CorporateLiveWire

CYBER SECURITY 2017

VIRTUAL ROUND TABLE

www.corporatelivewire.com

Introduction & Contents

In this roundtable we spoke with six experts from around the world to discover the latest trends and interesting developments concerning cybersecurity in their jurisdiction. Highlighted topics include an overview on new regulation, advice on how to implement and improve security measures and strategies, and a discussion on the impact of innovation and the emergence of disruptive technology. Featured countries are: Australia, Italy, Spain, United Kingdom and the United States.

James Drakeford
Editor In Chief

MEET THE EXPERTS

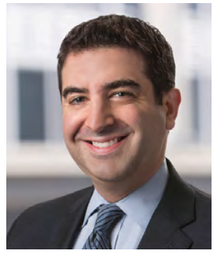
Fabrizio Cugia di Sant'Orsola - Cugia Cuomo & Associati
T: +39 06960 38103
E: f.cugia@cugiacuomo.it
W: www.cugiacuomo.it

Fabrizio Cugia di Sant'Orsola, founding partner of the Firm Cugia Cuomo & Associati, is an expert in regulatory law and telecommunications (domestic, European and international), intellectual property and media law, company law, competition. Fabrizio Cugia was a consultant for Ministry of Communications and Regulatory Authorities in the process of regulatory reform in telecommunications (including the beneficiary countries are: Italy, Luxembourg, Kazakhstan, Azerbaijan, Poland, Bulgaria, Albania). Already counsel to the Treasury Italian in the process of privatization of Telecom Italy, has lent its expertise in the drafting of the Italian part of the Green Book of the European Commission on multimedia applications in Europe and has been responsible for the regulation of many projects Light-Europeans in the areas of telecommunications and audio-visual services. Presta ongoing support in favor of national and international operators in the ' introduction of converged communication services as well as in all aspects of the service offerings of information and communication in Italy - in outsourcing - the allocation of numbers and frequencies, portability, personal communication, distribution and protection interactive services, roaming, interconnection agreements, housing and hosting services and video on demand, in the procedures relating to the offering GSM, WLL, WiFi, WiMax and UMTS licenses. Fabrizio was legislative assistant at the Parliament (1988-1991) and Professor of Communications Law (2000-2002) at the ' La Sapienza University in Rome.

Maria Vidal - Deloitte Legal
E: marvidal@deloitte.es
W: www.deloitte.es

María Vidal is a senior associate in the IP&IT law department at Deloitte Legal Madrid and a specialist in information technologies and intellectual property matters. Throughout her 13 years of experience, she has developed most of her career with Deloitte Legal, obtaining a Certified Information Privacy Professional from the International Association of Privacy Professionals. She is also co-author of data protection books and teaches data protection matters at Instituto de Estudios Bursátiles (IEB) and at Instituto Superior de Derecho y Economía (ISDE). She has been recognised as an "associate to watch" in TMT by Chambers and Partners 2016.

Liz Fitzsimons - Eversheds Sutherland
T: +44 (0) 1223 44 3808
E: lizfitzsimons@eversheds-sutherland.com
W: www.eversheds-sutherland.com



Bret Cohen - Hogan Lovells
T: +1 202 637 8867
E: bret.cohen@hoganlovells.com
W: www.hoganlovells.com

Bret Cohen practices in the areas of privacy, cyber security and consumer protection. With a particular focus on the internet and e-commerce, Bret has advised extensively on legal issues related to cloud computing, social media, mobile applications, online tracking and analytics, and software development. He counsels and is a frequent speaker on strategic compliance with global privacy laws, including cross-border transfer restrictions, data localization requirements, and the impact of government surveillance on the digital economy. Bret also spearheads efforts on cybersecurity incident preparedness and response, student privacy, marketing privacy, and workplace privacy.

Cheng Lim - King & Wood Mallesons
T: +61 3 9643 4193
E: cheng.lim@au.kwm.com
W: www.kwm.com

Cheng is an M&A partner who specialises in helping clients navigate complex legal, commercial and regulatory landscapes in telecommunications, technology and infrastructure. He continues to advise Telstra, the firm's most significant client, on all aspects of its most important transaction to date – the contractual arrangements between Telstra and nbn on the rollout of the national broadband network. Cheng is the global leader of the KWM cyber security initiative. He has advised numerous clients on privacy, cyber security and data breaches and has spoken at several global conferences and industry events about cyber security.

Rick Lauderdale - Hq.Doe.Gov
E: rick.lauderdale@hq.doe.gov
W: www.energy.gov

As the Innovation Architect for the Department of Energy, Rick Lauderdale is responsible for leading and defining the Enterprise Architecture (EA) strategic goals and objectives, by helping to develop, maintain, and govern the overall EA requirements across the organization.

1. Who are the main regulators and what are the key legislations that apply to the cybersecurity in your jurisdiction?

Lauderdale: U.S. Presidential Executive Order on Cybersecurity: Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

U.S. Federal Information Security Modernization Act (FISMA): FISMA establishes the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.

U.S. Federal Information Technology Acquisition Reform Act (FITARA): A historic law that represents the first major overhaul of Federal Information Technology management.

U.S. Department of Energy Cyber Strategy: A comprehensive cyber strategy rooted in enterprise-wide collaboration, accountability, and transparency.

Lim: Whilst there is no specific law or regulator that solely addresses the area of cybersecurity, Australia has a myriad of legislation that affects cybersecurity and information protection.

Most importantly, the Privacy Act 1988 (Cth) (Privacy Act) outlines laws to protect the privacy of information. The Privacy Act includes the Australian Privacy Principles (APPs), which apply to most federal government agencies and private sector organisations to regulate the collection, holding, use and disclosure of personal information.

The Office of the Australian Information Commissioner (OAIC), headed by the Australian Information Commissioner (the Commissioner), is the main body that deals with issues of privacy under the Privacy Act, as well as issues regarding freedom of information and government information. The Privacy Act confers powers on the Commissioner to impose fines for serious breaches of the Privacy Act and conduct independent investigations.

There are various other federal laws which also cover issues in the cybersecurity space. These include: the Criminal Code Act 1995 (Cth), which criminalises various behaviours regarding unauthorised use of data and electronic communications; the Spam Act 2003 (Cth), which is enforced by the Australian Communications and Media Authority and addresses the sending of unsolicited commercial electronic messages; and the Telecommunications (Interception and Access) Act 1979 (Cth), which makes it an offence to intercept communications in their passage over a telecommunications network.

In addition, each State has passed privacy legislation (e.g. the Privacy and Data Protection Act 2014 (Vic)) which regulates the collection, holding use and disclosure of personal information by State Governments and their agencies (as this is not regulated by the Privacy Act).

In recent times, the Australian Companies and Securities Commission (ASIC) has taken a very pro-active stance to educate listed companies and ASIC regulated entities (e.g. holders of Australian Financial Services Licences) of their responsibilities in relation to cyber-risk management.

Cohen: In the United States, cybersecurity laws are tied to specific data types that are deemed to be particularly sensitive. For example, there are laws regulating the security of health information, financial information, payment card information, student information, government identifiers, children's online information, credit report information, and online account information.

The regulators of these laws vary, depending on the type of data at issue, and include both federal sector-specific regulators as well as state regulators. Perhaps the most prominent regulator of cybersecurity laws is the Federal Trade Commission ("FTC"), the primary consumer protection regulator in the United States. Under Section 5 of the FTC Act, the FTC has the ability to prohibit "unfair" or "deceptive" trade practices. The FTC considers the failure to maintain reasonable and appropriate measures to secure sensitive consumer data to be an "unfair" practice, and false promises of cybersecurity for such data (for example, in a privacy notice or in advertising) to be a "deceptive" practice. States have enacted laws similar to the FTC Act, so state attorneys general have similar regulatory authority.

Another prominent set of cybersecurity laws in the United States are breach notification laws. 48 of the 50 states and a number of US territories have enacted these laws, which require entities to notify individuals, and in some cases state regulators, when they have experienced a breach of sensitive information. Each state defines the information covered by its breach notification laws differently, and have different thresholds for reporting, so it is a complicated exercise to determine a company's obligations if it has experienced a breach of the personal data of residents of multiple states.

A number of states have also enacted laws requiring entities to maintain certain minimum cybersecurity standards for categories of certain sensitive categories of information about residents of their states, including the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth.

Fitzsimons: The relevant legislation and applicable regulators will be dependent on the nature of the affected organisation and data as well as the nature of the cyber-security incident.

The main regulator is currently the Information Commissioner's Office. Other industry / sector specific regulators may also be involved e.g. Ofcom, the Financial Conduct Authority or Ofgem for the energy sector. Other authorities may also be relevant and become involved, such as the National Crime Agency and the Joint Cybercrime Action Taskforce.

The key legislation currently includes the Data Protection Act 1998 (shortly to be replaced by the General Data Protection Regulation), the Privacy and Electronic Communications (EC Directive) Regulations 2003, the Communications Act 2003, the Official Secrets Act 1989, the Computer Misuse Act 1990 and in future the implementation of the Network and Information Security Directive. In addition, the Regulation of Investigatory Powers Act 2000, the Investigatory Powers Act 2016 and related regulations may also be relevant.

Vidal: For several years national and European regulators have focused more and more on cybersecurity and cyber risks. This is reflected, for example, in the importance placed on cybersecurity in studies and in-

ternational forums such as the World Economic Forum where cybersecurity has been a significant concern for years. In Spain, the Critical Infrastructures Law was a turning point with respect to cybersecurity obligations. Also, all European regulations have for some time now taken cybersecurity into consideration in some way. For example, we have PSD2, the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR") or Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union ("NIS Directive"), which already take into consideration the reporting of cyber incidents. In this connection, one of the main problems is the heterogeneity of regulators and supervisory authorities on the basis of the type of data concerned, the sector, etc. Some of the examples of the regulators/supervisory authorities are, inter alia, the Spanish Data Protection Agency, the National Centre for the Protection of Critical Infrastructures, the Computer Emergency Response Team for Security and Industry (CERTSI), the Ministry of the Interior and the Ministry of Energy.

Cugia: The Intelligence System for national Security (*Sistema di informazione per la sicurezza della Repubblica*) is the national responsible body and is in charge for the identification of intelligence policies and the adoption of relevant procedures, as set by Law No. 124 of 3 August 2007 modified by Law no.133 of 7 august 2012.

The Intelligence System is a complex institutional body focused on protecting critical infrastructure and strengthening national cyber security. It includes the Prime Minister as coordinator of the national policy and members of the Interministerial Committee for the Security of the Republic ("CISR", formed by the Ministers of Foreign Affairs, Interior, Defence, Justice, Economy and Finance, Economic Development and the Digital Agenda Agency, AgID), the Security Intelligence Department (DIS – *il Dipartimento delle informazioni per la sicurezza*), the External Security and Intelligence Agency (AISE – *Agenzia informazioni e sicurezza esterna*) and the Internal Security and Intelligence Agency (AISI – *Agenzia informazioni e sicurezza interna*).

The Security Intelligence Department (DIS) is responsible for the definition of guidelines and security and intelligence policies also in coordination with the indicated Agencies. Such guidelines include the blueprint definition of national cyber security policies against threats and menaces, particularly aimed at bypassing national cyber defence measures.

The Ministry of the Economic Development - Communications Department is in charge of defining obligations on operators following the release of authorisations and homologation of apparatus and systems. Also, the Communications Department cooperates with international and EU entities, such as ENISA (European Network and Information Security Agency), particularly active in the definition of combined EU policies on the matter. The Ministry is aided in such task by the National CERT (Computer Emergency Response Team). Such Team has the purpose to enhance the national capability to survey and react to potential

cyber threats and menaces to systems and domestic infrastructures. The National CERT works as a cooperative public-private partnership supporting citizens and operators, also by means of national awareness and prevention campaigns.

The Data Protection Authority (Garante per la protezione dei dati personali) retains specific responsibilities in the definition of compulsory measures and cyber security issues for operators, as one of its key tasks is the definition of security and data protection policies due by operators active in electronic commerce, IT, online services and communications networks. In this regards, on November 2013, the Security Intelligence Department and the Italian Data Protection Authority established a Protocol of Intent aimed at establishing the minimum set of requirements in respect of the principle of proportionality and identified the thresholds due by operators in respect of protection of personal data protection, particularly in case of management of data banks and storage of data.

The Digital Agenda Agency (AgID) is in charge of the implementation of the Italian Digital Agenda objectives and national compliance to the EU Digital Agenda policies. AgID overviews the international cyber threats and defines protective measures, contributing to the diffusion of new information and communication technologies and adoption of safety protocols, all with the aim of fostering innovation and economic growth. It is also in charge of the implementation of the "National Strategic Framework for Cyberspace Security ("NSF") and the "National Plan for cyberspace protection and ICT security".

The fundamental legislation adopted in the field includes:

- Law No. 124 of 3 August 2007, as modified by Law no.133 of 7 August 2012, on the adoption of the Intelligence System for national Security;
- The Digital Administrative Code;
- The Data Protection Code;
- The Electronic Communication Code;
- The Prime Minister Decree of 24 January 2013, on Strategic Guidelines for the National Cyberspace Protection and ICT security");
- Prime Minister Decree of 27 January 2014, on the "The National Strategic Framework for the Cyberspace Security (NSF)" and the "National plan for cyberspace protection and ICT security (NP)";
- Prime Minister Decree of 1 August 2015, on cyber protection and national ICT security;
- Prime Minister Decree of 11 November 2015 no.5, on protection of State secrets and classified information.

2. Have there been any recent regulatory changes or interesting developments?

Lauderdale: U.S. President, Donald Trump, recently signed a new Executive Order on Cybersecurity on 11 May 2017. Each agency must develop a risk management plan that documents the risk mitigation and acceptance choices made by each agency head as of the date of this order, including:

- the strategic, operational, and budgetary considerations that informed those choices;
- any accepted risk, including from unmitigated vulnerabilities; and
- describe the agency's action plan to implement the Framework.

Lim: Mandatory data breach notification requirements

The recent Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth), passed in February 2017, amends the Privacy Act and imposes mandatory data breach notification requirements on APP entities. These entities will be required to notify the Commissioner, along with affected individuals, if an 'eligible data breach' occurs. 'Eligible data breaches' cover instances where there is unauthorised disclosure of personal information which could likely result in serious harm to any individuals whom the information relates to. The notion of 'serious harm' is quite broad, covering various harms such as emotional, financial and reputational harm.

Consequently, there is likely to be a noticeable increase in the number of cybersecurity incidents reported and made public. Whilst there are a few exceptions to notification, such as where the entity has already taken remedial action or where notification would breach secrecy provisions, the new laws will play an important role in keeping Australians' personal information more secure and encouraging organisations to improve their data security practices.

The Australian Signals Directorate's new cyber security baseline

The Australian Signals Directorate (ASD) has developed new mitigation strategies as of February 2017 that are 'essential' to effectively mitigate targeted cyber intrusions and ransomware. The ASD considers their eight essential strategies as baseline requirements for all organisations, with four of them already mandatory for Australian Government organisations as of April 2013.

Some of these 'essential eight' strategies include disabling untrusted Microsoft Office macros, blocking web browser access to Flash and Java, using multi-factor authentication to grant information access and regularly backing up data.

The Government's Cyber Security Strategy

The Australian Government's Cyber Security Strategy was released in April 2016 and establishes five themes of action for the Government over the next four years to advance and protect the interests of Australians in the digital age. These themes include:

- A national cyber partnership
- Strong cyber defences
- Global responsibility and influence
- Growth and innovation
- A cyber smart nation

The Government has supported each theme with concrete actions to improve Australia's cyber security. For example, measures targeted towards businesses include supporting cyber security start-ups as part of the National Innovation and Science Agenda and increasing the capacity of the national Computer Emergency Response Team to work with Australian businesses to better respond to cyber security incidents. The Government has committed to reviewing these initiatives annually and updating the Strategy every four years.

Cohen: New Mexico recently became the 48th state to enact a breach notification law. Connecticut enacted a law requiring that stringent security measures be applied by companies who educational services to students in the state.

In 2015, Congress enacted the Cybersecurity Information Sharing Act ("CISA"), which facilitates the sharing of information about cybersecurity threats between private companies and the US government. Among other things, CISA effectively provides private entities with immunity from liability for monitoring of their information systems for cybersecurity threats in accordance with CISA.

Fitzsimons: The European Union has published a proposal for a new Regulation on Privacy and Electronic Communications, as part of their Digital Single Market Strategy. This is envisaged to take effect from 25 May 2018, and the reforms are intended to ensure that e-privacy law and regulation keeps pace with technological developments (for example, in future including internet-based services enabling inter-personal communications, such as Voice over IP, instant messaging and web-based e-mail services, rather than being limited to traditional communications services).

The General Data Protection Regulation (GDPR) will take effect from 25 May 2018, and one of the biggest changes will be in relation to fines for personal data breaches (a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed). Infringements of Articles 33 or 34, in relation to notification and communications (respectively) of personal data breaches could result in fines of up to €10,000,000 or 2% of the total worldwide annual turnover of the preceding financial year for an undertaking, whichever is higher. This could have a big impact on the bottom line of businesses that control or process personal data. Under GDPR, for the first time, service providers will have direct legal compliance obligations, and be liable to the regulator and affected individuals for compliance. In addition, GDPR has extra territorial reach outside the EU in a number of cases.

There is currently an open consultation on the Protection of Official Data by the Law Commission. The Law Commission is proposing, amongst other reforms, to replace the Official Secrets Act 1989. The terms of reference for the review include assessing any deficiencies in the law, and research options for improving the protection of official information with the aim of providing an effective and coherent legal response to unauthorised disclosures. It remains to be seen how these reforms will affect cybersecurity.

Vidal: On 25 May 2016 the GDPR entered into force.

It will be directly applicable in May 2018. Spain is still working on the amendments to local legislation that this regulation requires in relation to data protection.

Also, on 6 July 2016, the European Commission approved the NIS Directive. The Directive was conceived to complement and harmonise the cybersecurity actions and legislation in the member states. Implementation of the Directive in Spanish legislation will require the creation of ad hoc legislation.

The main objectives of the Cybersecurity Directive are to guarantee a high common level of security in the member states, improve and expedite cooperation between member states in relation to providing early warnings on risks and incidents and to foster the implementation by operators of essential services of specific risk management and incident reporting policies. With respect to this last point, operators of essential services, which are also referred to as "critical infrastructure operators", include the energy sector, the transport sector, the banking sector, the health sector, public administrations and the key service providers, such as online search engines and cloud computing services.

Cugia: Italy has been target to recent international cyber threats. Along with this, new criminal cases involving cyber espionage practiced against national authorities, with transit and storage of key information outside national boundaries, have triggered a series of responses and protective measures.

On 18 February 2017, the CISR defined and approved a new National Cyber Security Strategic Plan, following which the Prime Minister set up the Cybersecurity Unit (*Nucleo per la Sicurezza Cibernetica*, NSC) in charge of securing the adoption of cyber protection measures and anticipating possible threats.

At European Union level, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 has defined the measures for a high common level of security of network and information systems ("NIS Directive") valid across the Union. Such Directive will be implemented in Italy necessarily within the set deadline of 9 May 2018, and similarly within such date Italy will also need to comply (within 25 May 2018) to the new privacy Regulation adopted in the EU (EU Privacy Regulation 2016/679) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Such EU Privacy Regulation also imposes specific security measures on operators.

In the recently-enacted NSF the Government has set the program for the implementation of the first and second package of measures issued in 2013 by OSCE (Organization for Security and Co-operation in Europe), titled "Confidence Building Measures (CBMs)" aimed to reducing risks from use of information and data in communication environments.

Finally, as a member of NATO, Italy is implementing the measures in the "Cyber Defence Pledge", adopted at the Summit of 8 July 2016, held in Warsaw. In such Pledge, cyberspace is recognised as a potential battleground, in which all NATO Members are called to defend themselves and actively adopt common pre-emptive protection measures.

3. Are there any compliance issues or potential pitfalls that firms need to be cautious about?

Lauderdale: (i) All U.S. Federal Systems must complete their Assessment and Authorization (A&A) requirements and obtain Authority to Operate (ATO).

(ii) All U.S. Federal Systems must be reported to Department of Homeland Security and Congress according to the Federal Information Security Modernization Act (FISMA).

(iii) If there is a compromise of mission critical systems or data there will be financial loss, public shame, reputation damage, and even employment termination.

Fitzsimons: One of the major difficulties in ensuring data security is in managing risk with third party outsourcing. Under GDPR, there will be much stricter requirements imposed, requiring additional and more detailed contractual obligations to be imposed on service providers handling personal data on behalf of their clients and strict obligations in relation to sub-processing arrangements and terms, as well as related data transfers. This, combined with increased potential fines under GDPR and the new direct liability which such service providers face, is likely to have a real impact on negotiation of relevant contract terms, liability and risk sharing. It will not only impact new contracts being procured to commence beyond May 2018 but current contracts which continue post May 2018.

Now, data controllers will need to ensure that processors provide sufficient guarantees to implement appropriate technical and organisational measures – but in future in such a manner that processing will meet the requirements of GDPR and ensure the protection of the rights of the data subjects. Businesses must be prepared to prove their due diligence, how and why they decided providers offered appropriate security and guarantees, how GDPR standards are met in contractual arrangements and how GDPR compliance is being delivered on an ongoing basis. This is in order to ensure that business can comply with their new GDPR obligation to evidence how their processing of personal data – even when outsourced – complies with GDPR.

Where working to prevent cybersecurity incidents, businesses may invest in security and scanning tools, checking traffic in and out of networks, checking use of IT equipment and access to the internet. When an incident arises or is suspected, businesses may conduct investigations and monitor staff and emails and voicemails. Care is required due to the rules controlling interception of communications and monitoring and the laws protecting the privacy and personal data of individuals. Whilst such checks and monitoring may often be undertaken lawfully provided they're carried out properly and proportionately, the correct measures must be taken to achieve this.

Vidal: The new obligations under the aforementioned laws, the GDPR and the NIS Directive, require that companies implement incident prevention and remediation procedures, which in the majority of cases represent procedural, system and organisational changes.

The obligation to compensate any damage a person may suffer as a result of an infringement of any provision of the GDPR, as well as the significant increase in administrative fines for infringement of the GDPR – these fines can total up to 4% of companies' total revenue – are matters which will necessarily make all companies

include in their procedures a new data-protection risk control box.

Cugia: International operators wishing to offer services in Italy or operating local proprietary infrastructure should perform a data protection and cyber security compliance due diligence check prior to the offering of services, as sanctions and/or suspension of titles may apply in case of default in the adoption of compulsory measures. Also, branch offices or local subsidiaries should be made aware that national legislation may apply on sensitive areas such as data protection and data breach compliance, homologation and interoperability duties on apparatus or infrastructure and, in general, in the adoption of safety measures.

With respect to data protection obligations, national regulation imposes the adoption of electronic security measures to protect personal data from any kind of cyber threats. In this respect operators are highly recommended to comply with the "National Cyber Security Framework" defined by the Cyber Security Report 2015, targeted to critical and IT infrastructures.

Albeit the application of the Framework endorsement is voluntary, it represents one of the essential tools to increase the domestic resilience of systems and networks against cyber threat, and may testify the attention of operators in ensuring protection of individual rights.

The Framework is tailored and scaled according to operators' dimensions, with a specific focus on small and medium enterprises (SMEs). It aims to provide organisations with guidelines to face cyber security menaces in order to reduce risks.

4. How can companies' best prepare for compliance towards the recently signed General Data Protection Regulation (GDPR)? As the new rules do not enter into effect until 2018, is it too early to start taking action now?

Lauderdale: Does not apply to U.S. Federal Government agencies.

Cohen: It is not too early to start taking action now. There is only a year left until the GDPR takes effect, and many companies in the United States will be newly subject to the GDPR due to its new jurisdictional provisions, which regulate any personal data collected in the provision of services to the EU regardless of the location of the company. Fines under the GDPR are significant: for certain violations, up to 4% of a company's global annual turnover, or €20,000,000, whichever is higher.

Cybersecurity is a key component of GDPR compliance. Both controllers and processors are required to implement appropriate technical and organisational measures to ensure a level of cybersecurity appropriate to the risks posed to personal data that they process. And the GDPR introduces new breach notification requirements, obligating controllers to notify breaches of personal data to supervisory authorities without undue delay and, where feasible, not later than 72 hours after having become aware of a breach. Notification of breaches to individuals is required in certain circumstances as well.

Fitzsimons: The changes required for GDPR compliance are numerous. New and prescriptive obligations are imposed. Organisations need to understand their use of personal data in new ways and many businesses will not have the necessary knowledge currently to enable them to comply.

For example, to give the necessary privacy notices to individuals whose personal data are collected and used, organisations need to understand in more detail what data they collect, when, and how so suitable notices can be provided at the appropriate time. Those notices need to state the legal basis on which the personal details are used, including what "legitimate interests" are relied on, if any, to do so. Privacy notices also need to go into more detail about likely data transfers, even explaining on what basis details are transferred, such as EU standard contractual clauses. Businesses therefore need to understand how personal data is used in the business, why, who it's shared with, where and on what basis to prepare the privacy notices. Privacy notices will need to be updated to comply with GDPR and provide individuals with the mandatory details required. Similarly, consents to use personal data under GDPR are subject to new rules and will need to be upgraded. Current indications are that pre GDPR consents will not be valid post May 2018 if they do not meet GDPR standards.

Other key requirements to comply with GDPR are to ensure that businesses comply with the principles of data minimisation and storage limitation. Firms will need to review what personal data they hold and determine to what extent the details should be securely deleted or destroyed before May 2018. Personal data held beyond May 2018 will need to be GDPR compliant, so reducing that volume makes sense and will reduce the target for individuals to exercise their enhanced GDPR rights against it, such as subject access and data portability.

For all these reasons, GDPR compliance preparations should start now and not be delayed. Businesses should consider a data audit or data mapping to better understand what details they collect and how they use them.

Privacy impact assessments should be undertaken to determine what personal data use is necessary and why. Records should be maintained to evidence GDPR compliance. In addition, privacy notices and consents must be reviewed and revised, as well as supplier due diligence and contracting arrangements to accommodate new onerous GDPR obligations.

Vidal: When the European regulator granted a two-year period for the law to be directly applicable, this two-year period is not granted gratuitously. This two-year period is the amount of time that the legislature deems necessary for companies to be able to implement all the necessary measures under the GDPR.

Certain of the new obligations, inter alia, that in my opinion cannot be implemented overnight are the following:

- Consent obtained validly in accordance with the requirements of the GDPR: In Spain's case, the understanding of consent as freely given by clear affirmative action means that lots of consents will have to be obtained again. To date, consent has been obtained through silence or pre-ticked boxes (these forms no longer constitute valid consent under the GDPR).

- To implement a consent remediation plan at a company requires extensive analysis of the data processing operations together with possible authorisations to which such processing operations might be subject, as well as a decision-making process for which, in many cases, it could be said that the two-year deadline is quite tight.

- The introduction of concepts such as privacy by design and privacy by default will require many procedural changes that take time to be agreed upon and implemented.

- Identification and creation of records of processing activities that will help to identify which processing operations necessarily entail privacy impact assessments. From May 2018 these risk methodologies must be available to the supervisory authority.

- The obligation, where required under the GDPR, to designate a data protection officer. This figure can be internal or external, but it must be designated on the aforementioned date. The design of data protection governance at companies where this figure is not developed requires time since its approval will likely require the voice of many of the affected areas as well as a long chain of approvals.

All these new requirements under the GDPR affect multiple areas at organisations (legal, organisation, technology, cybersecurity, etc.). In this regard, entities know the importance of the new regulation and of the effort the adaptation process represents; therefore, the entities are aware of the need to conduct in-depth analysis and to establish an appropriate project plan with sufficient time to enable its implementation for May 2018.

Cugia: As mentioned, although GDPR will be implemented by 25 May 2018, operators should not wait until the last moment to adopt the relevant compulsory measures.

Under the GDPR, operators acting as data controllers or processors, are called to implement strict measures on security of personal data. Data protection must be processed in a manner that ensures appropriate security and confidentiality of the personal data, including the prevention of unauthorised access to or use of personal data and the equipment used for processing.

According to GDPR, security equally covers confidentiality, integrity and availability. All measures by operators should be considered following a risk-based approach: the higher the risk, the more rigorous the measures that the controller or the processor needs to take. Taking into account the increasing use of digital and/or online data processing systems – often based on cloud services and smart IoT devices – operators should keep a particular eye on security risks associated to cache or automated hosting of personal data on IT networks and system components.

As indicated in the "SME Guidelines on the security of personal data" of ENISA, companies should address a privacy risk assessment process, in order to evaluate the risk level and proceed with the selection of appropriate security organisational and technical measures. Risks may be inherent in the processing and implement measures to mitigate those risks (such as in encryption devices). Measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

Given the above, it is certainly not too early to start taking action to comply with the GDPR, taking into account the need to perform an accurate examination and analysis of risks linked to technology utilised and type of services offered. Lack of prioritisation could compromise the outcome of the compliance exercise, or jeopardise integrity and confidentiality of personal data protection measures. Also, the General Data Protection Regulation identifies new measures and obligations and reinforces a series of data controller duties; as interpretation on the relevant compliance is still to come, operators should be aware that the adoption of new data protection policies could need prior filing of formal Q&A to competent Agencies.

In addition, under the GDPR, it is mandatory for certain controllers and processors to designate a Data Processor Officer. Even when the GDPR does not specifically require the appointment of a DPO, organisations may sometimes find it useful to designate a DPO on a voluntary basis. The Article 29 Data Protection Working Party ('WP29') encourages such voluntary efforts (16/EN ,WP 243). The GDPR recognises the DPO as a key player in the new data governance system and lays down conditions for his or her appointment, position and tasks, even though DPOs are not personally responsible in case of non-compliance with the GDPR. It is important that companies reorganise their divisions and set new responsibilities.

5. Why is it important for information security to be at the heart of the organisation?

Lauderdale: Information Security is as important to protecting data, information, people and intellectual property as physical security is to protection against unwanted intrusions and keeping the facilities where it operates secure. For any organisation to remain competitive, efficient, and productive it must use IT systems. Using IT systems relies on making use of networks, assets, printers, website and applications that store, transport and exchange data important to the business. To make sure that the data is used in the manner it is intended, it must be protected from unauthorised access. This is the reason why information security is or should be the heart of the organisation.

Lim: As well as inciting a range of legal consequences, information security breaches will have a material impact on an organisation's operations, costs and reputation. A single data breach may compromise every aspect of an organisation from the safety of its employees to the loyalty of its clients.

The costs of a cybersecurity incident can be substantive. For example, Target disclosed that its 2013 data breach resulted in it incurring some US$252 million in costs. Cybersecurity insurance was only able to cover US$90 million of this amount. With the increased interconnectedness of people and systems, as well as the quantity and value of information held online, the Government estimates that cybercrime costs Australians over $1 billion each year.

More importantly however, organisations must be wary of indirect costs that arise from the negative publicity accompanied by data breach incidents. In February 2014, when the Department of Immigration and Border Protection inadvertently released the personal details of one third of asylum seekers held in Australia, the Government saw a wave of criticism from the public. A further data breach later that year surrounding asylum seekers' details caused great embarrassment and loss of faith in the Government's ability to secure its information.

Clearly, cybersecurity is not solely an IT issue, but a governance issue for organisations, and subsequently for the nation. Moreover, ASIC's Report 429: Cyber Resilience – Health Check confirms that the obligations on company directors and officers to discharge their duties with care and diligence extend to cyber security. So whether it be to protect national, company or self-interest, failure to respect information security is not an option for any organisation going forward, as it can have dire consequences for stakeholders' safety and integrity.

Vidal: Information is one of an entity's most important assets; by information we are not just referring to clients' data, but to corporate information in general. Therefore, over recent years, we have seen information security gain greater importance at companies; companies launch more and more initiatives and projects focused on information security.

Poor management of information security might give rise to incidents that have a big reputational risk and, in addition, sound use of information and the quality thereof enable the use of new technologies such as analytics or big data, through which processes and clients' user experience are improved.

Cugia: Information security involves all crucial areas of organisations, and all measures taken to defend data from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording and/or destruction. In a certain sense, we could say that organisations need to develop and offer services around a set of core obligations pertaining to information security.

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). This puts security at the core of data protection together with the rest of data protection principles, i.e. lawfulness, fairness and transparency, purpose limitation, accuracy and storage limitation.

It must be remembered that the obligations regarding the processing of personal data apply regardless of whether the processing takes place in the European Union or not. The GDPR will apply to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (i) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (ii) the monitoring of their behaviour as far as their behaviour takes place within the Union; and to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

6. What are the key factors when building an information security strategic plan?

Lim: Seven Pillars of Cyber-Resilience

There are seven pillars of cyber-resilience that form a comprehensive framework when building an information security strategic plan.

Pillar 1: Govern

Organisations should ensure that their governance bodies take appropriate steps to make the organisation cyber-resilient and protect it against cyber-risks and threats. This involves educating both management and board members in this area, rather than allowing these issues to be dealt with solely by technology leaders.

Pillar 2: Know

Subsequently, it is crucial that organisations should know the data they hold, the value of that data, and how well it is being protected[1].

Pillar 3: Review

Organisations must review and test the adequacy of current cyber-resilience processes, procedures and systems. Companies need to remember that the resilience of their whole supply chain needs to be tested, rather than solely testing their own systems. Moreover, it will also be important to assess the risks of third parties they may deal with.

Pillar 4: Improve

This pillar involves identifying areas of weakness and improving an organisations' cyber-resilience processes, procedures and systems. There are various guidelines, such as the ASD's new cyber security baseline, that outline ways in which an organisation can strengthen its information security.

Pillar 5: Protect

Steps must be taken to ensure that organisations actually implement the processes and procedures that have been established. Organisations might want to allocate this task to a specific person or team who will oversee the execution of proposed cyber security strategies.

Pillar 6: Respond

In the event of a data breach, organisations must activate incident management plans immediately to address the situation. It may be wise to establish an incident-management committee who are capable of detecting and containing the impact of the incident.

Pillar 7: Recover

Organisations must have plans and mechanisms in place to recover as swiftly as possible from a cybersecurity incident and to draw key learnings from the incident.

It must be emphasised that successful cybersecurity plans come in different forms for different organisations. Whilst frameworks such as the NIST Cyber Security Framework or ISO 27001 provide a useful starting point to implement information security strategic plans, organisations need to ensure that these are not merely checklist exercises but a real analysis of the unique risks and threats that may be faced by a particular organisation.

Cohen: Information security starts with people. So the first key factor when building an information security should be to identify the individual or individuals responsible for the design, implementation, and oversight of the program. The organisation should then take stock of the information it maintains, the sensitivity of that information, and the types and variety of systems and repositories where the information is stored.

Armed with this information, the organisation should conduct a security risk assessment, identifying the key risks to the security of the information. It should then design and implement security controls, policies, and procedures tailored to mitigating those risks, taking into account the sensitivity of the information and a reasonable budget for those controls. Significant new products, systems, or features should undergo a security review before they are implemented. Once the security program is up and running, the organisation should train its personnel responsible for implementing the program, and should audit for compliance with its security controls, policies, and procedures, and make sure that any gaps are remediated.

But that is not the end. An organisation will always be facing new cybersecurity risks, new laws and regulations will be enacted, and key personnel will turn over. Therefore, the team responsible for running the security program should repeat this process on a regular basis.

Vidal: When preparing a cybersecurity master plan, it is important not to lose the overall view of the business in the analysis.

In this connection, we like to take four lines into consideration in all cybersecurity plans:

- Governance – alignment with the business, establishment of the policy, performance of risk analysis, etc.,
- Secure – preventive measures to protect against a cyber-threat,
- Vigilant – being vigilant to what is happening externally and internally, and
- Resilient – when suffering a cyberattack, having the mechanisms to be able to recover and provide a service to the business and clients.

At Deloitte we have proprietary models that consider these aspects.

Cugia: Information security and data processing assessments should be generally performed following a four-step approach:

Definition of the processing operation and its context: the organisation needs to consider the different phases of the information security and data processing (collection, storage, use, transfer, disposal, etc.) and their subsequent parameters;

Understanding and evaluation of impact: the organisation should evaluate the potential impact to the rights and freedoms of individuals and security obligations, particularly in case of breach, malware attacks or security menaces. Menaces and threats may be associated to

1. See Telstra's 5 Knows of Cyber Security

any type of breach of confidentiality, integrity or availability of personal data, stored, transmitted or temporarily hosted;

Definition of possible threats and evaluation of their likelihood (threat occurrence probability): threats should be related to the overall environment of the personal data processing performed by organisations (whether external or internal); assess of their likelihood (i.e. threat occurrence probability) should be performed and tested;

Evaluation of risks (combining threat occurrence probability and impact): After evaluating the impact of the personal data processing operation and the relevant threat occurrence probability, in view of measures, infrastructure and operations, a correct evaluation of risks is possible, and, more than that, presumably accurate.

7. What are the most common mistakes companies make regarding their information security strategy?

Lauderdale: A common mistake is that organisations spend a lot of time and resources in designing and developing grand solutions to address the security challenges. The solution that is designed is usually meant to be encompassing and elaborate. In most cases, these solutions fail. To be successful the approach that should be adopted is one that is designed with existing processes and data in mind. Use the information and tools available within the organisation to develop a security solution. Using the current tools, processes and people also helps ensure that the solution will be manageable and maintainable.

Another mistake is a lack of proper visibility on the patch updates of servers and effective monitoring of how the servers are vulnerable on an on-going basis. According to the Verizon Data Breach report published in 2015, 99.9% of the vulnerabilities identified occurred one-year after the manufacturer published a patch that fixed the vulnerability. Organisations don't have the proper visibility into what software products they are running and when those software products become obsolete (end-of-support) to protect against cybersecurity attacks.

Vidal: There are areas in which a company must strengthen protection and it is a common mistake companies make. Employees, and third-party service providers that can access the company's personal data area not enough covered.

From my point of view, these areas must be highly controlled to minimise risks. In the case of service providers, it will be necessary, in the provider engagement process, to perform a light assessment to identify whether or not the service provider in question will have access to personal data, what type of data, what processing, and so on, and, on the basis of the result, whether it would be advisable to request the provider to fulfil certain privacy requirements. These controls can either be the implementation of security safeguards, regular controls by means of audits, the obligation to report certain incidents, duty of secrecy and confidentiality obligations, or, in the case of providers that render their services at the company, by providing resources that are not connected to any of the company's systems that do not have external ports, in order to prevent information leaks.

The case of employees, a good level of awareness will be necessary, ranging from the highest-ranking position to the company's most recent recruit. The level of awareness will be as necessary in management positions as in employees who process customers' personal data. Everyone at the company should be trained regularly with regard to their obligations and the steps they should take in the event that certain situations arise.

The main mistake that we tend to make is forgetting the importance of people, our employees and clients. However robust the cybersecurity strategy of an organisation is, however many protection and vigilance measures that are implemented, security begins and ends with people.

Cugia: Companies sometimes adopt a copy/paste approach to information security, implementing and adopting strategies not fine-tuned with respect to their particular realities, operations or type of services. Also, they may defect in the compliance with data protection legal framework and relevant interpretations by Agencies, which may substantially differ according to type of services offered.

Correct assessment of associated security risks is a critical task. Considering the specific characteristics of SMEs, such as limited resources, unavailability of qualified personnel and specific sectorial regulatory provisions, companies may have difficulties in managing correctly their data flows and data processes to the same extent as bigger and better resourced organisations.

In this respect privacy regulation does not differ: the same rules apply to SMEs or large organisations in cases of security obligations from malicious internal or external attacks, accidental misuse of personal data due to human mistake or unauthorised disclosure of data by external contractors, all typical information security threats.

"Prevention is an excellent tool for organisational review. For instance, IT virtualised systems may determine important security gaps: as mentioned by ENISA, in order to prevent cyber security risks and treats on a virtual landscape, specific items must be secured"

- Fabrizio Cugia di Sant'Orsola

8. Is it fair to say companies place too much emphasis on risk management rather than risk prevention?

Lauderdale: I think with risk management comes risk prevention – just like buying insurance. You decide how much risk you can endure (financial impact, including legal and medical) and you set standards to manage this risk. If there is no risk there would be no need to manage. Doing nothing about risk could be unfortunate and costly. We are exposed to all kinds of risks every day and must prepare and use sound judgement to balance the potential impacts of either the known or unknown risks. I think risk management and risk prevention go hand in hand.

Cugia: Yes, I agree. Companies generally are not focused on prevention, albeit the obligation to implement security preventive measures is a clear compulsory measure on all operators, as set by the Data Protection Code and restated by the GDPR.

Prevention is an excellent tool for organisational review. For instance, IT virtualised systems may determine important security gaps: as mentioned by ENISA, in order to prevent cyber security risks and treats on a virtual landscape, specific items such as the following must be secured:

- Training of human resources involved in the process of managing virtualised environments, from specialised professionals to managers and users, in particular on reduction of risks and impact of attacks.
- Adoption and integration of assurance solutions in virtualised systems;
- Definition of security solutions and corrective actions in case of misbehaviours;
- Service-level agreement definition and enforcement of specific measures inherent to multi-tenant natures of virtualised environments.

9. How does implementing effective protective monitoring help mitigate risks?

Lauderdale: By being proactive one can mitigate various risks and escalate various responses depending on the severity of the event. Balanced procedures and appropriate responses will be based on the severity of the risks, life, economic, as well as long term effect to individuals or countries.

Cohen: Protective monitoring is a crucial component of an effective information security plan. Three factors have increased this risk in recent years. First, as technology has improved, more of it has become internet-connected, creating a greater attack surface for potential intruders or from which data may leak. Second, as organisations have moved more of their data to the cloud for greater accessibility, cheaper cost, and to outsource security, systems have become more distributed, creating a greater attack surface. Finally, attackers have gotten better at directing automated, remote attacks at networks, to the point where certain internet-connected systems are almost constantly being probed for vulnerabilities. In this landscape, in order to mitigate risks it is almost necessary to proactively monitor for intrusions.

Regulators and courts have realised this, and proactive monitoring has been incorporated into the applicable standards of care. For example, in one enforcement action, the FTC claimed that a business did not maintain reasonable security measures to protect sensitive consumer information in part by failing to maintain an intrusion detection system and by not monitoring system logs for suspicious activity. In this respect, implementing effective protective monitoring both mitigates security risks and legal risks.

Fitzsimons: Practically, appropriate and effective monitoring can help avoid and minimise cybersecurity risks. It can also help businesses to comply with their GDPR obligations in respect of data security, in particular "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services" as well as the need to have "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing".

Monitoring provides invaluable information about actual and likely attacks, such as a denial of service attack before a hack, allowing the business to reassess its relevant security and strengthen it in time. Failing to identify and deal with such threats has been shown to increase sanctions imposed by regulators following any resultant breach. Likewise, monitoring will give the business essential intelligence about compromised security, when and where and how it happened. This can allow a gap to be identified at a stage where the relevant incident and compromised data is minimal, allowing adjustments to be made to prevent further and more serious breaches taking place. Data from monitoring can also help the business with the essential knowledge needed to understand what data has been compromised or extracted, how many individuals or systems are affected and the severity of the incident. In a number of cases we have handled, businesses have been aware of a security intrusion but not realised until too late that a security vulnerability has resulted and/or data has been extracted. Better monitoring may facilitate improved and faster awareness of the consequences of such an intrusion to prevent the incident in advance, rather than reacting to it after the event.

GDPR requires a relevant personal data breach to be notified to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it. Monitoring will facilitate compliance with this critical mandatory new obligation.

Cugia: Prevention and the adoption of preventive measures may be key to securing organisational update in the workplace. Powers, delegations, information flux and organisational responsibilities may be reshuffled as an effect of new protective measures.

In this regard, under the GDPR, the Data Protection Officer (DPO) shall monitor privacy compliance and implement security measures. While the designation of the DPO may be mandatory in some cases (art. 37) for certain types of data processing operations (large scale monitoring activities, processing of special categories of data, etc.), the activities of monitoring and relevant techniques for preventing and mitigating risks is much to the organisation itself, for instance in the involvement of the other professionals in charge of the task.

Cyber-threat prevention has naturally evolved also as side-effect of international malicious attacks. In particular, new areas of intervention have been detected in the area of Destributed Denial of service (DDoS) and virtual currencies.

10. What measures can be implemented to help minimise risk following a security breach?

Cohen: The best way to minimise risk following a security breach is to plan ahead: by having an effective incident response and remediation plan, by designating a team to be responsible for leading the response, and by training the team on responding in accordance with the plan.

There are a number of components of an effective incident response plan. The primary goal should be to contain and control the incident, in line with standard technological best practices. Once the incident is controlled, the organisation should preserve evidence and determine the cause, nature, and scope of the incident; analyse the legal implications of the incident; and develop a communications strategy for affected individuals, media, and regulators. Once the dust has settled, the organisation should conduct a post-breach review, assessing what changes should be made to security controls and incident response practices to mitigate future risks

There are a number of steps that an organisation can take ahead of time to make this process go more smoothly. For example, it can pre-negotiate deals with incident response vendors, call centre vendors, and other organisations that can be on call in the event of an incident. It can maintain a list of contractual incident notification requirements, so that it can navigate these more easily during an incident. And importantly, organisations can develop a protocol on when to involve legal counsel in an incident investigation, so that communications about the incident can be subject to the attorney-client privilege.

Fitzsimons: Even before a security breach, measures must be put in place: training so that staff recognise security breaches and know how to react to them, who to report to, how quickly and with what details; and the business should have an appropriate cross-function team identified who will consider and manage the security breach in accordance with a pre-agreed incident plan and procedure. Having those measures in place prior to a breach is fundamental to successful management of a breach. The team and their response must be able to cover an incident 24/7, 365 days per year and depending upon the nature of the business, this may need international support.

The first priority is to isolate the breach and stop it to prevent further intrusion, data loss or damage. The next priority is to try to recover any data lost and/or to lock it down. Following that the team will need more information about the nature of the incident, what has been affected, how and likely consequences. This will drive mandatory and voluntary reporting, as well as communication and PR strategies. Also relevant will be to what extent the business is regulated, who the regulators are and whether there are multiple regulators and to what extent the organisation is deemed "critical" e.g. in respect of national infrastructure.

Cugia: In case of a personal data breach, the provider of publicly available electronic communications services must notify the Data Protection Authority without undue delay. When the personal data breach is likely to be detrimental to the personal data or privacy of the contracting party or another individual, the provider shall also notify the contracting party or the individual of the said breach without delay.

However, the notification shall not be required if the provider has demonstrated prior adoption of technological safety protection measures that may encrypt or render the data unintelligible to any entity having no authorisation to access it and that the said measures were applied to the data concerned by the breach.

Companies should define an incident response plan with detailed procedures to ensure effective orderly response to incidents pertaining personal data and report the personal data breaches immediately to the management. Notification procedures for the reporting of the breaches to competent authorities and data subjects should also include the incidents' response plan, including a list of possible mitigation actions and clear assignment of roles.

Operators should also keep an official file or record of the incidents and personal data breaches along with details regarding the event and subsequent mitigation actions performed, as indicated by ENISA Guidelines.

11. To what extent has a changing technological landscape and professionalisation of cyber criminals altered the way in which information security is delivered?

Cugia: New cyber-attacks involve virtual currencies, DDoS and cloud transfer apps. Attackers are streamlining and upgrading their techniques compromising organisations within minutes.

Operators must secure professionals having cyber security skills and able to manage assets, capable of ensuring coherent and up to date Risk assessment and management performances. Operators must be proactive in best mitigating current cyber threats and developing security models based on agility and evolving dynamics of cyber-threats. This should also include the use of cyber-threat intelligence to assess efficiency and performance of implemented security controls.

12. Has the trend in outsourcing certain security functions and the increasing reliance upon cloud computing and storage made it more challenging to protect private data?

Cohen: The trend toward cloud computing and storage has made more challenging to protect private data in some respects, and in some respects easier.

Inherent in the cloud computing model is distributing control over organisational data, and relying on third parties to maintain the security of that data. Adding additional access points for the data creates a greater attack surface for malicious actors. Risks are also introduced in the transfer of data between the company and cloud provider.

That said, one of key drivers toward the use of cloud providers is the ability of those providers to provide better security, in many instances more cheaply than organisations would be able to secure the data themselves. In that respect, some organisations may increase the security of their private data by utilising a cloud provider or an outsourced security function.

Fitzsimons: Outsourcing, including to cloud providers, may enhance security, bringing state of the art security within affordable reach of businesses who could not otherwise keep up and match that security. Whilst cloud technology has a wide range of benefits, it also carries inherent risks that organisations may not fully appreciate.

Currently, where personal data is being held on behalf of a business by a third party e.g. cloud platform provider, there is a legal requirement to have in place specific contractual obligations with the "data processor" and to ensure adequate safeguard for personal data if transferred outside the EEA, to ensure "matched" security and protection as in the EU. With cloud provision, it can be difficult to understand the multiple sub-contractors involved in provision of the cloud service (who, where and what) and on what terms they have been appointed. As such arrangements have often been put in place before the business buys the service, they will not be tailored to need. Some outsourced/cloud providers are very reputable and provide sensible terms and robust security. Others are less helpful and their terms do not meet the legal requirements imposed on business, or give the necessary insight and comfort on security – even where only dealing with confidential and proprietary information, rather than also personal data.

The obligations on businesses in relation to "data processors" increase under GDPR, both in respect of mandatory terms to be imposed, the fact that they must be imposed on sub-processors and the details required for record keeping and privacy notices. Compliant contracting of cloud platforms will be challenging under GDPR. That said, "data processors" have direct responsibilities and liability under GDPR so their approach to risk and contract terms is likely to change between now and May 2018, although most have not yet made their GDPR stance and suggested terms public.

Cugia: It certainly has. Cloud computing services address many challenges concerning the protection of personal data. Some of the security tasks (such as monitoring, patching, incident response) are generally outsourced, and it is essential that cloud service providers (using economies of scale) implement advanced processes to develop, deploy and maintain software reducing the likelihood of software vulnerabilities, which may become more attractive to attackers/hackers to exploit.

Cloud computing services are consumed and managed via internet connections, and this naturally entails control over infrastructure and adoption of security measures such as firewalls and gatekeepers. This means that customers need to be aware of the risk of network attacks, like spoofing websites, sniffing/eavesdropping network traffic, DDoS attacks, man-in-the-middle attacks, pharming, wiretapping, etc., on the normal end-user interfaces, as well management/administrator interfaces, application programming interfaces (APIs) and in general in the offering of Web services.

13. How is technological innovation – such as drones, wearable devices, cognitive thinking and the Internet of Things ("IoT") – altering the cybersecurity landscape?

Lauderdale: All technological innovations add to the increase in the cybersecurity risk. The technologies being introduced everyday such as drones, wearable devices, cognitive thinking, self-driving vehicles, artificial intelligence and IoT are being purchased for functionality and business benefit. Organisations do not adopt a security posture to the new, innovative technologies in the marketplace causing the vendors of these products to focus on delivering and selling the business benefit and making security an afterthought in their product offerings. When adopting new technologies, it is essential to consider the security upfront and force vendors to deliver value-added "secure" products to ensure the safety and security whilst using these innovative tools and technologies.

Lim: There is no doubt that cybersecurity risks will grow exponentially with the rise of new technological innovations. Consequently, novel approaches will need to be taken to protect data stored and processed by new technology.

The growing use of cloud computing services has risks and benefits in relation to cybersecurity. On the one hand, an organisation will be unlikely to have adequately fulfilled its responsibilities to sufficiently protect its data if does not know where the data it stores in the cloud is located, and who has access to that information. Storing data in multiple locations and allowing more people to access it can also increase the opportunities for information and networks to be compromised. On the other hand, a cloud service provider may have better cyber security protections and monitoring mechanisms than the organisation itself.

Furthermore, the sheer scope and potential of IoT devices will make cybersecurity a significant challenge in this space. In recent times, we have seen massive 'botnets' of unsecure IoT devices launching the largest ever experienced DDOS attacks. In addition, IoT devices may control essential infrastructure or may have access to very sensitive personal information (e.g. home security footage). IoT Alliance Australia acknowledges that this "Critical IoT" may require special attention from a security and resilience standpoint. As many traditional security practices are fundamentally unsuited for use in an IoT context, IoT Alliance Australia calls for 'security by design' and support of end-to-end architecture in order to protect the valuable information IoT devices collect now and into the future.

Finally, legislators, industry stakeholders and end-consumers are currently trying to build the regulatory foundations for Australia's growing drone market. The Senate inquiry into drones held on 16 March 2017 saw support for a drone registration system coupled with an app. This will no doubt connect the data collected by drones with live online platforms. With drone use in Australia rising rapidly each year, if such live data was hacked, there would be an abundance of private information in the form of drone videos and images that may be compromised. With a stable regulatory framework yet to be developed, there is still much to consider when it comes to data security in this rising market.

Cohen: The key technological innovation impacting the cybersecurity landscape is the proliferation of Internet-connected devices in the IoT. Consumers often prioritise convenience and speed over cybersecurity, so in many cases IoT products often go to market without basic security controls. For example, the Mirai malware searches the internet for and compromises Internet-connected devices running outdated versions of certain operating systems – such as security cameras and DVD players – and uses those compromised devices to launch attacks on others.

In the near future, many of the electronic devices that we use on a daily basis – and that will be incorporated into the modern workplace – will be connected to the internet. If these devices are not appropriately secured, or can be used to penetrate corporate networks, they will lead to a weakness in cybersecurity protections overall, particularly if there are no non-internet-connected options available.

Fitzsimons: Smart technology is being developed, plugged into systems and implemented at a rapid rate – which has not always allowed for the full security implications to be considered or addressed. In many cases, security considerations have not been a high priority since businesses have assumed that details obtained are not "personal" and have minimal if any privacy impact.

Unfortunately, regulators disagree and believe that the data collected by a great deal of smart technology has privacy implications and may often involve the collection and use of personal data, such as from metadata about usage and/or location.

Adding so many components, devices and interfaces to systems necessarily increases the potential routes into systems and increases potential security vulnerabilities. The risks of this should not be underestimated.

Cugia: M2M and IoT are rapidly developing in Italy, also in light of the infrastructure developments on the Smart electricity grid and parallel investments on the communications last mile. The relevant cyber security landscape is still to be defined, particularly on the obligations pertaining to cache memories of interconnected devices in the collection, exchange and processing of data dynamically adapted to the different contexts

The increase of data exchange and the offering of multiple services and assets leads to a higher degree of interaction and data storage by processors, along with general automation. As several critical services become interconnected, the need for cyber security surges to protect data exchanges, privacy as well as the health and safety of citizens. In this context, threats appear to be multifaceted and directed against information/data, applications and technology but also organisational structures

Particular emphasis on this topic has been raised by the Data Protection Authority, specifically on M2Ms able to impact on user's life and safety, and on fundamental issues pertaining to integrity, authenticity, confidentiality, non-repudiation and accountability of data, data aggregation connectivity and smart processing.

The most used countermeasures against information breaches and safety threats include digital access controls to data and networks, implementation of organisational and operational procedures and guidelines, disaster recovery and maintaining back-ups and monitoring for hardware/software faults, along with security by design.

14. What can we do to combat the security risks and challenges created by technological innovation? How do we balance innovations with cybersecurity and privacy risk exposures?

Fitzsimons: Security – especially of personal data and other higher risk data – should be considered from the outset and at every stage of the design and development of technological innovation. The process should determine whether the collection and use of data envisaged is lawful, necessary and proportionate to need. The amount and sensitivity of data involved should be assessed: has this been minimised and why is it essential? Could it be encrypted? The potential impact on individuals from the proposed technology should be considered and mitigated. In every aspect, the risk of attack and exploitation should be considered, addressed and engineered out completely or as much as possible and appropriate.

Privacy by design and default is a mandatory GDPR obligation from May 2018 but buyers of systems and products will be looking for comfort on compliance now if systems and products are to be used post May 2018. Businesses can address these issues by impact assessments throughout the design process.

Cugia: Security risks have much to do with international cooperation in adopting adequate measures against cyber-threats. Domestic information security protection may serve up to a certain point.

In recent years, Italy has been target to a growing of cyber-attacks and threats (one of which, a domestic criminal attack against the national institutions with automated transfer of data to foreign data banks, is still pending in its preliminary investigations as we go to print). Such threats have prejudiced strategic and critical national infrastructures, along with enterprise assets and financial and personal data of citizens.

A crescent voice in the national balance has to do with information security. On the other hand data protection is interpreted as a fundamental freedom of individuals. Balancing these divergent objects is a complex endeavour, considering the needs of all concerned parties related to security, privacy and surveillance requirements, both at national and international levels. Privacy vs. national security is an uncertain battle as never before.

We will see in the near future how different nations will interpret cyber-security policies and reshape privacy rights or limitations, in view of national security and surveillance rights.
In general, international governance of the Internet is still to be defined, and nothing should be taken for granted at this state of the art.

Censorship functions and control of massive traffic streams/bandwidths is still on top of the international agenda, and political developments show a trend towards de-globalisation.

Emerging commercial interests demonstrate willingness to rather weaken cyber-security and privacy. The existence of heterogeneity in security and privacy regulations is seen as an obstacle for service provisioning crossing geographical borders.

We will see how all this will boil down with respect to coexistence and balance between privacy and national cyber-security.

15. Who or what is the main threat to a company's security?

Lauderdale: (i) Negligence and or incompetence, (ii) Human error, (iii) Improper management of security controls, (iv) Lack of training, (v) Lack of accountability, (vi) Lack of standards, (vii) Lack of policy and governance, (viii) Lack of metrics, (ix) Poor security testing, (x) Reactive planning vs. Proactive planning.

Cohen: The main threat to a company's security is its personnel; and not necessarily intentional, insider threats. Even the best cybersecurity protections can be overcome if they are not set up properly, or if personnel do not comply with company policies and procedures.

Cybersecurity threats are constantly evolving, and bad actors look to take advantage of unsuspecting or naïve employees. For example, there has been an increase in phishing threats over the last few years, through which hackers seek to induce employees to click on a malicious link or open an infected attachment, which permits the hackers to compromise the network. Cybersecurity controls are often circumvented or ignored for convenience. For all of these reasons, it is imperative to train personnel on cybersecurity policies and procedures, and to refresh that training on a regular basis, in particular with respect to key threats.

Cugia: Poorly designed, implemented and/or maintained hardware and software components can pose serious risks to information security. According to ENISA, physical damage/theft/loss is considered one of the main reasons for data breaches and information leakage: device losses – such as laptops and USB drives – account for ca. 40% of confirmed data breaches.

The impact of this threat is achieved by low protection levels in end devices. Apparently, the exposure to this threat is still not being recognised in the way it presently demands, both by end-users and organisations, although protection by means of storage encryption would suffice to mitigate the risks emanating from data breaches. This threat will continue to bother users and organisations alike: IoT devices/tokens will also be subject to losses/theft. Moreover, unprotected IoT information on mobile devices will increase the impact of theft/loss. Given the increased number of mobile devices, securing the perimeter will keep being one of the challenges of cyber-security professionals. Device users will need to be more vigilant when purchasing and using mobile devices and gadgets.

In addition, when the processing is performed by external contractors, the organisation may lose partially the control over these data. It is important for the organisation to select contractors that can offer a high level of security and to clearly define what part of the processing is assigned to them, maintaining as much as possible a high level of control. In that sense, integrity implies maintaining the consistency, accuracy, and trustworthiness of information, over its entire life cycle. Data must not be changed in transit and measures must be undertaken to ensure that data cannot be altered by unauthorised individuals, entities or processes.

From a practical point of view, this means that data cannot be modified in an unauthorised or undetected manner.

> *"The most common cyber-attack types for financial sector and ICTs appear to be Distributed Denial of Service (DDoS) and malicious insiders, with the latter affecting also public administration/government sectors."*
>
> *- Fabrizio Cugia di Sant'Orsola*

16. Which industries are at highest risk for threats to their cyber security?

Lauderdale: (i) Banking or Financial Institutions, (ii) Government, (iii) Universities, (iv) Health Industry.

Cugia: In general, the most affected CII sectors seem to be financial, ICT and energy, which have the highest incident costs. The best data related to cybercrime comes from the financial sector, which is regulated and pays serious attention to cybersecurity.

The most common cyber-attack types for financial sector and ICTs appear to be Distributed Denial of Service (DDoS) and malicious insiders, with the latter affecting also public administration/government sectors. The most costly attacks are considered to be insider threats, followed by DDoS and web based attacks.

According to the European Commission, a recent survey of PWC, titled "the Global State for security Survey 2016" shows that at least 80% of European companies have experienced at least one cyber security incident over the last year and the number of security incidents across all industries worldwide rose by 38% in 2015.

17. What key trends do you expect to see over the coming year and in an ideal world what would you like to see implemented or changed?

Lauderdale: (i) Two-factor authentication, (ii) Bio-metrics identification, (iii) Proactive risk management planning, (iv) Artificial Intelligence cyber security tools.

Lim: It is clear that there are growing concerns surrounding data breaches, particularly with recent high profile information security incidents. With this, along with new legislative reforms, it is expected that more and more companies will report cyber risks in annual reports and in disclosure documents. In the past, AMP Capital found that in a spot check of 55 company annual reports from 2014, only seven referred to cyber risks. Going forward however, hopefully these gaps in reporting will cease to continue, and reporting would be consistent across industries so that investors are able to accurately assess a company's risks, including its cyber risks. The 2017 ASX top 100 Health Check, which is due out soon will also provide further information into the cyber readiness of Australia's top listed companies.

We expect that there will be a greater focus in the next 12 months around collaboration, cooperation and threat-sharing between government and business, and between business and business (across and within sectors). This is something we encourage and support strongly.

Vidal: Companies have started to come to terms with the fact that in order to comply with all the regulatory requirements, it is necessary to modify a lot of the established procedures and above all, how things are done compared to how they were done before.

The new regulatory trend grants more power to the users and gives them the tools to decide where they want to be and what they want to do with their data.

Any procedure, new campaign, new launch/product will require privacy risk analysis; therefore, in the coming years, we will become accustomed to seeing companies with increasingly specialist privacy and information security teams.

Cugia: Cyber threat intelligence and threat analysis have gone through significant developments regarding improvement of methods, further elaboration of good practices and adoption/implementation of paths. The trends will be an increase of awareness concerned cyber security and implementation of major security measures, taking also into account the future GDPR.
This trend will need to ensure coordination between operational security and business activities. Bridging threat intelligence and risk management is a crucial point for success. Business people and in particular decision makers, need to understand how threat intelligence will help them to mitigate business risks. In the next years Italy as other Nations will invest much in generating new services and functions that will also be made available in the civil market and in education. Cyber-defence is going to engage/attract available CTI capabilities and resources, and this will secure a competitive advantage of the system on availability of services and development of new protective measures, much to the avail also of foreign investments in crucial services such as financial services, IoT and e-commerce.