COSMOS
Navigate the Compliance Universe

Report on Supply Chain Compliance Volume 2, Number 16. August 29, 2019

Prepare for the worst: Interdepartmental crisis training improves data breach response efforts

By Sascha Matuszak

For compliance professionals, especially those working with the many vendors and other third parties that make up modern global value chains, building bridges between departments is a major task, because it is common for departments within an organization to operate as silos; for example, the accounting, marketing and information technology (IT) departments may have very little horizontal interaction. Those bridges are necessary in order to train employees, explain policies and procedures, and acquire the data necessary to understand where risks are and how to mitigate them.

With data and operations increasingly being relegated to automated and digital (i.e., cloud) software solutions, IT, in particular, plays a critical role in any organization's daily affairs. All the major compliance challenges — bribery, trade and labor issues, regulatory burdens, third-party vetting and management — increasingly require IT and compliance to work together.

But unfortunately, it is often the case that the two departments will only interact when a problem arises. In the worst-case scenario, IT and compliance will find themselves across the table from each other in a crisis, such as a data breach.

"A crisis is the worst time for them to get together," said Jonathan Armstrong. "They sort of mistrust each other, they have a deadline, the IT guys are blaming compliance and vice versa. ... Everyone is worried about being sacked and so compliance and IT meet like two opposing armies to try and agree on a common direction. That doesn't always work."

Armstrong has hosted data breach academies that bring together several parties (e.g., management, IT and compliance) for a test run at managing a breach. It turns out that much of the interaction is dysfunctional. Emotions are high, the stakes are huge, and both sides have to learn a common language. The simple step of "de-jargoning" their conversations can make a big difference.

"I've sat in on a data breach response meeting in which the two top individuals from IT and compliance waited for me to introduce them," Armstrong said. "With GDPR, you have 72 hours to report a breach. You don't have 30 seconds to play with introductions and protocol."

The academies produced some interesting findings, and Armstrong recommended a few steps that organizations can take to build the bridges necessary for an effective response to crisis.

Steps to take

- Do a rehearsal. For most organizations, its suboptimal for them to learn to work together in a crisis.
- Prepare common briefing notes. Have everybody working from the same set of facts, so individuals have a common understanding and common terminology.

- Distribute hard copy readings. There is a real difference between reading hard copy versus reading a projection on a screen.
- Have a war room where people can sit and do their reading together.
- Don't underestimate the stress involved. Making sure there is enough water, enough candies; that sort of basic stress relief stuff makes a difference. Any minor friction will be magnified.
- Decide who is going to lead the breach team. In the worst-case scenario, people are too polite and nobody makes a decision (everyone canvasses everyone else). In a real life situation, no one will decide. Armstrong described a situation in which the head of IT, the head of legal, and the head of compliance all told him, “You should make the decision.” Armstrong said, “I am outside counsel. Organizations need a more sustainable way of doing this in the future; someone needs to make a decision. You don’t coach in a crisis; you need a commander.”
- Make sure the data breach plan is fit for the purpose. There will be a language difference if the compliance team writes a plan, IT writes a plan, and each plan is very different and addresses different problems. “You need a plan that is like a fire evacuation notice on the back of hotel door,” Armstrong said. “Raise the alarm and await instructions.”

Data breach by a third party

Most major corporations do not process the majority of their data, and a vendor’s payments may be outsourced to a payroll company. When traveling, a company may use a third party to book the travel; when a person gets sick, the healthcare arrangements are often handled by a third party. Nevertheless, most organizations still behave as if everything that is relevant to employees is “in the building,” whereas none of the data relevant to the employee is in the building anymore.

The same is true for customers. Online payments are processed through a payment engine, and another third party collects the cash, while a logistics firm ships the product. A lot of organizations are still thinking their risks exist in the bricks-and-mortar world, but the risks aren’t there anymore.

Third parties often do not take data breaches as seriously as the primary organization and, even if they do, the policies and procedures differ. Creating bridges between departments within an organization is difficult, but creating those same bridges across the many vendors and third parties that make up the supply chain is much more complicated — and much more critical than it has ever been.

Look for a discussion on protecting data across the supply chain — including vendors and other third parties — coming soon in *RSCC*.

Takeaways

- Getting departments to work together effectively is a key component of a compliance program. A case-in-point is the cooperation necessary for IT and compliance to handle data security.
- Third parties and the dominant role of software and digital solutions in today’s business environment make compliance in those areas (i.e., supply chains, accounting and services) that much more complex and critical to business continuity.

Purchase Login