Corporate Investigations

WHAT A NEW SURVEY TELLS US

By Sheila Mackay

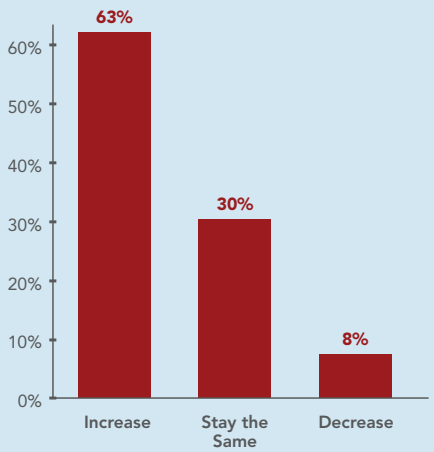
Corporate investigations are usually resource-intensive—not to mention costly—events that can both disrupt business and thrust an enterprise into an unwelcome spotlight. Although most companies strive to create a business environment with appropriate and enforceable compliance policies and procedures that will keep investigatory incidents to a minimum, they are nonetheless a fact of corporate life.

As today's social, ethical and communications landscape grows more complex, the ripples roll into the corporate realm with increasing consequence and frequency. Growing regulatory demands, heightened concerns about employee behavior, massive data quantities to protect from breach, more loopholes for bad actors to exploit—each of these realities increases the probability of a corporate investigation.

INVESTIGATIONS ON THE RISE

Those on the front lines of corporate investigations believe the situation will only get worse. In a recent Corporate Investigations survey of more than 315 corporate professionals conducted by H5 and *Above the Law*, 63% believe that investigations will increase at their companies over the next three years (the number was higher for non-U.S companies, at 72%). The survey, conducted in July and August of 2019, sought insights from legal and compliance professionals whose roles directly relate to various aspects of corporate investigations.

Increase or Decrease in Investigations?



INVESTIGATIONS DRIVERS EMERGING ON SEVERAL FRONTS

The anticipated increase reported by the survey is not surprising. The drivers of investigations are intensifying on several fronts. For one thing, given the rise in cultural sensitivity to harassment and discrimination (think #MeToo, for example), companies are becoming more engaged in addressing employee behavior that breeds misconduct, leading to an increase in what survey respondents say is their companies' most frequent investigation type: workplace investigations. In fact, a recent Proskauer survey about workplace investigations cites an increase in harassment claims, discrimination complaints, and other workplace misconduct that is not likely to abate any time soon.

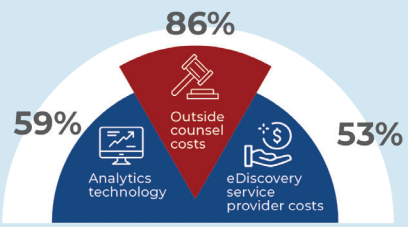
External pressures that increase investigation risk for companies are on the rise as well. The H5 survey cited regulatory/governmental investigations as the next most frequent type of investigation; and judging by statistics issuing from other arenas—from the SEC whistleblower program to anti-money laundering enforcement actions, to white collar incidents, to healthcare investigations—the number of investigatory incidents driven by regulatory pressures will continue to climb for the foreseeable future.

A WAKE-UP CALL

For companies who say they are already experiencing a cost and resource drain from their investigations burden, this is a wake-up call: Things are likely to get worse. In the H5 survey, nearly half of respondents said their companies face more than 50 potential investigations per year—22% said more than 100—with larger companies facing even more. Although a majority (64%) do report having a department or team specifically dedicated to investigations, generally reporting to legal, a continued increase can only put more strain on both legal and compliance teams who strive to stay ahead of potentially damaging situations before they become tomorrow's headlines.

COSTS AND RISKS

Aside from the risk of reputational damage, which can be devastating to any company (a concern highest for workplace and white collar investigations, according to the survey), investigations spend can be precipitously high, encompassing line-items similar to those incurred by corporate litigation. Although 27% of survey respondents did not know the all-in cost of investigations in their companies, those who did reported as highest the spend related to outside counsel (86%) and analytics technology (59%), with eDiscovery provider costs and contract review costs



Top Areas of Spend

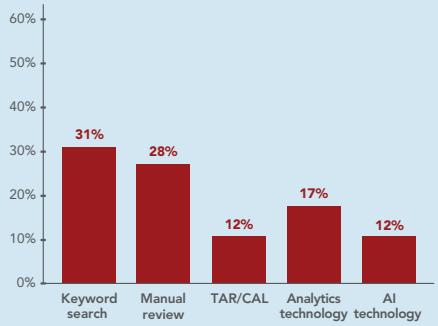
pretty much tied for third (at 53% and 52%, respectively). Costs vary by type of investigation, as different investigation types may have very different requirements. Regulatory and employee investigations, for example, tend to implicate more electronic data, which can raise costs as collection and review efforts to identify key documents add to the bottom line.

ELECTRONIC INFORMATION IS A CRITICAL FACTOR

To be sure, today's untamed data volume and complexity complicates both investigatory and litigation efforts in major ways, requiring both effective and efficient processes that challenge even the most forward-thinking companies. In the survey, 59% said that for the investigation type their companies face most often, collected data volumes top 100GB, with 14% saying more than 1TB. Despite any corporate efforts to the contrary, data volumes tend to grow, not decrease, over time; and tackling the data-wrangling aspects involved in such incidents takes more than just organizational and technical knowledge. A hybrid approach that effectively blends personnel and technology is required with full-on company commitment to a defined process, best-of-breed tools, and the ongoing cultivation of appropriate skill sets to handle the challenge.

This is especially true when it comes to finding key documents. In an investigation or litigation, it is, after all, the evidence that tells the tale, and finding the information quickly that will unearth the pertinent facts is an important part of the process. Survey respondents reported keyword search (31%) and manual review as the usual approach (28%), although more advanced technologies are available these days that would likely provide a more accurate and cost-effective method for homing in on key information. Generally, there is room for improvement here. The survey showed that satisfaction levels with finding key documents are mediocre, with lowest levels related to the speed at which key documents are identified.

Methods Used to Identify Key Documents



BEING PROACTIVE: PREPAREDNESS AND THE PROPER TOOLS

In fact, it is the ongoing development of technological tools that may have the greatest impact on the cost and risk of investigations as time goes on; the increasing use of analytics and AI technology to both process and proactively monitor data could make a significant difference. As it is, 67% said their companies proactively monitor electronic data (e.g., email review or network monitoring) to identify potential wrongdoing, notably much higher in the finance/banking sector (94%).

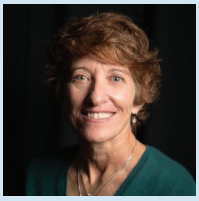
Proactive Monitoring

The growing use of technology for investigations appears to be a cross-border phenomenon. The survey showed no difference in U.S. vs. non-U.S. responses and anecdotal evidence attests to the efforts outside the U.S. to leverage more advanced solutions. In the UK, for example, Lisa Osofsky, Director of the Serious Fraud Office (SFO), indicated that AI robots were used to check for privileged material in the Rolls Royce case, leading to an 80% savings in the area where it was used. Further, she said that machine learning and AI-based technology-assisted review features would soon be used in investigations to create greater efficiencies and shorten decision-making timelines.

Although using advanced technologies can provide efficiencies across the board, the proactive angle is key: A reactive approach to any problem always tends to be more costly (and riskier), and the ability to address a worrisome situation before it gets out of hand can mean the difference between an internal reprimand and a visit from the DOJ.

Part of being proactive, too, is being well prepared. Having a plan in place in advance of a potential incident reduces reaction time and sets the stage for a more efficient response. Documented policies and protocols along with the appropriate training of both employees and response teams are crucial components. And, depending on the industry and types of data stored by a corporation, the ability to adhere to a variety of new data privacy regulations, such as the EU General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Biometric Information Privacy Act (BIPA), is also key. Identifying where sensitive data resides is necessary under the new privacy regulations and is helpful in a cyber incident.

Although the investigations landscape may be a bit rugged these days, no one seems to have their head in the sand. Acknowledging today's challenging realities is half the battle; the rest depends on the commitment and energy devoted to the proactive and innovative thinking that will lay the proper groundwork for success.



SHEILA MACKAY is Managing Director of eDiscovery at H5. She has more than 25 years of experience in the legal services industry including product development, professional services, operations, management and business development. An advocate of the use of technology to drive efficiency, Sheila works hand in hand with H5's client services, infrastructure and technical services teams to develop and deploy custom solutions for global and domestic companies and law firms.
smackay@h5.com