Raising THE BAR in information security

Gordon Smith is a freelance technology journalist

ByrneWallace has become the first large Irish law firm to be certified with an internationally recognised independent data security standard. Gordon Smith reports

Information security has steadily made its way from the server room to the boardroom, and what was once seen as purely a technology issue is now firmly on the business agenda. The latest Irish economic crime survey from PriceWaterhouse Coopers found that cyber-attacks against Irish businesses have almost doubled since 2012. Then, 25% of companies that suffered economic crime said they had experienced some form of cybersecurity incident. Now, that figure is 44%.

ByrneWallace had seen trends like this first-hand, having advised many of its clients about cybercrime and related issues like data protection, and having worked with others who had been

at a glance

- Cyber-attacks against Irish businesses have almost doubled since 2012
- ISO 27001 provides a set of standardised requirements for an information security management system that ensures that the highest standard of controls are in place to address several critical areas
- Achieving ISO 27001 certification helps keep confidential information secure, provides customers and stakeholders with confidence, and allows for the secure exchange of information

affected by security breaches in their own businesses. "Cybercrime is increasing exponentially, and the associated risk to law firms is very material," says Catherine Guy, managing partner of the Dublin-based firm.

Some 14 law firms in Ireland have reported cyber-attacks in recent months, reflecting a growing global trend. They're a favoured target of cybercriminals because of their data, explains Brian Honan, CEO of BH Consulting, an independent IT security company. "Many law firms have very sensitive information about high-value individuals or corporate firms – that could be mergers and acquisitions data, contracts and other valuable information," he says.

Business risk

ByrneWallace had identified cybersecurity as a business risk. One of the larger law firms by Irish standards, with 200 employees and 37 partners, it has a quality and risk committee whose remit includes assessing all business risks to the firm. After raising the cybersecurity issue, ByrneWallace's management committee decided to become certified for ISO 27001.

> The biggest challenge in obtaining the certification is because the standard is so extensive in scope

FOCAL POINT

steps to security

ByrneWallace took 13 months to complete the ISO 27001 project, starting in May 2015 with the research and planning, and culminating in the award in June 2016.

The project began with an assessment stage to research and plan what would be involved. Once the decision was made to proceed, the firm set up an Information Security Management Systems Committee to deliver the project. Director of finance and operations David Dinn led the group, which included IT head John Kelly, supported by the firm's HR manager, facilities manager, compliance manager and an associate lawyer with data protection expertise.

August-September 2015

Stage 2 was the 'gap analysis', which involved examining the firm's physical and non-physical security processes and controls and related documentation, in order to compare them to best practice as outlined in the standard. Here, ByrneWallace had an advantage in its favour, having been accredited for the Lexcel (an international quality standard for legal practices) in 2012. "This meant that roughly 50% of the processes and controls required by ISO 27001 had, in fact, been already implemented," Dinn explains.

October 2015-May 2016

Stage 3 was the risk-assessment process. Dinn emphasises that this process is never actually complete, but is a continuous loop between assessing, resolving, and reassessing.

December 2015-March 2016

Stage 4 was one of the biggest segments in the project: document preparation. "All processes and protocols must be fully documented to ensure compliance. Given the scope of the standard, this meant that we had to complete a detailed workflow for hundreds of processes," says Dinn.

January-March 2016

Stage 5 covered process implementation: rolling out the new processes and ensuring that all 200 staff received extensive and exhaustive security training. Dinn: "We constantly monitor that our processes are adhered to and we complete internal quarterly audits, with exception reports provided to the quality and risk committee for action."

January 2016 and ongoing

Stage 6 is the awareness campaign – actually a series of campaigns across the firm that included posters, intranet bulletins and questionnaires, 'lunch and learn' sessions, and publishing a handbook for each member of staff for FAQs and protocols applicable. "Cybercrime targets individuals in a business constantly, including via direct email contact such as ransomware," Dinn points out. "We understand very well that the system is only as good as the resilience and awareness of every individual staff member, and creating and maintaining awareness is a continuous and never-ending process."

The certification process itself involves two phases. The first involves careful external scrutiny of the applicant's documentation – which outlines processes, controls and responsibilities – to ensure they comply with the scope of the standard. The second-phase audit took place eight weeks after passing the first. "This is designed to ensure that you are 'living' the standard and that you actually do what is set out in your procedural manuals. There are then bi-annual audits to confirm continuous compliance and retention of the certification," says Kelly.

"ISO 27001 is an internationally recognised independent security standard that shows companies follow recognised best practices for treating the data their clients and customers entrust to them," says Honan.

ISO 27001 provides a set of standardised requirements for an information security management system that ensures that the highest standard of controls are in place to address several critical areas: confidentiality, integrity and availability of information about customers, continual protection of assets, IT governance and legal compliance.

David Dinn (director of finance and operations, ByrneWallace), Catherine Guy (managing partner, ByrneWallace), Rob Lyons (sales manager, Certification Europe), and John Kelly (head of IT, ByrneWallace)

In successfully obtaining the certification, ByrneWallace became the first large law firm in Ireland to be certified by Certification Europe, the ISO-accredited body. Certification Europe sales manager Rob Lyons says there has been growing interest in ISO 27001 among many businesses in Ireland, largely driven by the recently ratified EU *General Data Protection Regulation*, which comes into force on 25 May 2018.

Going for the certification wasn't a box-ticking exercise for compliance in ByrneWallace's case, according to David Dinn, finance and operations director. "We chose to do this, not because of any specific client demand or regulatory requirement, but because we understood the significance

of cybersecurity threats, the potential impact on our clients and their businesses, and the need to address the risk and threat that cybercrime poses. It is our view that protecting clients' data is one of our top priorities, given the material consequences of a breach," he says.

"The reality of the environment in which we operate is that just one significant cyber-hit could cause significant damage, including reputational damage. We have recognised that this is a real and significant risk and have moved to address and mitigate it. From our perspective, this certification was a 'must have' as opposed to an optional extra," adds Guy.

Strategic initiative

There are several benefits to achieving ISO 27001 certification, says Lyons: "It keeps confidential information secure, it provides customers and stakeholders with confidence in how you manage risk, and it allows for secure exchange of information." In addition, it helps organisations to meet their legal obligations and helps them to comply with other industry-specific regulations. "ISO 27001 certification manages and minimises your risk exposure, builds a culture of security, and it protects the company, assets, shareholders and directors," he says.

Catherine Guy describes the decision to obtain ISO 27001 as a "strategic initiative" for ByrneWallace, given the importance of ensuring the security of data belonging to both the firm and its clients. "The cybercrime environment is now so sophisticated and evolves so quickly, that in order to continuously combat the threats posed by cybercrime, we had to adopt a firm-wide standard that has the continuing buy-in and commitment from the entire ByrneWallace team," she says.

Once upon a time, information security was seen as a cost of doing business – but having a proven and certified method for managing cyber-risk can be a competitive differentiator in the market, Lyons adds.

Dinn says that this point was one of the key pillars in the firm's strategic rationale for doing the project. "ByrneWallace is the first Irish law firm to achieve this certification, and we are in a unique position to provide assurances to our clients about the security of their data," he claims.

Initial research and planning for ISO 27001 began in May 2015, with the formal decision to allocate the resources needed to pursue the certification made in August of that year (see panel).

Catherine Guy says the biggest challenge in obtaining the certification is because the standard is so extensive in scope. "It spans across many areas of the business and ultimately impacts how we all operate, day to day. With so many stakeholders involved in the coordination, buy-in and implementation of the appropriate controls, it took significant effort from all involved to undertake the project while also performing their normal day-to-day duties," she says.

Dinn estimates that the project took more than 2,500 hours, spread across teams including HR, finance, compliance, IT and facilities, along with specific legal input from its corporate department on data protection regulations. "From a money perspective, suffice to say that it is a material investment," he says.

Guy doesn't see the project in terms of a return on that investment, however. "Frankly, we do not expect that the cost will or should be repaid in a tangible way," she says. "Knowing what we know about the environment we work in and the constant threats posed from external sources, it gives us great comfort to know that we are applying internationally recognised best practices to ensure we have robust controls and processes for data security. It also allows us to give that assurance to our clients.

"Achieving this certification has enhanced our own understanding of the extent of the threats and the potentially very serious impact of cybercrime activity and has also given us a very pragmatic perspective on the issues," she reflects.

Dinn describes the project as intense, requiring "significant sustained commitment" from all involved to ensure a successful outcome. He points out that ByrneWallace worked with an external consultant with extensive experience in security certification at various points throughout the project, whose assistance was very significant.

Certification is one stage of a journey rather than a destination, because the standards required call for continuous compliance rather than hitting a one-off target. "That requires vigilance and a continuous improvement philosophy to ensure that our controls remain effective. Like any successful project of significance, this requires strong leadership and commitment to achieve that level of sustained buy-in from all of the team," says Guy.