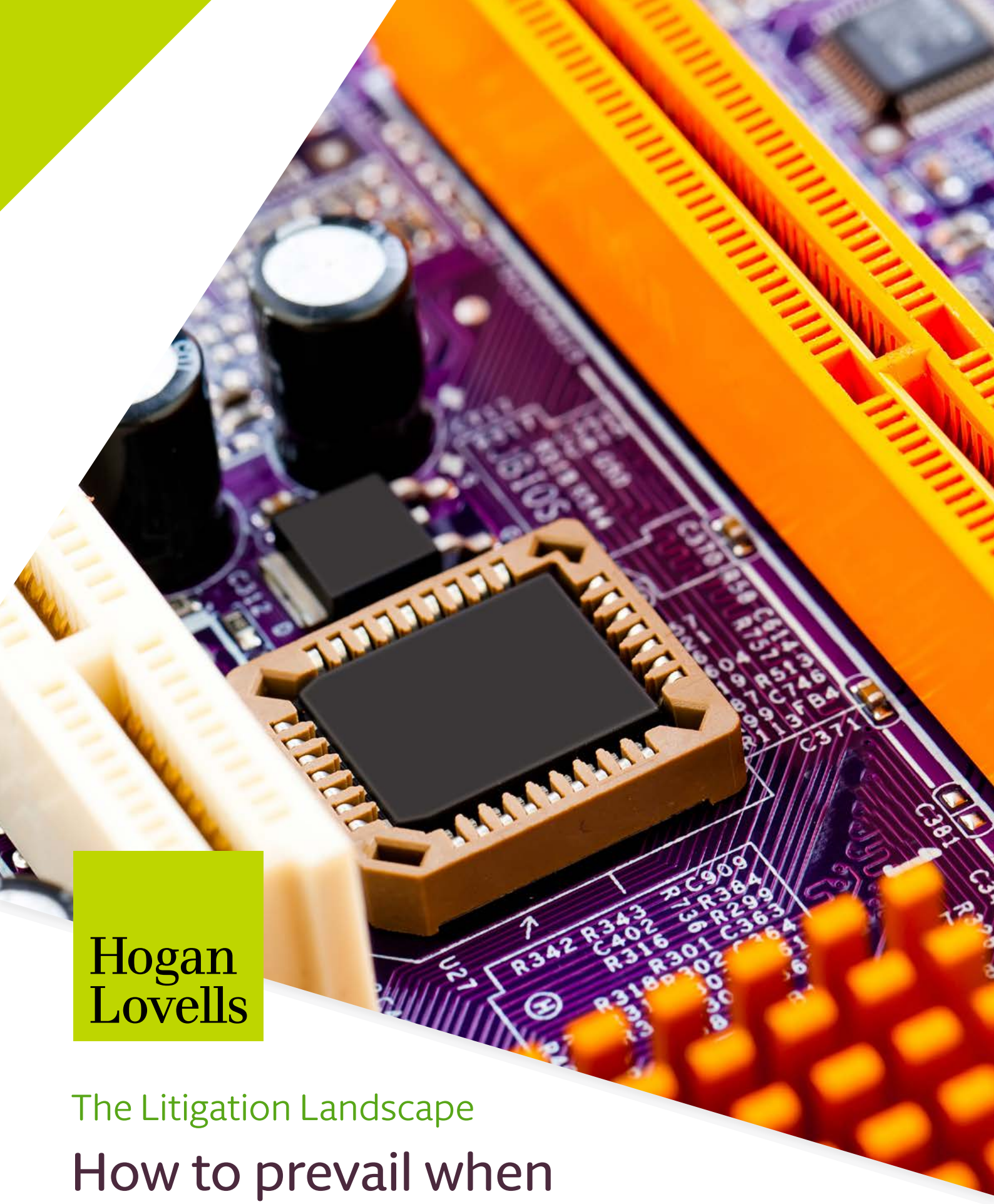


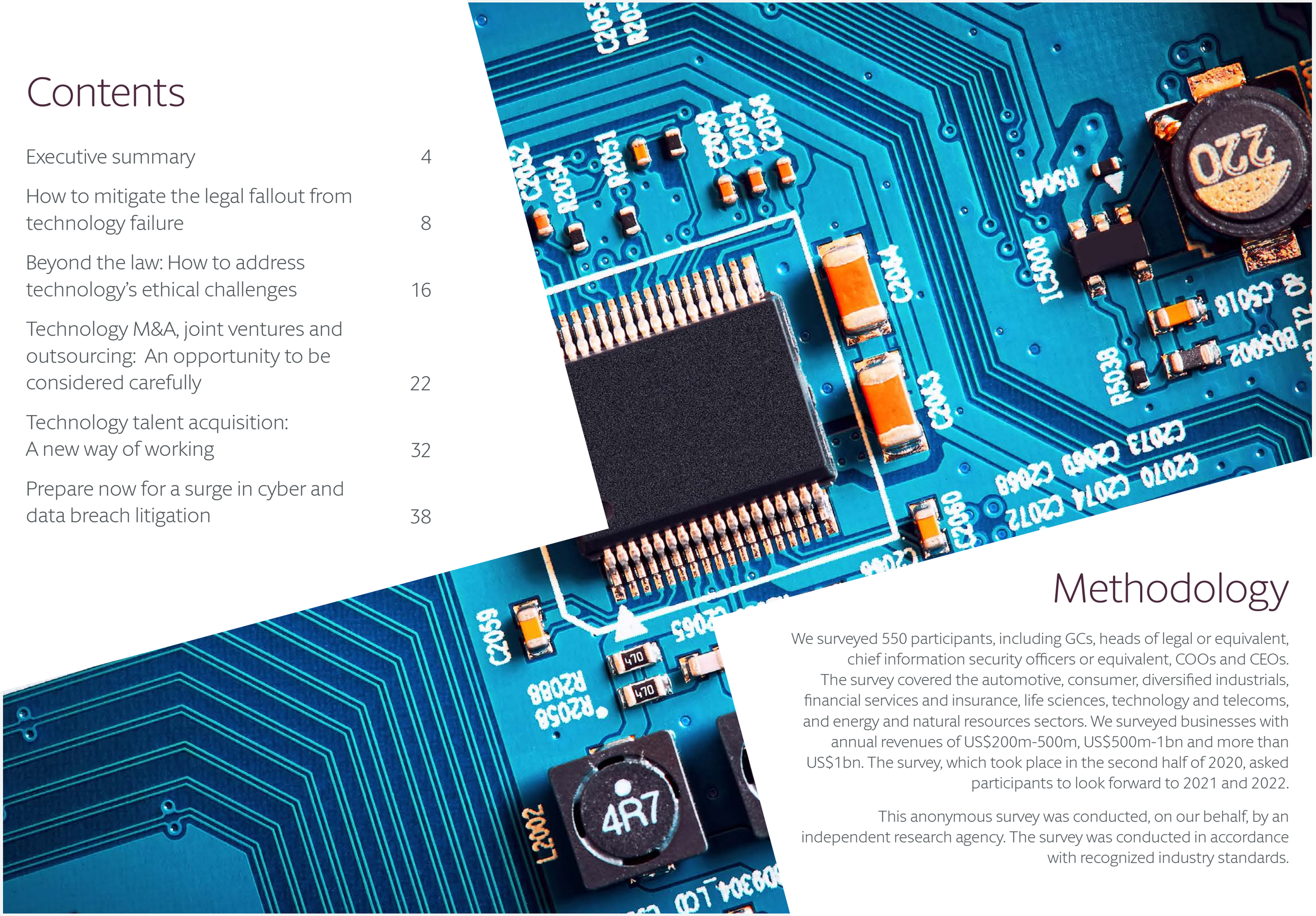
Hogan Lovells

The Litigation Landscape

How to prevail when technology fails

Building resilience into your tech strategy

Contents



Methodology

We surveyed 550 participants, including GCs, heads of legal or equivalent, chief information security officers or equivalent, COOs and CEOs. The survey covered the automotive, consumer, diversified industrials, financial services and insurance, life sciences, technology and telecoms, and energy and natural resources sectors. We surveyed businesses with annual revenues of US$200m-500m, US$500m-1bn and more than US$1bn. The survey, which took place in the second half of 2020, asked participants to look forward to 2021 and 2022.

This anonymous survey was conducted, on our behalf, by an independent research agency. The survey was conducted in accordance with recognized industry standards.

Executive summary

The transformative power of technology has made it integral to many businesses' growth plans: 61% of our surveyed businesses say the development and/or deployment of technology is a core part of their growth strategy.

That's because technology delivers tremendous benefits. Internet of Things technology installed into manufacturing lines can help predict when a key piece of equipment might falter. Cloud computing enables businesses to rapidly scale their online platforms. And artificial intelligence can automate the processing of hundreds of thousands of rules-based tasks. This is just a fraction of the ways in which technology can unleash huge benefits.

But technology fails. It may malfunction or not perform to spec, or it could have unintended consequences such as increased cybersecurity vulnerabilities. In addition, the joint ventures and acquisitions designed to accelerate tech's development and commercialization can also break down.

Failing technology does not just affect the business that developed or deployed it; it can also impact customers, employees and even wider society. Algorithms in analytics technology that were developed based on unrepresentative data sets might be discriminatory. And the technology that underpins encrypted messaging, cryptocurrencies and social media platforms can erode transparency, traceability and accountability if they are not governed effectively. Then there are the potential ethical issues associated with technology addiction and the spread of misinformation.

When technology goes wrong, it does not just cause significant operational, financial and reputational damage – it can also lead to a regulatory investigation or litigation, compounding the initial cost, and reputational damage.

Businesses have always had to grapple with these risks. But in today's volatile environment, their need to deploy technology quickly is increasing the likelihood of failure. At the same time, changes in regulation, such as tightening data privacy laws or developments that make it easier to bring collective litigation, increase the potential for disputes to follow.

To maximize the benefits of technology, businesses must carefully consider how to mitigate the risks. Based on our work with clients, we have established four principles for mitigating technology risk.

Fig 1 The majority of businesses say the development and/or deployment of technology is a core part of their growth strategy "to a significant extent"

Q. To what extent is the development and/or deployment of technology a core part of your company's growth strategy?
Base: 550 Note: Percentages do not total 100% due to rounding.

1

Tech risk should be a boardroom issue

Senior management and the board must devote time to understanding and overseeing technology risk. Not only is this mandated by regulators in some circumstances, it also makes good business sense – because technology risk and business strategy are linked.

In order to manage technology risk effectively, boards and senior management need to truly understand the nature of the threat. However, just 37% of our surveyed businesses are more than "somewhat confident" that their senior executives understand the risks associated with the technologies they are developing and implementing.

This lack of understanding could stem from the fact that boards are neglecting the problem. Just 9% look at technology risk "to a significant extent," which means they oversee management of a broad range of technology risks and deem them to be as important as traditional risks such as financial risk.

Without enough attention from the top, you will not carry out the crucial initiatives that could mitigate technology risk. Illustrating this, 35% of surveyed businesses have not identified all business-critical technology, which is necessary to design any mitigation strategy.

2

Legal teams should collaborate closely with the wider business

Close collaboration between legal teams and the rest of the business is essential to mitigate the risks of technology failure. For example, if there is a major data breach incident, key regulators will need to be informed and there may need to be a privileged investigation. But this could be hampered if legal teams are not involved in preparing how their business should respond. But just 31% of businesses in our survey involve their legal teams in creating their cybersecurity incident response plans.

Privacy experts should also work closely with product teams to ensure that they do not accidentally break data privacy regulations when they develop or update products. Yet just 28% of surveyed businesses say that privacy specialists are involved from the outset in the development and implementation of new technology that gathers and/or processes personal data.

3

Monitor risks across the entire technology lifecycle

It is imperative to assess technology risk not just when developing new products or forming new partnerships, but also on an ongoing basis.

Take artificial intelligence technology. Depending on the circumstances, companies need to check for biases not just when they purchase or develop this technology, but also on an ongoing basis to ensure that no biases emerge when it is being used.

The same is true of partnerships. Legal teams should assess risk associated with a technology joint venture not just before it is agreed, but also for the duration of the partnership to identify any risks that materialize and ensure that contracts are adhered to.

4

You're only as strong as your weakest third party

Even if businesses take every necessary precautionary measure to mitigate technology risks, they may still be vulnerable if their suppliers, partners or acquired businesses have not done the same. So you should assess the mitigation steps taken by third parties.

Our survey data reveals that many businesses are not doing this enough. Despite the numerous instances of data breaches stemming from compromised third-party systems, two-thirds of businesses assess only a small number of their suppliers' cybersecurity credentials.

And despite the increasingly complex risks of acquiring and partnering with technology companies, only the minority of businesses have increased the amount of time they spend analyzing risks during due diligence.

You will never be immune from technology failure. But by following these four principles, you will be well prepared to mitigate the legal risks if the worst should happen.

We hope you enjoy reading this report. Do let us know if you have any comments or feedback.

How to mitigate the legal fallout from technology failure

>3/4

More than three-quarters of businesses are concerned that a regulatory investigation or litigation could follow a major failure of the technology that underpins their business. And 67% are concerned about this following a major failure of the technology they use for consumer-facing products.

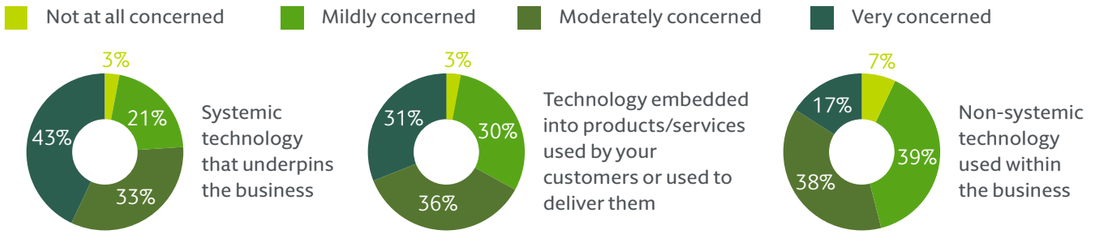
40%

Just 40% of C-suite business leaders are actively involved in the regulatory and litigation aspects of mitigating technology failure.

2/3

Two-thirds of businesses have a technology failure crisis-management playbook, but many do not contain vital guidance that could help mitigate the impact of a regulatory investigation or litigation.

Fig 2 Most businesses acknowledge the risk of a regulatory investigation and/or litigation following a major failure of their technology



Q. How concerned would you be about a potential regulatory investigation and/or litigation following a major failure of technology your business uses? Please answer with respect to technology that is embedded in products/services you sell, as well as internal systemic and non-systemic technology.
Note: Percentages do not total 100% due to rounding.

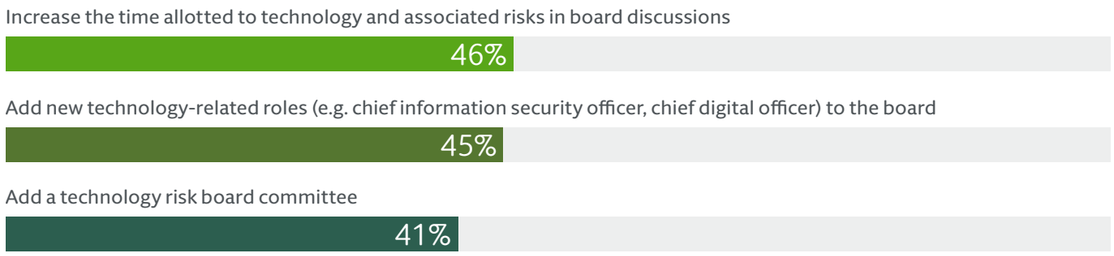
Three-quarters (76%) of businesses are moderately or very concerned about a potential investigation and/or litigation following a major failure of systemic technology that underpins their business.

Despite widespread acknowledgment of the threat, many businesses say that they are not doing enough to mitigate the risks associated with technology failure.

Just 46% have done everything they can to mitigate the regulatory and litigation risks of technology failing. And only 40% say that the C-suite is actively involved in mitigating the regulatory and litigation risks of technology failing.

That needs remedying. As more and more businesses use technology to drive growth, their C-suites will need to prioritize risk mitigation. Board directors should also enhance their oversight of technology risk by increasing time allotted to risks in board discussions, adding new technology roles to the board, and, where relevant, creating a technology risk board committee. The survey data reveals that fewer than half of boards plan to do any of this in the next two years.

Fig 3 Only a minority of boards plans to take measures that will improve their oversight of technology risk



Q. Which of the following does your business plan to do in the next two years to better manage the risks posed by your development and deployment of technology?

Changing regulation, industry convergence and advanced technologies increase litigation risk

Following technology failure or regulatory non-compliance, litigation may be brought by individual businesses or consumers, consumer groups, industry regulators or a group of consumers.

In Europe, the risk of collective litigation brought by consumers is set to increase when the new EU directive on collective redress is finalized. This makes it easier for consumers to sue collectively for mass harm.

The risk of technology failure leading to a regulatory investigation or litigation is increased by the convergence between the technology sector and traditional industries. For example, automotive manufacturers or MedTech companies which incorporate technology that gathers or processes personal data may not be fully aware of data privacy regulation, or may not have the resources to ensure compliance. Similarly, technology companies developing products for traditional sectors may not be fully aware of product liability or product safety directives.

As businesses deploy more advanced technology within their organizations, the legal consequences of failure grow more complex. Businesses in multiple sectors are increasingly exploring blockchain technology, for instance, and there are still important unanswered questions about which jurisdiction any dispute should be heard in and how judgments can be enforced if blockchain should fail.

"We're seeing legal disputes arise from technology failure where there is convergence between traditional and new sectors. Traditional manufacturing companies, for example, may not be aware of the complex data protection regulation that can apply to new products they develop, or may not practice privacy by design."

Lauren Colton | Partner, Hogan Lovells

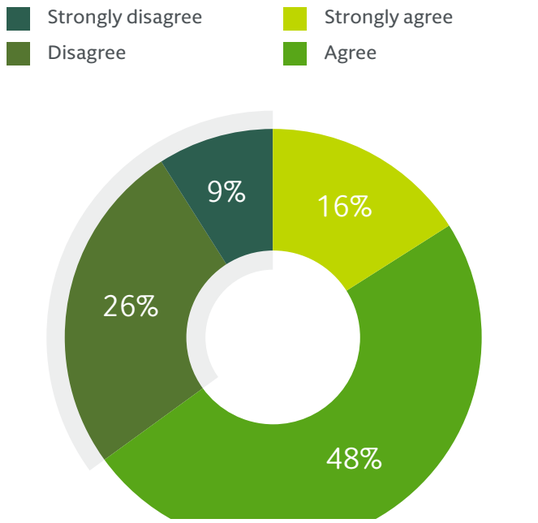
More than a third of businesses have not identified all business-critical technology

As well as not involving their senior leadership team, many businesses are not taking all of the necessary measures to mitigate the risks associated with technology failure.

The first step is to identify and document all business-critical technology. Then you can put in place special protections and backups in case of failure. But according to our survey data, more than a third of businesses have not done this. Small businesses and those in the industrials and life sciences sectors are least likely to have identified their key technology.

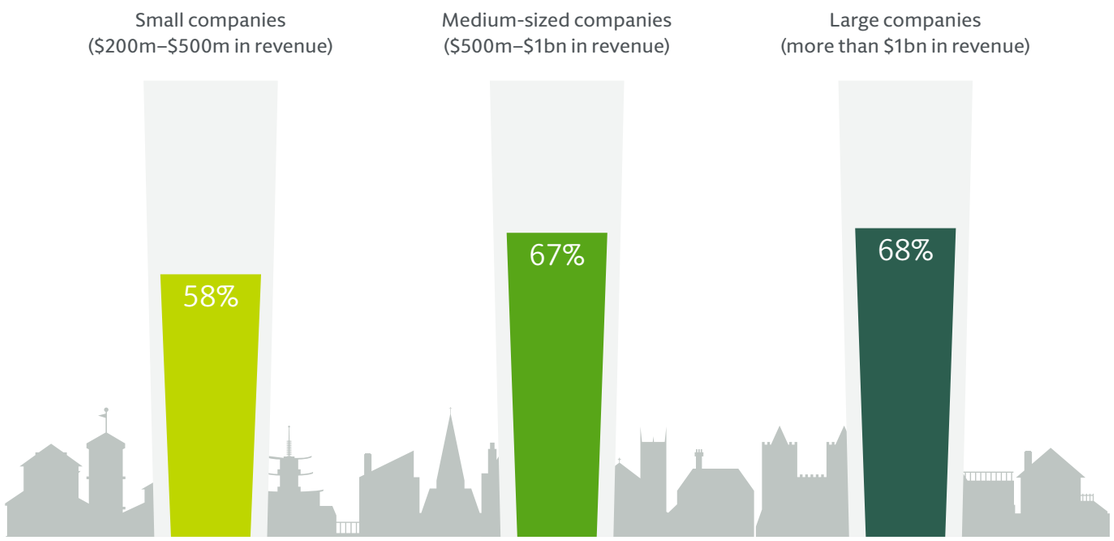
The next step is to determine what may cause that business-critical technology to fail and identify the risks this may pose to the wider business.

Fig 4 More than a third of businesses have not identified all of the business-critical technology within their organization



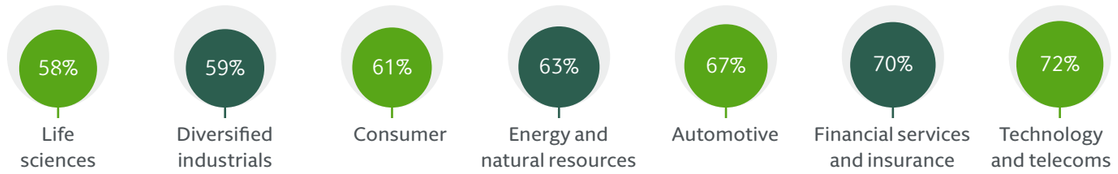
Q. To what extent do you agree with the following statement? "We have identified all of the business-critical technology within our organization."
Note: Percentages do not total 100% due to rounding.

Fig 5 Small companies identify their business-critical technology least frequently



Q. To what extent do you agree with the following statement? "We have identified all of the business-critical technology within our organization."
(Percentages indicate those that have identified all of the business-critical technology within their organization)

Fig 6 Industrials and life sciences companies are least likely to have identified their business-critical technology



Q. To what extent do you agree with the following statement? "We have identified all of the business-critical technology within our organization."
(Percentages indicate those that have identified all of the business-critical technology within their organization)

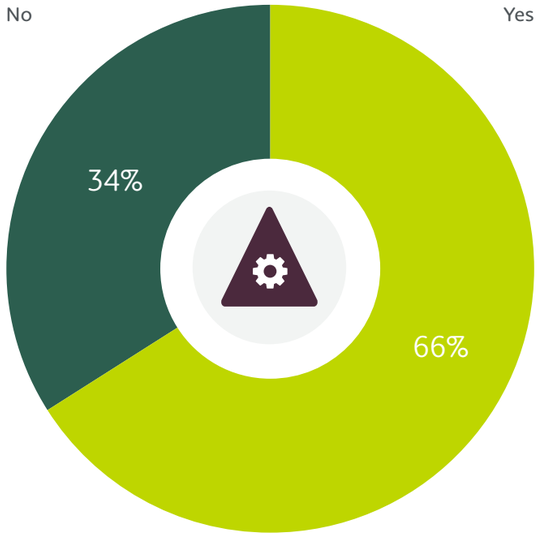
Write, tech, test, repeat: How to perfect tech failure response plans

Once all business-critical technology risks are identified, you need to develop policies and procedures to follow if it fails. These policies and procedures, often known as crisis-management playbooks, help to mitigate risks, identify gaps in defenses, and deal efficiently with issues as they arise.

Although the majority (66%) of survey participants have crisis-management playbooks – including 90% of companies generating more than $1bn in revenue – many of these exclude some important details and guidance. Only 42% include details of any regulators that may need to be informed in each jurisdiction the business operates in. And just 37% include details of the circumstances under which regulators should be informed.

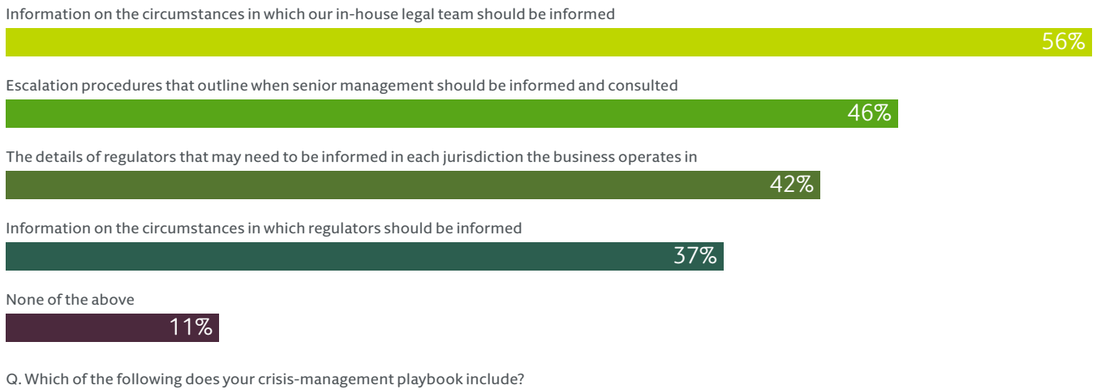
Producing these playbooks needs to be a collaborative effort. As with cyber plans, multiple parties will have to get involved, including management, technology, and legal teams. Having the information in writing for reference is important, but it is useless unless it can be acted on effectively. You will need to train your teams to respond to a major technology failure event. And one of the most effective ways to reinforce that training is to simulate the response through tabletop exercises.

Fig 7 Two-thirds of businesses have technology failure crisis-management playbooks



Q. Does your business have a technology failure crisis-management playbook or other such document that guides how you should respond to such an event?

Fig 8 Tech failure crisis-management playbooks lack vital information

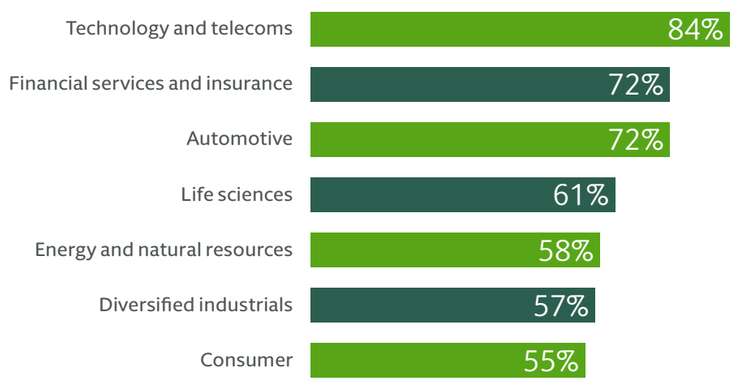


Q. Which of the following does your crisis-management playbook include?

The survey data also reveals that companies in certain sectors are much more likely to have developed a technology failure crisis-management playbook: 84% of technology and telecoms companies and 72% of financial services and insurance businesses have such a document, compared with fewer than six in 10 companies in the energy and natural resources, industrials, and consumer sectors.

The risk that a regulatory investigation or litigation may follow the failure of key technology is growing. It is therefore vital that senior management and the board implement the measures necessary to protect the business, and prepare their teams. By identifying business-critical technology and developing comprehensive crisis-response playbooks, you can prepare the business to act decisively and build resilience to ensure business continuity.

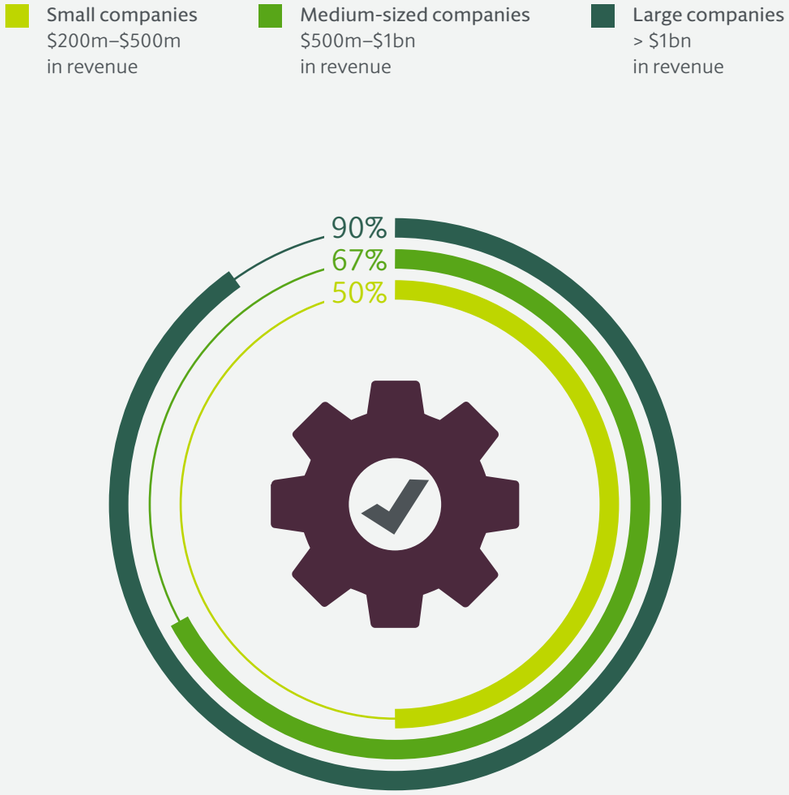
Fig 9 Technology and telecoms companies are most likely to have a technology failure crisis-management playbook



Q. Does your business have a technology failure crisis-management playbook or other such document that guides how you should respond to such an event?

Fig 10

Larger businesses are much more likely to have technology failure crisis-management playbooks



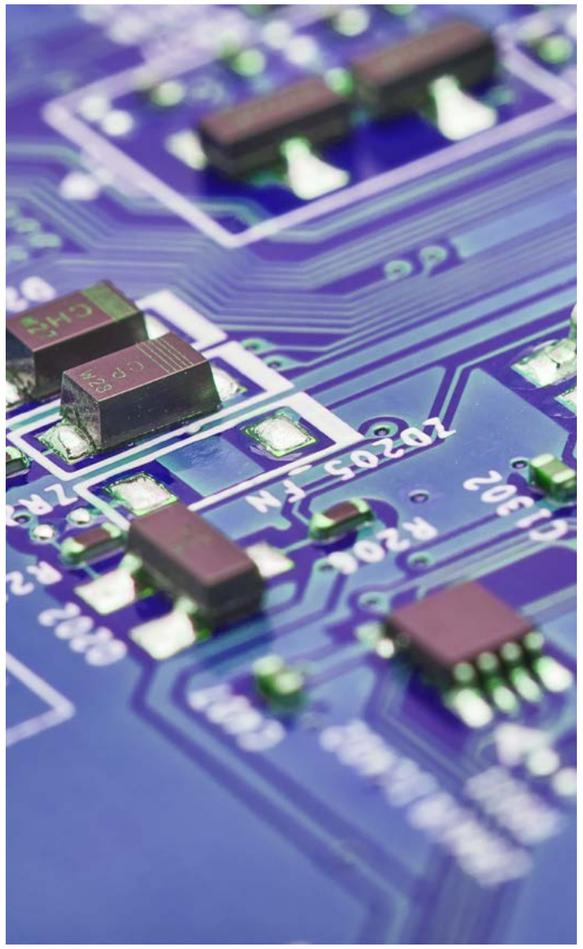
Q. Does your business have a technology failure crisis-management playbook or other such document that guides how you should respond to such an event?

Beyond the law: How to address technology's ethical challenges

45% of businesses do not vet technology supplied to them for technology bias.

In collaboration with the wider business, senior management must establish ethical principles that guide how new technology is used.

Businesses say that data privacy is their top technology-related ethical concern; data bias ranks second.



Data privacy is businesses' biggest ethical concern

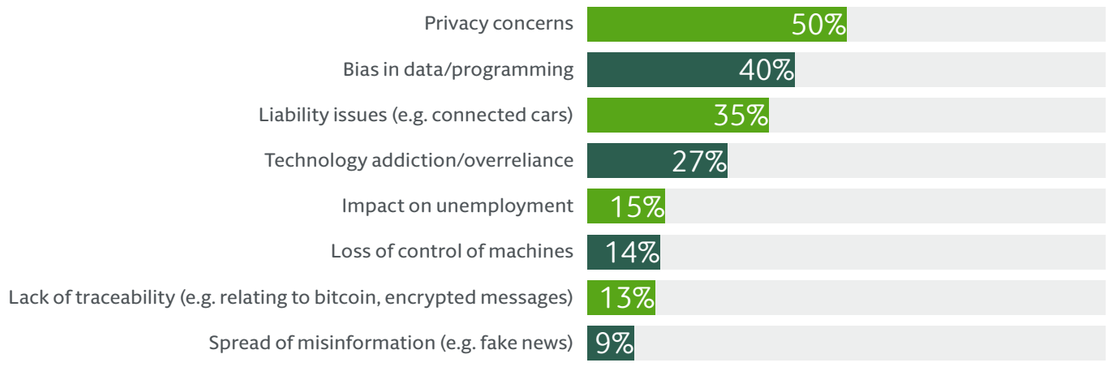
Businesses that use and sell technology increasingly encounter complex ethical issues. Managed badly, these can cause immense reputational and financial damage.

Which issues cause most concern? When they are asked which ethical issues they consider to be most important in the development and deployment of technology, survey respondents most frequently mention privacy concerns. This no doubt reflects many jurisdictions' tightening data privacy regulations in recent years, consumers' increased focus on their privacy rights, and the significant reputational and financial consequences that can result from failure to comply with applicable laws (see "Prepare now for a surge in cyber and data breach litigation").

It also highlights concerns about consumer trust – that it will be eroded if businesses use their data in ways that are not anticipated by or beneficial to the consumer, even if they comply with data regulations.

"The way we use data is not just determined by the law, but also by ethical considerations," confirms Matthew Owens, Global Head of Legal, Digital, at Novartis.

Fig 11 Privacy and bias are businesses' top ethics considerations



Q. Which of the following ethical issues do you consider most important when developing and deploying technology?

Almost half of businesses do not vet for technology bias

Bias in data and programming is survey respondents' second-most important ethical issue, and it is easy to see why. Created by humans, technology can reflect the biases – conscious or subconscious – of its creators, and sometimes biases only become apparent after the technology is deployed.

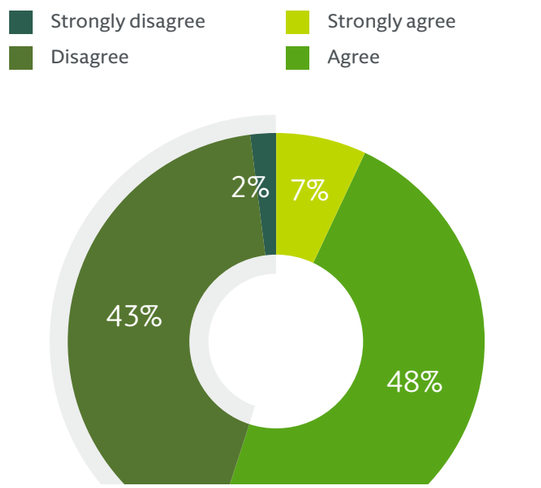
Discrimination often comes up in relation to the use of algorithms and AI technology to scan and review CVs in the recruitment process. There are concerns that the algorithms underpinning this software incorporate biased logic and therefore discriminate against people who live in particular areas or have certain names.

If technology is purchased rather than developed, you may not know whether it contains biases. The very least you should do is seek warranties and assurances that procured software does not contain biases, and conduct due diligence to check it. However, almost half of the businesses in the research do not currently vet for technology bias.

Another problem is a lack of representative data, which can cause technology-enabled products to perform badly for some sections of the population. Research in the U.S. has found that the error rates for facial recognition software developed by multiple companies are much higher for African American and Asian faces than for Caucasian faces[1].

In another example, consumer reviews and media reports say that certain brands of wearable health devices monitor the heart rates of people of color far less accurately[2]. That not only creates an inferior product, but it could also entrench bias further if data from these wearable devices is used to inform the development of other products.

Fig 12



Q. To what extent do you agree with the following statement? "We check that technology supplied to us has been vetted to not include any biases."

> "Businesses purchasing software should, if relevant, ask the provider what they have done to eliminate bias against certain population groups. These conversations happen a lot in the U.S., and it's starting to pick up in Europe."
>
> Desmond Hogan | Head of Global Litigation, Arbitration and Employment, Hogan Lovells

1. MIT Technology Review, A U.S. government study confirms most face recognition systems are racist, December 2019
2. STAT, Fitbits and other wearables may not accurately track heart rates in people of color, July 2019

Non-tech companies can tackle misinformation

Just 9% of businesses identify the spread of misinformation as an important ethical issue to address when investing in technology, which makes it the least frequently considered ethical challenge. This may be because only companies in the media and technology sectors feel directly impacted by and responsible for misinformation.

Companies like camera company Snap Inc. kept misinformation front of mind as it developed its multimedia messaging platform, Snapchat. "Fighting the spread of misinformation is important to us," says Dominic Perella, Snap's Deputy General Counsel and Chief Compliance Officer. "Our platform design doesn't allow misinformation to spread because much of the interaction on our platform is on a one-to-one or small group communication basis, and because of the way we designed our content platform. You can't forward things – there's no virality."

Although companies outside the technology and media industry are not directly responsible for the spread of misinformation, they can take steps to halt it. In June 2020, for example, a number of well-known brands paused advertising on all social media platforms because of concerns that they were propagating misinformation and hate speech.

Three steps to address the growing ethical challenges

The financial, reputational and increasingly litigation-related costs of not addressing the ethics of technology mean that this should be a top priority for management. Based on our experience advising clients, here are three simple steps that you can take to address ethical issues.

1

Establish ethical principles that govern technology use

When investing in technology that raises ethical challenges, it is imperative to establish and publish principles that govern how it will be used. This increases customers', employees', and other stakeholders' trust that innovative technology will be deployed within a clear framework. This is what pharmaceutical company Novartis is doing in relation to AI.

"The company is currently putting together our position on the ethical use of AI, and will likely publish it internally and externally," says Matthew Owens. "It reinforces how committed we are to being transparent about how we use the technology, how we are limiting or mitigating bias, and how we are building in safety, security and privacy by design."

2

Ensure that the entire business discusses ethical issues

Establishing an ethical position on the use of technology cannot be left to one team within your business. It must be directed by management and involve a variety of business functions, including legal and product teams.

3

Hold suppliers to the same ethical standards

It is essential to hold suppliers to your own ethical standards. In the context of AI bias, this means seeking assurances that AI technology does not contain biases. Once the technology has been deployed, it is then imperative to make sure it continues to be used in a way that adheres to the company's ethical principles.

Technology M&A, joint ventures and outsourcing: An opportunity to be considered carefully

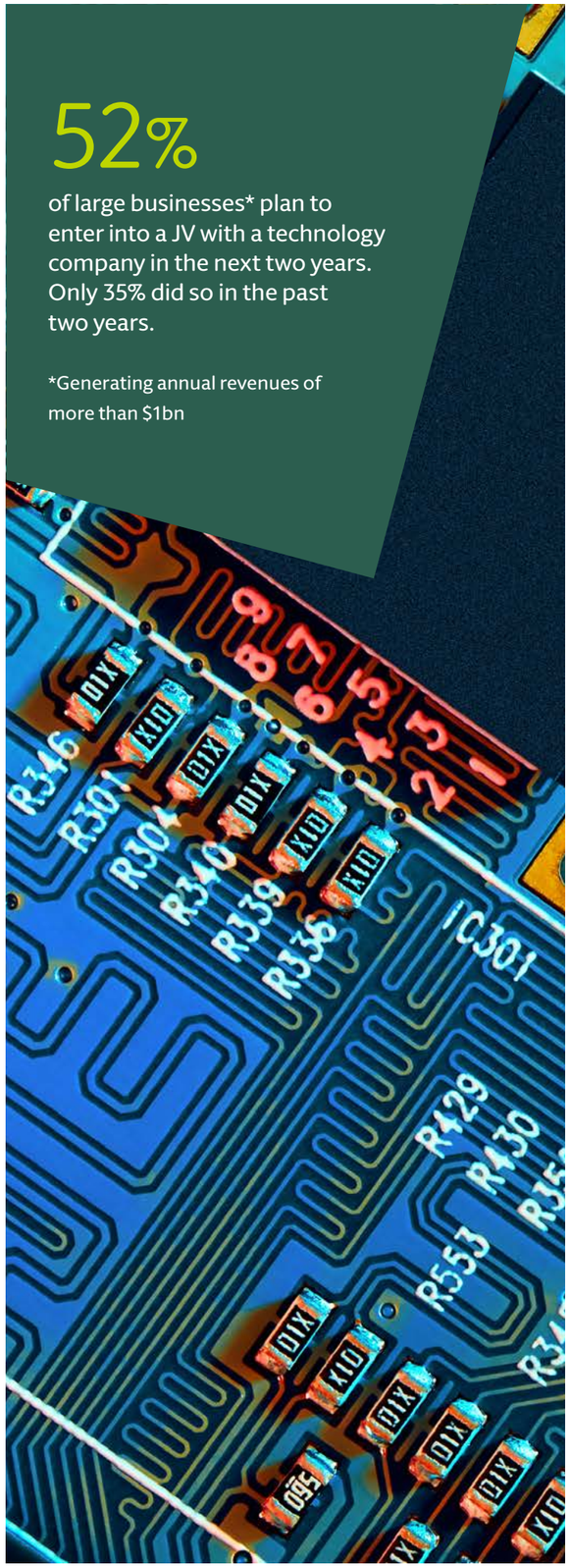
47%

Technology partnerships are increasingly popular: 47% of businesses plan to enter into a technology joint venture (JV) in the next two years. Just 39% did so in the past two years.

65%

Businesses increasingly target technology companies that bring a more complex set of risks: 65% expect the number of JVs with startups to increase, and 60% expect JVs with companies in emerging markets to rise.

Despite growing complexity, only the minority of businesses have increased the amount of time they spend analyzing risks or have involved a broader set of internal or external stakeholders during due diligence.



Tech M&A and partnerships grow in popularity

For the 61% of businesses that say technology is a key component of their growth strategy, a key question is how to obtain it. For many, M&A, JVs and outsourcing are going to provide the answer.

According to the survey data, 47% plan to form a JV with a technology company in the next two years, up from 39% who did so in the past two years. In parallel, half intend to outsource a key business function to a technology company in the next two years, up from the 44% who did so in the past two years.

Large businesses (those generating more than $1bn in annual revenue) and those based in the U.S. are particularly keen to forge technology partnerships.

These deals can be instrumental in helping businesses to get ahead – and stay ahead – of the competition. Traditional businesses outside the technology sector may find it quicker and easier to incorporate tech into their products or internal business processes by forming a JV with, or acquiring, a company that has either already developed it or is better equipped to do so. Businesses may also be able to generate significant efficiencies by outsourcing key business processes to a technology company.

To mitigate risks, legal teams must work in close collaboration with the wider businesses across the deal lifecycle – from pre-completion evaluation and documentation to post-completion operations management.

Fig 13 Businesses plan to increase technology acquisitions and partnerships in the next two years

Q. Which of the following, if any, had you executed in the two years prior to COVID-19 (2018–2019)? Which are you planning to execute in the next two years? For each time period, please select all that apply.

External partnerships and M&A come with added risk

There are many hazards of entering into technology M&A, JVs and outsourcing. First, there is the fundamental risk that the technology of an acquired business or JV partner does not work or is less advanced than expected.

Second, there is a risk that the JV breaks down because one party fails to deliver or relations sour. Third, a JV or outsourcing arrangement in which key business systems are interlinked could create cyber vulnerabilities.

And finally, there is the important emerging risk of government intervention. Governments and businesses are increasingly concerned that a JV partner could pass important technology to a foreign power. This could not only derail negotiations at the outset of the deal, but also affect longstanding JVs that are now considered by government to be a risk. The Committee on Foreign Investment in the United States (CFIUS), for instance, ordered a U.S. robotic suit manufacturer to terminate its JV with two Chinese parties in June 2020. This instruction was notable because it related to a JV outside the U.S. – CFIUS intervention had been primarily focused on U.S. JVs.

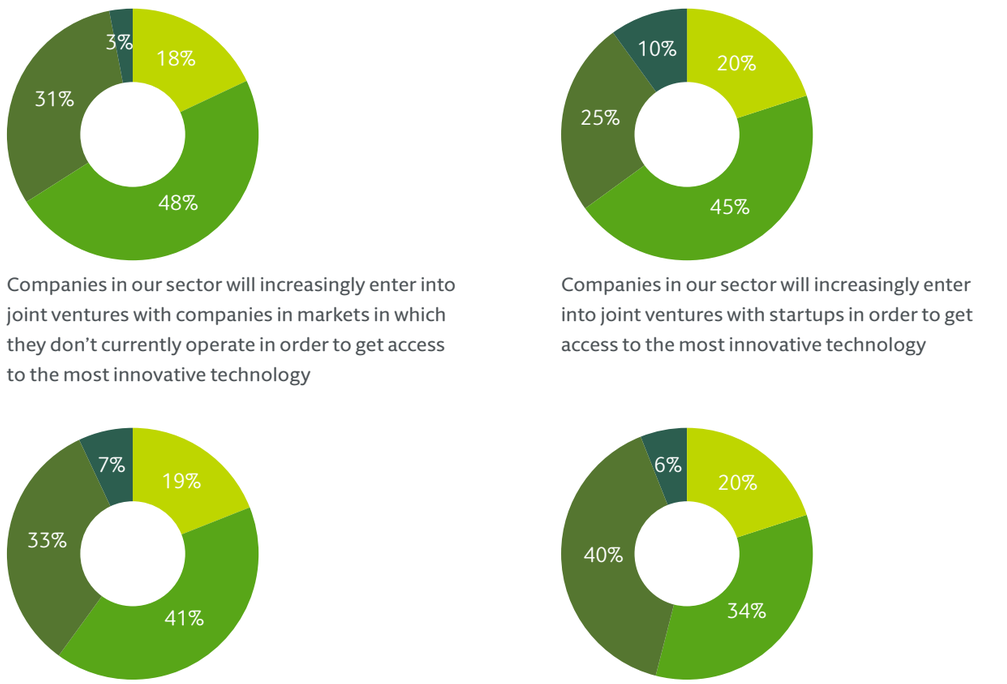
Technology acquisitions and partnerships bring unforeseen risks

Technology acquired or developed through a JV, for instance, may fail or not perform as expected. A JV could break down because of a deterioration in relations or if ordered by government authorities (which is increasingly a risk where the JV partner is based in China). Or a JV or outsourcing arrangement could create cyber vulnerabilities (see “External partnerships and M&A come with added risk”).

The survey data shows that businesses plan to increase their deals with particular types of businesses: 65% say that companies will increasingly enter into JVs with startups in order to get access to innovative technology, and 60% that companies will target emerging markets more frequently.

Unfortunately, some risks are particularly acute when businesses partner with or acquire these types of businesses. Startups may lack the resources to implement adequate cybersecurity protections. And businesses that are located in emerging markets may be subject to data privacy regulations that are not as strict as those in Europe or the U.S.

Fig 14 Risks associated with acquiring and partnering with tech companies are increasing

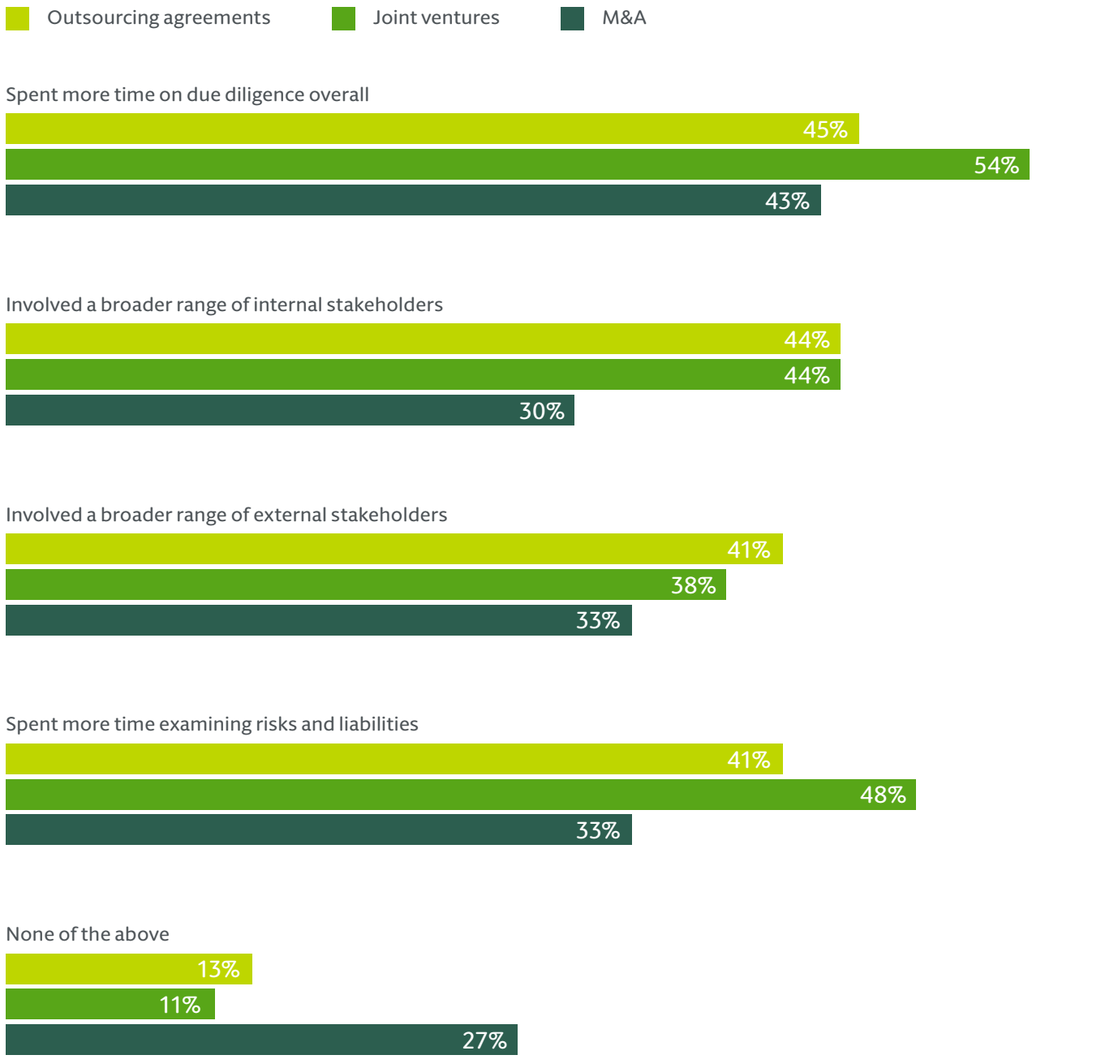


Q. To what extent do you agree with the following statements relating to acquisitions of and joint ventures with technology companies?

In order to spot and resolve issues that could be challenging once a deal is agreed, businesses will need to spend more time and resources on due diligence.

That increase in due diligence is not yet happening. Only a third of businesses spent more time examining risks and liabilities in their most recent technology acquisition compared with their previous deal of a similar size. And just 38% of businesses involved a broader range of external stakeholders in due diligence for their most recent technology JV compared with their previous similar transaction.

Fig 15 The majority of businesses have not improved due diligence in relation to technology deals



Q. Thinking about the last technology business you acquired or collaborated with, which of the following, if any, did you do in relation to due diligence compared with previous deals of similar size?

Seven ways to mitigate deal risk

You should involve internal and external legal counsel in the deal at the earliest opportunity. And legal teams should remain involved once the deal is in operation to help identify and manage any risks that materialize.

Beyond that fundamental step, our work with clients has revealed seven more ways to minimize the risks of these kinds of deals.

1 Plan ahead for divorce

It is important to agree a process for winding down a technology JV if necessary, and establish how the assets and liabilities will be divided. Defining this clearly at the outset will increase the likelihood of salvaging key technology and staving off the threat of litigation. The documentation must clearly define the circumstances in which each party can terminate the JV, how they must inform the other side, the rights of each party to background and foreground intellectual property (IP) and licenses and how the financial accounts will be dealt with. IP specialists should be consulted to review deal document at the outset to ensure that it can be protected in a dispute. It is also absolutely crucial to detail the dispute resolution mechanisms in the event that the parties cannot agree on how the JV will be dissolved.

2 Think carefully about director duties and shareholder rights

It is imperative to consider carefully who the directors of a new JV will be and what their respective duties are to the JV company. Typically, the JV directors will also be directors of the two separate business entities who formed the JV, so conflicts of interest may emerge. You should therefore discuss and then articulate in deal documentation the rights and responsibilities of each director and what happens to each director should the JV be terminated. It may also make sense to appoint a completely independent director to manage the JV.

3 Clearly define key milestones

The value of technology startups is difficult to assess, so acquirers often make payments against particular milestones such as achieving sales targets or hitting profitability. Litigation can follow if the acquirer believes that the target has not made reasonable efforts to achieve a particular milestone, or if the target believes the acquirer has hampered its efforts to do so. You can prepare for this in advance by discussing at the negotiation stage what constitutes reasonable efforts and then clearly defining this in the deal documentation. Legal teams should also work with the business to actively ensure that these contracts are well managed so that risks are identified early and rights are protected. Doing this protects the business and helps to avoid costly litigation.

“Many businesses don’t detail how a JV can be wound down. But not doing so creates multiple complex issues if the partnership fails.”

Nathan Searle | Partner, Hogan Lovells

"You must enter technology JVs with Chinese parties with your eyes wide open. You should assume that any technology will be shared with the Chinese government and come up with a plan B for enforcing judgments."

Antonia Croke | Partner, Hogan Lovells

4 Ensure that legal and technical teams work together during the lifecycle of the deal

If technology developed by a target company or JV partner malfunctions and results in a serious data breach and loss of revenue, litigation could either be brought by the individuals affected or by data protection regulators – or both. Technical and legal teams must work together in the due diligence phase to identify any issues with the technology that may not be covered by generic reps and warranties and design specific language. In parallel, they must consider the extent to which the business's rights to seek compensation from their JV partner or the directors of the acquired company if there is a problem need to be protected. These teams must also work collaboratively when an issue arises. By doing so, you will be best placed resolve the issue in a way that does not result in litigation.

"It's vital to understand and define what constitutes technology failure. If you don't, then M&A documentation will just include general warranties, which may not cover a specific failure event. Technical and legal teams must work together to craft this."

Bill Regan | Partner, Hogan Lovells

5 Assess cybersecurity and data privacy hygiene

A serious data breach or cyber attack that stems from a JV or outsourcing partner can lead to complex litigation. So you should assess how acquisition targets and JV and outsourcing partners protect their data and the strength of their data governance and cybersecurity incident-response plans. You should also find out whether the potential partner has experienced a breach before – and how they responded to it. If there has been a breach in the past, check for any outstanding regulatory or law enforcement enquiries or investigations.

6 Evaluate how government intervention creates litigation risk

In the U.S., CFIUS has become active in scrutinizing deals involving Chinese companies' investments into technology businesses. Litigation may result if it is not clear who bears the risk of CFIUS intervention or if one party believes the other has not made every effort to obtain CFIUS approval. It can also happen if government pressure or intervention results in other commercial contracts not being met. CFIUS aside, you should carry out extra checks to understand how their intellectual property will be shared when entering into JVs with counterparties in other jurisdictions. You should also stipulate in deal documentation where any dispute will be heard and how judgment will be enforced.

7 Take extra precaution when entering emerging markets

Assessing litigation risk in emerging markets is difficult because regulations and the degree of penalties for non-compliance may be less clear. You must conduct a more thorough risk assessment when considering acquisitions of, and JVs with, companies located in emerging markets, including checking for anti-bribery and corruption risks, and engage directly with industry, data protection and other relevant regulators to check whether your plans raise any obvious issues. It is wise to devise a plan that stipulates who should liaise directly with regulators.

You must also establish in deal documentation the mechanism for resolving any disputes and stipulate that any dispute should be heard in a neutral, independent and efficient forum with courts that have the expertise to ensure any decisions are enforceable in a reasonable time. Based on our work with clients, we are seeing arbitration used as the mechanism of choice for these types of transactions. This also increases enforcement options in a dispute with a partner whose assets are based in an emerging market where it might be more difficult to enforce a court judgment.

Technology talent acquisition: A new way of working

Businesses plan to use hiring to accelerate technology transformation: 53% plan to hire technology personnel in the next two years. Just 40% did so in the past two years.

Businesses that are hiring aggressively must consider the risks associated with employee misclassification and protecting confidential information.

Using personal devices for work purposes may save costs and keep clients happy, but it also creates complex legal risks.

53% vs 40%

53% of businesses plan to hire technology expertise in the next two years. Only 40% did so in the past two years.

Our survey data reveals that businesses plan to increase recruitment of individuals with technology skills: 53% intend to hire technology expertise into the business in the next two years – up from 40% that did so in the past two years.

Employee misclassification can lead to litigation

When recruiting, you must be mindful of misclassification risk. If contingent workers (such as freelancers, independent contractors and consultants) are deemed by tax authorities and regulators to be employees, you can be forced to pay employment related taxes owed in addition to penalties.

There is also a risk that contingent workers will independently or collectively seek rights and benefits if they believe they should be classified as employees. This is not just a risk to "new economy" companies, but also to traditional businesses that replace full-time employees with contractors or who seek to maximize flexibility through building a workforce model based on contingent workers.

It is a risk that is particularly complex for companies operating in multiple countries, because the law varies across jurisdictions. Indeed, Californians voted in November 2020 that freelance workers could continue to be classed as independent contractors rather than employees. But regulators in other jurisdictions may apply different rules.

"Any time you hire consultants or independent contractors to replace employees, you have significant risk of misclassification, the costs of which outweigh the savings of hiring these people as consultants rather than employees. The direction of travel is that employers will have less freedom to treat contingent workers differently, which is not just a risk for 'new economy' businesses – we're also seeing traditional automotive companies, for example, experiencing this."

Kerstin Neighbour | Partner, Hogan Lovells

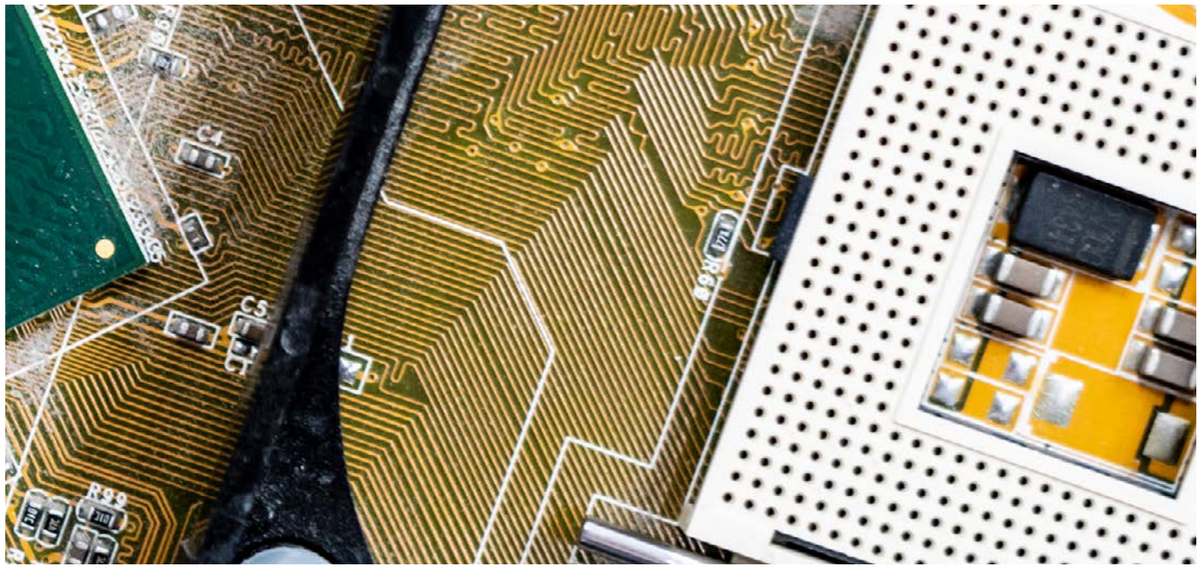
Information is even harder to protect with a remote workforce

Another risk of employees hired to work on sensitive technology projects is that if they move to a rival company, confidential information goes with them. Confidentiality risks like this need to be especially closely managed in jurisdictions and industries where it is common for workers to use personal devices or non-work systems to communicate. Today, the risk is higher across the board because of the shift to remote working caused by the COVID-19 pandemic.

It is therefore essential to have enforceable non-compete clauses and confidential information protections in place when employees are recruited to work on sensitive technology projects. The shift away from centralized workplaces has made these more difficult to enforce because employees are now more likely to be working from a jurisdiction that is not covered in the clause. You must therefore be more specific about where non-compete clauses can be enforced and use language that ensures enforceability in a number of jurisdictions.

"Non-competes are getting more difficult and expensive to enforce in the U.S. and the move to remote working will make this even more difficult."

Michael DeLarco | Partner, Hogan Lovells



Monitoring employee productivity: proceed with caution

As a result of the pandemic and the move to remote working, more and more employers are now deploying technology that evaluates employee activity and productivity. However, if they do not carefully consider which data they track and how it is used and stored, they could be at risk of employee claims and investigations by privacy regulators. In certain European markets, businesses must work very closely with works councils to clarify which data is tracked and what it is being used for.

"Employee monitoring is a hot topic at the moment, and advances in technology mean that employers can track more aspects of employee behavior. Employers need to think carefully about which features they switch on, which data they keep, and what they use it for. There's a risk of an employee claim or fine from a regulator if they cannot justify what they are doing."

Stefan Martin | Partner, Hogan Lovells

"Bring your own device" brings its own risks

Many companies now ask employees to use their personal devices for work. Commonly known as "bring your own device" (BYOD), this saves costs – but it also raises a number of important legal issues.

Even companies that do not encourage BYOD may find employees using non-work systems to communicate with each other and with customers. For example, it has become the norm in some markets for employees to communicate through apps such as WeChat and WhatsApp.

You need to help employees understand how and when to use non-work systems. And if it is customers that are driving this practice, you need to provide clear guidance on how employees should respond.

Where local law permits it, privacy policies could allow personal devices used for work purposes to be monitored for activity that might indicate fraud and accessed in the event of an investigation. However, in many jurisdictions it is not possible to require employees to hand over personal devices for investigations.

The risk here is clear, and more and more clients are coming to us for help with recovering work-related communications from personal devices. There is a balance to strike between the risks of using platforms that are not part of their own infrastructure and the benefits of meeting clients' expectations and saving costs.

"As a South Korean company that is extremely protective of our IP, we have to take extra precautions about the devices employees use and their connectivity. Employees simply cannot access work systems remotely without special authorization, and even within the office you cannot use the internet without special permission, or download anything to a thumb drive, for example. Our focus on security adds an extra layer of complexity, but it is necessary."

David Delman | Executive Vice President, Head of International Legal & Commercial Management, Samsung Engineering

Prepare now for a surge in cyber and data breach litigation

Two-thirds of businesses acknowledge that costly litigation or a regulatory investigation might follow a data breach. Our survey data shows that many are unprepared.

Board directors and C-level executives must pay close attention to technology risk, but the majority only do so “to a limited extent.”

Although 76% of businesses have a cybersecurity incident response plan, only 31% of these were prepared in collaboration with legal teams.

There are numerous instances of data breaches stemming from third parties. But two-thirds of businesses check the cyber credentials (the steps they have taken to protect their business from a cyber attack) of only a minority of their partners.

"Data breaches have happened for many years. But what's new, especially for those in Europe, is that collective or class action litigation now follows."

Christine Gateau | Partner, Hogan Lovells

Headline-grabbing penalties and damages mean that most businesses are now aware of the potential consequences: two-thirds of businesses acknowledge that there is a modest or significant risk of a regulatory investigation or litigation following a data breach. Our survey data also shows that many are not doing enough to mitigate this. More fundamentally, most boards are not yet giving technology risks enough attention.

Cyber risk is a boardroom issue

To ensure that the cybersecurity mitigation measures knit together to form the strongest-possible defense, senior management and the board need to play an active role in overseeing how cyber risks are managed.

There are two further reasons for this. First, major strategic business decisions can create cyber risks and vulnerabilities. A strategic move by a traditional manufacturing company into producing goods that process sensitive personal data, or a decision to invest significantly in new technology, can create extra cyber risks. Second, regulators increasingly call on board directors to actively oversee technology risks.

But our survey data shows that 60% of boards only oversee technology risk "to a minor extent."

Just 9% look at it "to a significant extent," whereby they oversee management of a broad range of technology risks and deem them to be as important as traditional risks, such as financial risk.

In order to manage technology risk effectively, boards need to understand the nature of the threat. But there is significant scope for improvement here: just 37% of surveyed businesses are more than "somewhat confident" that senior executives at their business understand the risks associated with the technology they are developing and implementing.

One practical way to improve executive management of technology risk is to establish an executive sub-committee that specifically addresses these issues.

"Technology risk should be a priority for C-level executives," says Matthew Owens, Global Head of Legal, Digital, at Novartis. "This is a key priority for us as we fulfill our strategic goal to go big on data and digital."

Litigation can strike on multiple fronts

Cybersecurity and data privacy litigation can take many forms. In some jurisdictions, consumers affected by a data breach may club together and bring a class or collective action (where a group of claimants that have been affected in the same way by an event bring action as a group) against the company that suffered the breach. Marriott International, for instance, is currently facing collective proceedings in both the U.S. and the UK in relation to a data breach that affected 339 million customers worldwide between 2014 and 2018[3]. In October 2020, the ICO, the UK's privacy regulator, announced it was fining Marriott International £18.4m for infringements of the EU's GDPR rules[4].

The growing number of sector-specific and generally applicable cybersecurity regulations make this type of litigation increasingly likely because they set out a duty of care. This can often be the basis on which subsequent litigation is brought.

Following a data breach, shareholders of the affected company may also bring litigation against the company and its directors. In 2019, for instance, a shareholder of commercial banking firm Capital One Financial Corp filed a lawsuit against the company after a data breach involving the personal information of over 100 million customers in North America[5]. The shareholder sought to recover losses from the decline in share price that resulted from the breach, and claimed that the company had made misleading statements about its data privacy protections.

Companies can also face huge fines and damages even in the absence of a major cybersecurity breach. For example, the record $5bn penalty imposed on Facebook by U.S. consumer rights regulator, the Federal Trade Commission (FTC), was for violating users' privacy – not because of any cybersecurity breach[6].

3. Financial Times, Hotel group Marriott faces London lawsuit over huge data breach, August 2020
4. ICO, ICO fines Marriott International Inc £18.4 million for failing to keep customers' personal data secure, October 2020
5. Bloomberg Law, Capital One Investor Sues Over Breach as Consumer Suits Unified, October 2019
6. FTC, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, July 2019

Fig 16 Most boards only oversee technology risk and how it is managed to a "minor extent"

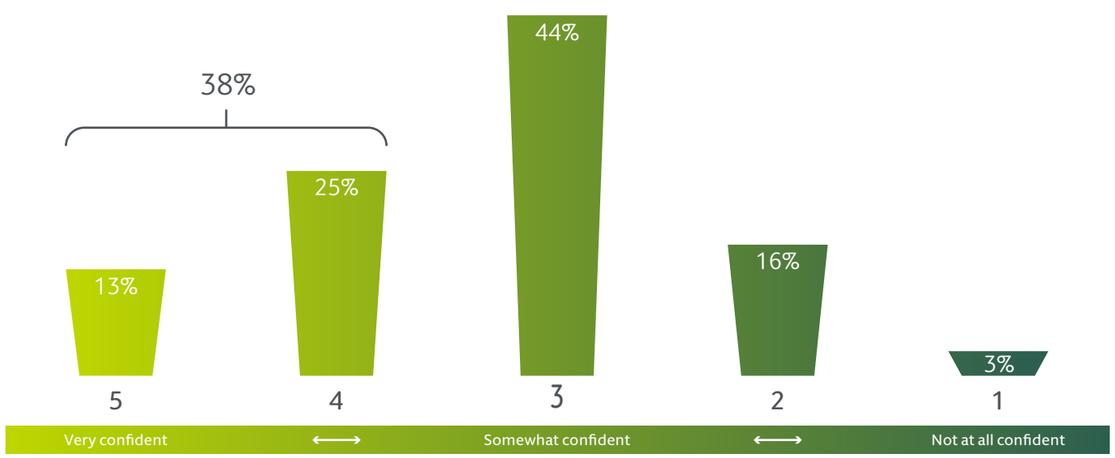
Q. How actively does the supervisory/non-executive board oversee technology risk and how it is managed?

Seven out of 10 businesses have not mastered privacy by design

One of the most critical times at which companies unknowingly introduce ways of using or storing data that break data privacy regulations is when new products that handle personal data are developed or updated. So privacy lawyers need to work alongside product teams on new product development from the start. This concept – "privacy by design" – has been around for years, but many businesses still do not practice it.

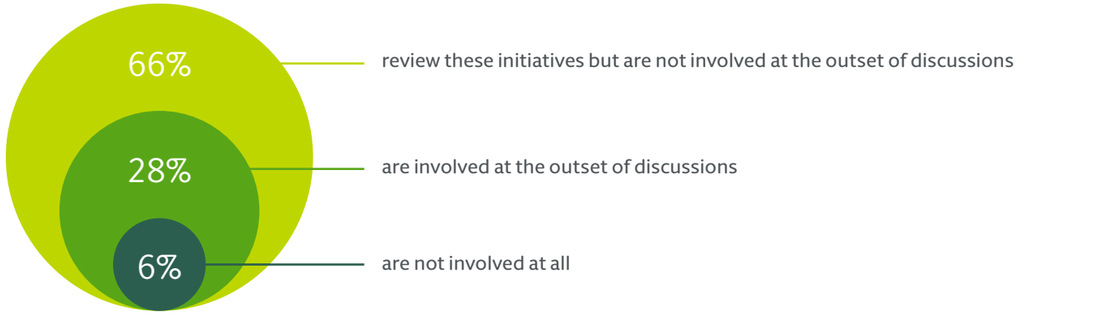
Just 28% of surveyed businesses say that privacy specialists are involved in the development and implementation of new technology that gathers and/or processes personal data from the outset. Without this early engagement from privacy specialists, you may find they have to abort a product at a late stage or face litigation once products have been launched.

Fig 17 Just 38% of businesses are more than "somewhat confident" that their senior executives understand the risks associated with technology



Q. How confident are you that your senior executives understand the risks associated with the technology your business is developing and deploying?

Fig 18 Data privacy specialists are rarely involved at the outset of the development of and implementation of new technology that gathers and/or processes personal data

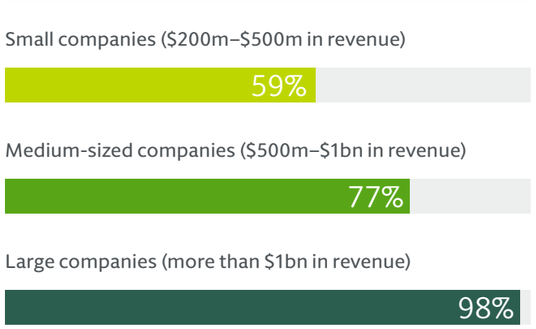


Q. Generally speaking, at what stage are data privacy specialists involved in the development of and implementation of new technology that gathers and/or processes data/personal data?

Getting the cyber response plan right

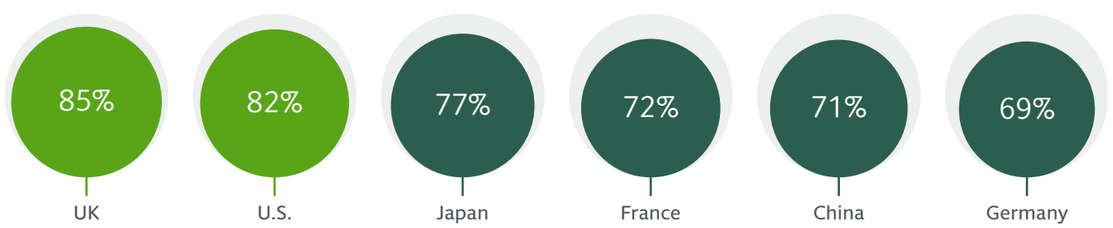
Nearly all large companies (98%) have a formal cybersecurity incident-response plan, but this is true of only 77% of medium-sized and just 59% of small companies. The survey data also reveals that businesses in China and Germany are less likely than those in the UK and the U.S. to have this kind of plan.

Fig 19 Larger businesses are much more likely to have cybersecurity incident response plans



Q. Does your business have a technology failure crisis-management playbook or other such document that guides how you should respond to such an event?

Fig 20 UK and U.S. businesses are most likely to have cybersecurity incident-response plans



Q. Does your business have a technology failure crisis-management playbook or other such document that guides how you should respond to such an event?

Fig 21 Legal teams are seldom involved in developing cyber incident-response plans

Q. Which of the following teams are involved in the creation of your company's cyber incident-response plan?

Creating a comprehensive cyber plan requires multiple parts of your business to collaborate, and silos between management, technology teams, legal teams, and privacy specialists to be broken down. Our survey results show that there is a collaboration gap: legal teams are involved in creating cybersecurity incident response plans at just 31% of our surveyed businesses.

In our experience if legal teams do not contribute to cybersecurity incident response plans – or worse, if you do not have one in the first place – there is increased risk that vital action that could better position the company for any potential investigation or litigation will not be taken in the immediate aftermath of a data breach.

For example, when a major breach happens, key regulators will almost certainly need to be informed and, where possible, privilege should be maintained. That means legal teams need to be involved in the response from the start. You may also want the legal team to review communications to customers and the media. Taking these actions swiftly and effectively puts you in a much better position if there is a subsequent regulatory investigation or litigation.

"We haven't had a major cyber event, but if one occurs, the cat is out of the bag and you're inevitably going to have a lot of litigation risk at that point," says the Head of Litigation at a public company. "But by simply having lawyers and litigators looped in immediately you can to an extent mitigate that risk in real time. You may for example be able to keep things under privilege to some extent and will know when to contact the appropriate regulator. Just having our head of privacy, general counsel and myself in the loop right away on a major incident is the best solution to allow us to identify issues."

"The legal team has focused on training and raising awareness across the business about cybersecurity risks. We have also established certain protocols about how to respond as soon as we learn of a breach. This goes beyond what we are required to do from a legal perspective to address what we should do from an ethical perspective."

Matthew Owens | Global Head of Legal, Digital, Novartis

Not enough firms are preparing in advance

A lack of collaboration with the legal team also increases the likelihood of not taking sufficient action to minimize risk before a data or privacy breach materializes.

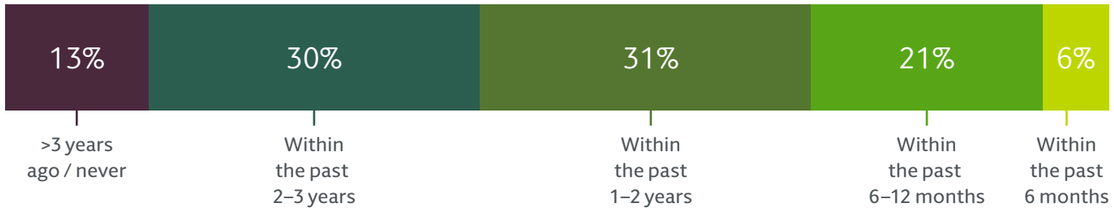
For example, it is essential to ensure that statements about data in disclosures, privacy policies, terms of use and advertising do not become outdated when technology and products change. Businesses in jurisdictions where class actions can be brought should also take a series of steps to prepare for class actions for data breaches or non-compliance with privacy requirements.

To identify where you might be going wrong, it's useful to simulate your response to a breach. However, less than a third of surveyed businesses had simulated a cyber attack in the past 12 months and only 58% had done so in the past two years. With much of the workforce currently working remotely, you should rethink and then re-simulate your response to a data breach.

"Many businesses spend lots of money on ensuring that outside actors can't access their systems and steal data. But for a technology company like ours, we also have to make sure that people on the inside don't pull stuff out. We've experienced this before and this threat should not be overlooked."

Anthony Walsh | Global Commercial Counsel, GE Power

Fig 22 Fewer than a third of businesses conducted a cybersecurity response exercise in the past 12 months



Q. When did you last conduct a cybersecurity response simulation exercise?

The majority of businesses accept risk in their approach to suppliers

Despite numerous, well-documented instances of cyber attacks stemming from vulnerabilities in suppliers' defenses, two-thirds of businesses assess only a small number of their suppliers' cybersecurity credentials.

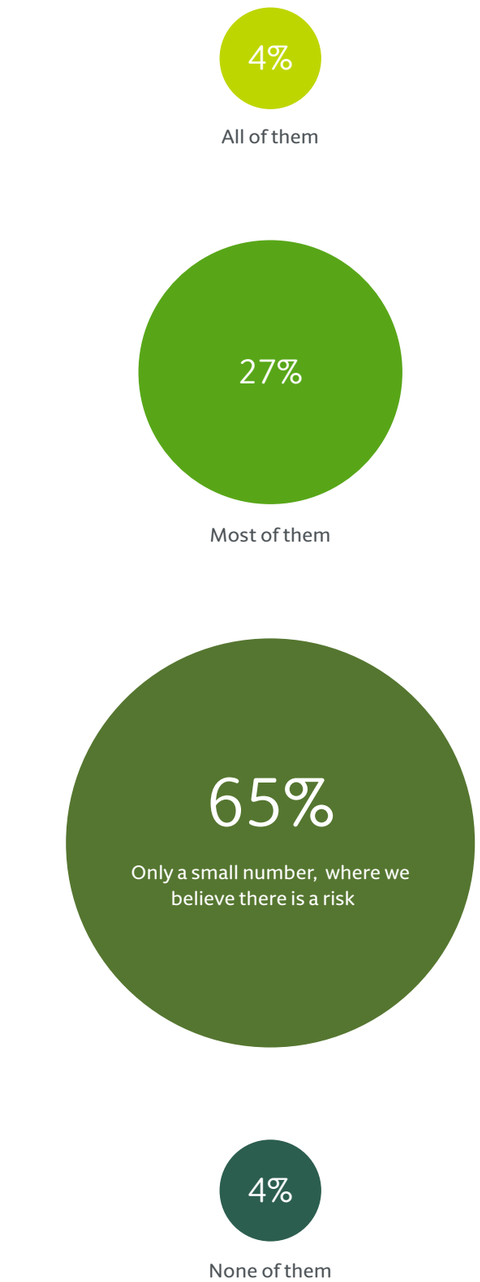
Remember that cyber vulnerabilities can be created by the unlikeliest of suppliers. For example, U.S. retail giant Target experienced a data breach in 2013 that compromised 41 million customer payment card accounts. The breach started with the theft of credentials from its heating, ventilation, and air-conditioning supplier[7].

"Fundamentally, any supplier who is going to hook into our technology, online ecosystem or payment and HR processes in any way through an API or otherwise is going to have to go through a full data security review," says Dominic Perella, Snap's Deputy General Counsel and Chief Compliance Officer. "It's best to err on the side of caution." Given the number of suppliers a business can have, implementing a robust supplier oversight program is essential.

"We've worked with many clients that have suffered a breach due to the fault of a vendor. This adds a layer of complexity because there may be a potential second front for the litigation. Depending on the relationship with the vendor, you may want to litigate against them or seek some indemnification."

Michelle Kisloff | Partner, Hogan Lovells

Fig 23 Most businesses only assess the minority of their third-party technology suppliers' and vendors' cybersecurity credentials



Q. How many of your third-party technology suppliers' and vendors' cybersecurity credentials do you assess?

Remote working exacerbates cyber risk

The sharp increase in remote working in response to the COVID-19 pandemic brings new cybersecurity and data privacy risks. Instances of phishing and ransomware have surged, and employees are more likely to work on personal devices – which may not have the latest cyber defenses installed.

Companies also need to deal with the different risks that remote working presents, such as the difficulties of maintaining confidentiality over business information, including personal data, if people live in shared accommodation. Six out of 10 surveyed businesses plan to implement cybersecurity work-from-home guidelines in the next 12 months. This is positive, but more action is required. You must regularly train employees in cybersecurity hygiene and bolster security with technologies such as two-factor authentication.

Increased remote working will lead to more data being stored in the cloud than on internal servers. You therefore have to add cloud providers to the list of crucial suppliers to review, and ensure that those providers' data retention policies are aligned with your own legal obligations in the event of an investigation or litigation.

7. CIO, 11 Steps Attackers Took to Crack Target, September 2014

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

*Our associated offices
Legal Services Center: Berlin

Get in touch with your Hogan Lovells contact to find out more about how we can help you manage your technology risk.

hoganlovells.com/litigationlandscape

www.hoganlovells.com