PRIVACY BY COMPLIANCE

NAVEX GLOBAL®

RACONTEUR

Expert advice provided by

Jessica Wilburn
Data Privacy Officer and Senior Counsel
NAVEX Global
—
jwilburn@navexglobal.com

Shon Ramey
General Counsel
NAVEX Global
—
sramey@navexglobal.com

Carrie Penman
Chief Compliance Officer and
Senior Vice President
NAVEX Global
—
cpenman@navexglobal.com

PRIVACY: A LOOMING COMPLIANCE CRISIS OR POTENTIAL OPPORTUNITY?

A dynamic regulatory environment has elevated privacy and compliance to a C-suite concern, but should we be talking about more than just "risk"?

Steve Smith

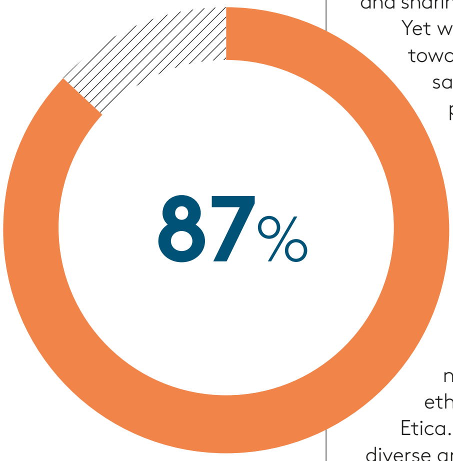
Vice President, EMEA & APAC
NAVEX Global

61%

of firms have reported one or more data incidents in 2018, up from 45 per cent in 2017

Hiscox, 2019

Respondents experiencing delays in their sales cycles due to customers' data privacy concerns



Cisco, 2019

The treasure trove of information available in today's data economy is unrivalled. By 2020, for instance, forecasts suggest that for every person on Earth, six gigabytes of data will be created every hour.

It's spawned new markets, business models and growth opportunities, fuelled by rapidly advancing technologies and a hyper-connected society. But with this power, as the saying goes, comes great responsibility.

Consumers are more aware than ever of the value, and inherent risk, in their personal information. How much they're giving away, what companies can do with it and the consequences of it being mismanaged. Get it wrong, and they have both the means and motivation to vote with their feet.

Meanwhile data breaches, cyber-risks and corporate manipulation have become headline news. Regulators have given legislation teeth and taken terms like GDPR from the back office to mainstream society.

This is being felt sharply in all corners of the business world, as executives grapple with the implications of growing consumer, media and regulatory scrutiny. "Despite a two to three-year runway towards GDPR implementation," cautions Michael Wiedmann, of counsel at international law firm Norton Rose Fulbright, "many organisations remain unprepared or even unaware of the extent and ramifications of their data collection, access and sharing practices."

Yet while much attention has been directed towards the fallout, too little has been said about the impact on compliance programmes, teams and their leaders.

Navigating compliance

With processes and governance designed for a different data era, compliance teams now face a barrage of new challenges and considerations they need to ask for their organisations.

"The GDPR directive is so broad," notes Vera Cherepanova, founder of ethics and compliance consultancy Studio Etica. "It finds its applications in so many diverse areas, many of which I'm sure regulators didn't intend or foresee."

Without doubt, stakeholder and regulatory expectations have elevated data privacy and governance to a cross-functional, strategic imperative that has clearly landed on the boardroom agenda.

But the prevailing narrative of risk, damage and downside shouldn't be our only focus. There's another side to this, an upside that's less about adding cost and complexity to business decisions. It's more about seeing the opportunity to help businesses to protect people, to make better choices and forge more productive relationships with customers, as well as instil trust, confidence and transparency among employees.

"This isn't about policy for policy's sake," says Andreas Klug, chief privacy officer at Ladbrokes Coral. "It's about embedding regulation at the heart of the business, providing essential protections for our relationship with our customers and positioning a business to succeed in today's data economy."

Simply reworking internal policy and process to comply with the minimum viable requirement of regulation misses the point. With compliance leaders placed into the spotlight they now have an opportunity to enact real change in their organisations, but they will need both the resource and leadership mandate to do so.

Privacy by compliance

Privacy is fast becoming a competitive advantage for some, but to achieve it needs compliance teams to engage with the relevant stakeholders and help drive the organisation's privacy strategy, so the required tools and training are in place.

This "privacy by compliance" model ensures the knowledge, skills and attitude will fit for a more ethical, privacy-oriented organisation.

Why is this important? So your employees can play their part in delivering a quality of service and experience to customers, helping to engender loyalty and differentiation. And to give them the confidence to speak up in the face of bad practice, harnessing the collective energy of your workforce to root out wrongdoing and mitigate organisational risk.

This puts compliance on the front foot and is an opportunity for the taking. ◆

PRIVACY DRIVING NEW PRIORITIES FOR COMPLIANCE LEADERS

Amid recent high-profile security breaches, increased regulation and rising client expectations, data protection has shot up the boardroom agenda

200bn

devices will need securing by 2020

Information Commissioner's Office (ICO), 2018

With financial, reputational and legal risks at stake, businesses are quickly learning to embrace a company-wide privacy and protection strategy.

A consequence of this shift is the evolution of the chief compliance officer (CCO), a role seemingly best placed to champion the issue at the forefront of business decisions. Given the complexity of the topic, especially considering how industry dependent the rules can be, this is no easy feat.

"Data privacy is a full-time job and a huge risk area," says Carrie Penman, CCO at NAVEX Global. "The sheer number of issues is new and it's definitely growing."

Working out the right approach to deal with this amplified number "requires more than one person as privacy officers on their own can feel like they're playing a game of whack-a-mole", she says.

Compliance redefined in the privacy age

For compliance teams, the introduction of data privacy as a key priority has meant the need to encompass IT, risk and even human resources when understanding how to build a culture of compliance adherence.

"If people are running fast and loose with data requirements, then that's going to involve HR to ensure we have appropriate accountability in place," says Ms Penman.

"There may be some organisations where the CCO is already an expert in data privacy, but I certainly wasn't expected to be the expert on everything."

When companies analyse what data privacy entails, it is clear there are a number of granular elements, including IT security, ethics and compliance.

> Data privacy is a full-time job and a huge risk area

"It's almost impossible for someone working within a large organisation to cover all the bases," Ms Penman explains. "The point is this particular area requires very specific expertise."

Instead, the demands of data protection for compliance teams has highlighted their importance of not necessarily providing direct solutions, but knowing enough about different areas of the business. They can then effectively reroute the issue to the most appropriate department.

Ms Penman describes the CCO as a lynchpin role that effectively joins up different parts of the organisation, all of which are dealing with data privacy. "It's really about having the ability to be a good partner with all the other departments, whether it's IT or HR," she says.

As requirements of effective compliance leadership go beyond understanding the technical or legal elements around new breaches, there is now a sharper focus on building relationships and sharing knowledge. "It's about all of us keeping each other informed," says Ms Penman, adding she'll often distribute articles she deems relevant to other teams.

Keeping up with evolving demands

So how are CCOs adapting to the new demands of their role? "I think most compliance officers stay in touch and attend a variety of conferences," says Ms Penman. "It's incredibly important to do a lot of reading; the first thing I do every morning is read, everything from *The Wall Street Journal*, law firm articles to compliance journals."

Where companies have appointed a designated data protection officer, he or she will tackle the fine detail of data protection procedures. The CCO, on the other hand, is expected to offer a more holistic and high-level perspective. It's a role of "co-ordination and oversight", explains Peter Swabey, policy and research director at ICSA: The Governance Institute.

While the shift has placed compliance teams in a more strategic and high-level position, the pace has also quickened. Ms Penman notes:

Enforcer of company ethics

Ethics and compliance are often grouped together, but as terms they are not interchangeable. The latter refers to abiding by the law, following rules or policies; the former means doing what is right, regardless of the law.

Given ethics is proactive and compliance is reactive, in practice businesses need both to embed an ethical culture. The reason that most compliance policies exist is because they enforce in a formalised procedure what is ultimately the right thing to do from a moral standpoint. Businesses should be protecting their customers, employees, suppliers not just because it's part of a legal contract, but because it is inherently ethical.

This is the message chief compliance officers are increasingly having to enforce from the top, educating the company on not just what the policies are, but why they exist in the first place.

"When Westinghouse asked me to become their organisation's chief ethics officer, I thought they dialled the wrong number," says Carrie Penman, now CCO at NAVEX Global. "I said, don't you want an attorney for this role? The general counsel said to me, I want somebody who can go out and talk to the people at the company."

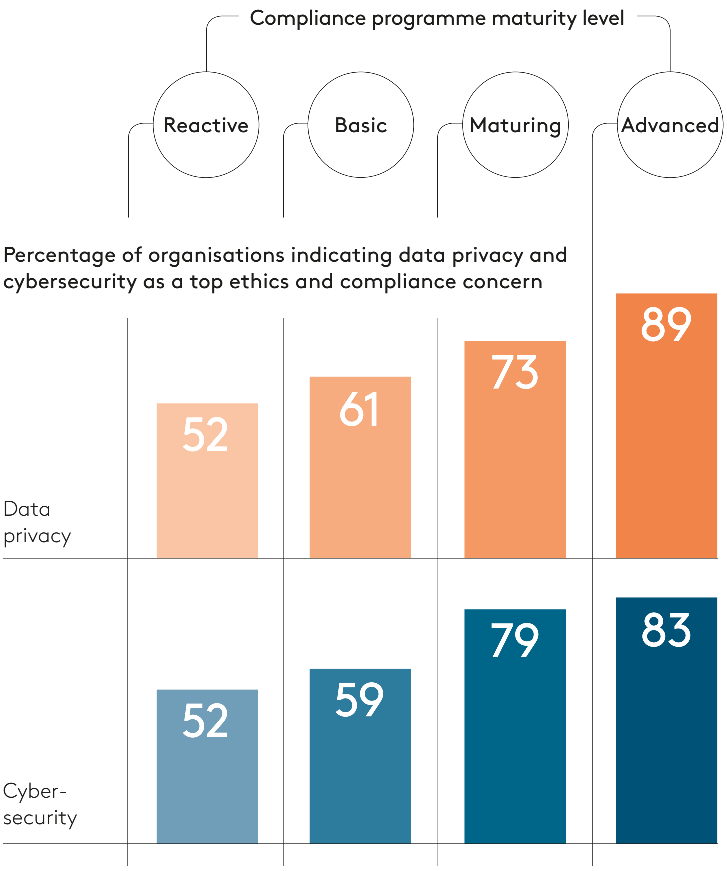
Jessica Wilburn, data privacy officer and senior counsel at NAVEX Global, adds: "Training is key as it brings things back to the fact that you're trying to protect people's data."

People can get lost in the regulations. Providing in-person and online refresher training helps to remove any ambiguity and confusion about what constitutes acceptable behaviour. It should provide clear examples of how to act in certain situations. For example, should staff discuss someone's medical history over email? This enables employees to start thinking about sharing information in an ethical and respectful manner.

"New alerts come out every day; you have to stay on top of what's being written and what's happening in other organisations."

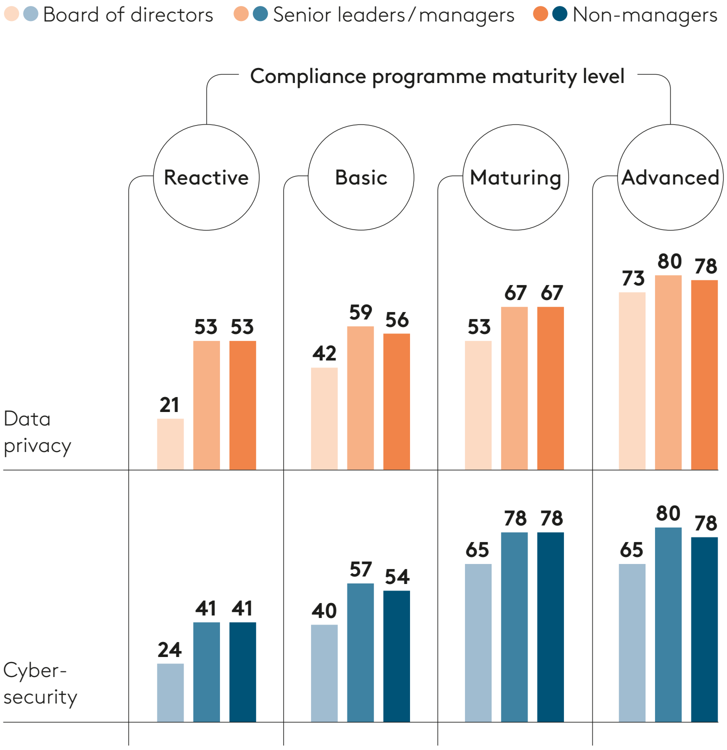
After all, businesses would much prefer to learn about a new type of attack that's happened elsewhere, rather than hearing of it for the first time at their own company. ◆

How does compliance programme maturity relate to engagement with data privacy/security



Percentage of organisations indicating data privacy and cybersecurity as a top ethics and compliance concern

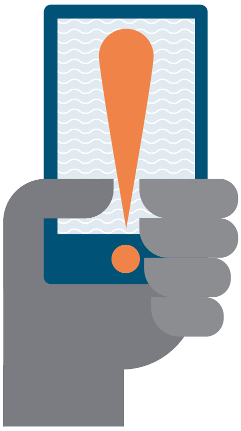
Percentage of organisations providing training on topic by audience



NAVEX Global, 2019

PRIVACY BY DESIGN: WHY COMPLIANCE SHOULD LEAD THE CHARGE

How should organisations manage people, embed processes and harness technology to increase transparency and mitigate data privacy risk?



4 of 5

top causes of data breaches are due to human or process error

Information Commissioner's Office (ICO), 2018

The concept of privacy by design has evolved far beyond its engineering origins. Data has become nothing short of a currency with which brands win or lose, and new business models have emerged. The regulatory environment in which firms operate, by way of response, has increased in both scope and complexity.

For businesses, these changes over the last decade present a two-sided coin. On the one hand, increased risk, cost and vulnerability. But on the other, the opportunity to increase corporate transparency, to forge stronger and more meaningful relationships with customers, and to provide a form of insurance for an organisation's growth ambitions.

Privacy by design can prevent businesses from falling foul of customer, employee, regulatory and societal expectations, and can go some way to reducing cost and complexity, rather than adding to it. But it calls for compliance leaders, as an organisation's most independent arbiters of standards, to take the mantle of nurturing an ethical approach to data. Not just settling for the bare minimum, but instilling an organisation-wide commitment to privacy as a first principle, in any organisational decision.

"Privacy by design too quickly becomes a conversation about GDPR or a marketing opt-in choice," says Adreas Klug, chief privacy officer at Ladbrokes Coral. "In reality, countries all around the world are creating laws that make collecting, managing and transferring data more difficult. This goes beyond communications choices to where you put your data centres and how you navigate increasingly complex regulatory burdens. Putting these ethical choices and responsibilities firmly at the top of the agenda of business leaders: that's true privacy by design."

It all starts with people

Arguably, revised company policies, internal communication and enhanced training alone are not a silver bullet for ethics and compliance professionals. But it's a good place to start. Raising internal awareness, comprehension and commitment to privacy can provide an essential foundation for improved data governance.

This begins at the top. Executive engagement is crucial to securing the mandate, resources and visible leadership that will send a signal to the wider workforce, as well as partners and vendors, that privacy is an organisational imperative, not a nice to have or afterthought.

"Boards are chiefly concerned with the 'three Rs': revenue, risk and reputation," says Shon Ramey, chief legal officer at NAVEX Global. "In the face of widespread consumer attention and a progressive regulatory environment, privacy ticks all three boxes. It's essential to start a conversation with leadership teams about the benefits of privacy in building customer and employee trust, as well as the reputational, commercial and financial risks of breach or misuse. Once this is understood, you're pushing at an open door."

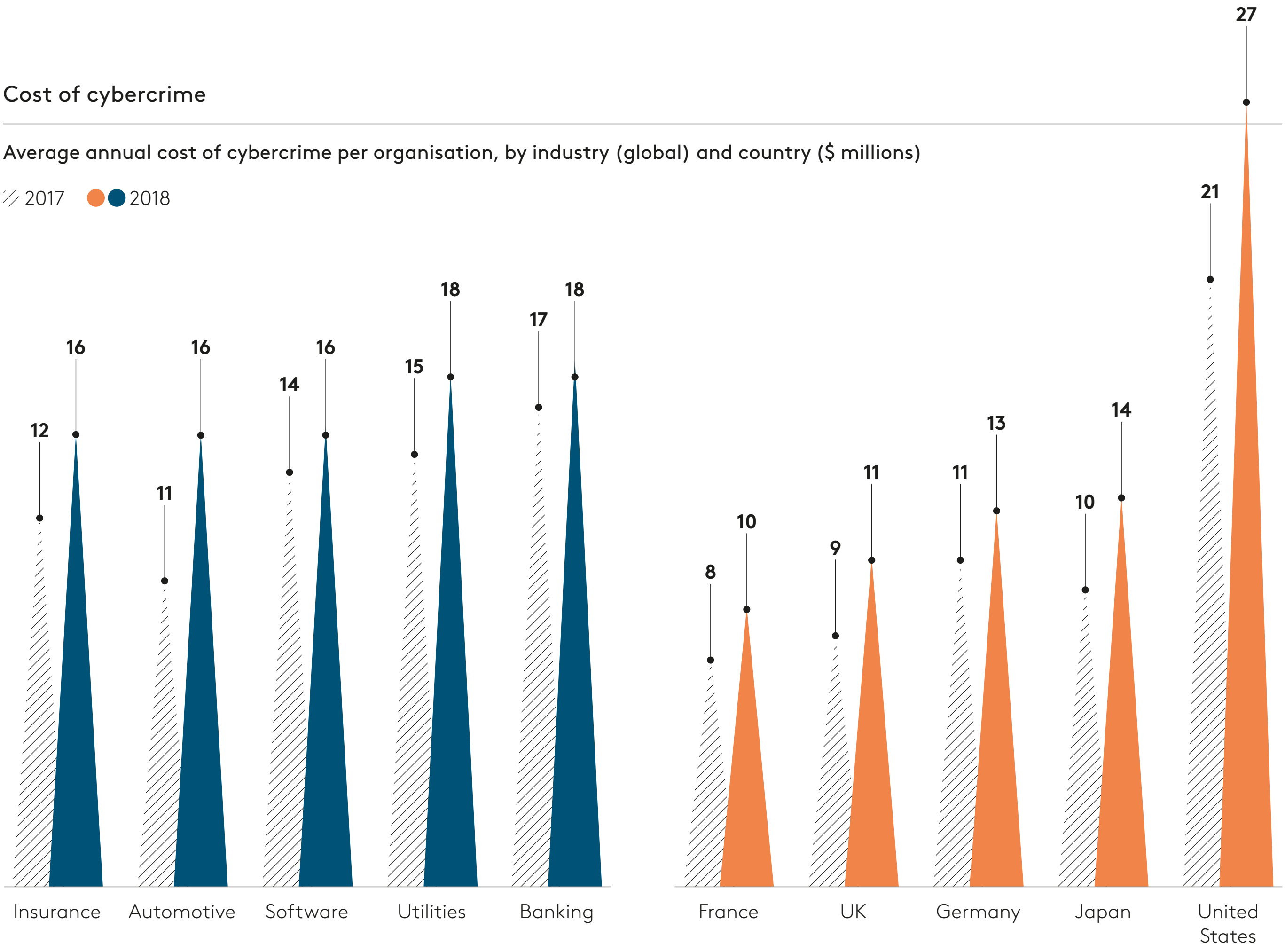
Jessica Wilburn, data privacy officer and senior counsel at NAVEX Global, adds: "Internal communication and education programmes are essential tools in supporting data governance and compliance. Yes, it's important to translate privacy into what it means for different departments, teams and roles, but it's even more impactful when we start the story with what this is really all about: protecting people."

Process gives structure

Communication and education provides a solid foundation, but they must also be translated into new ways of working, by providing a framework to guide employees on how to put policy into practice. And that first requires robust policies to be in place, which is a task not to be underestimated, given the myriad of instances in everyday working life that can lead to honest mistakes with unintended consequences. Given its scale, this challenge can seem overwhelming, but starting small is better than not starting at all, prioritising risks in a simple and actionable way.

Cost of cybercrime

Average annual cost of cybercrime per organisation, by industry (global) and country ($ millions)



Accenture, 2019

Embedding privacy by design and an ethical approach to data will involve different processes and nuances from one organisation to the next. But two common priorities emerge.

Firstly, analysing and evolving the countless organisational processes and decisions that involve customer or employee data must address both legacy and future data. "Initial audits will help ensure data capture, storage and access decisions are both legally compliant, as well as consistent with the ethical standards an organisation aspires to. But this then needs to be overlaid with appropriate governance and ongoing iteration, best done in partnership with compliance and legal teams, to ensure future data decisions meet the standards you're aiming for" adds Mr Ramey.

Secondly, collaboration is key. "Privacy and compliance professionals alone cannot hope to address the burden and opportunities presented by data. It requires a shift from being seen as a gatekeeper or final check and balance in decision-making, to playing the role of business partner" he concludes. Compliance leaders can help to actively shape decision-making processes and organisational choices, constantly reinforcing the ethical standards that will help individuals to do the right thing. This will encourage organisations to go beyond the regulatory requirements to gain agility and innovation from having the appropriate data controls in place, increase operational efficiencies, reduce delays to sales processes and achieve a real and valuable competitive advantage.

Only 16%

of CISOs say employees in their organisations are held accountable for cybersecurity

Accenture, 2019

Technology is only an enabler

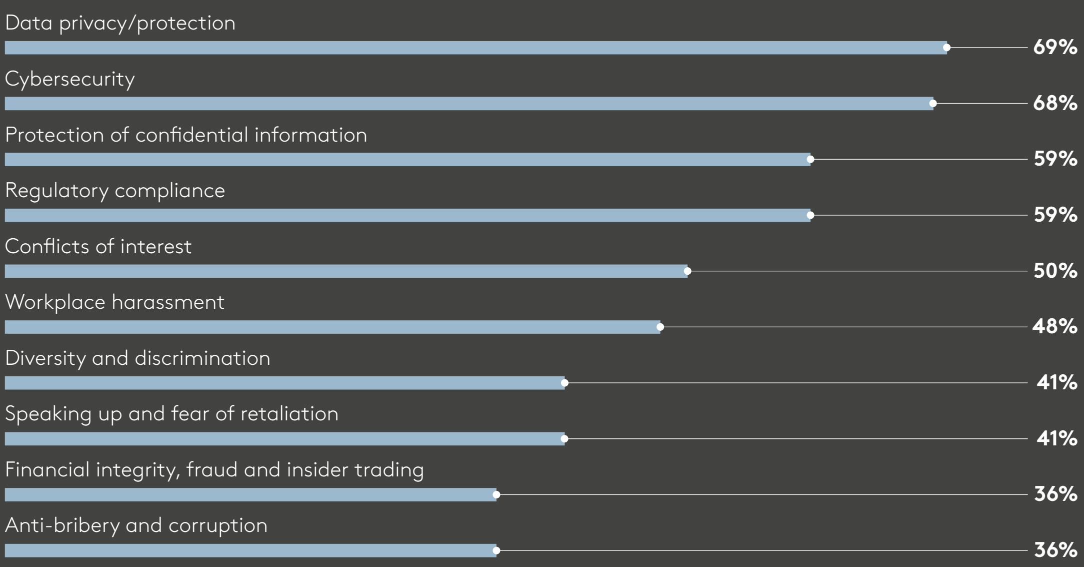
The final consideration is technology, but it carries a caveat. It would be easy to assume that smart systems can somehow liberate compliance professionals from the burdens of complex regulation, and that the promise of technology can automate or alleviate the heavy-lifting.

"If you look at most data breaches, beyond the bad actors lurking in dark corners of the web, it comes down to human error. The wrong thing being shared with the wrong party, even if for the right reason," says Simon Owens, data protection officer, Europe, at Chevron. "We're tackling privacy by design by systematically identifying these pinch-points where innocent mistakes can be made and either adapting or leveraging technology to eliminate or mitigate the risk."

Privacy is complex and nuanced. Compliance must establish the ethical foundations to ensure people consider the implications of their actions across the thousands of decisions that both employees and leadership make. It isn't an overnight endeavour. It requires a commitment for the long run, but with this comes greater protection for the organisation, as well as its customers, employees and stakeholders. ◆

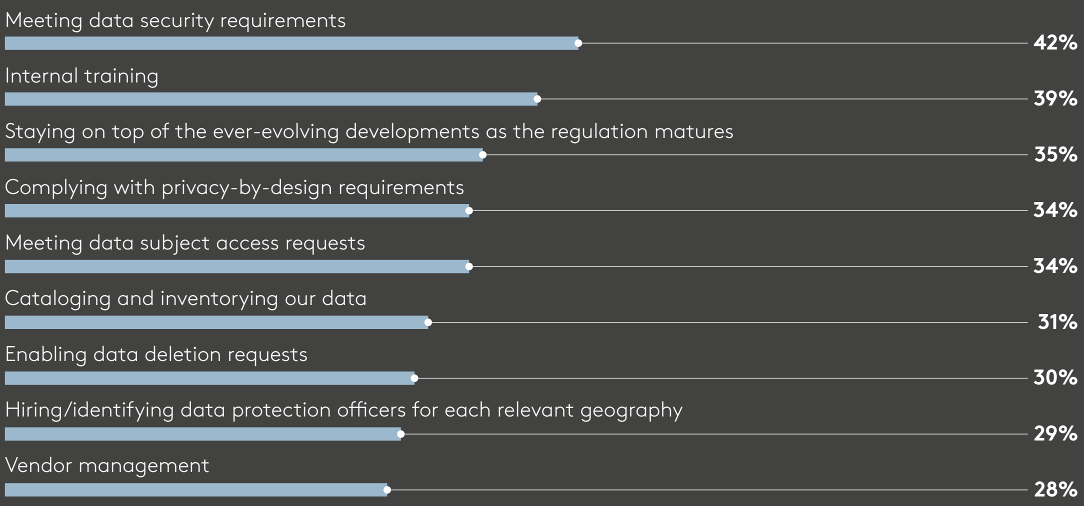
WHAT KEEPS CHIEF COMPLIANCE OFFICERS UP AT NIGHT?

Top ethics and compliance topics in organisations

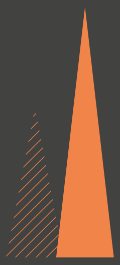


NAVEX Global, 2019

Most significant challenges in getting ready for GDPR



Cisco Data Privacy Benchmark Study, 2019



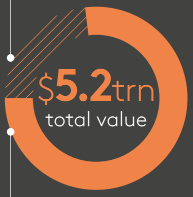
67%

increase in security breaches in the last five years

Accenture, 2019

Consolidated global value at risk from cybercrime over the next five years

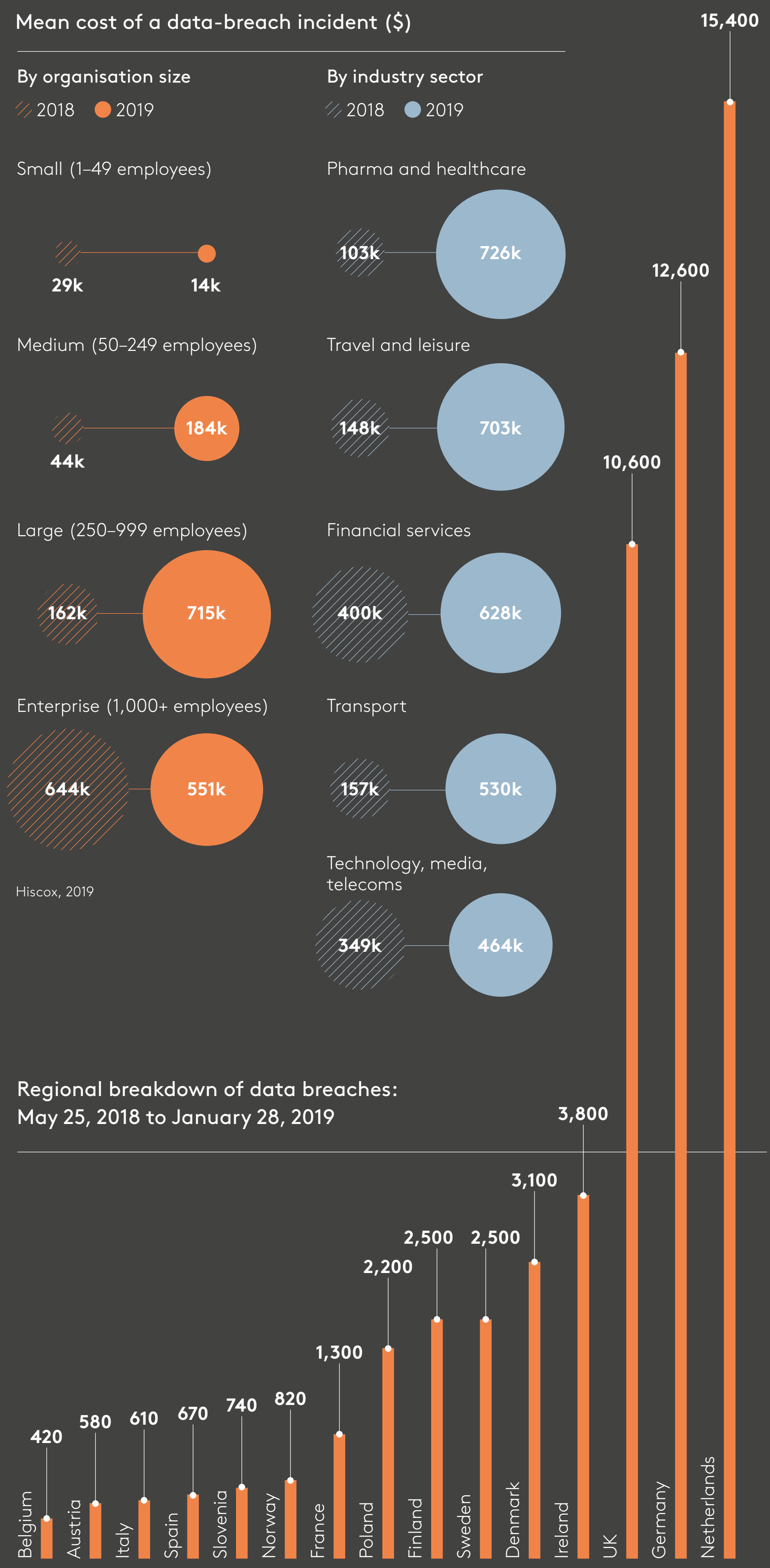
23%
value at risk from indirect attacks



77%
value at risk from direct attacks

Accenture, 2019

Mean cost of a data-breach incident ($)



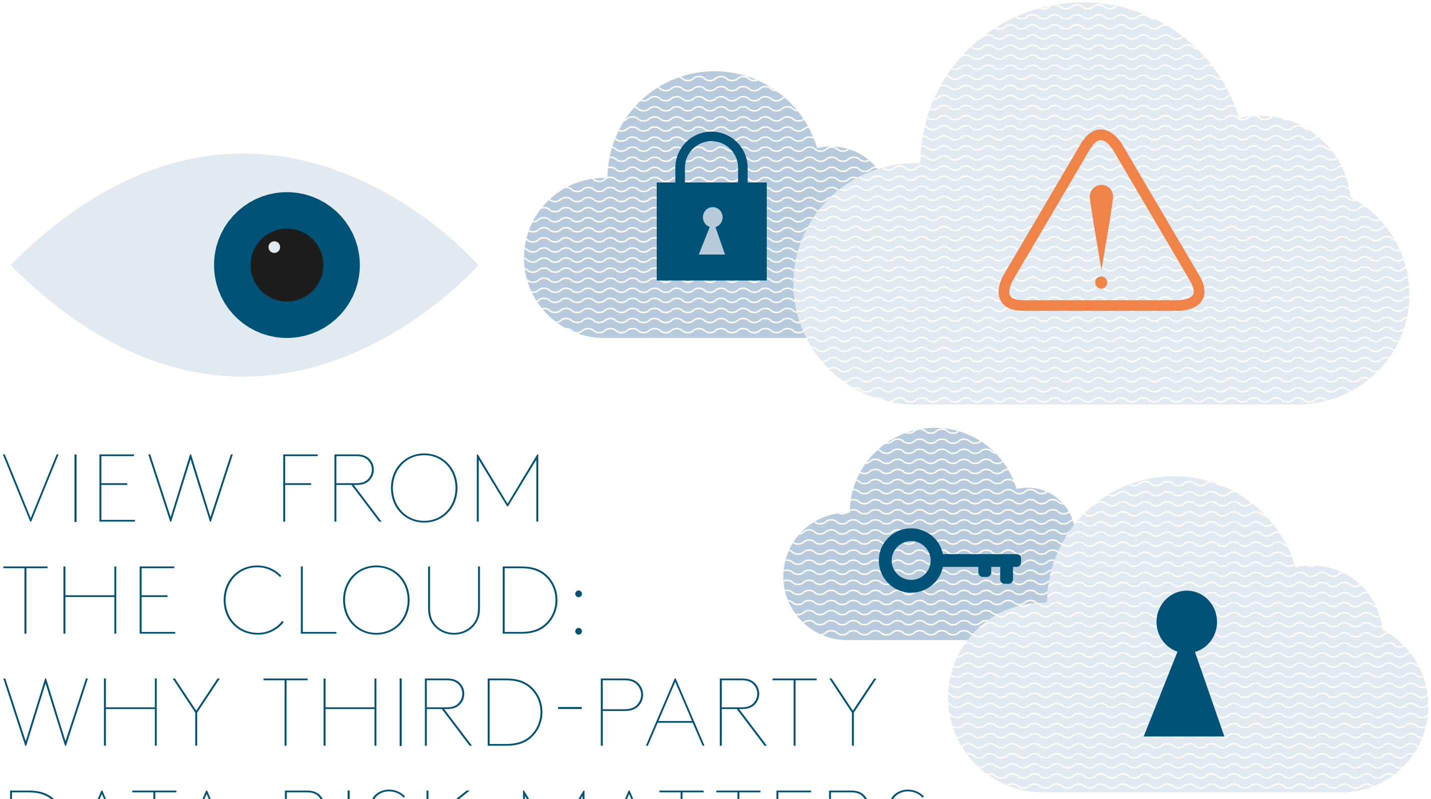
Hiscox, 2019

Regional breakdown of data breaches: May 25, 2018 to January 28, 2019

DLA Piper, 2019

What constitutes a good data privacy framework?

- ○ Clear data privacy strategy set by multiple stakeholders
- ○ Data privacy is reported and discussed regularly at board meetings
- ○ Dedicated data privacy officer and committee in place
- ○ Data privacy and cyber-awareness training for all employees including the board
- ○ Adequate cybersecurity budget
- ○ Regular security evaluation of supply chain and security KPIs included in supply contracts
- ○ Readiness to learn, respond and make changes after a data incident
- ○ Data privacy and cybersecurity included as part of the policy management programme



VIEW FROM THE CLOUD: WHY THIRD-PARTY DATA RISK MATTERS

Failing to ensure the security of data available to third-party suppliers can cost companies dear

“Third-party networks pose a massive threat to businesses. As more and more companies move to, and work with partners in the cloud, the lines between one company and the next are blurring,” says David Francis, information security consultant at KCOM.

Company supply chains have grown increasingly long and complex in recent years, spanning the globe, often in high-risk jurisdictions. This means there are now many more third parties in the value chain and the volume of digital connections and applications increases the opportunity for third parties to access companies’ data.

Yet many companies are delegating their responsibilities to organisations they know little about at the most fundamental level. Some companies don’t even know who their suppliers are, how many of them have access to their confidential data or how many suppliers they have, let alone what information of theirs they are handling.

There are three main areas to consider, according to Ben Lorica, chief data scientist at O’Reilly Media, a tech educational platform. “Firstly, a company might have some real exposure of their own data, due to their relationship with a third-party provider.

“Secondly, data supplied by third-party providers can be mission critical. Being cut off even temporarily can affect important products and services.

“Finally, there may also be instances where breaches involving a third-party provider will include press coverage of companies that might be exposed due to their usage of that service, and this can damage an organisation’s reputation and trust with the public.”

David Emm, principal security researcher at Kaspersky Lab, adds: “If external dependencies aren’t included in a company’s risk assessment, the supply chain could become the weakest link in their security.”

Nigel Ng, vice president, international, at RSA Security, highlights the example of a global entertainment company, where a recent security breach affected up to 40,000 UK customers because of malicious software on its third-party customer support product.

“Although the company itself wasn’t breached, it was still held accountable for the data that was compromised, and suffered a hit to its reputation and trust from consumers,” he says.

Verity Blair, director of third-party risk at NAVEX Global, comments: “Protecting your organisation against reputational exposure from your third parties is as big a risk for data governance as it is with more recognised third-party risks such as bribery and corruption.

“The public don’t make the distinction that it is the third party at fault; it is you they entrusted their data to.”

Strategising for risk

When it comes to building a risk strategy, the

65%

of firms say they had experienced one or more cyberattacks as a result of a weak link in their supply chain over the past year

Cyber Readiness Report 2019, Hiscox

first step is to conduct a risk assessment to identify all your partners and the risks they pose, says John Sheehy, vice president of strategy at ethical hackers IOActive.

Only 20 per cent of respondents to a survey for the Ponemon Institute, *Data Risk in the Third-Party Ecosystem*, say their companies know how their information is being accessed or processed by vendors with whom they have no direct relationship.

So being able to identify which risks are relevant to your company and to control that screening process effectively would be a huge leap forward for many organisations, says Ms Blair.

It is crucial senior management are involved right from the start of the process, says Professor Kevin Curran, senior Institute of Electrical and Electronics Engineers member and professor of cybersecurity at Ulster University. "The process should begin with due diligence where each company's chief security officers or chief technology officers are involved in agreeing the protection, access and allowable sharing of the data."

> "The public don't make the distinction that it is the third party at fault; it is you they entrusted their data to

The initiative needs to be spearheaded by the chief executive or executive team, adds Dr Guy Bunker, chief technology officer at cybersecurity provider Clearswift, so the third party knows security is being taken seriously.

The compliance team is central to getting on top of this issue. But the Ponemon Institute survey shows that in 21 per cent of companies, there is no clear accountability for the correct handling of third-party risk management. Just 12 per cent of those questioned say their general counsel or compliance department managed third-party risks, and 8 per cent say the compliance department is responsible for ensuring privacy and security language is included in all contracts with third parties.

Some 63 per cent of respondents say they did not have a comprehensive inventory of their third-party vendors because of a lack of centralised control over third-party relationships, while half say it is not a priority. Almost as many (44 per cent) say they lack the resources to track third parties, 41 per cent say the relationships are just too complex and 37 per cent say they cannot keep track of third parties because of the speed of turnover in third-party relationships.

To reduce the data risks posed by partners, it is clear that many companies need to strengthen their third-party compliance and internal controls. ◆

Clarifying confusion around third-party strategy

There can be numerous barriers to building a robust strategy towards third-party risks, the most basic of which is a lack of understanding around the risks involved.

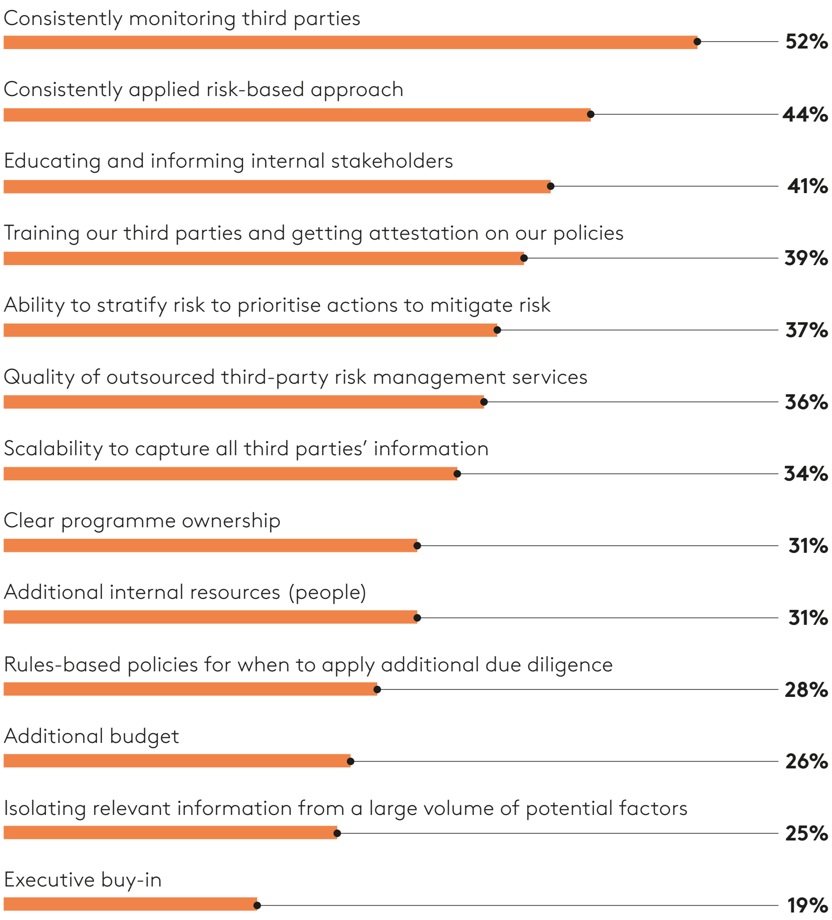
Andrew Martin, chief executive of DynaRisk, says: "There is a real lack of knowledge about cybersecurity. Crimes are evolving and becoming more sophisticated and people are still failing to spot even basic phishing scams. Companies need to do more to raise awareness among employees and empower them by giving them the tools they need to protect themselves as well as the wider business."

David Emm at Kaspersky Lab agrees. "The greatest barrier in the C-suite's way of building a robust strategy towards third-party risks is a lack of recognition of the problem itself," he says.

"It is easy to focus on things that are under the direct control of the company and overlook the dangers of third parties or for businesses to think that it won't impact them. The first step is to understand the potential issues posed by the supply chain."

A further problem is the risks are always evolving, so even if you have done due diligence, audited suppliers and trained staff on the risks, the dangers are different a few months down the line.

Top factors for improvement in relation to risk management programme



NAVEX Global, 2019

WHISTLEBLOWING INVESTIGATIONS: WHERE'S THE PRIVACY RED LINE?

Internal investigations can make or break employee and wider stakeholder trust, so how do businesses strike the right balance between transparency and confidentiality?

The notion of privacy in internal investigations and whistleblowing is as much a concern for employees as for compliance, human resources and legal professionals.

However, the ripple effects of recent and emerging regulations, such as GDPR and the EU Whistleblower Protection Directive are posing fresh dilemmas about privacy and the rights afforded to all parties involved.

"We no longer have a handful of regulators that may scrutinise our data privacy behaviours," says Rose Chapman, global head of compliance and ethics and deputy data protection officer at Travelport. "Each one of our employees and each one of our customers has effectively become a regulator. We now have thousands of people who can ask detailed questions at any time, all holding rights."

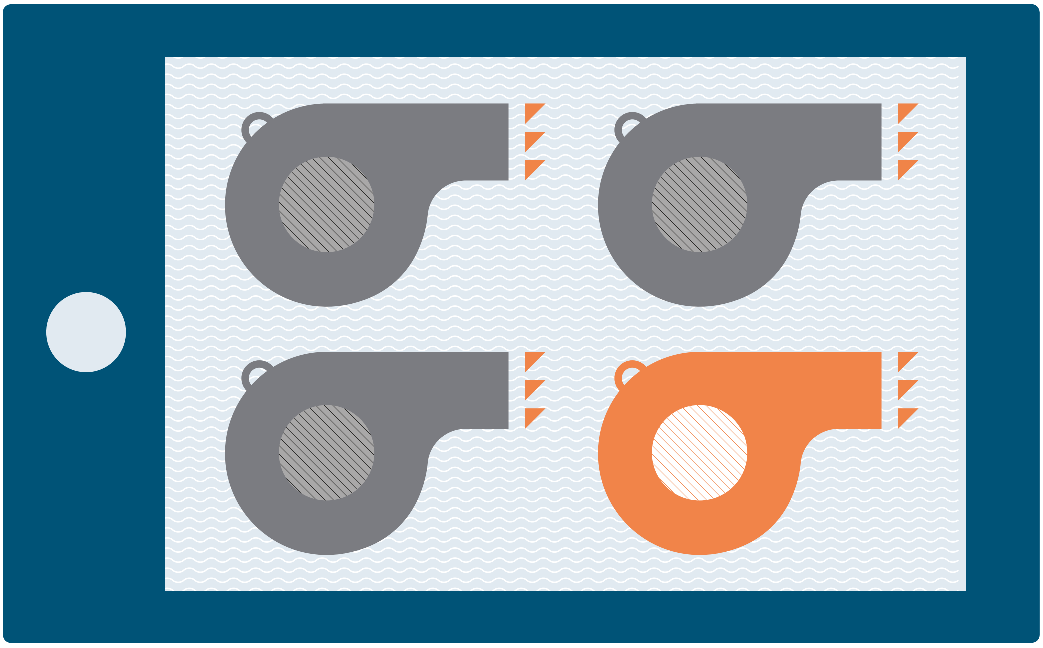
With regulatory, media and public interest heightening, the use of non-disclosure agreements, or NDAs, and confidentiality agreements are under the spotlight. The advent and widespread adoption of social media has shown that official entities, governments or individuals can truly and visibly be held to account, creating greater expectations and a growing sense of empowerment among employees.

"Complaints and whistleblowing are no longer dirty words," says Ed Mills, partner and head of employment at Travers Smith. "It's all about risk and not just reputational. Organisations are in a drive for disclosure; if problems exist, they want to be on the front foot and in a position to manage the issue, rather than it manage them."

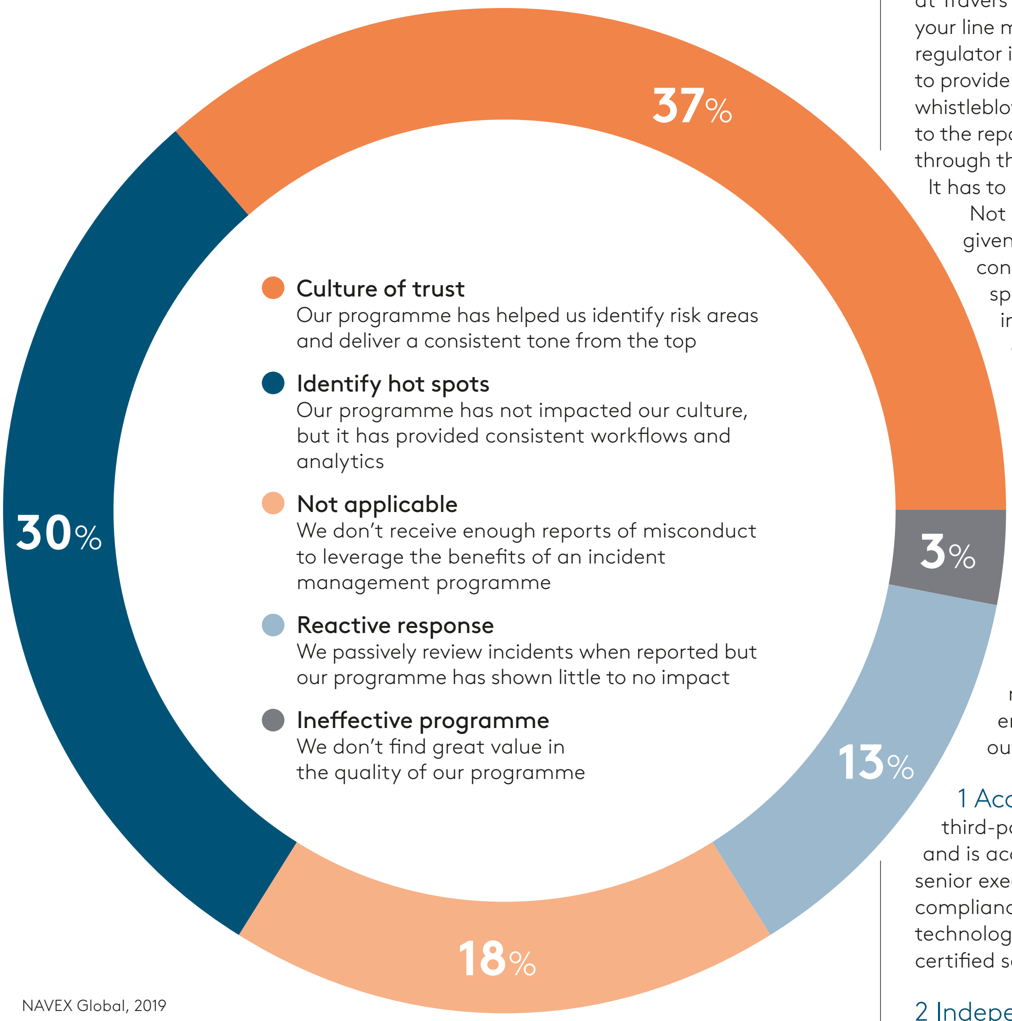
24%

rise in whistleblowing complaints to the Financial Conduct Authority (2017-18)

Financial Times, 2019



Impact of hotline/incident management programmes on organisations

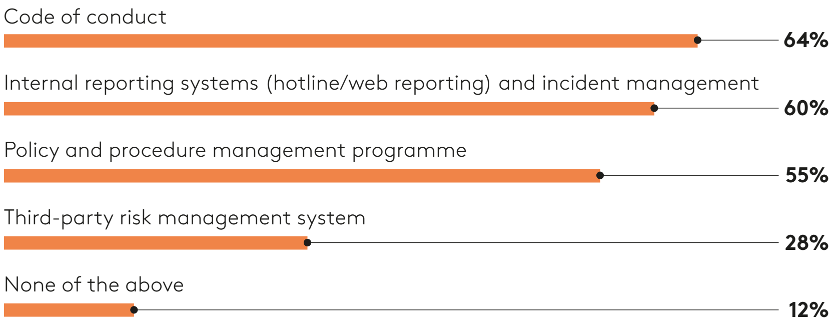


NAVEX Global, 2019

65% find ethical and compliance training programmes helpful in preventing ethical violations

NAVEX Global, 2019

Elements of ethics and compliance programmes that helped prevent ethical violations



NAVEX Global, 2019

Encouraging disclosure

Anna West, professional support lawyer at Travers Smith, adds: "A choice between your line manager, HR or, as a last resort, a regulator is insufficient. Organisations need to provide multiple routes for complaints and whistleblowing that prioritise what's important to the reporting employee, whether internally or through third parties, anonymously or otherwise. It has to be on their terms."

Not only do employees need to be given a choice of how they report their concerns, they also have to trust that the speak-up process has the safeguards in place to manage their information appropriately.

"It's critical to keep the circle tight," says Ms Chapman. "People won't come forward if they don't feel confident they will be protected, whether they are seeking anonymity or whether they fear retaliation. It's essential to choose your team carefully, and to restrict knowledge and access only to those who can be trusted to maintain an investigation's integrity."

Making confidentiality a reality, not just a promise, is a multifaceted endeavour, but four factors stand out most.

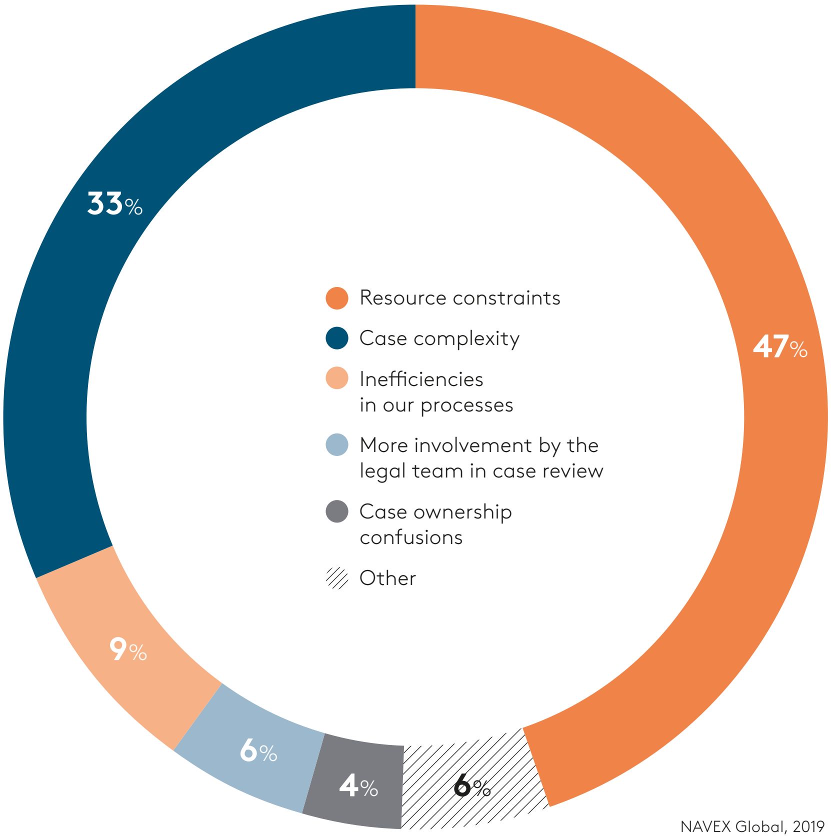
1 Accountability Ensuring any external third-party whistleblowing provider "lines in" and is accountable to the most appropriate senior executive role, typically in legal or compliance. Access to information, and any technology used, must be regulated with certified safeguards and permissions in place.

2 Independence Ensuring leaders in compliance, legal and HR have the formal mandate and authority to act on concerns and complaints without oversight from the board or chief executive, which could present a conflict of interest or discourage employees from speaking up.

3 Involvement Ensuring knowledge of a complaint, its origins and details, and the investigation process itself, is limited only to the essential minimum of internal and external individuals, to enable it to be conducted comprehensively and effectively, without compromising its integrity.

4 Process Ensuring what happens when an employee makes a complaint anonymously or otherwise, how investigations are conducted and the rights of all parties involved, and the potential outcomes following investigations are clearly articulated across the organisation in terms that can be understood and incorporated into management training.

Confidentiality in investigations carries both risks and benefits. On the one hand, investigators need to avoid prejudice, prevent leaks, protect reporting parties and witnesses, Greatest impact on the time it takes to investigate and close a report



NAVEX Global, 2019

and avoid unintended reputational damage by association. In each of these instances, it may seem favourable to restrict specific details of an investigation, limit who is made aware or the extent to which conclusions are reported.

On the other hand, each of these steps, even if made for the right reason, carries risk. Pursuing confidentiality to an extreme can lead to investigations failing to reach the right conclusions or coming across as a fishing exercise to the subject of the concerns or complaints. Controlling awareness of an investigation or its conclusions could be seen as counter to openness and transparency, and lead to accusations of denying, or attempting to bury, the problem.

Protecting reporting parties and allaying fears of retaliation, especially when it comes to small teams, can benefit from more robust whistleblowing policies and processes.

"You've got to have good governance structures in the first place," says Ms Chapman. "A whistleblower doesn't have to be the catalyst for an investigation; they can simply flag up where you need to look, but you need the processes and audits in place to start with.

"A complaint about the misuse of an expense account, for example, could be picked up in the next regular expenses audit rather than associated with a whistleblowing report – but you need that governance infrastructure in place. It's a hard slog, but it goes a long way to supporting confidentiality and is well worth the effort."

Good governance occurs when the privacy of all parties associated with complaints or whistleblowing is protected in accordance with both regulatory and ethical obligations. But true respect is only created when transparency and openness are cultivated and promoted within a business.

Organisations must demonstrate that problems are acknowledged when they arise; that complaint procedures are taken seriously and acted upon and, when conclusions are reached, they are followed through to both the spirit and the letter of their policies and, where relevant, the law. Transparency is fundamental in creating a culture of trust with your employees. ◆

> Each one of our employees and each one of our customers has effectively become a regulator

Speaking up: risk or reward?

Blowing the whistle has consequences, typically giving rise to a number of questions for employees considering taking such a step.

How should I report my concerns or complaint?

Context is key: who the complaint relates to; their seniority, influence and standing in the company; the severity of the accusation; the potential consequences if upheld; and the relationship between the reporting party and others involved. Whether to use an internal system, turn to an external body or simply not pursue a complaint all comes down to confidence in the whistleblowing process the organisation has adopted.

Should I remain anonymous?

Whistleblowers typically face two considerations: am I putting myself at risk of negative consequence if I'm named in a complaint; and will my anonymity mean any investigation is either taken less seriously or is less likely to reach the outcome I'm hoping for?

Can I know about the outcome?

Whistleblowers want a sense of closure and, if nothing else, they want to be kept informed and regularly updated during the investigation. Providing some details of the outcome, even if restricted in nature, will ensure that life after making a report is not a forgotten one.

NAVEX GLOBAL®

RACONTEUR