CIS0 – The what, how much and will they stay

The demand for Chief Information Security Officers (CISOs) is outstripping the availability of experienced professionals in a big way and is likely to do so for some considerable time. As you'd expect, this arrangement means filling CISOs roles with suitable candidates will remain an expensive and difficult task for the foreseeable future – keeping a CISO could be even harder.

Before rushing headlong into the race for an experienced CISO, let's take a quick look at what they do, whether you need one, how to keep one and whether outsourcing is a way of managing security despite the challenges.

What does a CISO do?

A CISO is a senior executive who is ultimately responsible for creating the vision and strategy that protects the data an organisation processes, but in a way that also supports its operational objectives. The CISO ensures appropriate security technologies, processes and awareness exist and that these are applied, adopted and maintained in order that the security posture is unaffected by malicious attack, accidental behaviour and unintended consequences or external influences. The CISO also ensures legal and contractual security obligations are met with regulators, standard bodies, contracted customers, partners and employees.

Key to the CISO's role is understanding the organisations information security assets along with their current and future risks and translating these into people, process and technology security measures that keep information confidential, accurate and available. To support the corporate risk management programme, the CISO ensures the board understands where information risks sit against their appetite and recommend strategies for managing those risks.

The CISO is also responsible for the third-party supplier's management programme from a security perspective and the assessment and monitoring of suppliers where they could potentially impact security or privacy in a negative way.

The CISO role interfaces with almost every department to ensure security is embedded into their operation but in a way that enables rather than unnecessarily constrains.

How much do they cost?

Like all roles, published salary scales can be misleading however as a general guide, a good one (after all that's the one you want) employed in a small to medium size enterprise will typically command a UK salary of between £110k and £150k per annum, at the upper level, around 80% of this will be base salary. These figures grow exponentially for large listed enterprises and other parts of Europe and the US often pay more. As with other executive positions, you would expect to add private healthcare, a generous pension and car allowances. Given the high demand and current relatively small pool of qualified professionals with 5 plus years' experience, you should be aware they will be receiving 4-5 direct approaches a week from recruiters – therefore, if you plan to hold onto a CISO it's important to arrive at a package that is financially attractive and also offers status and an environment where they are free to explore how emerging technologies and risks will impact the organisation. Variety of work and the space to undertake research are essential elements in keeping a CISO happy.

Do you need a CISO and will they stay?

There is a strong chance your organisation needs a CISO but here are few quick checks to help you decide. The more you answer no to, the greater the need for a CISO

- Do you understand your organisations regulatory and contractual obligations for protecting data?
- Are you confident the organisation is meeting its contracted or regulatory obligations for protecting information?
- Are you confident a data incident will not derail your organisation's objectives?
- Is the board confident it has the expertise and time to take ownership of the responsibilities of a CISO?
- Do you have the ability to translate data risk into the business risk and technical and security measures?
- Are you confident the essential security activities are routinely undertaken?
- Are you confident you will be able to navigate an incident in a way that limits the financial, legal, reputation and operational risks?
- Does your organisation have a culture of security that is adopted by all employees?

With regard to the question of keeping your CISO, here are a few more questions:

- Will the board accept this role as a senior level position and afford the CISO the respect of the role?
- Will the board be happy/able to pay the salary of a top ranking CISO?
- Will the board support the CISO with resource as required to address issues above their stated risk appetite?
- Will the board afford the CISO time to cultivate an understanding of potential future risk?
- Will the board be willing to review salary and benefits packages on an annual basis?

Is outsourcing a better option?

For many organisations, the first set of questions almost always identifies a need, however the second set often stimulates lengthy debate where large enterprise organisations arrive at a yes vote whereas small Enterprises may be less certain. In the case of the latter, it may be that an outsourced CISO will provide a better option.

Outsourcing the CISO function to a consultancy may offer organisations a credible alternative to insourcing if the consulting company can provide a consistent, highly skilled and experienced consultant on a regular basis. It becomes even more attractive if the consultancy can provide access to a wider talent pool capable of consulting across a broad range of specialist security and privacy subjects.

A significant benefit of outsourcing is the integrity of the advice passed to the board, which can be unencumbered of internal politics and be solely motivated by protecting data in a way that supports the organisations operational objectives.

Critical however to the success of this model is the frequency with which the consultant is contracted. A consultant who is working in a large organisation for less than 2 days per week us unlikely to get through the volume of work or to remain informed on moving parts such as projects, partners, regulator requests and security incidents. However, a 3 day per week arrangement with access to remote support for the remainder, can bring consistency, reliability, strong progress and enough visibility and access to the board to make outsourcing a realistic option.

But what about the financial cost?

A further consideration is cost, when calculating hidden costs of employment such as recruitment fees, employers NI, benefits, IT and management, a 3-day per week outsourced service is likely to be similar to that of a full-time CISO. However, there may well be other benefits associated with an outsourced CISO service that can tip the argument in the favour of outsourcing, these include the external validation, decision making and advice that is unencumbered by internal politics and with the right consultancy partner comes accessing a whole team of specialists rather than just one person.

Want to understand more about this subject ? Get in touch at info@cortida.com