XANTRION

I.T. AS IT SHOULD BE

USE CASE

Law Firm

To serve companies in two highly regulated and security-conscious industries, defense and health care, the firm needed to minimize its own security risks.

See what makes up a cybersecurity roadmap.

xantrion.com/roadmap

Xantrion
651 20th Street
Oakland, CA 94612

xantrion.com

866-926-8746

The Challenge

A growing law firm with offices in San Francisco and Washington was expanding its client base to include companies in defense and health care. To serve these two highly regulated and security-conscious industries, the firm needed to minimize its own security risks. First, it needed to ensure confidential client information was adequately secured. Second, it needed to be able to prove to prospective clients that its security practices conformed to industry standards. Finally, if its data was ever compromised, the firm needed to protect itself against accusations of negligence by being able to prove it had taken reasonable care to protect client information. These goals would have been challenging enough on the firm's constrained IT budget, but they also needed to be achieved using systems simple enough to be used by senior partners who were not tech-savvy.

The Solution

The firm initially considered giving their business to a costly intrusion detection service (IDS) that was a client of the firm. Before making a purchasing decision, however, the senior partners called in Xantrion to assess what security threats they actually faced and what measures would best mitigate the risk.

We scored potential threats both by likelihood and by their potential consequences, including not only financial losses but damage to the firm's reputation. For each threat, we then recommended ways to eliminate it or mitigate its impact. Finally, we listed, in order of priority, measures to address the most urgent or damaging risks at the lowest cost and least inconvenience to end users.

To generate buy-in from senior partners for changes such as introducing a stronger password management policy, we provided benchmarking comparisons to other firms, published recommendations of respected standards bodies, the ABA's own recommendations, and anonymous anecdotes drawn from other law firms among our clients. We also provided training in simple techniques for generating passwords that are easy to remember, but hard to guess. Our two most significant recommendations required no action from end users at all:

- First, our evaluation indicated that the firm was most at risk from potential data breaches caused by a lost or stolen laptop or smartphone. By implementing a device encryption program, we were able to address this risk without requiring end users to make any changes in the way they worked.
- Second, our evaluation showed that IDS monitoring was not appropriate for the types of risks the law firm was most likely to face. This saved the firm the expense of investing in services that did not meet their true needs.

The Outcome

Today, the law firm has established security measures that address its most significant exposures to risk cost-effectively, without excessively burdening end users. It also has a roadmap suggesting additional security measures, such as obtaining third-party certification of its security practices. Most importantly, because Xantrion involved the firm's key decision-makers in this evidence-based approach to risk mitigation and security management, the firm is far more likely to maintain an effective defensive posture—making it more attractive to prospective clients in its security-conscious target markets.