How General Counsel Can Enable Collaboration Without Increasing Business Risk

Intellectual Property

Fueled by the use of Slack, Zoom, Google Drive, Microsoft Teams and a host of other cloud-based collaboration apps, companies are innovating faster than ever. Work has changed, the collaboration culture is here to stay, and that's a good thing. But all of this collaboration technology comes with an often overlooked down side — the collaboration technology that enables the sharing and movement of data within an organization also makes it easy for employees to put that data at risk, whether unwittingly or maliciously.

Indeed, research conducted by Code42 in 2019 revealed that while 69 percent of all data breaches involve insiders, only 10 percent of security budgets are focused on insider risk. That's a big gap. And the faster businesses work and the more freely employees collaborate, that gap — and the insider risks that go along with it — will only get bigger. Employees, partners, and contractors are now routinely doing their jobs off of the corporate network, which means security teams have little visibility into file activity. One employee might upload a file to a personal Dropbox account to share it with a colleague. Another might email a file to his personal cloud-based email address so he can access the file from another computer. Yet another employee might download customer lists or business plans to a thumb drive as she prepares to leave for a competitor. The point is that it's easier than ever before for employees to put your intellectual property, business strategy, brand, and reputation at risk. And all of this is exacerbated by the COVID-19 pandemic and the shift to remote workforces.

The general counsel as change agent

Collaboration and data security are not, however, mutually exclusive. They can co-exist. And when companies look to mitigate their insider risk problem, GCs have a unique opportunity to be organizational change agents to help foster and secure collaborative cultures. Here are three things you can do to transform your legal department into an active partner to facilitate digital transformation and manage insider risk:

1. Understand your data and where it lives

You can't protect something if you don't know what or where it is. Yet, that's challenging for many organizations, particularly those with more complex IT technology stacks. You'll need to answer the following questions, and the only way to do so is to do data mapping:

- *What data do we generate and collect?*
- *On what systems does the data reside?*
- *Who has access to the data?*
- *What access controls are in place?*
- *Do we need to have the data? If so, for what purpose?*
- *When is the data no longer needed?*

Your IT technology stack and the company's internal data use cases are likely to be pretty dynamic. Work with IT to establish a process so new applications can be evaluated as they are onboarded to understand how they create and retain data. Further, revisit the overall data mapping on a regular cadence (e.g., semi-annually) to ensure that changes are understood and documented. As an added bonus, doing so will also support your ongoing compliance with data privacy regulations such as the EU's General Data Protection Regulation and the California Consumer Privacy Act.

2. Balance the business risks

An important part of your job as in-house counsel is to mitigate risk. So why not simply prevent employees from accessing or sharing certain files? Why not block use of collaboration apps altogether? Because doing so creates an even greater risk — stifling productivity, slowing down business cycles and losing in the marketplace.

In today's hypercompetitive environment, employees need to leverage collaboration tools to move fast. But if data is compromised, you need the ability to quickly figure out:

- Who did it?
- What data did they take?
- When did it happen?
- How did it happen?
- Where did the data go?
- If it was a former employee—where did they go?
- Why did they do it?

It is crucial, therefore, that you partner with the chief information officer, chief information security officer, and chief human resources officer to choose a technology solution that provides the best capability to rapidly detect, investigate and respond to data breach incidents with the appropriate

level of insight. That begins with the capacity to collect and monitor files and file activity for all users and every device. Why? Because when it comes to investigation and response to insider risk, context and speed are everything.

All too often, though, insider threat breaches — 73 percent — go undetected for months. When a threat is detected and the investigation begins, it becomes a game of “turn back the clock” — the impacted computer is sent off to a third-party forensic analyst to gather evidence. By the time the situation is resolved — months or even years later — it’s often too late to avoid damage to the business and brand.

Without the appropriate tools, the cycle perpetuates, and legal is an important stakeholder in selecting the right solutions to mitigate insider risk.

3. Be transparent

Transparency is a best practice when it comes to managing insider risk and building a culture that values both collaboration and security. Employees should know — from day one — that your organization continuously tracks file activity. They should understand that the program is applied universally without privileges or exceptions — and they should understand how the program is designed to support their productivity while protecting the business. When a traffic camera is installed on your street, what happens? People stop speeding. The same principle applies to your insider risk mitigation program.

Transparency also includes building an insider risk program based on trust. Legal should proactively collaborate with stakeholders to execute the insider risk program and back it up with clear and complete policies, procedures, training, and communication. This includes building strong relationships with security to create disclaimers and privacy policies that are consistent with business goals; with HR to build a collaborative culture that is safe and secure; with IT to create as much transparency as possible from a cultural and privacy perspective; and with employees to help them understand the data security policies that are in place and why they are important.

When employees understand how their actions could put the business at risk and why everyone loses when insider risk makes an organization vulnerable, they are less likely to breach this trust. They are more likely to remain valued allies rather than adversaries. In this way, transparency deters insider risk in and of itself.

It's time to take insider threats seriously

Insider risk poses one of the greatest risks to an organization’s culture, reputation and viability — but data security shouldn’t come at the expense of speed or collaboration. It’s time for the general counsel to step up. Rather than saying “no,” the legal department can be seen as an enabler of the business — looking for ways to foster collaboration and innovation throughout the organization in a safe and secure way.

David Huberman

General Counsel

Code42

David Huberman is general counsel for Code42, a leader in insider risk detection and response, and a contributor to Code42's new data security book *Inside Jobs: Why Insider Risk Is the Biggest Cyber Threat You Can't Ignore*.