlights that security and productivity are intrinsically linked in a data-driven economy.

Brand reputation is at risk due to a heightened focus on productivity over data security

There's an ever-persistent balancing act between productivity and data protection in the modern enterprise. Now there is added pressure on ITDMs to help the enterprise rapidly recover from a breach, if it hopes to minimise a hit to reputation and ensure customer loyalty. The vast majority (80 percent) of CEOs and 65 percent of BDMs say they use unauthorised applications/programs to ensure productivity. However, half of ITDMs (50 percent) say that their ability to protect corporate and customer data is vital to their company's brand and reputation — a sentiment that is shared by 50 percent of CEOs and 61 percent of CIOs. The majority of ITDMs do have laptop (86 percent) and server backup (95 percent) in place. However, at least 13 percent and 8 percent, respectively, have not tested their laptop or server backup programs. This tells us their approach is more of a "checkbox for compliance" and not a solution that adds practical value to the employees. If an enterprise-wide failure, such as a widespread and devastating ransomware attack, took place today the questions would be: "Is your IT team prepared to get you back up and running?" and, "How long would you take to be productive again, considering the amount of data held laptops and desktops?"

"Modern enterprises are fighting an internal battle between the need for productivity and the need for

security—both of which are being scrutinised all the way to the CEO. By using unauthorised programs and applications, business leadership is challenging the very security strategies they demanded be put in place. This makes it clear that a prevention-based approach to security is not sufficient; recovery must be at the core of your strategy," said Rick Orloff, VP and CSO at Code42.

An ever-evolving threatscape requires focus on both prevention and recovery

Now is definitely the time for change, and the enterprises that want to remain competitive are starting to act. It is a time for IT security visionaries and leaders to step forward. While 66 percent of BDMs and 66 percent of ITDMs agree that it will be up to CIO/CISOs to help their businesses adapt to the realities of the new threatscape in 2017, these figures also suggest there's an opportunity for change. The question remains that, if it's not the CIO or CISO, then who should take leadership on this front? One thing is certain: Globally 88 percent of enterprise ITDMs and 83 percent of BDMs believe that their companies will have to improve their breach remediation in the next 12 months. After all, as the saying goes, "It is not if, but when you will be attacked" — with as much as 48 percent of enterprises revealing that they have been breached in the last twelve months.

"The CTRL-Z Study brings a new perspective to my own experience in advising enterprises globally. When it comes business success it is all down to productivity and agility. Security in the modern enterprise is no different. Your strategy has to be built on three key pillars. First, you have to be able to spot risk sooner. Gaining visibility over where your data is, how it moves and who accesses it could act as an early warning system to alert you to both inside and external threats. Second, the enterprise as a whole always needs to be able to bounce back quickly and efficiently. Should a breach occur, your internal teams and the backup solutions you have in place need to be tested and ready to face the activity without it looking like a fire drill. Finally, if your business is to remain competitive, it needs to be able to recover quickly. Time is money, and in the modern enterprise, so is data," concludes Orloff.

Press contact: Tom Hunt
Telephone: 020 7680 5500
Email: code42@madebychameleon.com