EIP

Interview: Mark Challis talks Information Security

EIP achieved ISO 27001 certification last year and, in October 2020, we completed our year one surveillance audit.

EIP IT Operations & Security Manager, Mark Challis, answers questions about Information Security in the context of the Covid-19 pandemic.

Why is ISO27001 certification important to EIP and have recent events made it more important? If so, how?

Like everyone, we had been following the earliest developments of the burgeoning pandemic throughout the world at the beginning of 2020. By early February, the Information Security Management Team met for our quarterly meeting (regular meetings are a requirement of the ISO 27001 standard), to conduct a risk assessment and identify what operational and security challenges the Covid-19 pandemic could potentially bring to the Firm and our day-to-day operations.

Even though the notion of a national lockdown was just an implausible eventuality back then, we started to evaluate the logistics as well as assess our level of preparedness at a very early stage. Thankfully with our ISMS (Information Security Management System, another ISO27001 requirement) at the core, we were able to approach the identified risks with confidence and ultimately work together with our BCP (Business Continuity Planning) Team to come up with a solid plan of action.

In the end, the combination of ISO 27001, our business continuity plan and a robust hybrid IT infrastructure with disaster recovery at the core, enabled us to securely shift everyone to a work from home (WFH) environment from day one of the lockdown.

How did you address the security implications of this sudden change of working environment?

Roughly two-thirds of the firm were already setup to work remotely but, from a security perspective, the sudden increase in remote working brought an additional level of risk. Could we, or instance, allow staff to use their personal devices to connect to our network without compromising security?

As well as raised internal security threats, there were also external factors that had to be taken into consideration. An example being the huge increase in phishing and malicious email attacks being reported since the beginning of the Covid-19 pandemic. A lot of these additional security threats are often overlooked due to a lack of resources available to IT departments.

At EIP, being ISO 27001 certified meant that we had an existing framework, ensuring the necessary remote working policies, compliant IT systems and staff security awareness training were already in place. This helped us remain compliant throughout.

What were the unique challenges of going through the year-one surveillance audit during the pandemic?

Despite lockdown restrictions and government guidelines on working from home, we were still able to conduct our year one surveillance audit remotely in October 2020.

Having worked on many ISO 27001 projects over the years, this was my first remote audit, and I am pleased to say that it went very smoothly. This was undeniably facilitated by our IT environment; the main differences with a traditional onsite audit included virtual office tours, which were completed via Microsoft Teams, as well as remote interviews with home-based staff members.

Whereas we would have normally given the auditor hard copies of the various documents required to demonstrate compliance with the standard, they were instead shared remotely within a secure environment with access being granted and revoked in a matter of seconds.

What does being ISO 27001 certified mean for EIP's clients and potential clients?

At the beginning of the Covid-19 pandemic, we had several clients enquiring whether we would be able to continue meeting all of our contractual obligations in terms of information security. Thankfully, with the ISO 27001 framework in place, we were able to reassure them immediately that it was business as usual.

From a more general perspective, ISO 27001 is widely regarded as the gold standard in information security; as an IP law firm, we deal with a lot of sensitive information and securing our clients' data is a top priority for the firm. ISO 27001 certification shows our strong commitment by demonstrating that formal security and risk management controls are in place to protect the confidentiality, integrity and availability of sensitive company, client and personal information.

Historically, the completion of complex and lengthy security questionnaires was often part of the tendering process with potential new clients. Being ISO 27001 certified has had a significant impact in streamlining this process as it instantly vouches that a security framework is in place and is regularly audited by an external certifying body.