The Most Cost-Effective Way You Can Protect Your Trade Secrets

October 28, 2016 by James Pooley

I was giving a talk recently when a senior executive asked me, “If we have the time and resources to focus on just one thing to improve our information security, what would you suggest?” I didn’t hesitate: “Train your workforce.”

As we know from multiple studies, the biggest threat to information assets comes from “insiders,” which means (mostly) your employees. It’s not that you have a team packed with spies; but employees notoriously misunderstand their confidentiality obligations. In a recent survey of software engineers, 55% reported that they thought it was acceptable for them to take their work product with them when leaving the company – and that they intended to do it!

But not understanding the rules is only a fraction of the problem. The main challenge lies in a negligent attitude, a mental fog of inattention that can lead to mistakes.

What kind of mistakes am I talking about? The kind that make you slap your forehead in disbelief. The sales manager at a trade show who, excited about closing the deal at hand, lets slip the existence of an unannounced product. The engineer who brags to his friends on Facebook about a patent application he’s just filed. The R&D director who hires someone from his former employer in order to get an “update” on what they’ve been doing since he left. The business development executive who examines potential licenses of technology without walling off company employees who are working in the same area. These are the kind of mistakes that provoke litigation, and they are all preventable.

Good training is the single most cost-effective step you can take to reduce the risk of information loss or contamination. What makes for an effective training program?

Whatever IT systems or management processes you deploy to mitigate the risks to your trade secrets, those systems and processes are operated by people. So the way that they engage is critical to success. Training reinforces their focus and attention.

This is especially important with today’s workforce, a population that has never been more distracted. Think about it: for years now, social media have been silently encouraging people to use their laptops and smartphones to share every last detail of their personal lives. Sharing information is a good thing, and the more the better. When these same people come to work the next morning and connect their mobile devices to the company network, can we really expect them to shift their mindset and suddenly become models of discretion? Remember, a great deal can be revealed in 140 characters.

Here are some principles for designing an effective training program.

First, make the process inclusive. Not just people who you think are most likely to be exposed to confidential information, but everyone in the company should understand the importance of the issue. Even contractors, consultants and interns should be part of the effort. In fact, they may be even more important because they have inherently less loyalty and are more likely soon to be working somewhere else.

Second, make the training interesting. To keep it fresh and positive, consider using specialized vendors or products that can present serious material in a lighthearted but memorable way, rather than relying only on internal managers to conduct classes.

Third, don’t focus exclusively on protecting information from loss or leakage, but also from contamination. This happens most frequently from new employees who think they’re being helpful by passing on what they learned at their last job. So focus on the on-boarding process and train employees to recognize off-limits information.

Finally – and this is the most important principle – be sure that training is not an event but a continuous process. A single orientation video is not enough. Follow up with email tips, stories, and refreshers. And if business conditions worsen and you start to lose employees, this is a time to increase your training effort, not cut back, because the people who remain represent the source of your intellectual capital.

Let me emphasize that last point. Training is not about ticking a box. You are conditioning the attitude of those who are the primary handlers and protectors of your most important and vulnerable assets. Pay attention to that attitude and they will pay attention to your assets.

www.pooley.com