



in association with
 IDG
CONNECT

SPECIAL REPORT

MIXED STATE OF READINESS FOR NEW CYBERSECURITY REGULATIONS IN EUROPE

French, German and UK organisations need more clarity on compliance requirements for 2015-2017

Survey conducted by IDG Connect on behalf of FireEye

Role: Decision Maker

Segment: European Organisations

Orientation: General Education

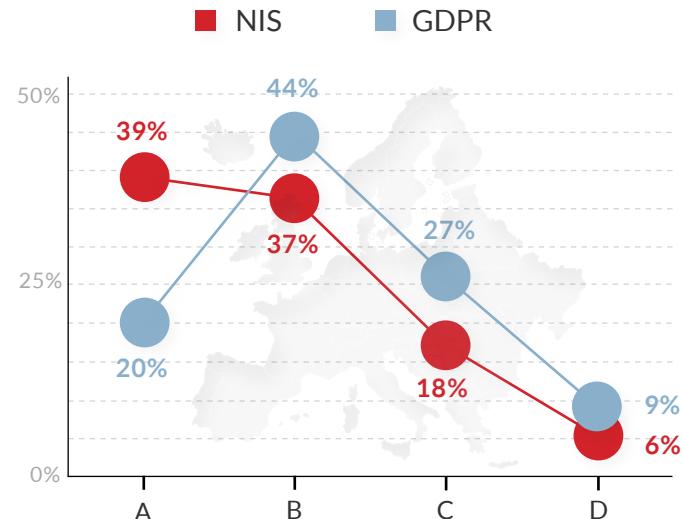
Region: UK, France, Germany

SECURITY
REIMAGINED

2.

EXECUTIVE SUMMARY

Organisations Better Prepared for NIS than GDPR



A - All Required Measures are in Place

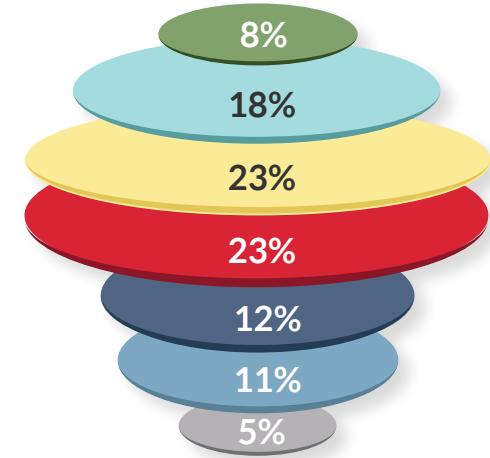
B - Most Required Measures are in Place

C - Some Required Measures are in Place

D - No Required Measures are in Place

The majority of those in France, Germany and the UK still have work to do in implementing sufficient security measures to meet new requirements mandated by new EU Networking and Information Security (NIS) and General Data Protection Regulation (GDPR) which will come into force in the next two to three years.

Cost and Complexity Remain Significant Challenges



- Incident Reporting Process Requirements
- Policy Complexity
- Implementation Costs
- New Hardware/Software Investment Requirements
- Sourcing Sufficient Expertise
- Pre-enforcement Confirmation of Systems, Processes and Policies
- Incident Reporting Timeframe Requirements

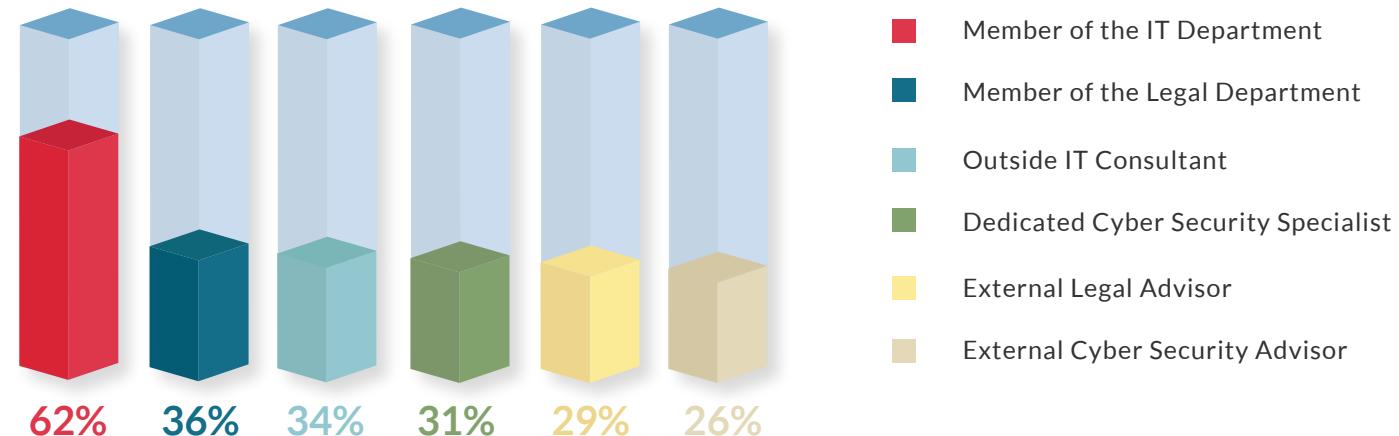
Investment in new hardware and software to support NIS/GDPR compliance initiatives is seen as the biggest challenge to IT departments, closely followed by implementation costs and more complex security policies.

2a.

EXECUTIVE SUMMARY



Responsibility for NIS/GDPR Planning



In-house IT departments are widely expected to bear the brunt of responsibility for assessing NIS/GDPR compliance requirements and formulating appropriate policies and reporting frameworks.

3.

INTRODUCTION

New European Community (EC) laws governing data protection set to be implemented in the next two to three years will have a fundamental impact on the way that most organisations in European Union (EU) member states implement security policies and report breaches. The Network and Information Security (NIS) 'cybersecurity' directive is set to be finalized in 2015 depending on how long it takes for the EU Council and Parliament to agree on a final version. Member States will then need to immediately begin preparing for compliance and complete implementation by approximately the end of 2017. In addition, there is a separate plan to unify existing data protection regulations in force within the different EU countries under a single law – the General Data Protection Regulation (GDPR) – currently set to be finalised in early 2015, compliance with which will become mandatory in 2017.

When finalised, the NIS Directive will impose new security and incident reporting requirements on a broader range of private sector companies. It will demand that 'operators of critical infrastructures' or 'critical national infrastructure (CNI) market operators - which include those working in the energy, financial services, health and transport sectors, alongside public sector bodies - adopt appropriate steps to manage security risks and report serious incidents to a national competent authority, such as a computer emergency response team

(CERT) which will represent a 'single point of contact' if not necessarily the only competent authority in each member state.

The original framework proposed extending these security and reporting requirements to 'key providers of information society services' (app stores, cloud service providers, e-commerce platforms, Internet payment gateways, search engines and social networks, for example). This idea has since been put on hold following objections from various industry groups and after the European Parliament deemed it 'disproportionate and unmanageable' although these companies will be encouraged to voluntarily report incidents.

Several aspects of the NIS Directive are aimed at member state governments themselves, requiring that they adopt a national NIS strategy, implement the aforementioned NIS competent authority and create a 'cooperation mechanism' to share security information and best practice across the European Union and circulate early warnings on security risks and incidents. The NIS Directive is now being finalized and is expected to be adopted by the EU government in the first half of 2015.

3a.

INTRODUCTION

The GDPR proposes a single law for data protection to cover the entire EU in place of current data protection regulations which have ended up being implemented differently in each member state. It will extend to organisations operating in Europe irrespective of whether the data they handle is stored within the boundaries of the EU or not, broadening the definition of personal data to include email addresses, computer IP addresses and posts on social media sites. Besides proposals which mirror NIS Directive calls for bigger fines and the establishment of 'one stop shop' national authorities in each member state, the GDPR calls for specific regulations to govern the way that EU citizens' personally identifiable information (PII) is handled. Those organisations must:

- Inform users of data breaches without undue delay (within 72 hours) after they become aware of it
- Give end users the right to request a copy of their PII in a portable format which can also be transmitted electronically from one processing system to another.
- Provide the right to erasure: the end user can request all PII be deleted if there are no legitimate grounds for retaining it.
- Obtain valid consent to collect PII, consent which can also be withdrawn.
- Obtain regulatory approval to transfer PII outside of the EEA to countries not approved as having adequate data protection measures in place.
- Appoint a data protection officer to ensure compliance (likely applicable to companies with more than 250 employees and/or those who process more than 5,000 data subjects within 12 months, and all public bodies).
- Publish contact information for the data controller.
- Build data protection into business process, product and service development (Privacy by Design).

IDG Connect surveyed 260 people working for organisations based in France, Germany and the UK each of which employ over 500 staff. Of those polled, an aggregate of 31% were IT managers and 20% IT directors, with a further 27% occupying specific IT related executive positions such as chief information officer, chief technology officer or chief security officer. The largest contingent (20%) worked in the software and computer services industry, with 11% employed in electronics, 8% engineering and 7% in financial and healthcare sectors respectively.

This paper assesses respondents understanding and expectations of the NIS and GDPR legislation being proposed, gauges the scale and importance of the impact they expect new regulations to have on their business, and attempts to predict how organisations within France, Germany and the UK are most likely to prepare themselves for compliance.

4.

ORGANISATIONS BETTER PREPARED FOR NIS THAN GDPR

Respondents demonstrate a slightly higher degree of preparedness for the NIS Directive than they do for the GDPR, with 76% reporting that either all or most measures were already in place to meet NIS compliance compared to an equivalent figure of 64% for the GDPR. Of those, many more (39%) felt they had ticked all anticipated NIS boxes compared to just 20% for the GDPR.

In both cases, however, there is clearly still a lot of work to be done - 18% and 27% reported that only some required measures had been put in place with 6% and 9% believing that either the two proposed cybersecurity frameworks do not apply to them or that their organisations have not put any required measures in place as yet. With the precise terms of both the NIS and the particularly the GDPR yet to finalised and the existing proposals

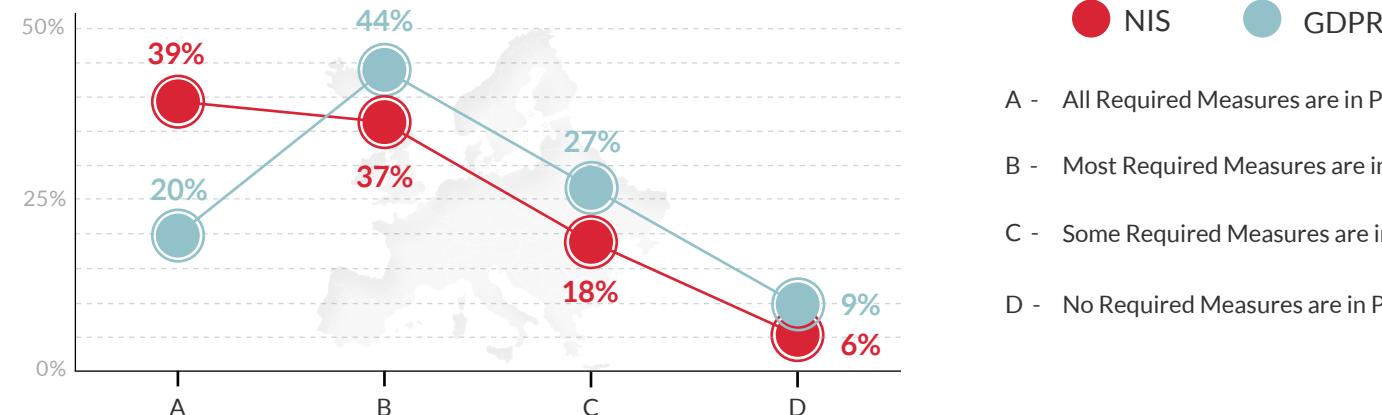
criticised for being too vague (a finding which is reinforced in the responses to Question 5 documented in Tab 8) some IT departments may either be guilty of a little too much complacency when it comes to assessing their current understanding of requirements, and/or that they have adopted an all too common attitude to data protection regulation which demands outward confidence towards compliance which is only punctured once breaches occur.

The findings indicate that organisations within Germany consider themselves better prepared for the NIS directive than those in other European countries with 46% believing that all required measures are in place compared to France (38%) and the UK (34%) with a further 36% reporting most required measures were in place (roughly equal to those in France and the UK). Fewer numbers of German respondents also

felt that their employers currently had no required measures in place to meet anticipated GDPR requirements - 6% compared to 12% for France and 8% for the UK – indicating slightly higher levels of confidence in existing provision.

This may be due to the strict requirements of existing data protection regulation in Germany which is already mature. The Bundesdatenschutzgesetz (BDSG) is a federal data protection act first implemented in 1970, for example. Each individual German state also has its own separate data protection laws, applicable to all companies operating within its borders (except for telecommunications companies which are directly supervised by the federal regulator) and overseen by regional commissioners.

Majority Are Not Currently Fully Prepared for Compliance with Either Framework



5. ORGANISATIONS FEAR FINES, LEGAL COSTS AND LOST BUSINESS

Worries about potential fines levied by regulators for admissible breaches of the new regulations are understandably high (rated as a concern at 58%). This is not least because the GDPR proposals suggest that the highest penalty could be increased to a maximum of €100m or 5% of annual, global turnover whichever is the greater, which dwarfs the fines imposed in the past.

In the UK, the Information Commissioners Office (ICO) has issued multiple fines where breaches have led to data loss in the past, including £250,000 to Sony in 2013 after its PlayStation Network was hacked and £200,000 to the British Pregnancy Advice service in March 2014. The same year saw regional privacy regulators in Hamburg penalise Google €145,000 for recording signals from WiFi networks whilst collecting photographs for its Street View service, arguably little deterrent for a company whose 2013 revenue was estimated at \$58bn and one reason why the EU is keen to increase the maximum penalty. France's data protection authority, the Commission Nationale de l'informatique et des Libertes (CNIL) also fined Google €150,000 in 2014 after ruling that its new privacy policy did not inform users exactly how their personal data was being used or collected.

The European Union Agency for Network and Information Security (ENISA) has noted that the number of data breaches reported to regulatory authorities varies significantly from

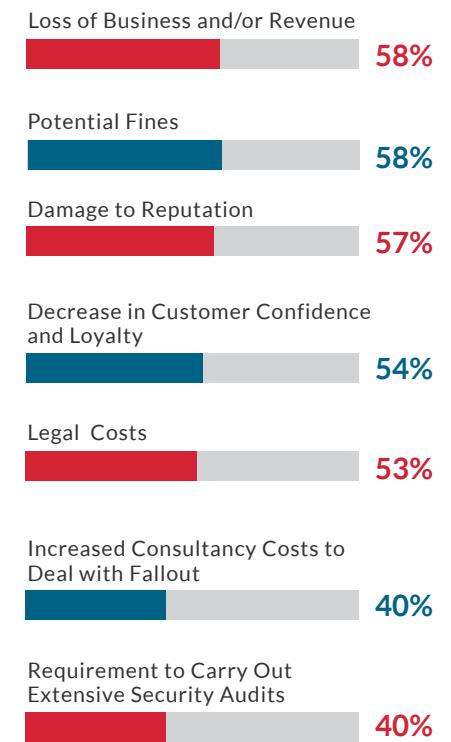
one EU member state to another, however, and depends greatly on the local legislation in place. With some countries reporting far more data breaches and imposing far fewer fines than others, the impact of the NIS Directive in these territories could be far more hard hitting.

Nor is the prospect of much larger fines seen as the only element of financial loss – the majority of respondents rate damage to their business reputation (57%) contributing to lost business or revenue (58%) as equal concerns. The possibility of decreased customer confidence and/or loyalty and the legal costs associated with the judicial and/or auditing process are also perceived as negative consequences, rated at an importance level of 54% and 53% respectively.

Another indication that most of the fallout of any breach is more likely be handled in-house can be seen in the lower level of criticality attributed to increased consultancy costs and the requirement to perform extensive security audits (both given concern ratings of 40%), suggesting that the job will be left to internal IT staff rather than external advisors. Interestingly, those legal costs are expected to become more of a concern in three years' time than they are today (38% vs 32%), indicating that respondents feel either that the chances of having to report a breach are higher and/or that lawyers will look to capitalise on the situation through higher fees.

There was little regional variation across the three countries in these findings, though organisations in France were slightly more worried about the impact of financial penalties (61%) than elsewhere whilst appearing to place less emphasis on security audit requirements (32%).

Damage to Reputation and Customer Confidence Also Causing Consternation



6.

TWO THIRDS BELIEVE THEIR ORGANISATIONS FULLY UNDERSTAND THE IMPACT OF PROPOSED NIS/GDPR REGULATIONS

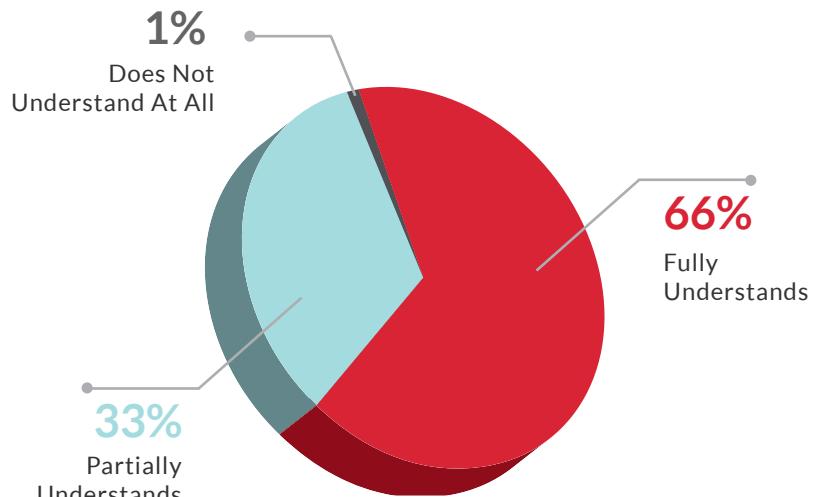
Two thirds (66%) of respondents believe that their organisations fully understand the impact that the new NIS and GDPR regulation will have in terms of any additional measures which may be required to maintain cyber security compliance and an incident reporting framework, again suggesting a degree of complacency amongst some of those polled. Those in the UK appear less certain than respondents elsewhere however, with only 60% believing their organisation fully understands the requirements compared to 69% in France and 68% in Germany.

The third of respondents (33%) which said that their organisations only partly understood the potential impact appear to have a more realistic view of the situation with anecdotal evidence also suggesting that much confusion around NIS/GDPR requirements, the extent of their overlap and whether they are applicable to every organisation remains.

The scale and diversity of recently reported data breaches suggests most organisations suffer regular incidents. A study published by the Risk Based Security and Open Security Foundation Report estimates that 2,164 data loss incidents were reported worldwide in 2013, in which 822m personal records were exposed. The majority of breaches (75%) involved external hackers with the remainder caused mainly by human error and accidents.

Just over half (53.4%) originated in the business sector, followed by government (19.3%), healthcare (11.5%) and education (8.2%). A survey commissioned by the UK Department of Business Innovation and Skills in 2013 also found that 93% of large organisations and 87% of small businesses suffered security breaches in 2013. With so many organisations already required to notify regulators of breaches, it is clear that the more onerous reporting requirements demanded by NIS/GDPR compliance will present a bigger burden to IT departments.

Current Lack of Clarity Suggests Some Complacency for Many



7.

NIS PROPOSALS SEEN AS MORE POSITIVE

Part of the NIS remit is to set a minimum required level of data security protection and encourage more European companies to implement a one stop ICT security policy which can be regularly reviewed. It is not yet clear how, when or by whom that review should be carried out though the EC has called for an 'NIS competent' national authority to be appointed in each member state.

The proposed requirement for European organisations to move beyond voluntary reporting and security assessments and towards regular reviews yielded mixed reactions from respondents to the IDG survey, with many (45%) seeing the measure as having a strong, positive impact if it does actually result in less formal security assessments which are easier to perform and simpler to report (only 16% believed it would have either a negative impact or no impact at all).

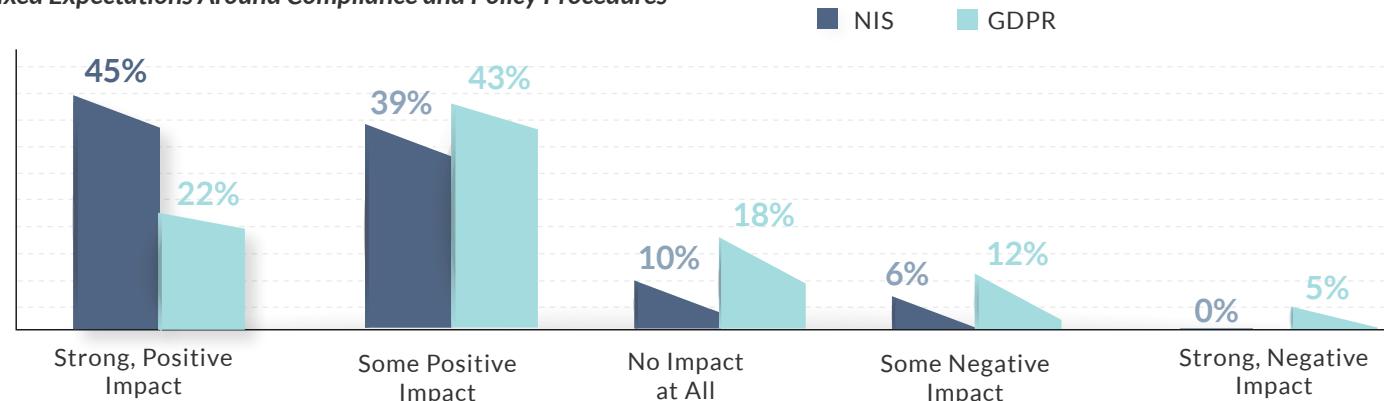
Things are perceived very differently for the GDPR however, which looks set to continue in its requirement that data protection impact assessments have to be conducted when specific risks occur to the rights and freedoms of data subjects, with the prior approval of the national data protection authority for high risks and data protection officers to ensure compliance within public authorities and companies processing more than 5,000 data subjects within 12 months. In contrast to the NIS proposals, only 22% of respondents thought the GDPR would have a strong positive impact, with 17% believing it would be yield a negative impact.

There was some slight regional variation in these findings. Relatively high numbers of respondents in the UK (26%) and France (24%) felt that the GDPR in particular would yield a strong positive impact, compared to

17% in Germany, the country which saw the most number (7%) believing that the proposed GDPR legislation would have a strong, negative impact on their organisations compliance policy and procedures.

That those in Germany anticipated that the GDPR will have either a strong positive or negative impact on current procedures may again be related to the policies they already have in place in order to comply with more stringent and mature federal and regional data protection rules already being applied in that country. In general though, aggregate levels of optimism (those predicting either a strong or some positive impact) and pessimism (strong or some negative impact) concerning GDPR were roughly equivalent across all three European countries.

Mixed Expectations Around Compliance and Policy Procedures



8.

NO CLEAR UNDERSTANDING OF NIS/GDPR REQUIREMENTS

Having approved the draft NIS directive in March 2014, the European Parliament is currently negotiating the exact terms of the text with representatives of the 28 EU member states. The draft GDPR legislation has been adopted by the European Parliament following a first reading in March 2014, but not yet approved. It will need to be discussed further by the Parliament, the EC and European Council prior to its finalisation over the next two years with exact timings for ratification still uncertain.

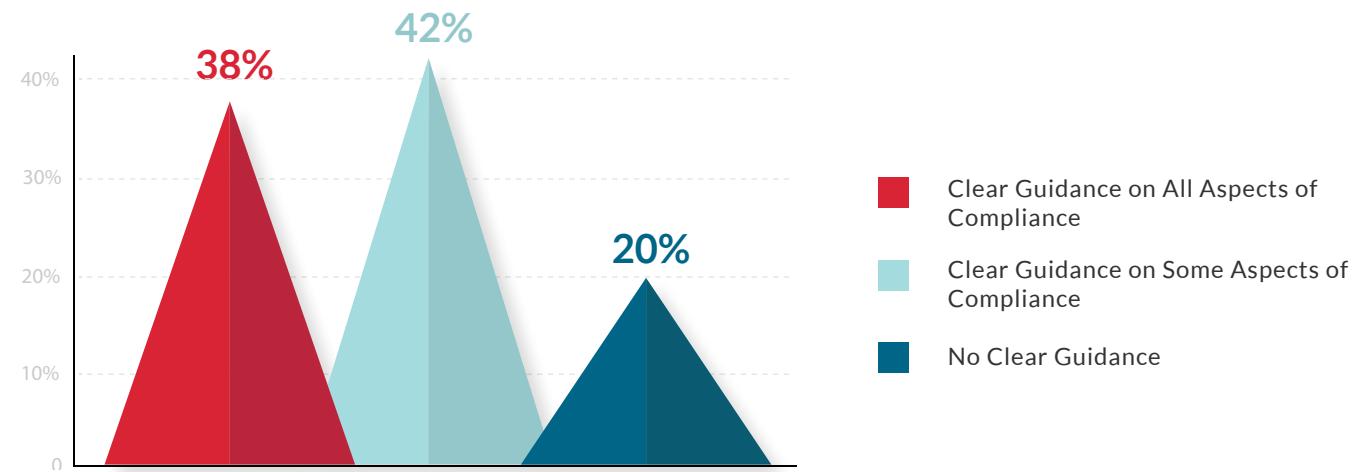
Whilst for now, the NIS Directive can be said definitely to apply to organisations involved in the supply of critical

infrastructure – energy, healthcare, transport and financial services have been named specifically – its remit may be extended to other organisations at a later stage. The legislation could also potentially apply to any industry which, under EC terms ‘the disruption or destruction of which would have a significant impact in a member state’, for example.

Even when both the NIS Directive and GDPR framework are finalised, the European Parliament will only issue associated policy guidelines and is unlikely to either set out specific technical standards required for compliance, or propose any associated certification scheme.

With so many aspects of the both the NIS and GDPR proposals still to be finalised, and so little practical advice on compliance requirements either currently on offer, or likely to be in the future, it is no surprise that 42% of the survey feel they have little or no (20%) clear guidance on what they need to do to meet the terms of legislation which is still open to debate. This situation may effectively hamstring those IT departments which are either already in the process of upgrading data security provisions, or are planning to do so in the near term, because they cannot be sure the processes solutions they are implementing will deliver compliance at a later date.

Continuing Confusion on What Specific Security Upgrades Will be Needed



9. COST OF COMPLIANCE MEASURED IN BILLIONS

The EU has estimated that the total costs of compliance that would have to be borne across different industry sectors to meet proposed requirements for the NIS directive alone could reach between one and two billion Euros, with each small to medium enterprise (SME) paying out between 2,500 and 5,000 Euros. By way of justification, the European Parliament has said that it expects that cost would be matched by stimulated demand for secure ICT products and services in the member states which would also serve to increase business and consumer confidence and investment in digital services.

Certainly, the impact of those cost requirements is not lost on European businesses who face not only potentially large bills for new

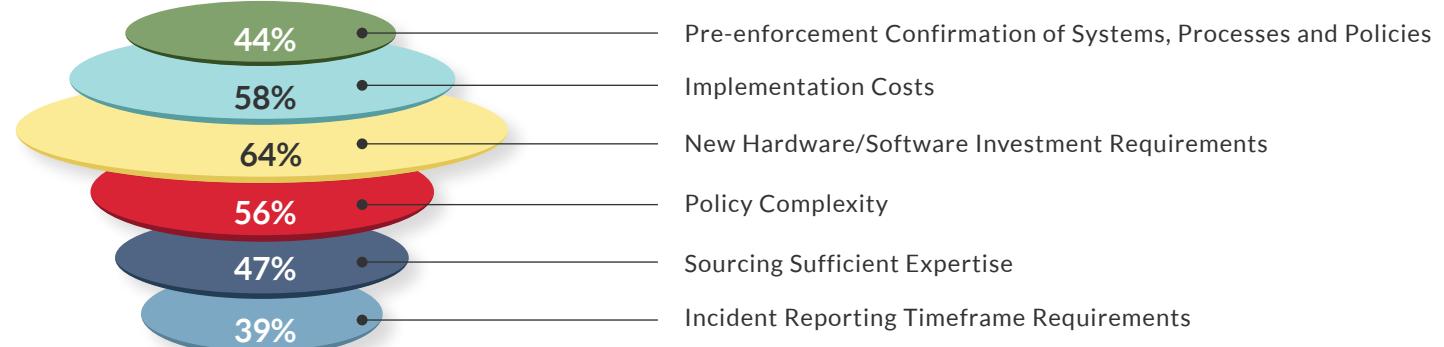
or upgraded hardware, software and services, but also additional costs for legal and consultancy advice. Almost two thirds (64%) of respondents to the IDG survey cited additional expenditure on security related hardware and software as a challenge, with 23% rating this as the single most important barrier they believed they would face.

Implementation costs, cited as a challenge by 58% rated equally as highly in terms of criticality, again cited as the most significant challenge by 23% - IT departments are seemingly under no illusion as to the extent of the evaluation, procurement, testing, deployment and maintenance overheads they are likely to encounter when ensuring adequate systems, processes and policies are put in place. Over half (56%) are also daunted by

the anticipated complexity which the implementation of those compliance policies is likely to present (with 18% seeing this is the most important challenge).

And 47% reported that sourcing sufficient legal and security expertise to understand the definitions and requirements would create problems, indicating that many will look to external consultants to help them certify the systems, processes and policies they put in place. Whilst incident reporting process and timeframe requirements were rated as the least important challenges compared to the other options, an aggregate of 42% still saw them as significant.

Purchase and Installation of Security Hardware and Software Is Most Significant Challenge



10. INTERNAL IT STAFF BEAR BRUNT OF COMPLIANCE BURDEN

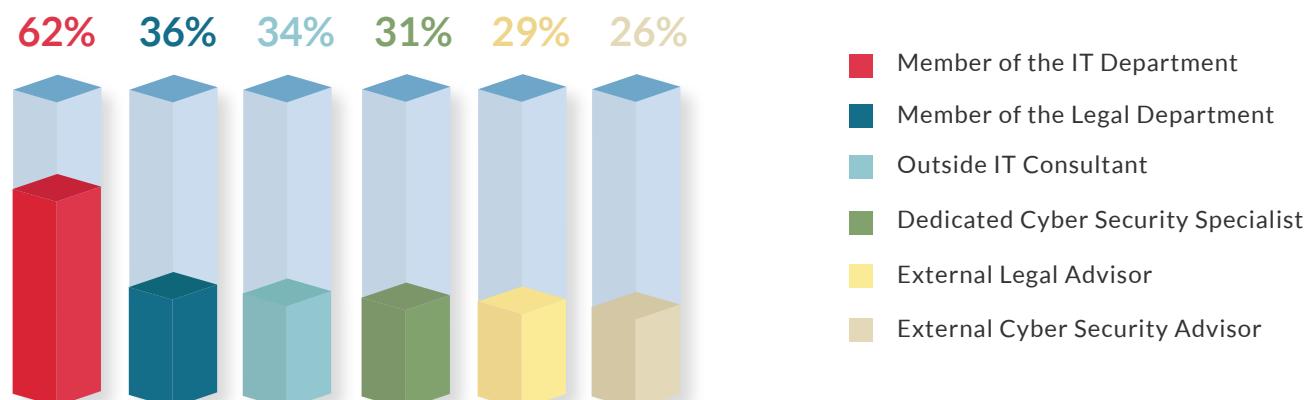
Clearly most organisations (62%) expect that members of their own IT department will be tasked with assessing NIS/GDPR requirements and formulating appropriate compliance and reporting policies, though this is likely to vary significantly depending on the size of the business and the availability of dedicated staff, irrespective of whether current knowledge or skills is considered up to the job.

Over a third (36%) also anticipate that members of the internal legal department will be responsible for the project, with previously indicated expectations of high legal and costs perhaps surfacing again in the smaller number (29%) who expect external legal advisors will be given the responsibility.

As ever, the availability of those in-house staff is likely to be a key determining factor, a metric also applicable to those who expect their organisations to contract outside IT consultants (34%). Fewer organisations are likely to turn to dedicated cyber security specialists (31%) or external cyber security advisors (26%). This finding may indicate that IT departments associate these job functions with practical knowledge of hardware/software security implementation rather than understanding of data protection compliance requirements, but is perhaps also a symptom of an ongoing skills shortage which affects their ability to source and hire suitably qualified cyber security staff or consultants.

Significant regional variations across the three territories are apparent, with Germany (76%) the most likely to assign responsibility to internal IT staff compared to roughly half of organisations in France (49%). This appears to suggest a higher degree of self confidence in the data protection compliance knowledge within German organisations, which may again derive from a greater familiarity and experience with Germany's more mature regulatory frameworks. The conclusion is reinforced by the slightly higher number (39%) of those in Germany which would also trust a member of their own internal legal department to assess NIS/GDPR requirements compared to the UK (35%) and France (34%).

Who Within Your Organisation Will Be Assigned the Task of Assessing New NIS/GDPR Requirements and Formulating Compliance and Reporting Policies?



11.

ADVANCED INTERNET BASED MALWARE EXPECTED TO PROLIFERATE

New types of cyber security attacks are constantly emerging as hackers develop and expand the diversity of malware they can throw at existing data protection defences, so it is no surprise that respondents cannot predict anything beyond the most common types of threats in evidence today which will also present the same threat levels in two years' time.

Advanced persistent threats (APTs), defined as stealthy and continuous hacking processes which direct carefully orchestrated attacks at specific entities, usually large public or private sector organisations for business or political reasons (of which Stuxnet is perhaps the most famous example) are increasingly prevalent.

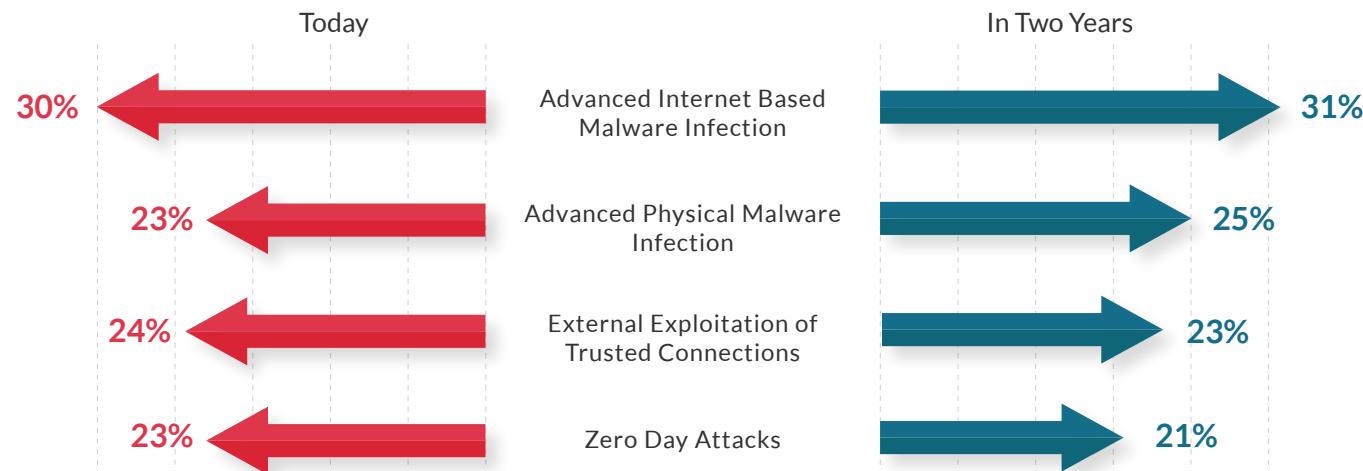
APTs usually involve the covert insertion of malicious code into systems without being picked up by existing security tools, with malware remaining active and undetected over long periods in order to maximise its spread and the volume and diversity of information being collected whilst simultaneously laying a foundation for future exploits.

Various types of APT are in evidence, with advanced Internet based malware (delivered via email, phishing or social engineering, for example) seemingly considered the most dangerous (rated at 31% importance by respondents on aggregate). Advanced physical malware infections (those which involve cyber criminals breaking into the premises to gain physical access to systems such as bank ATMs or retail point of sale systems) also scored highly (24% on

aggregate) as the threats most likely to require protection against both now and in two years' time.

External exploitation of trusted connections - APTs which see hackers gain entry to an organisation's network by using hijacked end user, employee or business partner credentials - were given a slightly lower importance rating of 24%. And zero day attacks characterised by vulnerabilities which are identified and exploited by hackers within a 24 hour period - recent examples of which include the Heartbleed bug affecting the OpenSSL web security protocol and a flaw affecting all versions of Microsoft's Internet Explorer web browser discovered in April 2014 - were given a importance rating of 23% (21% in two years' time).

Common Attacks Today Expected to be the Same in Two Years' Time



12. CONCLUSION

The results of the survey demonstrate a mixed state of readiness amongst organisations in France, Germany and the UK, many of which do not appear fully prepared to meet the compliance requirements of the forthcoming NIS and GDPR regulations, or comprehend the true extent of their potential impact on current security policy and reporting procedures.

The EU's proposal to increase the maximum penalty for serious breaches of its new data protection regulation to either €100m or 5% of an organisation's annual income clearly taps into extant fears of the consequences associated with data loss. Fines and loss of business are seen as the major concerns, slightly ahead of damage to reputation/customer confidence and legal costs which are perceived to have an equally damaging effect on profitability and/or financial survival.

But despite fears of being hit hard in their pockets, only 39% of organisations in France, Germany and the UK indicated that they have all required measures in place to guarantee NIS compliance. The remainder exhibit a more piecemeal approach which is even more widely apparent when it comes to the GDPR though this is more understandable considering that the requirements of the latter are yet to be finalised by the European Parliament. A third of respondents admitted that they only partially understand the impact that the new NIS/GDPR regulation will have on their existing data protection and security provision, whilst a similar number (38%) currently believe that the EU is currently providing sufficiently clear guidance on all aspects of the compliance requirements. With the EU unlikely to either set out specific technical standards required for compliance, or propose any associated certification scheme, that confusion is likely to be exacerbated when it comes to assessing current data security systems and planning upgrades.

What most organisations do consider a certainty is that additional spending on security hardware, software and policy implementation will be needed to achieve compliance with the new regulations, and that these projects will present them with significant challenges. Deployment and upgrade initiatives are expected to be both complex and difficult to support due to a lack of in-house knowledge and expertise in the relevant data protection definitions and requirements.

Nevertheless, the burden for assessing company security requirements to ensure NIS and GDPR compliance and reporting policies is expected to fall predominantly on non-specialist IT staff rather than internal or external advisors and lawyers, though an ongoing global cyber security skills shortage and fears of high consultancy costs may present many firms with little alternative. Despite these barriers, most (84%) believe that the NIS Directive will have a strong positive impact on their existing data protection compliance policy and procedures, indicating it is perceived as a constructive measure overall. This is less true of the GDPR however, with 17% forecasting a strong negative impact – a clear indication that a sizeable portion of IT departments fear the legislation will be overly prescriptive in its requirements.

About IDG Connect

IDG Connect is the demand generation division of International Data Group (IDG), the world's largest technology media company. Established in 2005, it utilises access to 38 million business decision makers' details to unite technology marketers with relevant targets from any country in the world. Committed to engaging a disparate global IT audience with truly localised messaging, IDG Connect also publishes market specific thought leadership papers on behalf of its clients, and produces research for B2B marketers worldwide. www.idgconnect.com