VIRTUAL ROUND TABLE

CorporateLiveWire

Cyber Security 2014

MEET THE EXPERTS

James Bowden - Afridi & Angell
T: +971 4 330 3900
E: jbowden@afridi-angell.com
W: www.afridi-angell.com

James Bowden is a senior associate with Afridi & Angell's Dubai office. His practice includes corporate and commercial, mergers and acquisitions, technology outsourcing and employment matters. He advises on and negotiates technology and business process outsourcing agreements, as well as associated data, privacy and risk management issues. James was previously in-house counsel with one of Canada's leading technology outsourcing companies. He also practiced in the Toronto office of a large global law firm. He obtained an LLB from Queen's University in Ontario, Canada and is admitted to the Ontario Bar.

Christian Schroeder - BDO Legal Rechtsanwalts mbH
T: +49 211 1371 305
E: christian.schroeder@bdolegal.de
W: www.bdolegal.de

Dr Christian Schroeder is the head of BDO Legal's IP/IT practice group which closely cooperates in particular with Frank Wißing of BDO AG's IT Advisory Services. Frank Wißing contributed to this round-table by providing the IT security related answers.

Dr Schroeder has many years of experience advising clients, including US and UK headquartered multinationals on IP, IT issues with a special focus on data protection matters. He also interned with the German Federal Data Protection Commissioner and Electronic Privacy Informational Centre in Washington, D.C.. Dr Schroeder's PhD-thesis on comparative US-American and German data protection law won a scientific award from the German Institute for Data Protection and Data Security (GDD). He is Scientific Board Member of Germany's major data protection journal, Zeitschrift für Datenschutz.

Steven Brower - Buchalter Nemer
T: +1 714 549 5150
E: sbrower@buchalter.com
W. www.buchalter.com

Steven Brower is a Litigation Partner in the Orange County, California office of Buchalter Nemer. Concurrent with his time at UCLA (both undergraduate and law school) he was a computer programmer. As a result of that experience he has been involved with legal matters relating to computer technology, cyber-security and e-discovery (including insurance coverage for those risks) for over 35 years. Mr. Brower was possibly the first public user of the internet, having gained regular access in 1973. He was interviewed by "60 Minutes" on matters related to computer security in 1983. He was credited as being the first attorney to ever get a civil injunction under the Computer Fraud and Abuse Act (18 USC § 1983). He has represented both vendors and customers in the hardware and software fields.

Kelly Frey - Dickinson Wright
T: +1 615 620 1730
E: kfrey@dickinsonwright.com
W: www.dickinsonwright.com

Kelly Frey is a member in Dickinson Wright's Nashville office. His practice focuses on the areas of corporate transactions, information technology, and corporate compliance. Mr. Frey is one of less than 10 attorneys in private practice to be inducted as a Fellow into the World Technology Network (selected by over 1000 internationally recognized experts and futurists who are current Fellows for innovative work recognized to be of "the greatest likely long-term significance" in technology law) and has been a co-inventor on business process patents for Fortune 100 financial services clients for systems designed to mitigate risk and is listed in Best Lawyers in America and Super Lawyers for Information Technology and Technology Law.

Francoise Gilbert - IT Law Group
T: +1 650 804 1235
E: fgilbert@itlawgroup.com
W: www.itlawgroup.com

Francoise Gilbert is the Founder and Managing Director of the IT Law Group (www.itlawgroup.com), a niche law firm that focuses on

MEET THE EXPERTS

information privacy and security, cloud computing, and data governance, and represents a wide range of global or publicly held companies and selected start-ups. An internationally recognized thought leader and expert in privacy and data protection law, Francoise has been named Best Lawyers' "2014 San Francisco Lawyer of the Year for Information Technology Law." For several years, the prestigious Chambers USA and Chambers Global, The Best Lawyers in America, and the Who's Who in E-Commerce have recognized her as one of the leading lawyers in the field of information privacy and security. She was listed as one of the top privacy advisers in the recent Computerworld "Best Privacy Advisers" list, and for several consecutive years as been selected by Ethisphere for its list of the "lawyers who matter."

James Bowden - Afridi & Angell
T: +971 4 330 3900
E: jbowden@afridi-angell.com
W: www.afridi-angell.com

James Bowden is a senior associate with Afridi & Angell's Dubai office. His practice includes corporate and commercial, mergers and acquisitions, technology outsourcing and employment matters. He advises on and negotiates technology and business process outsourcing agreements, as well as associated data, privacy and risk management issues. James was previously in-house counsel with one of Canada's leading technology outsourcing companies. He also practiced in the Toronto office of a large global law firm. He obtained an LLB from Queen's University in Ontario, Canada and is admitted to the Ontario Bar.

Christian Schroeder - BDO Legal Rechtsanwalts mbH
T: +49 211 1371 305
E: christian.schroeder@bdolegal.de
W: www.bdolegal.de

Dr Christian Schroeder is the head of BDO Legal's IP/IT practice group which closely cooperates in particular with Frank Wißing of BDO AG's IT Advisory Services. Frank Wißing contributed to this round-table by providing the IT security related answers.

Dr Schroeder has many years of experience advising clients, including US and UK headquartered multinationals on IP, IT issues with a special focus on data protection matters. He also interned with the German Federal Data Protection Commissioner and Electronic Privacy Informational Centre in Washington, D.C.. Dr Schroeder's PhD-thesis on comparative US-American and German data protection law won a scientific award from the German Institute for Data Protection and Data Security (GDD). He is Scientific Board Member of Germany's major data protection journal, Zeitschrift für Datenschutz.

Steven Brower - Buchalter Nemer
T: +1 714 549 5150
E: sbrower@buchalter.com
W: www.buchalter.com

Steven Brower is a Litigation Partner in the Orange County, California office of Buchalter Nemer. Concurrent with his time at UCLA (both undergraduate and law school) he was a computer programmer. As a result of that experience he has been involved with legal matters relating to computer technology, cyber-security and e-discovery (including insurance coverage for those risks) for over 35 years. Mr. Brower was possibly the first public user of the internet, having gained regular access in 1973. He was interviewed by "60 Minutes" on matters related to computer security in 1983. He was credited as being the first attorney to ever get a civil injunction under the Computer Fraud and Abuse Act (18 USC § 1983). He has represented both vendors and customers in the hardware and software fields.

Kelly Frey - Dickinson Wright
T: +1 615 620 1730
E: kfrey@dickinsonwright.com
W: www.dickinsonwright.com

Kelly Frey is a member in Dickinson Wright's Nashville office. His practice focuses on the areas of corporate transactions, information technology, and corporate compliance. Mr. Frey is one of less than 10 attorneys in private practice to be inducted as a Fellow into the World Technology Network (selected by over 1000 internationally recognized experts and futurists who are current Fellows for innovative work recognized to be of "the greatest likely long-term significance" in technology law) and has been a co-inventor on business process patents for Fortune 100 financial services clients for systems designed to mitigate risk and is listed in Best Lawyers in America and Super Lawyers for Information Technology and Technology Law.

MEET THE EXPERTS

Scott Ganow - Faruki Ireland and Cox P.L.L.
T: +1 937 227 3716
E: sganow@ficlaw.com
W: www.ficlaw.com

Scot Ganow is an attorney in the Dayton, Ohio, office of Faruki Ireland and Cox P.L.L. With ten years of corporate and compliance experience in Fortune 500 companies prior to becoming an attorney, Scot has a diverse background in information privacy and security. A former chief privacy officer for healthcare and pharmaceutical informatics companies, Scot also holds the Certified Information Privacy Professional certification. Scot's practice at Faruki Ireland and Cox P.L.L. involves all aspects of information privacy and security compliance to include policy development, risk analysis, third party agreements, incident response/data breach management and de-identification of personally identifiable information.

Rosemary Jay - Hunton & Williams
T: +44 (0) 20 7220 5753
E: rjay@hunton.com
W: www.hunton.com

Rosemary Jay is a senior attorney at Hunton & Williams with over 25 years' experience in privacy and data protection law. She is recognized as one of the top lawyers in the area in the UK. Rosemary is author of Sweet & Maxwell's Data Protection Law & Practice, a contributing editor to The White Book on data protection and an editor of the Encyclopedia of Data Protection and Privacy. She has worked with the Council of Europe, the European Commission, the Commonwealth Secretariat in West Africa and has advised non-EU states on the adoption and drafting of privacy laws. Rosemary speaks frequently and is a regular contributor to journals, conferences and workshops, as well as participating on a number of advisory committees in the area of privacy and data protection.

Olga Finkel - WH Partners
T: +356 20925100
E: olga.finkel@whpartners.eu
W: www.whpartners.eu

Olga Finkel is regarded for her vast experience in advising on electronic and info-security matters. She has advised both private entities and government bodies. She also acted as an appointed expert for the European Commission on legislative development in e-security, and designed and delivered workshops on e-security and data protection organised by the Commonwealth for the public sector of various Commonwealth countries. She has also recently been assigned as an expert in a current EU study on e-privacy. She has been selected as one of the best 400 lawyers in electronic commerce and internet law by Who's Who Legal.

Olga is a Malta qualified lawyer with an MSc in Information Technology. Her relevant professional memberships include the Society for Computers and Law (UK), the International Technology Law Association (USA).

Michael Hopp - Plesner
T: +45 29993014
E: mho@plesner.com
W: www.plesner.com

Michael Hopp, Attorney-at-law, has been with Plesner since 2000 and is a partner in Plesner's TMT group. He is specialised in data protection, marketing law, e-Commerce and consumer protection, and is responsible for Plesner's work in these areas. Together with his team, he advises on contentious as well as non-contentious matters. Within data protection, Michael has advised clients for the last 10 years across a wide range of sectors. He works with providers of internet services, consumer goods, consumer appliances and has strong experience in data protection matters related to the life sciences industry.

Cyber Security 2014

Cyber Security has presented itself as a major thorn in the side of many companies in recent years, which has demanded firms go the extra length to mitigate any potential risks. In this Roundtable we take a look at some of the trends of the past year as well taking a look at what the future holds. Nine experts from around the world have come together to offer opinion on the prevalent issues surrounding the topic.

1. Have there been any recent changes or developments relating to privacy and regulation in your jurisdiction?

Schroeder: Two recent court decisions will likely have a significant impact on German privacy law:

The Federal Labor Supreme Court recently ruled that a breach of data protection law by an employer might lead to the inability to use evidence gained against an employee in, for example, termination proceedings. Such a strict "fruit of the poisonous tree doctrine" was not common under German law before. As a result, internal investigations now have to even better focus on data protection compliance.

The European Court of Justice (ECJ) declared the Data Retention Directive (Directive 2006/24/EC) to be void. The Data Retention Directive provided that "providers of publicly available electronic communications services or of public communications networks" (i.e. telecommunication carriers including internet providers) had to retain traffic and location data as well as related data necessary to identify the subscriber or user for a period of at least six months. The purpose of this directive was to harmonise the retention schemes within the EU and to ensure that the retained data were available for the purpose of the prevention, investigation, detection and prosecution of serious crime. The ECJ now ruled that by requiring the retention of the afore mentioned data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data which are guaranteed under the Charter of Fundamental Rights of the EU. In Germany, the ruling has no direct impact on private businesses as there was no valid implementing law that required data retention. The Federal Constitutional Court in Germany had declared the implementing national law to be unconstitutional already in 2010. In other EU countries, data retention implementing laws may have to be revised. In addition, the ECJ's ruling will likely put more burden on the EU to better protect EU citizens' data against eavesdropping by other countries. The ECJ's ruling will thus not ease the current political and legal data privacy issues between both sides of the Atlantic.

Ganow: In the United States, we recently had a significant court decision (FTC v. Wydham) concluding that Section 5 of the FTC Act gives the Federal Trade Commission authority for data protection compliance issues ranging from a company's failure to follow its posted privacy policies to a failure maintain adequate safeguards against data breach. This is really not so much a change as a "affirmation" of the FTC's authority in data protection matters. If they haven't already, companies that collect, use, transfer and store personally identifiable information or sensitive information need to get familiar with FTC guidance and prior complaints and consent decrees.

Jay: The importance of up-dating the legal framework to deal with both privacy rights and security threats has been recognised at EU level. Currently the EU is in the process of legislating in both areas; a draft regulation on data protection is going through the legislative process as is a draft directive regarding network and information security. These are both important developments. However, as we know, laws take time and these are both contentious area with many different interests and views to be reconciled. Equally cybercrime and security risk is a fast-growing threat and needs responses now. In the UK the Government published its Cyber Security Strategy in 2011 and has been working towards achieving that strategy employing a range of activities. One of the most recent was the launch last year of the information-sharing partnership on cyber security in which government and industry exchange information on threats and vulnerabilities as they happen. Other initiatives have included addressing the need to develop more expertise by encouraging and training more young people in this area, and the launch of the Cyber Essentials Scheme, a cyber-security certification scheme available to organisations operating in the UK.

Gilbert:

- January 2014 – California Bill AB 370 regarding Do Not Track disclosures became effective
- February 2014 – NIST Cybersecurity Framework

- March 2014 – EU Parliament vote in favor of the Albrecht Draft of the European Data Protection Regulation
- April 2014 – Determination by the European Court of Justice regarding the validity of the 2006 EU Data Protection Directive
- May 2014 – European Court of Just Ruling regarding "right to be forgotten."

Hopp: No, the rules regarding data security have been the same for a long period of time.

2. Are we becoming over-reliant on cloud computing?

Schroeder: We do not expect such a development. Cloud computing is a new technology with still often rather intransparent technical structures and service descriptions. In addition, almost daily reports on new cybercrime assaults do not increase the confidence in cloud technologies. For this reason, from our experience companies are actually very careful with putting critical data into the cloud.

However, cloud computing has also clear advantages: Cloud Computing Providers are often able to offer secure cloud services for a rather competitive price. In addition, a high availability rate of 99.99% is not uncommon. We thus do not see an over-reliance on cloud computing. In fact, we even encourage our clients to explore cloud computing options if the security offered and the possible threats are carefully weighed against each other.

Bowden: I would have expected the opposite question. We are far from over-reliant on cloud computing. Cloud computing is being adopted at an increasing rate as organisations become more comfortable with the security and reliability of the pieces of hardware and software that collectively make up the "cloud". The legal risks that are typically associated with cloud computing relate to this perception that there is no way to control the location of your data and the security features protecting it at every stage of its movement, storage and processing, which is (or has been) a serious misconception. There is growing acceptance that the "cloud" is a perfectly controllable, transparent environment that is serviced by reputable providers. Reliance on cloud services will increase rapidly in this region, as it should.

Brower: Although there are good reasons to worry about security and control in "the cloud," the recent major security breaches have generally involved "non-cloud" systems. The message is that security (both initial and ongoing) needs to be a major part of both planning and on-going operations. The additional challenge with cloud based systems is that verification of security-based policies and procedures (which includes backup) is so much more difficult to control, since the vendor might not even be willing to allow physical audits. And many companies, while appreciating the savings potentially available from cloud-based solutions, are reluctant to allocate the resources involved in an off-site audit, especially where it might be in another country, even though that is really part of the "cost" of a cloud-based system.

Ganow: I don't think we are overly reliant so much as it has become a necessity in the face of economic and competitive pressures on companies today. Cloud computing, while not perfect, has come a long way in the past decade. But, in the end, it is a risk to be managed like any other. Similar to the manner in which companies need to complete risks assessments, draft solid agreements and conduct audit compliance. They likewise need to exercise due diligence to balance the gains of cloud technology with the risks and deploy sound data classification and segregation regimes.

Jay: We have to be careful not to be too simplistic here. Cloud can offer serious advantages in terms of flexibility and cost. We should not assume that cloud is an insecure solution as some cloud solutions apply high levels of security. While there are some key differences between cloud computing and traditional out-sourcing many of the security risks associated with cloud also apply to traditional out-sourcing. The important point in any use of a third party service provider is to carry out a very focussed risk assessment and due diligence exercise. If you are going to out-source the processing of personal data and you are using a third party processor, the Data Protection Act requires you to choose one that offers adequate guarantees of security.

Gilbert: Cloud computing offers tremendous capabilities that have the potential to make companies more efficient and to give access to sophisticated computing powers to more entities than ever before. However, the tool presents numerous challenges. For example, while many companies are reputable, financially stable, and have adequately trained personnel, other organisations may lack competence, be financially unstable, or provide little or no training

or supervision to their staff.

Pressured by the lure of financial savings, some customers rush to the cloud without having conducted a proper risk assessment, evaluating both their internal risks in entrusting their data to a third party, and the risk inherent to the service provider, which itself may be vulnerable to cyber attacks or the acts of disgruntled employees. In this case, they may transfer to the cloud too much data (e.g., sensitive data that should be kept internally), too soon (e.g., without proper due diligence) or too lightly (e.g., without proper contractual protection).

Hopp: Companies storing and handling vital business information, customer databases and business records electronically are highly dependent on cloud computing. The advantages of handling a wide range of business information using cloud-computing are obvious. On the other hand the electronic data may compromise confidential business information, and the disclosure of such information to competitors may be fatal. The handling of big data and use of cloud computing is, in my opinion, not to be limited, and that makes the cyber security issue even more vital.

3. What are the main cyber security trends we should be keeping an eye on in 2014?

Brower: Years ago there was substantial attention paid to "teenage hackers." Those of us with experience said then, and continue to say now, that the most significant risk is not from immature vandals, but from people who are making serious efforts to obtain an unlawful financial benefit. Companies (and individuals) need to put significant effort into protecting those portions of the cyber resources which could provide financial gain to others or financial harm to themselves. I predict that we will see a "major" company go out-of-business as a result of a cyber-attack which was intended not to produce financial gain, but which was actually intended to cause financial ruin. And the recent demise of Mt. Gox (the bitcoin trading company) may just be such an example.

Frey: I see three main trends in cyber-security evolving this year:

First, I think that 2014 will be the year where the general public finally comes to the realisation of what technologist always knew – the internet was never designed for security. The internet was designed for redundant communications and all of the various security protocols that have been added to make the internet more secure are merely an exercise in "plugging the holes in a leaking basket." That is not a negative or fatalistic comment – it merely recognises that we live in an insecure digital environment and we have to accommodate to that. Starting with an expectation that breaches will, of a certainty, occur creates a context in which we can more effectively and methodically establish control processes that will better protect us and our data.

Second, cyber-threats are becoming much more organised. "Hacking" has become almost a naïve expression of the threats we face in the digital environment. The term hacking conjures up images of an underage misanthrope or socially inept loner in the wee hours of the morning up to mischief. Such images totally misrepresent the most common and severe threat profiles evolving in 2014. Organised crime and governmental entities have made cyber-breaches a permanent part of their repertoire. Cyber-breach teams numbering in the hundreds are currently at work, full-time, looking for and exploiting bugs in devices, software code, communications protocols, and network connectivity. If you have anything of value, digitally, governments and professional criminals will be making concerted efforts in 2014 to find and exploit such value.

Third, cyber-security is no longer just the province of Information Technology ("IT") specialists, but rather has become a board level and C-suite topic. While IT may have the substantive knowledge re technology threats and methods to deal with and remediate those threats, cyber-security threats are enterprise-wide threats to operational integrity and cash flow, to be dealt with at the highest levels of companies. One clear indication of this trend in escalation up the corporate decision-making ladder is the release of the US Securities and Exchange Commission guidelines for disclosure of cyber-security breaches (elevating the threats from technological concerns to disclosures related to the basic economics underpinning the capitalisation of publicly traded companies and how such economics can be jeopardised by cyber-breaches).

Jay: We need to keep focussed on the big threats from criminal and terrorist networks. There are fashions and fads in security worries as in every area. For example in the past twelve months we have seen companies expressing concern that US entities may be vulnerable to notices from US Government Agencies in some circumstances, partly

as a result of heavy press coverage. This has resulted in reluctance to use the services of those with US operations.

We would say however that , although there is some risk, it should not be over-blown. The U.S. legal framework contains substantial restrictions on the government's ability to collect private data and the risk can be assessed and managed, including by ensuring the legal arrangements around control of information between US and non-US companies are addressed. In addition, in part due to the extensive press on U.S. government data collection, the White House and some members of Congress are attempting to significantly curtail U.S. government data collection.

Gilbert:

- Effect of the NIST Cybersecurity Framework
- Effect of the Target breach of security

Hopp: In the wake of the recent data breach cases and the increased media focus on cyber security, more and more companies acknowledge the need for data protection. National politicians and the EU politicians focus on privacy issues and their push for better data protection, meanwhile an increasing number of private persons require companies to provide a certain level of data security. All together it builds up awareness of the need of cyber security.

That awareness from private persons and the politicians is going to be a trend to keep an eye on in 2014.

Finkel: One should always strive to be several steps ahead of up-and-coming security risks. I believe that the main emerging threats are social engineering attacks that use social networks like Facebook where an innocent looking friend or connection request can be the prelude for a social engineering scam; advanced persistent threats (APTs) and precision targeted malware where long term quiet attacks are used to gain unauthorised corporate network access and steal information, a small chunks at a time, of over a long period of time (and therefore more difficult to detect); internal threats due to malicious users and the increase in usage of personal smartphone devices for both work and personal uses; and attacks that focus on vulnerabilities in HTML5 browsers.

4. Can you outline some of the more successful measures firms are taking to mitigate risks?

Bowden: Each organisation will have different requirements. A self-assessment process is a good starting point. There are excellent providers available who can provide this service. Whichever technical solution an organisation decides is best for its needs, the following are some well established measures that are highly effective for risk management:

- *Appoint a Technology/Security Officer:* In order to effectively implement a new policy or procedure, most organisations will require a single individual who is responsible to ensure that the new policy or procedure is followed, or else it will likely be ignored.
- *Policies:* Take the time to develop good, practical policies relating to IT usage, including in particular employee use of personal devices for work, controlling access via any device that access your organisation's systems, network security, encryption practices, password usage, etc. Ensure the policies are followed. Spend time and money doing it right as it will be resisted, like any organisational change.
- *Clear Response Plan:* Have a clear, step by step plan which sets out how the company will respond in the event of a data security breach. For breaches of any significance, a quick reaction is usually critical from the perspective of damage and reputation control. A plan that has been approved in advance permits a company to respond quickly. Damage control is extremely important after a breach occurs.

Ganow: Firms have to realise they are a tantalising "one stop shop" for cyber criminals seeking to hit a mother load of information in one hack because such firms have the information for multiple clients in one location. Any firm or business has to implement the appropriate administrative, physical and technical safeguards to safeguard information. These firms know where their data is (data mapping) and what comprises their data (data classification). They control access to such information on a need-to know basis (role-based access) and regularly track such use (audit). Enterprise-wide, these firms also implement layered security measure, or "security in depth" to provide redundancy in these safeguards.

Gilbert: Risks can be divided into internal risks and external risk. Internal risks are those that are connected with acts or failure to act by individuals.

Cybersecurity risks caused by employees can be reduced with proper training and monitoring of personnel activities. It is important and useful to take the time to properly train staff and raise their awareness of the known and potential risks. Further, internal incidents

may be caused by disgruntled employees. In this case, the company management and the Human Resources Department play an important role in identifying and promptly addressing the problems.

It may be more difficult to anticipate and prevent attacks by outsiders. Companies have been able to protect against external attacks through their participation in special interest groups, networks, or communities, where they exchange tips and information or alert each other. In all cases, of course, appropriate technical, physical, and administrative measures are always useful, to the extent that they are actually applied, updated as needed, and their efficiency and efficacy test periodically.

Hopp: Drafting of guidelines, best practices or a Personal Handbook might be some of the means to mitigate the risk of employees committing data breaches - and after all, a significant part of the data breaches are simply due to the lack of awareness and compliance on a personal level amongst the ordinary employees.

Furthermore companies should have a strict policy on which employees are granted access to what data. Access should be granted to the relevant employees only and may be limited to certain types of data. Technical limitations on deletion, editing, printing and forwarding data may also be necessary safety precautions. As always, the most simple data security measure is a well-drafted data retention policy, which is applied effectively. Once superfluous data has been deleted properly, it is no longer a security risk. It may sound simple, and it is, but it is still a fact that many data security breaches, internal as well as external, concern data that should have been deleted.

Finkel: Risks can be mitigated by having a data-centric governance plan that evaluates the employees' roles and their data needs and maps them to data types and virtual machines, therefore limiting the rights strictly on the need-to-know basis. The business context is also important: identifying the paths of information utilisation within the organisation, the weakest link in the internal procedures and understanding a profile of likely attackers is vital to take the appropriate security control options. Knowing your data users thoroughly and monitoring suspicious data access behaviours also allows security resources to be used in the most effective way.

5. Are there any case studies that highlight standards of best practice?

Bowden: In terms of legal risk and contracting practices, I often direct clients to the Cloud Security Alliance website for a good starting point on what they should be looking for in their contracts, key issues and risks, etc. Some best practices are also suggested here. Ultimately, an off –the-shelf list of practices will suit no one perfectly. Take advice from professionals who can help design practices that work best for your organisation.

6. If you were newly in charge of cyber-security at a financial institution, what would be your first priority?

Frey: I would try to transform the institution from an absolute to a relative perspective on cyber-security and cyber-breaches. At the institutional level, cyber-security is much more than just following IT guidelines for patches, updates, and bug fixes and reporting on the quarterly success of following industry standard practices (all of which are minimal requirements for sustaining institutional value and integrity). What is needed is a dashboard that will allow all stake-holders across the institution to evaluate the impact of gaps in digital security and that appropriately escalates issues up the organisational structure and adequately informs decision-makers in real time. For example, an institution's stakeholders could decide that there are six metrics related to decision-making on cyber-threats: business impact (impact across the institution on operations), organisational impact (number of institutional impacts and level/number of users affected), qualitative impact (impact to reputation, brand, or stock value); financial impact (financial result of a cyber-failure), contingency plan (relative jeopardy which the failure would have on mission/business continuity), and data quality (amount of digital degradation resulting from a failure). Each of these could be scored on a linear scale. Total scores on all of these metrics above a threshold (or scores above an institutionally approved value for any single metric) could result in differential workflow routing within the organisation. Where severity and risk are high (as indicated by the objective metric score), the board and C-suite executives are informed by real-time alerts and participate in resolution through real-time messaging (fulfilling their fiduciary duty to inquire and be informed). Where severity and risk are both low (once again, as indicated by an objective metric score), IT will handle on a routine basis and report up the chain

only as needed. Such transformation takes an institution from being reactionary to proactive in dealing with the inevitable cyber-threats that will occur.

Ganow: While I would look to PCI-DSS, Gramm Leach-Bliley, the Fair Credit Reporting Act, and other laws for general guidance, my approach would be the same no matter the company. First, I would want to understand exactly what kinds of data my institution held (data categorisation) and exactly where that data was stored and accessed (data mapping). You really cannot implement a new cybersecurity plan or improve an existing one until you know these things. Now, this may seem remedial and overly simplistic to many. However, in my experience and as so many data breach stories have shown over the years, many times the violated entity did not understand where its sensitive information was and therefore had inadequate safeguards in place.

7. Can companies adequately protect themselves against cyber threats without devoting significant expense and human resources to security?

Schroeder: In most companies, the majority of business processes are supported by IT. An efficient IT is even often a necessity for any modern and effective business operation. Thus, almost all companies are heavily reliant on information technology which - on the other hand - entails a certain vulnerability as towards cyber attacks. An appropriate IT security requires an effective security management with appropriate concepts and efficient IT security measures. Developing and maintaining such a security management requires the deployment of either adequate in-house or external personnel and also significant expenses. Such expenses are unavoidable. However, if such measures are applied based on a good risk assessment and in accordance with modern IT standards, the costs are not excessive. In addition, when assessing the costs, one also has to look at the benefits of an efficient IT for the business.

Bowden: The expense does not need to be crippling, but it does need to be realistic for today's environment, and it needs to be continuous. What you cannot do is think about cyber security once, buy a solution, and ignore it for the following 2 years. It is a rapidly changing environment and it requires continuous attention from people who understand your organisation's technology. You can utilise in-house expertise, or you can outsource, both are good options. It is time to accept that it is worth spending time and money on this.

Brower: In order to avoid spending any significant money on security, a company needs to have: a) no concern about its public image; and, b) nothing worth stealing. And there aren't too many successful companies which meet those criteria. However, that doesn't mean that security needs to be a financial burden. As with many other aspects of business, an experienced team making plans before there are problems, and implementing a combination of automated controls and human factors, can provide security at a reasonable price point.

Frey: The question is not so much what is "significant" as what is "adequate" or "appropriate". There is a cost associated with cyber-security and over the last year that cost has been re-categorised as a "cost of doing business". Cyber-threats in the past have been dealt with on an exception basis; our business is running fine, a cyber-breach occurs, we scurry to remediate the breach as if we are totally shocked by its occurrence. That is by far the most costly way to treat any recurrent business problem. If we assume that threats will occur, continuously and at an increasing rate, then we can create objective control processes that incorporate the cost of cyber-security appropriately within the corporate budget. The NIST guidelines are a good first step toward objectifying the actual risks and creating a gap analysis framework within which to change corporate cultures to accommodate the type of business-interruption threat inherent in any digital operating environment.

Ganow: Both as an attorney and former compliance officer, I definitely believe that information privacy and security can be scaled accordingly. In other words, it does not have to be overly burdensome or expensive, provided the information is categorised and mapped accordingly. One size does not fit all. The question for any entity is with whom, where and how is it going to do business and what are the commercially reasonable safeguards in its industry to both secure the information and meet the industry or regulatory standards. For example, HIPAA does not require specific solutions or systems, rather it allows covered entities and business associates to build their security program in line with the applicable risks and their business's resources to meet its implementation specifications.

Jay: It takes real commitment to address real risk. Cybercrime and the threat of terrorist or hostile action through cyber

attack are real risks. We have to be prepared to invest adequately in response to the risk involved. One of the important issues business has to address is how they identify risk. Businesses need to take a 360 degree approach to risk and realistically address contingencies. They should be aware of common "blind spots" in some cases people's private and personal information is not regarded as being as important as financial data. Also that the nature and type of risk may vary with the service, and then ensure that they devote adequate resources to cover all areas of risk.

Finkel: A risk-based approach in conjunction with adequate data access limits can help focus the expenditure of financial and human resources for the best positive impact on security. While it is said sometimes that using cloud computing may increase uncertainty and the security risks and uncertainty, in my view, when implemented correctly, switching to cloud computing can increase the overall data security and at the same time significantly decrease the cost, especially when using providers that have dedicated and experienced security teams that are unlikely to be at the disposal of most typical companies and users.

8. What support can the private sector expect to receive from the government in your jurisdiction?

Brower: Twenty years ago, when we had a client attempt to meet with the US Secret Service, which had sole statutory jurisdiction over certain types of cybercrimes, about a software "time-bomb" in their medical computer, they were told "Sorry, this is an election year, we are too busy with candidate protections to handle cyber crimes." That attitude has changed dramatically. In Southern California (and many other jurisdictions) we now have inter-agency teams (including both Federal and State authorities) which include experienced personnel who will meet and discuss significant matters. However, as a practical matter, law enforcement alone is rarely the solution to a client's problems, especially where the investigation will require depositions, industry specific expertise and/or forensic accounting.

Ganow: In the U.S., the cynical response would be "nothing." But I think there is evidence of government agencies seeking to provide support for the private sector in information privacy and security compliance. The FTC has a history of distributing guidelines, educational programming and has maintained an open dialogue for companies big and small to understand compliance. I have also found the Office of Civil Rights (enforces HIPAA) willing to proactively meet with regulated entities to help those entities comply with the Act, especially when it comes to data breach response. Enforcement is the goal, yes, but there are examples of support, too.

9. What procedure should a firm take when outsourcing or contracting work which contains important data and security, be it hosting their website or obtaining passwords to secured information?

Schroeder: The firm should first evaluate the sensitivity of the data to be concerned by the outsourcing and conduct a proper risk assessment. Such a risk assessment leads the firm almost automatically to the need of a security management which is prerequisite for a secure outsourcing. The company security management may consist of several concepts e.g. data protection concept, company wide security concept, emergency concept. In a second step, the firm should approach appropriate market players with the request to submit offers and proper documentation on their data security measures. In order to obtain meaningful offers a requirements' specification is essential. Such specifications help the provider to offer the right level of security.

Bowden: Data protection and security are usually the biggest concerns when outsourcing IT. You can protect yourself with an appropriate contract, and by selecting providers with excellent reputations. As a lawyer specialising in IT, my work focuses on the contract. Make sure the services you are taking and the security you require is stated in detail in the contract (not just in the salespitch), and that you understand what is being provided. Ensure the provider takes a reasonable amount of liability for its failures. Ensure you have strong audit rights. Ensure the data is encrypted and that only you hold the encryption key. There are many other ways your contract can protect you (or expose you), so seek professional advice.

Frey: Most large institutions attempt to "push down" compliance and risk profile requirements to their vendors in contract language. However, such efforts merely create a legal remedy for failures in implementation by the vendor – they do not, in and of themselves, solve the issues or prevent/minimise harm to the contracting company resulting from a vendor lapse. Every vendor relationship needs to be evaluated based upon not only the vendor's own security/risk profile, but the security/risk profile cre-

ated as a result of incorporating the vendor within the institution. For example, having an annual security audit that requires penetration testing of the vendor or disaster recovery testing of vendor-hosted sites/operations may be totally insufficient if the vendor's control processes do not integrate well within the institution (i.e. how does the integrated system perform, not just how the vendor and institution systems perform or function independently).

Ganow: Administrative, technical and physical safeguards is critical to ensure that a third party treats information no differently than your organisation. Depending on the nature of the third party relationship, a company should have policies of varying degrees to manage the risk associated, to include what work is reserved exclusively for internal resources and what can be outsourced. Agreements should ensure the third party's skin is in the game for data breaches, require the third party to provide notice and assist in mitigating any harms resulting from a security failure. Lastly, where appropriate, companies should secure the right to audit their third party contractors and *then actually complete such audits*.

Jay: They must know precisely which data is being out-sourced, for which processes. The nature of the data and the type of process are critical to assessing the level of potential risk. If personal data is involved it can be helpful to carry out a Privacy Impact Assessment as part of the security evaluation process.

They should have regard to best practice and industry standards in determining the level of security required for that data and then carry out rigorous due diligence of the supplier against those standards.

Bear in mind that different industries and types of organisations are subject to different legal obligations relating to security, for example financial sector institutions have to consider and apply security measures as part of their regulated role. From a legal perspective they should be aware of any specific legal or regulatory obligations, for example there might be rules that some types of information cannot be sent outside the UK.

Gilbert: Entrusting a third part with the company's most sensitive assets should only happen if no other practicable, secure, safe solution is available. Thus, the first questions should be "Is outsourcing the only way to do this? What is needed to keep and process this information internally? "

Assuming that there is no alternative than outsourcing the processing, then the steps should include:

(a) Conduct a thorough due diligence of the third party's processes, procedures, operation; (b) Check references, and speak with current or past customers of that organisation;

(c) Evaluate the use of encryption; its feasibility, its efficacy, its applicability to the specific circumstances;

(d) Learn from others, but don't copy what they have done; their circumstances are not necessarily the same as yours;

(e) Establish requirements for the security and privacy of the data transferred to third parties; remember that there are three sorts of attacks: against data in storage, data in use, and data in transit;

(f) Put in place a reliable structure that includes appropriate back-up, disaster recovery plan, business continuity plan;

(g) Define an "exit strategy," i.e. Determine what would happen if you want to terminate that vendor, or if the vendor is bankrupt.

Hopp: In our experience, the first, but least covered, risk is that the companies do not know what important data they process. This is a problem for two main reasons: Firstly, because superfluous data will not be deleted in time, leading to an increased risk of data breaches. Secondly, because it is difficult to protect an asset that you are not aware that you hold. Your data security practices will only be tailored to the data that you have identified.

These issues are only enhanced when the data is transferred across borders to jurisdictions where they are often out of sight and out of mind.

Finkel: Outsourced and contract workers may represent a significant security threat that many firms are inadequately prepared to handle, especially when dealing with sensitive data. Outsourced providers must be vetted carefully and ideally come referred from a trusted third party or be directly known and trusted by a number of the firm's personnel. When dealing with sensitive data, background checks may also be appropriate. Strict limits and monitoring/logging of such personnel's actions needs to be implemented, with data encryption measures and the use of password safes utilised to reduce the risk of

unauthorised access, copying and use of information.

10. To what extent are internal risks as dangerous as external risks?

Schroeder: Experience shows that internal threats are at least as dangerous as external threats.
External threats often use weaknesses in a company's software to get information about the company or its employees. Alternatively, external perpetrators compromise the security systems which should guard the company. All such attacks have to be expected. As a result, appropriate measures, which include the development of a security concept, can effectively help to mitigate such risk. This does not necessarily apply to internal risks: There are two main sorts of internal attacks: intentional and unintentional internal use of security weaknesses. Internal perpetrators often have internal knowledge about the security measures of the company and can therefore easily identify weaknesses and then block implemented safeguards. In addition, the weaknesses that are exploited unintentionally are not less dangerous. For example, an ordinary data sharing can cause significant damage due to data loss or disclosure of business secrets even if conducted without any intent of harming a company.

Bowden: Most internal risks to data security arise from a lack of awareness rather than deliberate criminal intent by an employee. If data security is not taken seriously in an organisation, and employees are not made aware of the risks and the seriousness of them, breaches are likely to occur often. For example, confidential information should be kept out of plain sight and not left visible on a table or desk in the open; each employee's computer should be password protected; confidential information should not be shared unnecessarily or discussed openly in elevators or hallways or other public spaces; and employees should not be given access to information they do not require for their role. A culture of respect for the confidentiality of information would help reduce these kinds of exposures, and this requires regular education, reminders and management buy-in. Simply preparing a policy is not sufficient. Other internal security measures include limiting access to confidential files (both physical and electronic), maintaining responsible back-ups of electronic files, and maintaining appropriate physical and logical security measures (the latter being especially important in any organisation that has a "bring-your-own-device" policy or where employees work off-site regularly).

Frey: Both are equally dangerous – the distinction being that external risks are typically viewed as malfeasance, while internal risks are typically viewed as negligence-related. That is not always the case (and certainly employees can have malfeasance as the core of any action that jeopardises the institutional's digital integrity). But practically, significant amounts of data are being accessed because of internal risks such as employees bringing their own personal devices into the workplace for use (without proper control process and policies being in place), failing to encrypt downloaded files, or lose/theft of devices upon which sensitive institutional data is stored. One local example involves the loss/theft of a laptop that included personally identifiable information on all registered voters within the capital city of one US state (which data was stored in native, unencrypted form). Similarly, we tend to emphasise monitoring more of in-bound attacks designed to access data and build stronger firewalls to keep people out, than focus on outboard packets of information that may be triggered by internal risks – although both could be equally as severe.

Ganow: Each year information security surveys always point internally when identifying the top source of security breaches. Employees can be just as much a risk as contractors, service providers or even hackers. Companies should have clear policies and procedures for all employees: the rookies and the "seen it all, done it all" veterans, whose complacency can be as dangerous as a rookie's ignorance. But this is not enough. A company must actually train and audit (yes, audit) compliance with those policies and procedures to make sure employees are not letting the horse out of the barn (intentionally or unintentionally).

Gilbert: The probability of these risks tends to be equivalent. Acts by insiders, who know where the valuable assets or information are located can be more devastating than acts by outsiders who might be shooting in the dark. Insiders tend to have more time to prepare for their attack. They also usually have the flexibility to wait for a better opportunity, and the ability to cover their acts.

Hopp: Employees on a mission to harm their company pose a danger potentially as great as the one arising from external attacks. In that sense, the internal risks are as dangerous as the external risks.

11. How important is it that organisations include cyber security in

their insurance policies?

Brower: As a long-time participant in the technology insurance industry, I believe it is essential that companies be adequately insured. Even companies with significant assets look to their insurance policies when they suffer losses and they are always grateful when we find that they have coverage. Many companies still don't realise that their first-party property insurance doesn't cover many cyber-risks, because the recovery, protection and re-creation of electronic data usually doesn't constitute "tangible property." Moreover, unlike other types of insurance, cyber-insurance is still evolving. That means that the language of the policies has not yet been standardised, so it is necessary to have the actual policy language reviewed by counsel before there is a claim to make sure that proper coverage is in place. I am also a proponent of placing the responsibility for insurance and risk management in the legal department, rather than in treasury/finance, so that legal is more actively involved in controlling insurance and so that there is attorney-client privilege with the risk management function.

Ganow: This is interesting question and one I get often. As an attorney and former compliance officer, I say extremely important and encourage clients to find some level of coverage because the depth and duration of a breach can be financially and operationally crippling. But, as a former business executive, I know there are only so many dollars to spend on managing risk, and cybersecurity policies are still relatively expensive. That said, there is no question any organisation doing business in the digital economy has to scale cyber insurance to their business. I encourage them to seek value-added services as many policies also include legal support and breach coaching benefits.

Gilbert: All organisations, whatever their size are exposed to cyber security risks, whether the assets to be protected are their trade secrets, their 5-year strategic plan, their employees' personal information, or their customers' credit card numbers. If any of these assets is compromised, lost, modified, or stolen, the company is likely to incur significant costs and expenses, damages, attorneys' fees, etc. With appropriate insurance coverage, some or all of these expenses might be reimbursed to the company.

In addition, it has become commonly known that that most organisations should have cybersecurity insurance. If an organisation failed to have proper insurance coverage, it might be exposed to shareholder action for failure to take reasonable and necessary measures to protect the company, where the causes of action would be based on negligence and breach of fiduciary duty.

Finkel: As cyber security breaches are becoming a major risk for modern data-centric organisations, it is beneficial to cover this risk in an appropriate insurance policy, which can cover data loss incidents, business interruptions and network outages. However, while an insurance policy can cover the financial risks associated with security breaches, including the damages caused to third parties, no policy can ever bring back lost data or recall back leaked sensitive information or erase potential reputational damage. Accordingly, insurance policies are not a substitute of, and should always work in conjunction with, data security policies and processes that minimise the risk in the first place.

12. **How important is incident management and analysis when something does go wrong?**

Schroeder: The recently discovered heartbleed attack demonstrated the vulnerability of even key market players. It also showed how important it is to being prepared for such an incident as only prepared companies could quickly take appropriate steps to (i) mitigate the risk of further attacks and (ii) inform the concerned data subjects in accordance with German data protection law. If companies are not prepared, companies face severe penalties and civil liability.

Ganow: I think often more important than the "something" that went wrong, or so it often seems. I say that because how a company responds to the incident can do one of two things: minimise the resulting harm or blow it up and add salt to the wound. If there is one thing I counsel every client on it is the need to have an incident response plan, assign accountability for the plan to people with power to execute it and to practice that plan for when, not if, an event occurs.

Jay: Incident management is critical to handling a breach incident effectively. Every organisation should have in place a response plan which covers investigation, containment and responses. Increasingly there are reporting obligations when there has been a security breach, both to regulators and to individuals who have been affected. The obligations to report mean that it is no longer possible in many cases for

businesses to deal with security breaches "discreetly". The way they handle a breach can be as much a story as the breach itself so getting it right is crucial.

Hopp: Incident management and analysis is very important. In the wake of the recent cyber security problems and the increased media focus on data security, more and more companies acknowledge the need for incident management and analysis.

National politicians and the EU politicians focus on privacy issues and their push for better data protection, meanwhile an increasing number of private persons require companies to provide a certain level of data security. All together it builds up awareness of the need to protect personal data, which makes it even more important for companies to implement sufficient incident management procedures.

Finkel: Incident management and analysis are absolutely vital when something goes wrong. Incident notification and emergency and escalation plan activation is important to have a quick mitigation of an incident followed by a quick resolution. Analysis and follow-up is needed to ensure that the organisation learns about vulnerabilities and updates its risk matrix assessment, and also understand the underlying reasons and context that enabled the incident to take place in the first place. Finally, the results of such analysis should be used to update policies and processes to prevent further or minimise the incidence of similar incidents to occur in the future.

13. In your opinion, should major companies have a cyber-expert on their board of directors?

Schroeder: We would currently not give any general recommendation to having a Cyber Security on the board of directors. Companies of a certain size should have cyber security experts. Only then a timely response to threats and especially attacks is possible. In addition, the innovation cycles in IT are getting shorter. As a result, it is increasingly difficult to be up-to-date which the newest standards. However, Cyber Security is only one of various important topics for a company. And there is no need to have an expert on the board of directors for each of the important topic.

Brower: It is a good goal to seek a diversity of expertise on the Board. But, in fairness, I don't think that most Boards "need" a cyber-security expert. Cyber-security, if handled properly by management, should be one of dozens of areas in which the Board has sufficient diversity of skills and patience to listen and advise and, if it becomes a unique problem, to act. While it is an area of particular importance to those of us who are involved, if managed correctly, it should not be an area of ongoing crisis. Also, as a practical matter, I don't think there are enough "experts" who have all the other necessary criteria (other Board qualifications, availability, lack of conflict) to staff all of the Boards of Directors of all of the companies who have a legitimate cyber-security concern.

Frey: While boards (like all decision-making groups) in general benefit from diversity, a cyber-expert on a board of directors is not essential as long as all board members are adequately educated and informed in this area. Boards in general tend to rely upon and be deferential to experts (and in fact US law allows board members to reasonably rely upon "experts" in mitigating their individual risks for decision making). But a robust response to cyber-security requires that threats be articulated in language common enough to be understood by the non-professional and allow cyber-threats to be placed in an institutional context (not just a technological context). Not every cyber-threat is a "cry wolf" event – but Board members need to know when a true crisis occurs. IT can help educate the Board on such basic distinctions, but an IT professional's opinion cannot replace the strategic decision making required of Board members who are adequately informed of the enterprise –wide risk involved with the cyber-threat. For situations where board members do not have adequate knowledge or experience with respect to security, adding a board member with this specific knowledge may be helpful in encouraging active debate and intervention when needed at the board level. The critical element with such an addition is that the added member to the board should focus on the cross-enterprise operational issues of the company and should act as a catalyst for strategy decisions by the board in dealing with cyber-threats, not just convey and be depended upon for expert knowledge.

Ganow: For the longest time I would have said no, provided the competent resources are accessible and the responsibilities delegated; a tried and true management principle, right? However, with as fast as information technology is expanding in all industries, I don't think company leadership can remain levels removed from an understanding of the relevant technologies. Whether

it's providing sound fiduciary oversight to budgets with too much or too little money being thrown at information security, or helping a company respond to a data breach, you need Board visibility. And don't forget about dealing with the media which is more technically savvy than ever, as evidenced in the information security blogs that have broken the news on several large scale security issues in the past year.

Gilbert: Yes. A well-rounded Board of Directors should be comprised of individuals with a wide variety of backgrounds and experience that cover the scope of the company's needs and activities. Most companies are exposed to significant cyber security threats from a variety of factors such as outsider cyber attacks, employees' errors, or bad acts. The frequency, nature, and consequences of cyber attacks can be devastating for a company's reputation, cause significant drop in share value, and affect the lives of millions of individuals. Despite numerous highly publicised cases showing that even the most well know companies (e.g. Target, Neiman Marcus, TJ Max) could be victim of breaches of security, CIOs, CISOs and others appear to have significant trouble bringing their management's attention to the serious problem caused by breach of security and cyber attacks. Data protection and information security are not yet taught in business school, and it is becoming clear that the current class of board members significantly lacks knowledge and appreciation of the importance of cybersecurity for a company.

Thus, so long as directors lack the proper knowledge of cyber security to adequately guide a company's management, it would make sense to urge or require companies to have a cyber expert on their Board of Directors. This individual would be able to educate the other board members and raise their awareness of the risks to which the company is or might be exposed, the methods that are available to address these risks (legal, procedural, technical, physical, administrative, insurance, etc.), or the nature of the financial investment required to achieve these goals.