greenbox

Warning! Blind Spot.

Data Breach may be closer than it appears. Why every Director should be talking about their data security policy blind spot.

Email this article:

Cyber security policy is generally focused on the risks of a breach for live on-network devices, but there are usually few or no policy settings for how devices and their associated data are to be managed at end-of-use. It's a little understood risk, with catastrophic repercussions.

A 2013 Osterman study revealed 16% of the companies surveyed suffered a data breach due to improper disposal of data bearing devices.

The recent OCC case against Morgan Stanley for an ITAD (IT Asset Disposition) related data breach found that they 'failed to adequately assess risk...' and 'failed to exercise adequate due diligence...' resulting in a $60M fine with further actions pending.

Shane Mulholland GAICD, Australian ITAD pioneer and innovator, says that company boards lack awareness of the policy shortfalls which are leading to data breaches. Mulholland says, "The velocity of this risk is totally identifiable, totally avoidable and totally stoppable with the right policy and compliance settings in place."

Mulholland notes the lack of ITAD policy is the key driver in end-of-use asset disposition data breaches. "Junior decision makers are often left to apply their own criteria. This is due to policy blind spot; that is, the lack of a clearly defined policy covering the key areas of data erasure standards, compliance and environmental objectives." says Mulholland.

Unfortunately, as with the Morgan Stanley case, when the financial outcome is the primary decision criteria, the risk of a breach significantly increases.

One of the world's largest lab study of second-hand storage media conducted by Stellar® provides empirical evidence of the lack of awareness concerning safe data disposal practices. This study revealed that over 71% of the devices analysed contained personal data and business information. Further, an alarming number of the devices studied were disposed of in secondary markets without using proper data erasure tools.

This policy blind spot is potentially a multimillion-dollar mistake as seen with European Union's tough data protection regulation, GDPR (General Data Protection Regulation), which is now effective across the EU. GDPR violation can result in fines of up to 4% of the company's annual turnover, or $32M AUD.

The international ITAD industry has in recent years reached a point of maturity where an internationally recognised standard, R2, has been adopted. This ultimately ensures compliance and accountability. ITAD's opt to adhere to the standard and have their adherence verified by an independent body. ITAD's with R2 are scrutinised to ensure that what they say they are going to do for a customer is, in fact, what they do.

It is essential now more than ever, that your business has policy in place around the decision making process of end-of-use devices. Remember to check that your ITAD has the R2 certification, guaranteeing external oversight of the ITAD process. If your business is potentially vulnerable and needs a confidential ITAD risk assessment or policy drafting advice, reach out to Greenbox for assistance.

greenbox.com.au