Creating a Risk-Aware Culture

Advisor360°

Information Security (InfoSec) was once seen only as a part of the larger IT organization. However, as the number of high-profile cyberattacks and data breaches have risen, so has InfoSec's profile and its role within organizations. Today InfoSec not only has a higher profile within a firm, it's also transitioned from being technology-only focused to one of the biggest risk-change agents in the firm. Below we discuss how an InfoSec team can help create and lead a risk-aware culture throughout the firm.

In any enterprise, from the CEO to the person in the cube next to you, all staff need a heightened awareness of risk and how it impacts their organization. This is defined as *any significant, uncertain event or circumstance which could impact the achievement of the company's business objectives*. The InfoSec team alone can only do its best to reduce risk, but if the rest of the firm doesn't feel involved in managing risk, any employee could be making uninformed decisions without considering what's at stake. Risk management is a serious team sport.

Without a strategy, some passion, and a desire to drive change, it's exceptionally difficult to instill a risk-aware culture in any enterprise, especially when InfoSec is often seen as "the team that will slow us down" or the "NO police." At Advisor360°, we've found that if you approach the topic of risk in the right way, you can grow a risk-aware culture where everyone knows they have an important role to play in our collective success.

HERE ARE FIVE STEPS WE'VE TAKEN TO ESTABLISH AND GROW ADVISOR360°'S RISK-AWARE CULTURE:

1 Start the talk from the top.

What type of risk does InfoSec help manage? It's a common misconception to think that InfoSec is solely concerned with *technology* risks, but the reality is that we're helping manage one of the largest *business* risks most firms face.

If a breach happens and your company's most sensitive information is compromised, is that simply a technology problem? (Of course not!) One security event can make or break your business. InfoSec needs representation at the top of the chain with the opportunity to engage with other senior executives to help facilitate risk discussions.

2 Education is the key to success.

If you aren't actively orienting your staff on their role in managing risk—or what your enterprise's risk appetite is—they aren't going to be part of the solution.

Consider this simple thought experiment. Let's say you're playing a dice game where:

- You have one die to roll.
- You win if you roll anything but a six.
- The payback is five-to-one (if you bet $10 and win, you net $50).

How much would you bet? With the odds so far in our favor, I'm sure most of us would at least go up to $10, maybe even $100. But what about $1,000? We all have a different amount we'd bet—or a different tolerance for risk.

Likewise, with business risks, if your staff doesn't realize what they could potentially be giving up, they won't be prepared to make the right decisions. Your enterprise must be aware that risk is everyone's responsibility—and everyone needs to have the same idea of risk tolerance—or else they may think they have nothing to lose.

3 Talk the same talk.

Employees don't have to understand every little thing InfoSec does (the same way executives shouldn't have to know the details of every protection we've implemented), but we must communicate to one another clearly and effectively, or we won't have the same understanding of our motivations and goals.

The secret is to learn the language of risk and educate everyone on it. If we all know what our company means by "risk" or "threat" or "impact" (and we have a uniform way of measuring such things), we can all be aligned on how our roles fit into a risk-aware culture and the firm's success—from executive management's decisions, to InfoSec's policies and controls, to other teams day-to-day processes.

This isn't hard to put into practice. Start by incorporating the subject of risk into your onboarding and follow up with regular trainings to reinforce the fundamentals. In every communication you send to your staff, consistently refer to the same risk terminology so that everyone is familiar with it.

4 Explain the change and provide context.

As the threat landscape evolves, InfoSec teams are constantly trying to mitigate new threats. A lot of times this can lead employees to see these changes as "taking things away" or "making my job more difficult" rather than minimizing the risk of our firm being the next data breach headline.

For example, let's say you're implementing URL filtering to block untrusted sites. If you don't explain why, what will employees think? Probably that they aren't trusted to use the internet—or that they need to be more productive. (Assumptions like this can contribute to InfoSec's negative reputation.)

But if you're transparent about the security reasons, such as . . .

- "We're reducing the likelihood of malware from suspicious websites infecting our network."
- "We're reducing the risk of our sensitive information being accidentally uploaded to an inappropriate website."

. . . your staff won't make those unfounded assumptions. They'll better understand protecting the firm's information and systems is critical, and they'll be more receptive to embrace the change.

5 Embrace being a business enabler.

When employees run an idea by InfoSec, their worst fear is that InfoSec will just say "no." Or worse, employees will avoid running ideas by InfoSec.

Contrary to this, InfoSec must strive to be a business enabler, not a road block. Although the InfoSec team has needs of its own, they also understand the needs of the business to better serve it. It isn't our responsibility to say "no"; it's our responsibility find a solution that meets everyone's needs within the firm's risk tolerance.

A firm like ours wants to provide innovative technology to stand apart from the competition, while at the same time providing our customers with a level of trust. But what stands out more than innovative tech that has security built in? Today, when consumers are looking for software, they're not just looking for software that works and provides a great experience, but also software that works securely. In that way, InfoSec is truly a business enabler.

PUTTING IT ALL INTO PRACTICE.

At Advisor360°, we've established and continue to grow our own risk-aware culture by:

- Including our Chief Information Security Officer (CISO) as part of our Executive Management team
- Introducing the risk discussion early with our staff, and finding new ways to keep the discussion going
- Collaborating with everyone (both the firm and our partners)—not just InfoSec— to find solutions
- Being less technology-only focused and taking a more people/process/technology view to our challenges
- Taking the time to find solutions that allow us to innovate and embrace new opportunities, while still infusing security best practices into the Advisor360° culture

Even with all this, the job of an information security change agent is never finished. Keeping everyone risk-aware is your ongoing responsibility. But by following these steps and establishing a strong foundation, your enterprise will be in a much better position to manage risk and become a differentiator in your industry.

Advisor360°
133 Boston Post Road
Weston, MA 02493
877. 360. 3601

INFOSEC-109102

Advisor360°