CIO

BUSINESS TECHNOLOGY LEADERSHIP

AUGUST 28, 2015 | CIO.COM

Law firm makes a case for security certification

A big law firm handling sensitive documents uses its ISO security certification as a competitive differentiator.

By Mary K. Pratt

International law firm Shook, Hardy & Bacon touts more than its legal skills to current and potential clients: It also pitches its ability to protect sensitive client information from cyberattacks.

A key selling point is Shook's recently earned ISO 27001 certification for information security management. "We wanted to make sure we had the processes in place so [clients] had confidence that we were doing the best we could," says the firm's chair, John Murphy.

Organizations have ample reason to seek reassurances that their business partners are doing enough to protect their data. In a recent PricewaterhouseCoopers survey, 61 percent of 1,322 global CEOs polled listed cyberattacks as a key threat to their organizations' growth prospects. That's up from 48 percent in 2014. Meanwhile, a study by the Ponemon Institute pegs the average total cost of a data breach at $3.79 million.

John Anderson, Shook's CIO, sought the ISO certification in 2013 at the urging of the firm's information governance committee. "We wanted a methodology and a framework that ensures we're using best practices for information security. And, secondly, we wanted third-party verification that proved our commitment to information security to external parties," Anderson says.

Credit: Anthony Freda

According to Anderson, Shook spent about $30,000 in 2013 and another $30,000 in 2014 on consultants and auditors to earn the certification; that's on top of additional cybersecurity-related spending to support the firm's security strategy.

Murphy says certification has strengthened Shook's position in the legal market. He says prospective legal clients ask the firms they're evaluating about their data security policies and procedures; some even specifically ask firms whether they have the ISO certification.

That's not surprising, Murphy says, considering that Shook clients let the firm have access to highly confidential, and often regulated, data. Those in the pharmaceutical industry, for example, share sensitive healthcare and drug discovery information.

Security certifications not a panacea

However, Steve Wilson, an analyst at Constellation Research, cautions that businesses shouldn't view ISO 27001 as an iron-clad guarantee of great data security. "ISO 27001 is a management process standard--it doesn't tell you what to do exactly in security; it tells you how to go about managing the security function. It leaves all the heavy lifting to the enterprise," he says.

Wilson advises organizations to do in-depth evaluations of their business partners' cybersecurity standards to ensure they haven't taken a merely robotic approach to earning the ISO certification.

Nevertheless, Shook executives say the market does indeed see the ISO certification as an endorsement of the firm's cybersecurity measures. Anderson notes that, because the certification requires organizations to not only uphold specific standards but also continually review and improve their security postures, the certification demonstrates Shook's commitment to cybersecurity.

"When we do pitches to clients, it's something we mention, because it's a differentiator. It's a competitive advantage right now," Anderson says.

Mary K. Pratt is a freelance writer based in Massachusetts.