A triple threat across the Americas: KPMG 2022 Fraud Outlook

Sector Spotlight: Life Sciences

Five things life sciences executives need to know

KPMG's "A triple threat across the Americas" highlighted the overlapping fraud, non-compliance and cyber attack challenges that confront businesses across all sectors today. This follow-up piece reviews the dangers facing life sciences companies, and outlines five things that sector executives need to know:

01 Life sciences companies are facing the biggest compliance challenge of any sector covered in our survey, but only a minority are investing in the resources they will need to deal with it.

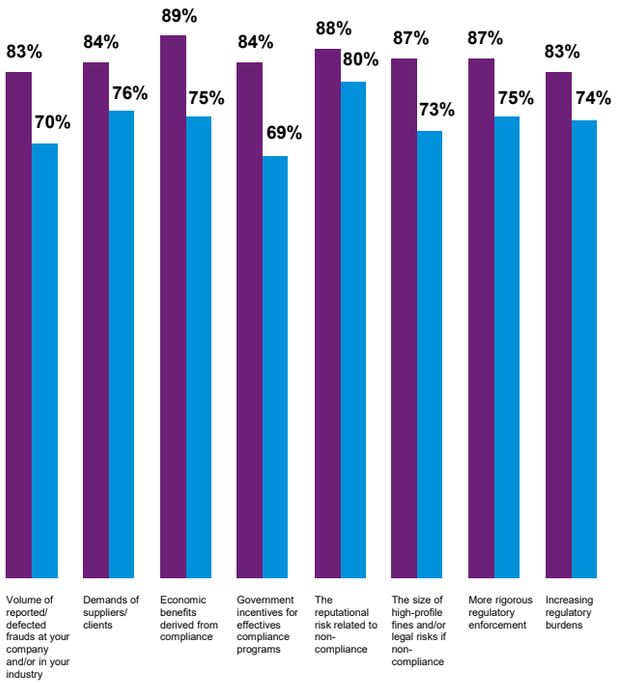
This sector was hit by far the hardest by compliance fines in the past 12 months — the equivalent of 0.76% of profits during that period. This dwarfs the survey average of 0.46%. Respondents are also more likely than those in other industries to say that each of a range of factors is driving leadership to pay more attention to compliance issues [see chart].

Finally, other elements of the triple threat are exacerbating compliance problems for life sciences companies. As discussed below, companies in the sector face significant challenges related to cyber security and types of fraud that use cyber attacks as a vector. Both kinds of issues, in turn, raise compliance difficulties: 36% of all sector respondents report that a cyber attack in the past year has led to a legal/compliance review or investigation at their companies.

Nor do industry executives expect these problems to diminish: 73% of survey respondents expect compliance risk to grow in the coming year — again the highest figure for any sector.

It appears troubling, therefore, that only 37% of life sciences respondents expect to see increased spending on compliance efforts in the coming year, the lowest number for any of the sectors covered in these reports.

To what extent are the following increasing the time and attention that your company's leadership is paying to compliance issues? (Percentage answering significantly or greatly.)

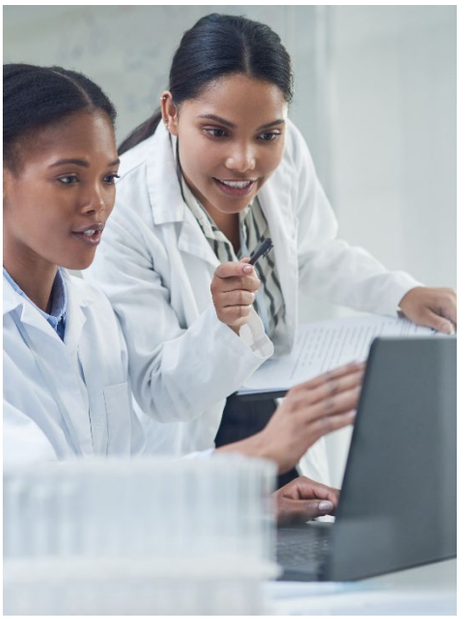


NDP357435-4A

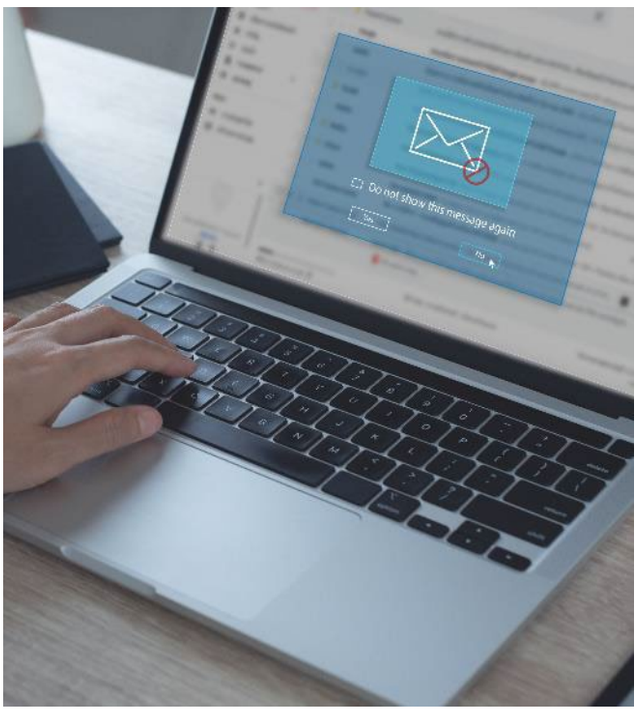
02 Life sciences companies show high confidence in their fraud defenses, despite the highest fraud burden of any sector.

Life sciences companies suffered the biggest losses to fraud of any industry in our survey in the past 12 months, reaching 0.54% of profits during that period. The proportion hit by at least one instance of fraud (76%) was also higher than the survey average (71%). Looking ahead, 76% of life sciences executives foresee growth in the risk of attempted fraud by actors outside the company (72%).

Again, there are worrying signs of overconfidence. These respondents are the most likely to report that anti-fraud policies (85%) and fraud prevention (79%) at their businesses are somewhat or extremely effective, but only 40% of these executives expect their companies to increase spending on anti-fraud measures in the coming year. This is the lowest figure for any sector and well below the survey average of 53%. This may reflect overconfidence: in the last year, 23% of life sciences companies learned of an instance of fraud, non-compliance or cyber breach from a government regulator or a police report — also the highest figure in the survey. Across all other firms the average was 15%.



03 Cyber attacks, in particular ransomware and intellectual property (IP) theft, are the dominant fraud challenges in the life sciences sector.



Perhaps predictably for such a knowledge-based field, sector respondents were the most likely to report experiencing recent IP theft or industrial espionage. One-quarter of life sciences businesses had suffered such an attack in the past year, compared to just 9% of companies overall. During the same period, fraud committed through cyber channels was common, seen at 27% of life sciences companies.

The sector was also a particular target for ransomware: one-third of life sciences companies say that attempts to defraud them in this way increased during the past year. This is also the highest figure for any sector, substantially above the overall average of 20%.

Here, too, overconfidence may be an issue. Far more life sciences respondents (84%) believe that their companies are somewhat or very good at preventing ransomware attacks than in any other sector (the overall average is 65%).

04 The main kinds of fraud perpetrators which have affected life sciences companies reflect the dominant types of fraud the industry faces.

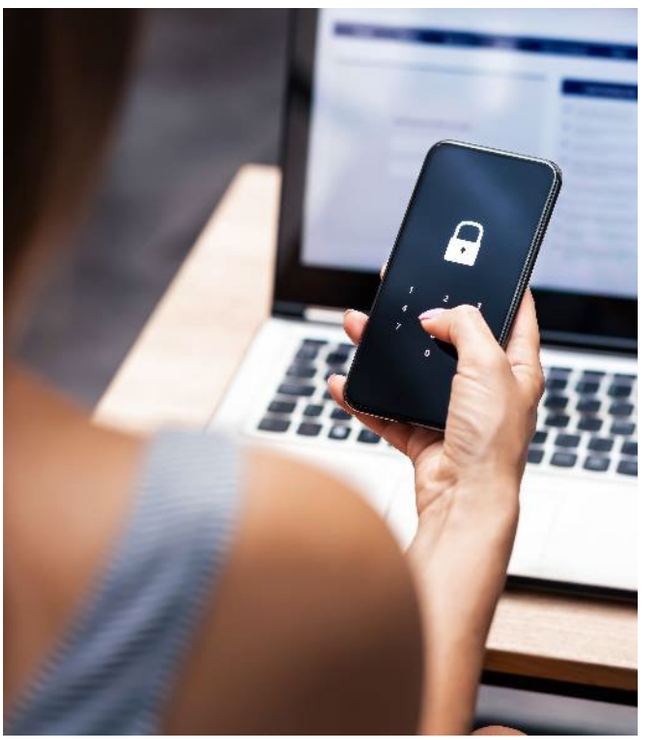
Those engaging in fraud against life sciences companies differ from the norm in important ways. Employees of vendors, suppliers and partner companies were known to be involved in such activity at 43% of sector companies in the past year, the highest level for any sector. Similarly, 40% suffered at the hands of organized crime and hackers, also the largest sectoral number and much higher than the 26% overall survey average.

These kinds of crimes reflect the struggles of the sector to provide life-saving vaccines and, eventually, medication to bring COVID-19 under control. Life sciences companies frequently have global supply chains. The need to procure materials amid pandemic-induced disruption, and often to find alternative logistics and warehousing arrangements, have made it more difficult to follow the strictest controls about onboarding third-party suppliers and other partners. Finding better ways to address these risks amid ongoing, potentially long-term supply-chain disruption is a priority.

05 Cyber security is another area for this industry where extensive risk and overconfidence co-exist.

Life sciences respondents were the most likely of those from any sector to report an increase in the past year of phishing (53% compared to 40% overall), scamming (44% to 25%) and, as discussed above, ransomware attacks (33% to 20%). It is, therefore, no surprise that sector leaders have a near-universal belief that cyber risk will continue to rise in the coming year (92%).

The inability of many IT systems to respond to these dangers raises concerns. Only 21% of those surveyed in the life sciences sector say that their companies can identify a cyber attack within 1 week or less of it beginning, and just 8% believe than they can contain one within 1 week of its being discovered. On the latter metric, it is the slowest of any sector. More worrying still is the attitude of life sciences leaders to these responses: 91% are somewhat or very confident in how quickly their companies can recognize attacks and 81% in how fast they respond.



KPMG's viewpoint: Make your defenses fit for purpose

The world is always changing but, occasionally, it experiences a dramatic inflection point. The COVID-19 pandemic reset all kinds of assumptions about how people live and work. Now, geopolitical events are exposing the fragilities of people's assumptions about the international environment.

The risk landscape that businesses are grappling with has been similarly reshaped. The need to maintain access to supplies has driven many companies to rely on previously unvetted partners, potentially raising new fraud risks. On compliance, the drive for net zero is expected to create further environmental regulation and new global sanctions may lead to more stringent oversight of financial and trade activity. Finally, cyber attacks, already on the rise during the pandemic, are allowing cyber threat actors to pursue a range of aims.

In short, if your company has not recently conducted a full review of its fraud, compliance, and cyber security risks, it should conduct one as soon as possible. Otherwise, your defenses may not be tailored to combat today's threats, or be able to react as those risks rapidly evolve.

More generally, many companies in the life sciences sector need to re-focus on the triple threat. Overconfidence is a widespread problem. To cite a glaring example, sector executives assess the quality of their companies' defenses against ransomware attacks very highly, but some of this apparent success may simply be because of some cyber-criminals choosing to avoid the healthcare sector. Hence, the industry's security systems may not be good so much as untested.

For those ready to grapple seriously with the new triple threat environment, the basic framework of prevention, detection, and response remains the soundest foundation for addressing fraud, non-compliance and cyber attack. The environment in which these defenses are deployed, however, means that they should retain the most effective elements and build upon them to defeat evolving threats.

Prevention

In our view, certain elements will remain largely the same, such as implementation or enhancement of internal controls; risk-based integrity due diligence on employees and third-parties; security assessments of critical information systems; and simulated cyber attacks to expose exploitable vulnerabilities. Others are expected to take a new shape. For example, implementing rules on exceptions to vendor due diligence policies may be necessary amid supply-chain shortages, but companies need to balance strategic necessity with the imperative to avoid falling victim to fraud and staying on the right side of regulation.

Detection

We believe tools such as data analytics, internal audits, and cyber intrusion detection protocols will remain fundamental, but the misbehaviors they look for may be different. Moreover, even where more employees are working at home, theirs are the eyes and ears that will see compliance failures or fraud. Measures that companies should take include updated training on fraud and compliance risks, and on the importance of reporting unusual behavior through existing incident-reporting mechanisms

Response

Protocols must be in place to respond to fraud, instances of non-compliance and cyber breaches. Companies also need to be ready for the emerging challenges within today's risk triangle. This might include, for example, deciding ahead of time whether you are willing to pay in the event of being hit by ransomware or choosing in advance who would make that call.

For further information on how KPMG may help you, please contact us:

David Nides
Principal, Cyber Security Services
Forensic
KPMG US

Jennifer Shimek
Principal, Forensic
Health & Life Sciences
KPMG US

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities