Date:	25 July '15
Frequency:	Daily
Circulation:	Unavailable

The CIO P (Chief Information Security Protection) Factor By @ABridgwater | @CloudExpo #Cloud

What should the CIO's strategy be in protecting company IP and other assets in today's mobile enterprise?

The CIO P (Chief Information Security Protection) Factor

It's easy to invent additional C-suite job title designations. We might conjure up Chief Data Analytics-Insight Officer (CDAIO - pronounced "see-day-oh") for example.

Equally, we can see that the role of the CIO quickly gained additional layers some time ago - and we now see the CSO (Chief Security Officer) quite commonly being ranked as the CIO's right hand man or woman.

IT facilitator & IT protector

With this expansion of the CIO role itself in mind (some companies won't be able to afford a dedicated CSO or will fail to formally create the role for other reasons), we should perhaps offer greater empathy, deference and respect to the new CIO who has to serve as both IT facilitator and IT protector.

Why is this? Because, quite simply, security today is definitely a business issue - and managing risk is growing in importance, according to the 2014 State of the CSO Study (conducted by IDG Enterprise).

That very study found that heads of security (whatever job title we adorn them with) are more involved in both IT and corporate/physical security decisions compared to non-heads of security (i.e. lower ranking staff), who are more involved in IT security decisions alone (i.e. without the physical/corporate element).

This suggests two things:

- The CIO (or the CSO if he/she exists) has to place trust in the hands of the practitioners who use the software tools and platforms that are in place in terms of these individuals knowing what protection is needed where.
- The board C-suite level of responsibility for corporate/physical security decisions is increasing.

This second point might seem comparatively obvious; but it leads us to highlight the fact that users' devices (and the increasing rise of the Bring Your Own Device practice) are creating a security risk that is increasing all the time. Every week sees another story surface on smartphone theft and the scamming tricks used by cybercriminals in 'new' risk areas such International Revenue Share Fraud (IRSF).

The situation is so worrisome that even Europol (the EU's law enforcement police service) has started getting involved with local national European police forces - work carried out in Spain is just one example.

Which CIO strategy?

What should the CIO's strategy be in protecting company IP and other assets in today's mobile enterprise?

Note: To answer this question: managing security/addressing risks around mobile devices, BYOD was the number one security-related challenge in the coming year, cited by 54% of respondents in the IDG study.

How can the CIO protect the data center from cyber threats? How can they reduce the risks to their businesses? Is cyber security even on the CIO agenda? These are the questions that CIOs need to be asking themselves -- and, unfortunately, it appears that an unhealthy percentage of firms classed in the SME/SMB (small to medium sized business/enterprise) fail to take adequate steps to prevent themselves.

Some of the steps needed here can be quite physical and practical i.e. why use USB drives when you can use encrypted drives that come with password controls?

One of the superior models in this field is the iStorage datAshur.

The iStorage datAshur is the world's most secure, easy to use and affordable USB flash drive, employing PIN code access with military grade AES 256-bit hardware encryption. The datAshur incorporates a rechargeable battery allowing the user to enter a 7-15 digit PIN onto the on-board keypad before connecting the drive to the USB port.

Remember, some of the larger firms fail to appoint a direct CSO at all, so it falls to the CIO in any size firm to take on the responsibility for security protection -- and that means a whole lot more than basic anti-virus and/or firewall protection these days. It stretches from the risk to physical devices across to corporate phishing scams and cyber-espionage.

With a growing number of vendor options, it is necessary for vendors to produce solutions that align with business needs. But we can not sit back and rely on the vendors themselves to produce cross-platform cross-use case products -- it is the responsibility of the CIO to map his or her firm's own threat landscape out and look to engineer protection from the range of solutions currently available.