Security Think Tank: Outsource responsibility, not accountability

What critical security controls can be outsourced and how do organisations, SMEs in particular, maintain confidence that they are being managed effectively and appropriately?

I often use the saying: “If it is not your core business, consider outsourcing.” This generally works when it comes to business support functions, such as accounting, bookkeeping, legal services and design, for example.

However, when it comes to information security, the cut is less clear because “security is the responsibility of everyone”. Although it is a cliché, it sums up the intertwined nature of security in any business. While the various business functions can be seen as verticals, security cuts right through them all.

For the purpose of this article, a small to medium-sized enterprise (SME) should strongly consider the following in-house/outsource advice:

- Security policies – keep in-house and consult with a professional.
- Organisation of information security – consider outsourcing the chief information security officer (CISO) function to external professionals.
- Identity and access management – keep the people management function in-house, while outsourcing technical access control to a managed services provider (MSP).
- Asset management and data classification – keep in-house and consult with a professional.
- Operational and network security – outsource to MSP.

- Physical security – outsource to MSP.
- Systems acquisition, development and management – outsource to a professional development company.
- Resilience to incidents – keep in-house and consult with a professional.
- Supplier relationship – keep in-house and consult with a professional.
- Compliance – keep in-house and consult with a professional.

The above might differ for various types of SME verticals. In all cases, however, it is critical to retain overall accountability for information security in-house.

Finally, a good set of key performance indicators (KPIs) and metrics should be agreed with one or more MSPs.