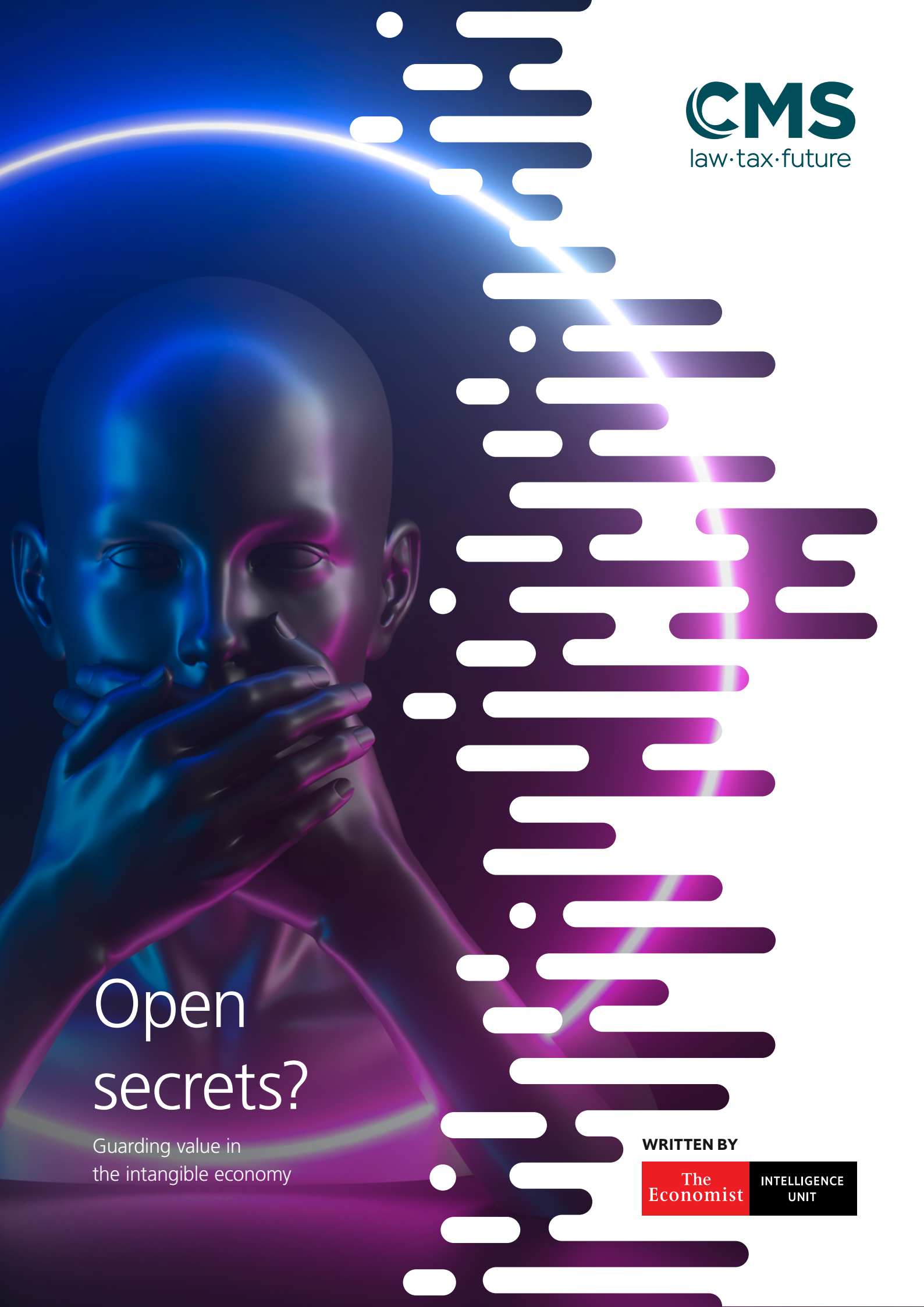


CMS
law·tax·future

Open secrets?

Guarding value in the intangible economy

WRITTEN BY

The Economist INTELLIGENCE UNIT

About this report

Open secrets? Guarding value in the intangible economy is a report commissioned by CMS and written by The Economist Intelligence Unit. It explores the extent to which firms identify intangible assets as trade secrets and implement protective measures to safeguard them accordingly. The report is based on a survey of 314 senior corporate executives located in China, France, Germany, Singapore, the United Kingdom and the United States, and across six sectors: consumer goods and retail; finance; energy and natural resources; life sciences; manufacturing; and technology, media and telecommunications. The survey was conducted in January and February 2021.

Expert interviews

To supplement the survey results, The EIU conducted an interview programme with trade secret and intellectual property experts between February and March 2021, with the aim of validating and guiding our research. Our thanks are due to the following experts for their time and valuable insights:

Anil Cheriyan, Executive Vice President, Strategy and Technology at Cognizant
Professor David Hsu, Richard A. Sapp Professor of Management at the Wharton School, University of Pennsylvania
Professor David Teece, Thomas W. Tusher Professor in Global Business at the Haas School of Business, University of California, Berkeley
Professor Matt Marx, Bruce F. Failing Sr. Professor of Entrepreneurship at Cornell University

About CMS

Founded in 1999, CMS is an integrated, multi-jurisdictional organisation that offers full-service legal and tax advice. With more than 70 offices in over 40 countries across the world and more than 4,800 lawyers, CMS has long-standing expertise both in advising in its local jurisdictions and across borders. From major multinationals and mid-caps to enterprising start-ups, CMS provides the technical rigour, strategic excellence and long-term partnership to keep each client ahead in its chosen markets.

About The Economist Intelligence Unit

The Economist Intelligence Unit (EIU) is the research arm of The Economist Group, publisher of The Economist. As the world's leading provider of country intelligence, The EIU helps governments, institutions and businesses by providing timely, reliable and impartial analysis of economic and development strategies. Through its public policy practice, The EIU provides evidence-based research for policymakers and stakeholders seeking measurable outcomes in fields ranging from gender and finance to energy and technology. It conducts research through interviews, regulatory analysis, quantitative modelling and forecasting, and displays the results via interactive data visualisation tools. Through a global network of more than 650 analysts and contributors, The EIU continuously assesses and forecasts political, economic and business conditions in more than 200 countries.

For more information, visit www.eiu.com.

The report was produced by a team of EIU researchers, writers, editors and graphic designers, including:
Syedah Ailia Haider – Project manager
Jeremy Kingsley – Project director
Katherine Stewart – Project advisor
Tom Nolan – Survey lead
Emma Ruckley – Copy editor
Marina Da Silva – Graphic designer

Foreword by CMS

Some leaks can't be fixed

"Confidential information is like an ice cube … give it to the party who has no refrigerator or will not agree to keep it in one, and by the time of the trial you have just a pool of water." This, from the so-called *Spycatcher* case (1987), applies well to corporate assets: fail to store them correctly and all you might have left is an expensive mess.

The consequences of even a minor exposure of a trade secret can be huge. As this report reveals, the protection of trade secrets is rightly recognised by most senior executives as a priority issue. But the research also reveals gaps that leave companies unnecessarily exposed to risks.The top named threats – cybersecurity attacks and employee leaks – resonate with what we see impacting our clients. Increased home and remote working is straining security measures and employee loyalty. Added to this, an 'innovate or die' attitude in highly-competitive sectors can motivate new joiners to arrive with questionable material from their previous employer, or worse: outright theft between competitors. But while it is easy to focus on the lurking threats from weakened cyber security and disgruntled employees – and they are important – there are more routine actions a company can take to safeguard its secrets than just updating its IT systems or the employee handbook. Commonly, those who most need our help already have a trade secrets policy but have not properly implemented it in relation to the secret in question. Or the policy has not been updated to reflect the intangible assets the business now owns. Or protection was taken for granted.

With trade secrets – which for many businesses are strategically more important than a public patent portfolio – it is always costlier and messier to find solutions after a theft or a leak. Identifying the trade secrets and the threats posed to them, combined with rigorous internal processes and well-drafted contracts, can help prevent such problems from happening.

Harder, but just as necessary, is engaging hearts and minds in corporate culture, to know why trade secrets are important, why we are all are responsible for protecting them, and what may happen if we do not (to both the company and the individual).

In our experience, the businesses with the strongest defences have not only thought strategically about their intangible assets and how best to protect them but are also prepared for the worst. The trick to avoiding an asset becoming a crisis is to be wise before the event.

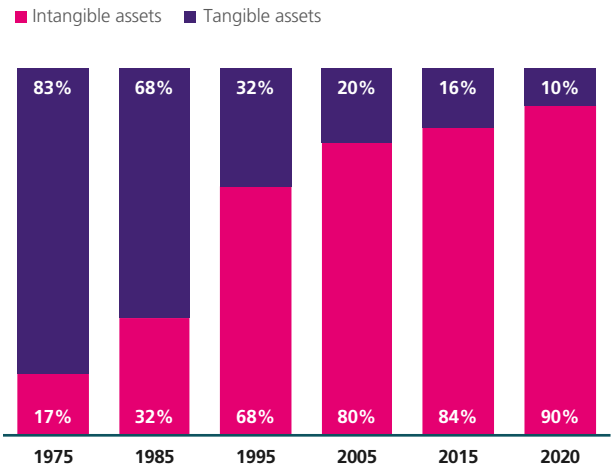
Tom Scourfield,
Co-Head, Intellectual Property Group, CMS

The rise of the intangible

Half a century ago a company's value was overwhelmingly derived from its physical capital – the assembly lines and buildings it owned, and the products it made. Today's firms are built on intangible capital, with assets in the form of software algorithms, brand, customer data, business plans, engineering specifications, product formulas and organisational capital accounting for as much as 90% of the S&P 500's total assets – up from just 17% in 1975.[1,2]

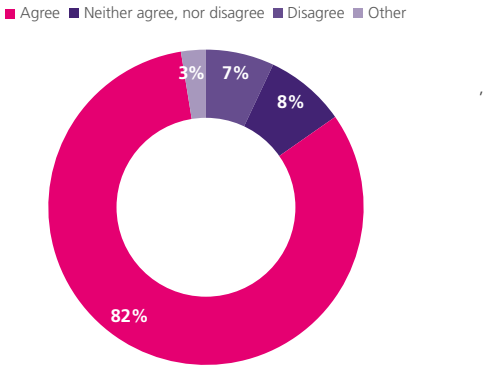
Privileged access and secrecy are inherent to the value of many of these assets, making them by definition "trade secrets". Whether or not firms identify them as such, these assets are vulnerable to employee leaks, competitor theft and cyberattacks – risks that continue to grow as more business is conducted online and across borders, and as more employees work remotely. Yearly, the cost of trade secret theft reaches up to USD 1.7trn.[3]

Figure 1
The value of intangible assets in the S&P 500



Source: Visual Capitalist (2020); Ocean Tomo Intellectual Capital Equity (2020)

Figure 2
The importance of proprietary information
'Proprietary information is essential to my organisation's value' (% of responses)



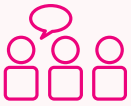
Source: EIU Trade Secrets Survey (2021)

To better understand the extent to which firms identify intangible assets as trade secrets, and seek to protect them accordingly, The Economist Intelligence Unit (EIU) conducted a survey, supported by CMS, of more than 300 corporate executives based in six countries. Our research finds that the risk to high-value intangible assets is a growing concern which warrants proactive protective

measures: firms widely recognise that proprietary information is essential to their organisation's value, and many have already taken steps to protect it, primarily through targeted cybersecurity measures and increasingly through employee regulation. A majority of respondents report that a breach to trade secrets would have significant financial consequences for their organisations.

Figure 3.
What is a trade secret?

A trade secret is a piece of information that is valuable to an enterprise, gives that enterprise a competitive advantage and is treated as confidential. In order to be protected as a trade secret, the piece of information must meet the following criteria:



Known to only a limited group of people

Provides the owner enterprise with an economic or competitive advantage

Subject to sufficient protective measures to keep it secret

Subject to sufficient investment to develop the information

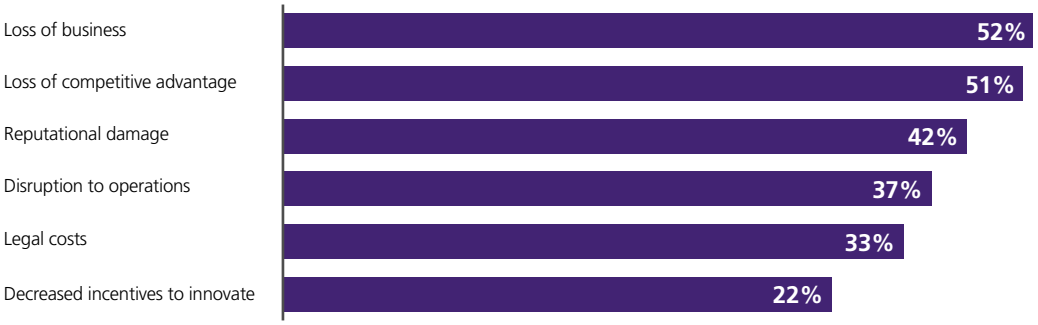
According to our survey, the three most valuable types of proprietary information held by organisations are customer databases (42%), product technology (40%), and research and development (R&D) information (23%).

Source: World Intellectual Property Organization (2020).

Corporate executives expect the risk of trade secret theft to rise in the next five years as firms increasingly store and share sensitive information across distributed workforces.[4] The covid-19 pandemic and associated changes to business continuity – from redundancies to remote working –are further driving organisations towards trade secret protection.[5] Companies have seen an uptick in unauthorised disclosure of company confidential information by employees, resulting in lost business, reduced competitive advantage and reputational damage. This increased threat has put trade secret protection on the agendas of both legal departments and C-suite decision-makers. Indeed, our survey finds that trade secret protection is seen as a top priority in the upmost reaches of business decision-making, with more than a third of board directors and C-suite respondents deeming it an "essential priority".

> "Trade secret protection is seen as a top priority the upmost reaches of business decision-making, with more than a third of board director and C-suite respondents deeming it an essential priority."

Figure 4.
Consequences of misappropriation
In your opinion, what would be the consequences of trade secret theft to your organisation? (% of responses)



Source: EIU Trade Secrets Survey (2021)

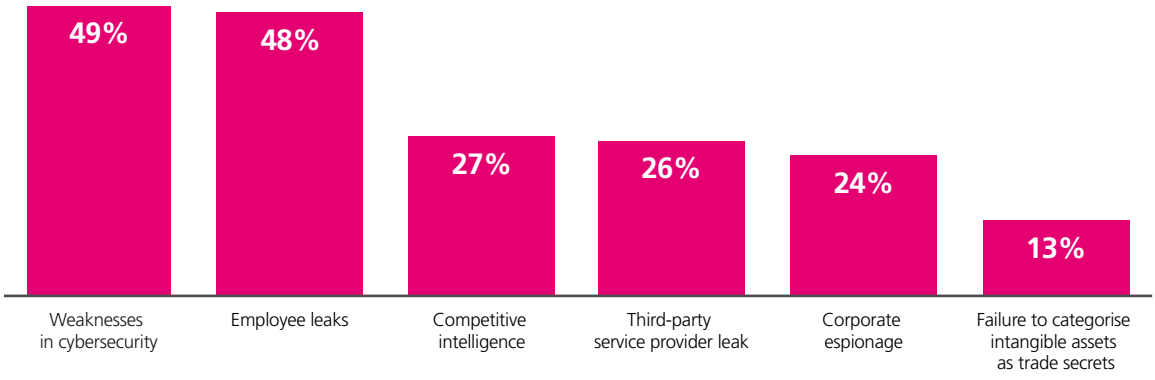
Looming threats

The vulnerability of trade secrets stems from legal and illegal, internal and external, and intentional and unintentional threats. Before companies can develop a toolkit of protective measures, they need to identify the most prominent concerns and threats.

Despite the growing importance of trade secrets to corporate value, companies often fail to formally recognise proprietary information as a trade secret – an important first step towards protecting that information.[6] In the event of theft and other disclosure, companies must be able to prove that the stolen information is accurately defined as a trade secret (see Figure 3) in order to be legally protected. According to our survey, a fifth of respondents cite difficulty in defining trade secrets as one of the biggest obstacles to safeguarding proprietary information. Difficulty in providing sufficient proof of misappropriation is the second highest ranked obstacle to trade secret protection.

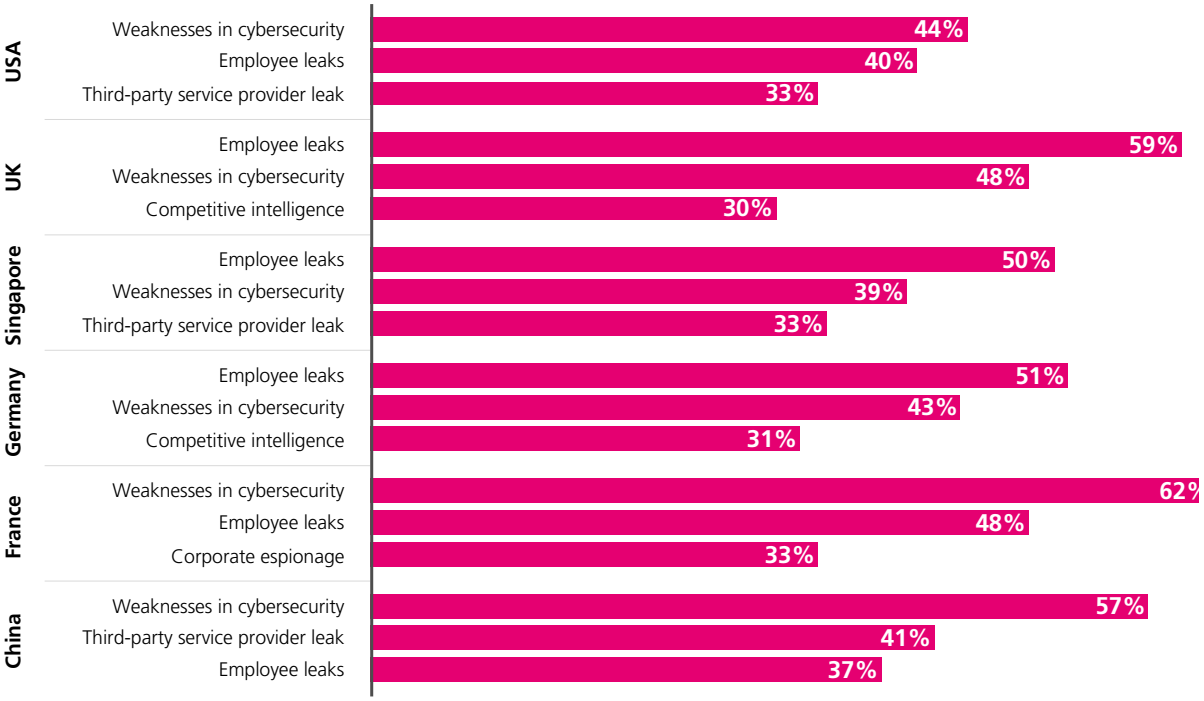
> Clearly identifying what you would call your 'crown jewels' is an exercise in and of itself. Not all data and information has the same value and defining the company 'crown jewels' is well worthwhile.
>
> ***Anil Cheriyan***
> *Executive Vice President, Strategy and Technology at Cognizant*

Figure 5.
Top threats to trade secrets
What do you regard to be the most significant threats to the security of your organisation's trade secrets? (% of responses)



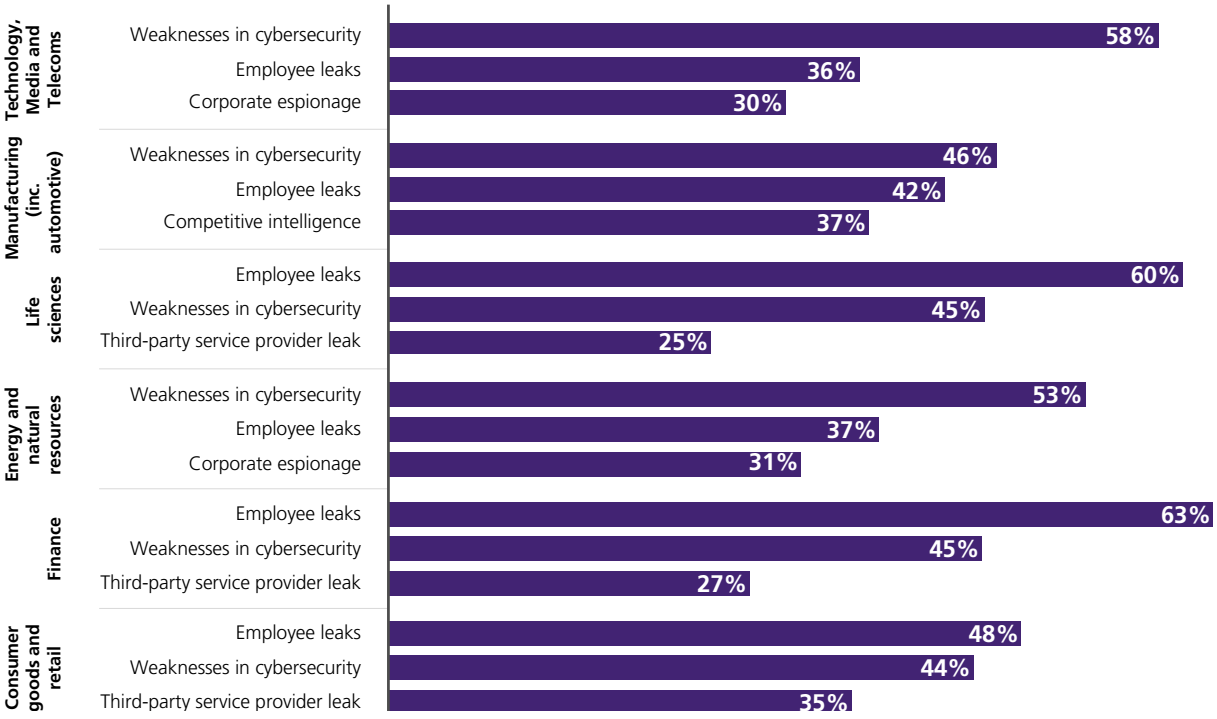
Source: EIU Trade Secrets Survey (2021)

Figure 6.
Top threats by country
What do you regard to be the most significant threats to the security of your organisation's trade secrets? (% of responses, by country)



Source: EIU Trade Secrets Survey (2021)

Figure 7.
Sector-level threats
What do you regard to be the most significant threats to the security of your organisation's trade secrets? (% of responses, by sector)



Source: EIU Trade Secrets Survey (2021)

Globally, cybersecurity and employee leaks are cited as the leading threats to companies' trade secrets. Third-party leaks are also a high priority for companies in the United States, Singapore and China, where a majority of respondents also believe that their organisations' contractual protections are not sufficient to protect trade secrets.

Cybersecurity concerns are top of mind for the energy and natural resources sector, the manufacturing sector, and the technology, media and telecommunications sector, while employee risks lead in the consumer goods and retail, finance and life sciences sectors.

> The worlds of trade secret theft and corporate 'bring your own device' policies are connected—this is possibly risky practice that has become a corporate norm.
>
> ***Professor Matt Marx***
> *Bruce F. Failing Sr. Professor of Entrepreneurship at Cornell University*

Cybersecurity: The leading concern

Valuable company assets are particularly vulnerable to cybercriminals who are able to hack computers and bypass security systems.[7] Executives are becoming aware of the potential threat of cybercrime to their assets, with almost half of respondents identifying cybersecurity weaknesses as the top threat.

Case study 1: ThyssenKrupp

Threat: External cyberattack

What happened?: In 2016, ThyssenKrupp, a German industrial conglomerate, revealed that it fell victim to a "massive" organised cyberattack in which hackers stole technical trade secrets.

Lesson learned: The company's senior leadership highlighted the importance of providing cybersecurity training, raising awareness about trade secrets and enhancing international co-operation to prevent such attacks in the future.

Ongoing digital transformation and the acceleration of remote working brought on by the pandemic have exacerbated cybersecurity challenges. As employers embrace flexible working models and employees work from home on personal devices and networks, it is increasingly difficult for companies to keep track of and secure the flow of data – including valuable proprietary information – across internal networks.[8] "The worlds of trade secret theft and corporate 'bring your own device' policies are connected," says Professor Matt Marx, professor of entrepreneurship at Cornell University. "This is a bad idea that has become a corporate norm." As companies increasingly bring external stakeholders into their digital ecosystems and use multiple cloud-based services, the risk of third-party breach also rises.

Employee leaks: An insider threat

Companies also need to take stock of their employees' role in exposing trade secrets. Just under half of the executives surveyed in this research regard employees as a critical source of leaks, whether intentional or not. In recent years the number of trade secret misappropriation cases linked to employment litigation has risen,[9] and in the United Kingdom one such case reached the Supreme Court (see Case study 2a)."

Case study 2a: MVF

Threat: Misappropriation by ex-employees

What happened?: In 2016, after years of dispute, the Supreme Court found that former employees of public health goods company MVF had misused confidential information about the company's insecticidal mosquito nets to produce a competing product under the name of Bestnet Europe Ltd.

Result: The case resulted in MVF being awarded damages for breach of confidentiality.[10]

Case study 2b: Google

Threat: Misappropriation by ex-employees

What happened?: One of the most notable cases of employee theft involved a former Google engineer, Anthony Levandowski, who unlawfully downloaded 14,000 files on self-driving cars from Google, only to use them in his next role at Uber.[11]

Result: Mr Levandowski was found guilty of trade secret theft and sentenced to 18 months in prison – an outcome that has been lauded as progress for trade secret legislation in the technology sector.[12]

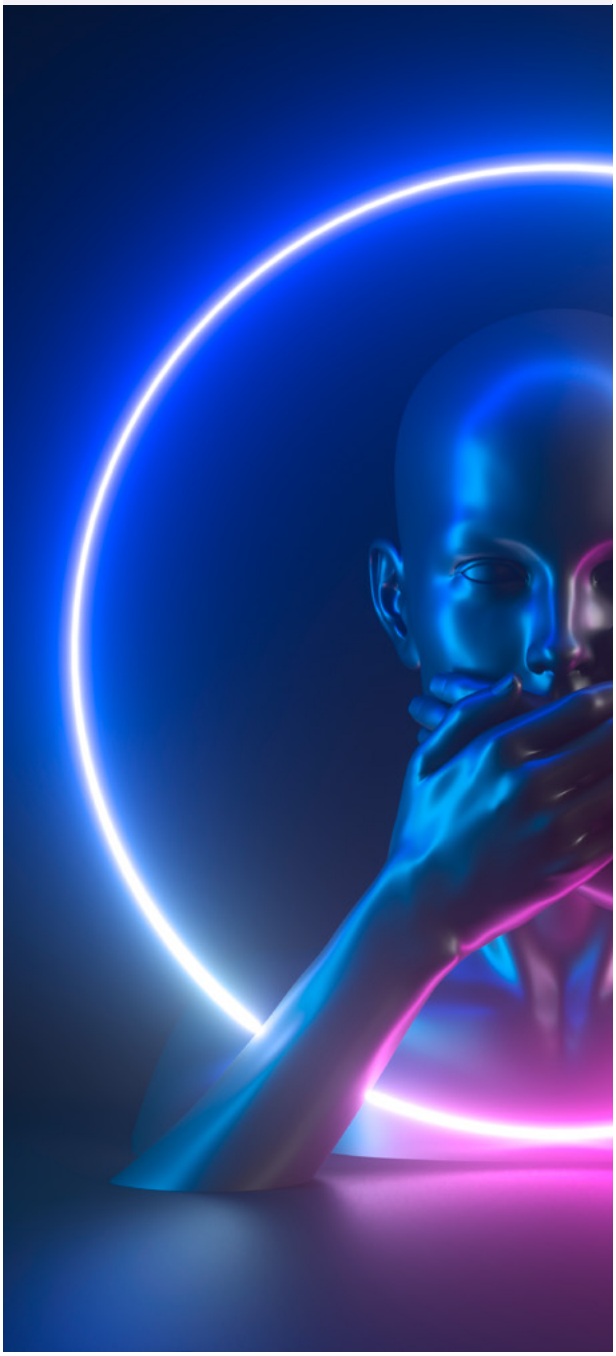
Lesson learned: Both of these cases highlight the importance of maintaining a culture of confidentiality among employees, especially those leaving the company.

As firms digitise, it has become easier for employees to accidentally or purposely access and expose confidential information, with or without external pressures. The normalisation of remote working will only increase this risk. Accidental exposure of employees' family members or housemates to confidential information, the use of unsupervised devices and overheard conversations can all result in confidential information leaks.[13]

The pandemic has also opened doors to a broader range of intentional employee threats[14] as layoffs, furloughs and redundancies increase the incidence of disgruntled employees. (For example, 55% of furloughed employees feel neglected by their employer.)[15] Laid-off and even furloughed employees are becoming more eager to spill secrets to competitors.[16]

"The biggest threats are often when employees leave, typically combined with a move to a competitor. Organisations need to create an environment in which their secrets are protected, by auditing and updating onboarding and offboarding processes, and by managing working practices and culture, especially remote working. Simple actions like deactivating access to cloud accounts are often overlooked, but can be critical."

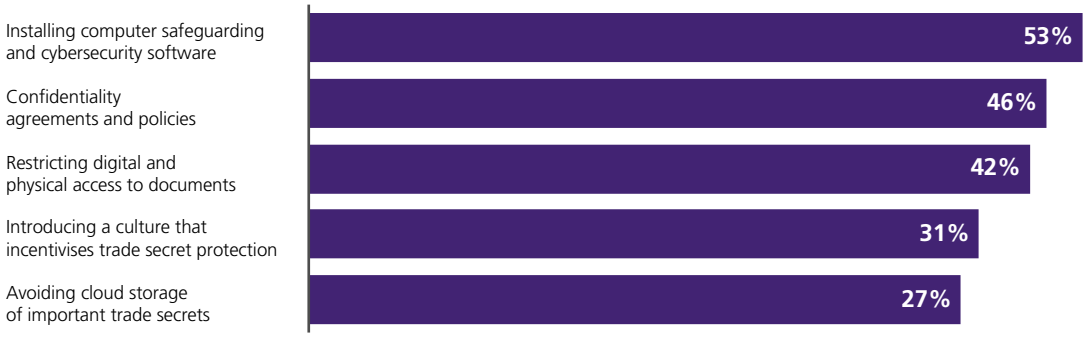
Hannah Netherton,
Partner, Employment Team, CMS



Safeguarding trade secrets

Figure 8.
The five key types of protective measures

Figure 9.
Protective measures at the top of the C-suite agenda
Which of the following practices would be most effective in preventing any of the potential threats to trade secrets? (% of responses)



Source: EIU Trade Secrets Survey (2021)

Enhancing cybersecurity efforts

More than four in five respondents identify cybersecurity as a vital component of their companies' successful trade secret protection strategy. Cybersecurity is regarded as particularly important by executives in industries where the costs of a data breach are high, including the finance, energy and natural resources, manufacturing, and technology, media and telecommunications sectors.[17]

Survey respondents rank basic cybersecurity measures such as digital watermarks and encryption of confidential materials as among the most effective measures firms can take to protect trade secrets, with one in five respondents ranking these as the most important measures overall.[18] Other cyber risk mitigation efforts to consider include providing sufficient training for all employees on cybersecurity best practices, planning incident-response scenarios and regularly revisiting the company's overall cybersecurity strategy.[19] Such measures are expected to remain at the top of executives' agendas. Indeed, one-fifth of all surveyed respondents' companies plan to roll out these measures over the next two years.

82%
of corporate executives agree that leveraging **technology** and **cybersecurity software** is key to their organisation's long-term success in protecting trade secret.

53%
of corporate executives believe leveraging **cybersecurity software** is the most effective countermeasure to trade secret theft.

Source: EIU Trade Secrets Survey (2021)

Employee regulation

Our survey finds that firms have, on the whole, already implemented key cybersecurity measures to shore up their trade secrets against threats from external actors. Looking ahead, however, firms are increasingly turning to measures to prevent threats from within. With employees posing a growing threat as a source of trade secret disclosure, company executives are increasingly focused on preventing threats from disgruntled or departing employees.[20]

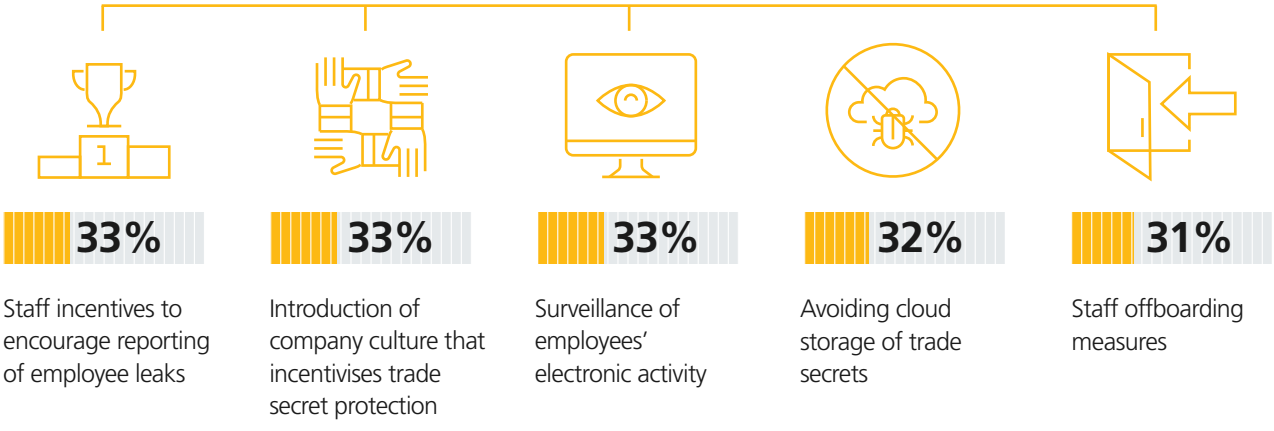
Importance of staff off-boarding measures

50%
Have already implemented these measures

31%
Plan to implement in the next two years

A third of the surveyed executives report plans to implement surveillance of employees' communications and electronic activity. Willingness to snoop is highest in China, Singapore and the United States. Respondents in Europe are less likelyto report such plans due to the complexities of balancing surveillance with the requirements of restrictive data protection regulations.[21] Employee surveillance is a top priority for executives in the technology, media and telecommunications sector, where 36% of respondents plan to implement surveillance over the next two years, reflecting growing tensions between employers and employees in the technology sector in recent years.[22]

Figure 10. Employees in the spotlight
Four of the top five measures that companies are planning to implement over the next two years focus on minimising employee leaks:



Source: EIU Trade Secrets Survey (2021)

Bolstering contracts and business procedures

A notable line of defence for businesses with trade secrets is strengthening policies and procedures to maintain confidentiality.[23] This is the second most effective countermeasure, according to 46% of survey respondents. Useful agreements range from non-disclosure agreements, work-for-hire, non-competition and non-solicitation obligations. However, while respondents recognise the effectiveness of these measures, over half also agree that their organisations' contractual protections to safeguard intangible assets are currently insufficient to protect their business, suggesting that more still needs to be done in this space.

> If you're a small company, or even a less reputable larger company, you may not have the power to enforce confidentiality. This depends on your kind of status as a company.

Professor Matt Marx
Bruce F. Failing Sr. Professor of Entrepreneurship at Cornell University

Case study 3: Kerry Ingredients

Threat: Lack of confidentiality agreements

What happened?: In 2016 the UK High Court ruled that the Bakkavor Group, a food supplier, improperly used confidential information that food company Kerry Ingredients had supplied regarding its trade secret (edible infused oils). Kerry Ingredients had shared this information to meet food safety and labelling requirements, but the Bakkavor Group used it to develop its own competing product.

Result: Kerry Ingredients was granted damages, legal costs and a time-limited injunction to prevent further use of this information by the Bakkavor Group.[24]

Lesson learned: This case underscores the importance of being able to prove the confidentiality of information in the event of trade secret theft.

"These confidentiality contracts are pretty standard, but where you see failure to do this is with smaller start-ups, especially at a very early stage," says Professor Matt Marx from Cornell University. This is evident in our survey findings, which reveal an almost 30% gap between small companies' and more established companies' implementation of confidentiality agreements and policies.[25] A common example is the case against Facebook by Tyler and Cameron Winklevoss, who argued that Facebook founder Mark Zuckerberg stole the idea of the social networking platform from them. Their argument fell short because they were unable to prove that they had taken reasonable steps to maintain confidentiality and ultimately could not prove that theft had occurred.[26]

"That 55% of people surveyed are limiting access to confidential documents suggests 45% are not. This is worrying. It seems nearly half are not putting in place routine practices to safeguard information. Improving legal protection through measures like document storage and restricting access to information is an achievable, non-costly thing companies can do to prevent the worst from happening."

Tom Scourfield, Co-Head, Intellectual Property Group, CMS

Restricting access to confidential information

A more obvious proactive strategy for safeguarding intangible assets is limiting access to confidential information. However, only 55% of the surveyed executives report that their firms currently employ this strategy. The more people who have access to confidential information, the higher the threat of theft. Despite this, 13% of executives' companies do not plan to implement such measures. Companies that are thinking about this are increasingly restricting physical and digital access to important documents, limiting access to "need-to-know" personnel or even destroying old information that is no longer needed.[27] If companies cannot limit access, they need to clearly communicate the importance of keeping certain information confidential through regular reminders, training and clear labelling of confidential material.[28]

55%

of corporate executives have already implemented measures to restrict digital and physical access to confidential information.

Source: EIU Trade Secrets Survey (2021)

Integrating trade secrets into company culture

Over ten years ago it was common for trade secret protection to be a matter for firms' legal teams, with the rest of the business kept out of the loop. This approach is evolving.[29] A third of the surveyed executives cite the introduction of a company-wide trade secret culture as one of the most effective measures to ensure trade secret protection. As part of this corporate culture, survey respondents (33%) are turning to employee incentives to push forward trade secret protection. This may include trade secret – specific measures, such as implementing a reward scheme for employees who identify new trade secrets or who raise concerns about gaps in security. It may also extend to broader measures designed to boost employee satisfaction, have a healthy "speak up, listen up" culture and minimise the incidence of disgruntled employees.[30]

33%

of corporate executives plan to introduce a company culture and values that incentivise trade secret protection.

Source: EIU Trade Secrets Survey (2021)

Each approach has a significant impact on safeguarding trade secrets but there are clear links between them. Companies that are looking to maximise legal protection in trade secret theft cases need to be able to prove that they have taken reasonable steps to protect their trade secrets, which will involve implementing a diverse combination of relevant elements of each approach to maximise resilience.[31] This will allow companies to cover any potential threat vectors – from the digital to the physical – while building proof that reasonable protective steps are being taken.

Looking to the future

As trade secrets gain importance, companies must take reasonable steps to understand the threats to their trade secrets and how to ward against them. However, companies must overcome significant hurdles in order to successfully safeguard their trade secrets.

Figure 11. Problems with protecting secrets
What are the biggest obstacles to safeguarding trade secrets? (% of responses)

Source: EIU Trade Secrets Survey (2021)

Our survey identifies a clear gap in cybersecurity expertise. This gap reflects a dearth of IT talent, but it also reflects poor adoption of cybersecurity best practices across organisations. It is more important than ever to stay ahead of the curve in terms of cybersecurity innovations, and to source the necessary skills to navigate and implement those innovations.[32]

> Cybersecurity is everyone in a company's responsibility. It is a team sport, and has real commercial business implications.
>
> ***Anil Cheriyan***
> *Executive Vice President, Strategy and Technology at Cognizant*

For a third of respondents, a further obstacle is a lack of experience and awareness of trade secrets. It is hard to protect trade secrets if employees are not aware of their value or sensitivity. This is a particular pain point for the energy and natural resources sector, the technology, media and telecommunications sector, and the manufacturing sector, three sectors that are particularly vulnerable to trade secret theft due to the high levels of innovation needed in their output.[33]

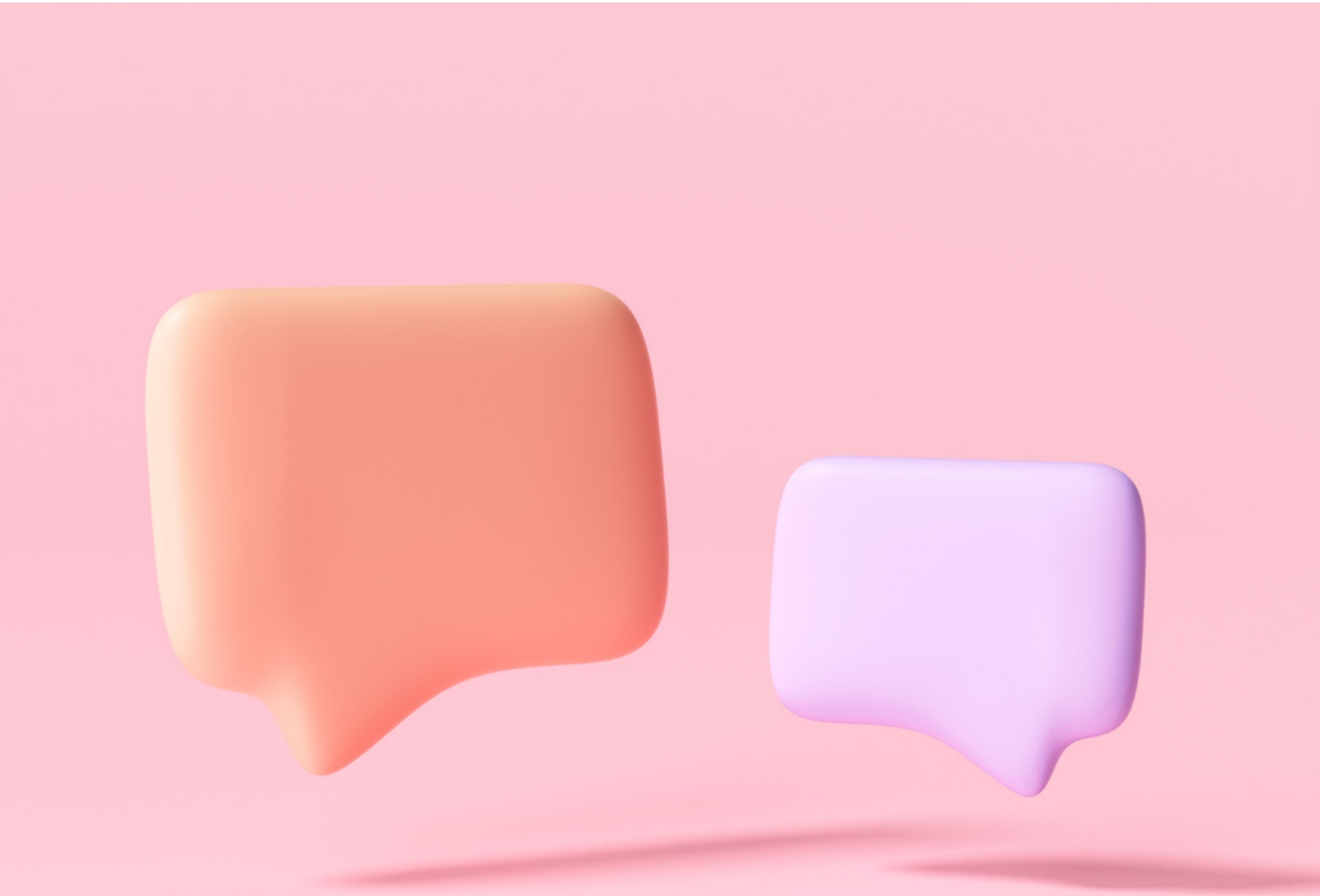
A third of survey respondents also report difficulty in supplying sufficient proof of trade secret misappropriation. To overcome this, companies can develop and implement a holistic trade secret strategy that enables them to properly classify, value and protect confidential and commercially valuable information.[34]

"We often see enterprises using off-the-shelf non-disclosure agreements (NDAs) but the Trade Secrets Directive makes it important to review and align NDAs to main agreements. While cybersecurity is important for electronic documents, physical versions must also be safeguarded –paperwork lying on a desk might not be considered a trade secret. The directive also requires entities to take 'reasonable steps' to protect trade secrets. This could mean that large companies would have to take more stringent measures."

Dirk Loycke, Co-Head, Commercial Group, CMS
Aukje Haan, Co-Head, Commercial Group, CMS

Leveraging the latest technology can be instrumental here for example, using blockchain to prove the existence and protection of secrets.[35] Another approach may involve seeding data to prove copying of databases.[36] Without such a strategy, protecting trade secrets may remain an uphill battle for many.

As companies navigate accelerated digitalisation, greater flexibility in working practices and fragile economic conditions in the post-covid-19 era, the threat of trade secret misappropriation is growing.[37] As our survey shows, the prioritisation of trade secrets is moving beyond legal departments, with corporate executives increasingly conscious of the threats posed by cyber risks and internal leaks. With these heightened threats comes a louder call to action for all levels of an organisation to take proactive measures to raise awareness around trade secrets, and take reasonable steps to ward off any risks to their crown jewels.



[1] https://www.wsj.com/articles/accountings-21st-century-challenge-how-to-value-intangible-assets-1458605126
[2] https://www.visualcapitalist.com/the-soaring-value-of-intangible-assets-in-the-sp-500/
[3] https://www.g4s.com/en-us/academy/our-views/articles/business-espionage
[4] http://www.rmmagazine.com/2019/06/01/the-reality-of-trade-secret-protection/; https://www.financierworldwide.com/trade-secret-theft-in-the-digital-age#.YHX-gxNKhQI
[5] https://blog.jipel.law.nyu.edu/2021/03/rethinking-trade-secrets-under-the-work-from-home-model/; https://www.ipwatchdog.com/2020/03/26/homework-keeping-trade-secrets-safe-working-remotely/id=120185/; https://hrdailyadvisor.blr.com/2021/04/06/5-ways-to-protect-trade-secrets-during-after-pandemic/; https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and-Impact.pdf
[6] https://www.csoonline.com/article/3268810/protecting-trade-secrets-technology-solutions-you-can-use.html
[7] https://gtr.ukri.org/projects?ref=EP%2FP005039%2F1#:~:text=Cyber%20criminals%20target%20valuable%20company,their%20value%20from%20their%20secrecy; https://www.sciencedirect.com/science/article/pii/S0167404819300616
[8] https://www.mckinsey.com/featured-insights/future-of-work/whats-next-for-remote-work-an-analysis-of-2000-tasks-800-jobs-and-nine-countries; https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time; https://www.forbes.com/sites/waynerash/2020/06/17/your-vpn-may-be-your-greatest-security-risk-during-covid-19/?sh=4bcc5d9231a6; https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact-cybersecurity.html
[9] https://www.stout.com/en/insights/report/trends-in-trade-secret-litigation-report-2020
[10] https://uk.practicallaw.thomsonreuters.com/8-629-6845?transitionType=Default&contextData=(sc.Default)&firstPage=true
[11] https://www.bbc.co.uk/news/world-us-canada-53659805
[12] https://www.forbes.com/sites/elanagross/2020/08/04/anthony-levandowski-sentenced-to-18-months-in-prison-for-stealing-trade-secrets-from-google/?sh=7464af3f2d01
[13] https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact-cybersecurity.html; https://www.weforum.org/agenda/2020/06/coronavirus-covid19-remote-working-office-employees-employers
[14] https://blog.jipel.law.nyu.edu/2021/03/rethinking-trade-secrets-under-the-work-from-home-model
[15] http://hrnews.co.uk/65-per-cent-of-uk-employees-feel-mistreated-by-their-employer-during-the-covid-19-crisis/
[16] https://blog.lighthouseglobal.com/prevent-ip-theft-during-a-covid-rif-dont-let-your-trade-secrets-depart-with-employees; https://news.un.org/en/story/2021/01/1082852
[17] https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[18] https://akki-greatlearning.medium.com/advanced-cyber-security-innovations-and-updates-for-2020-65b8d48fc256
[19] https://www.aon.com/getmedia/4f75d9d2-3876-4acd-8dff-2fa3b76918fc/Aon_C-suite_Cyber_Report.aspx; https://www.aon.com/unitedkingdom/insights/cyber-criminals-on-the-hunt-for-ip-riches.jsp; https://www.csgcybersecuritylaw.com/2018/10/protecting-trade-secrets-cyber-threats/
[20] https://blog.lighthouseglobal.com/prevent-ip-theft-during-a-covid-rif-dont-let-your-trade-secrets-depart-with-employees;
[21] https://edps.europa.eu/data-protection/data-protection/reference-library/private-use-electronic-communications-workplace_en; https://www.peoplemanagement.co.uk/experts/legal/gdpr-implications-monitoring-your-workforce#gref
[22] https://www.edelman.com/sites/g/files/aatuss191/files/2019-06/2019TrustBarometer_TrustInTechnology.pdf; https://www.edelman.com/insights/techlash-silicon-valley
[23] https://www.lexology.com/library/detail.aspx?g=0330e373-3f7e-4b38-9f63-d472baaf27b1
[24] https://www.jdsupra.com/legalnews/infused-oils-investment-managers-and-32880/
[25] Small companies are defined as those with annual revenue below $500m or less; larger companies are defined as those with annual revenue greater than $500m
[26] https://blog.kunvay.com/what-the-winklevoss-twins-can-teach-you-about-copyright-intellectual-property-so-you-dont-get-zuckerberged-facebook-uconnect/
[27] https://www.hoover.org/sites/default/files/corporatecybersecurityrealism.pdf
[28] http://www.rmmagazine.com/2019/06/01/sworn-to-secrecy/
[29] https://www.forbes.com/2010/02/19/protecting-trade-secrets-leadership-managing-halligan-haas.html?sh=522fbce81372; https://www.ipwatchdog.com/2020/01/03/four-things-c-suite-executives-need-to-know-about-patents/id=117516/
[30] https://www.lexology.com/library/detail.aspx?g=0330e373-3f7e-4b38-9f63-d472baaf27b1; https://www.workforce.com/uk/news/hr-takes-steps-to-protect-trade-secrets
[31] https://www.uschamber.com/co/start/startup/how-to-define-and-protect-trade-secrets
[32] https://akki-greatlearning.medium.com/advanced-cyber-security-innovations-and-updates-for-2020-65b8d48fc256
[33] https://s3-eu-central-1.amazonaws.com/evermade-fsecure-assets/wp-content/uploads/2019/04/15105531/F-Secure_energy_report.pdf; https://iiot-world.com/ics-security/cybersecurity/industrial-espionage-is-a-major-threat-to-the-manufacturing-sector/; https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and-Impact.pdf
[34] http://www.rmmagazine.com/2019/06/01/the-reality-of-trade-secret-protection/;
[35] https://www.bernstein.io/blockchain-and-trade-secrets
[36] https://www.itgroup-uk.com/news-insights/how-seeded-data-could-help-protect-your-intellectual-property/; https://www.dataiq.co.uk/articles/articles/seed-you-court
[37] https://www.natlawreview.com/article/trade-secret-seesaw-after-economy-goes-down-cases-go