Information Security Industry Predictions for 2014: Government Compliance

Infosecurity asked the industry to share its 2014 trend predictions, and the industry delivered. We have categorised the predictions into five topics and created a news article for each. We were not able to include all predictions in these news articles, thus created these documents, listing all of the industry's contributions for our readers to view. There are five pdfs for you to download.

Mark Shirman, President and CEO, RiverMeadow	Government Regulation Will Drive the Management of Data As always HIPPA and other government requirements will drive the way people manage their data. With an increasing utilization of all types of cloud strategies, this focus will continue in 2014 and may even intensify.
Jason Fredrickson, senior director of application development, Guidance Software	NSA intrusions will drive encryption efforts The extent to which the NSA has penetrated companies' networks has been staggering. The NSA and PRISM will be a driver for companies tightening up security and developing ways to protect their data from decryption. In the coming months, more companies will ask, 'How can we prevent the NSA from looking at data on our employees and customers?' We'll also see more companies trying to circumvent gag orders by openly stating what information they cannot disclose. Tech giants Apple, Google, Microsoft, Yahoo, Facebook and LinkedIn are already pushing back on the government, arguing they should be allowed to share data about NSA requests for confidential, customer data. As a result, we will see a renewed distrust of the government and potentially legal battles.
Aaron Titus, CPO/General Counsel at Identity Finder	ID Thefts to Target Affordable Care Act Newly created health insurance exchanges under the Affordable Care act are not required to comply with HIPAA/HITECH security and privacy regulations, and some are underfunded. The situation increases the risk for healthcare data breaches of personal health information. Potentially, millions of identities could be at risk. More Focus on Data Classification It's no secret that big data is getting bigger and harder to manage. In fact, sensitive data discovery and classification is the starting point for many regulations including HIPAA and PCI-DSS 3.0. Discovering and classifying sensitive data is becoming more critical to preventing breaches, and we should expect to see greater emphasis on this practice by organizations of varying sizes. Better Accounting for Costs of Data Inventory It is estimated that more than two-thirds of all breaches occur when data is at-rest. Forward-thinking businesses will begin to account for the liabilities associated with sensitive data, much like they account for carrying costs of inventory. Enterprises that underestimate shrinkage, inventory control and other costs will be more prone to data breaches and losses in 2014.
Lancope CTO TK Keanini	I think the EU will lead in regulation and show the world how to implement a common data breach framework across a diverse set of national boundaries. US Federal should play close attention to this as it matures in 2014.
Charles Sweeney, CEO, Bloxx	The ICO has shown that it isn't afraid to flex its muscle and issue fines for data losses. To date it is public sector organisations that have felt its wrath. The result being that the Government has started to take its own rules very seriously indeed and public sector organisations now have a lot less regulatory leeway. To try and avoid any more data being lost in embarrassingly easy fashion, such as a lap top left in a cab, we're hearing from our public sector customers that they won't be able to connect mobile devices to their network. This should act as a warning to private enterprises. Once the public sector has its own house in order, I wouldn't be surprised if in 2014 a private enterprise hits the headlines courtesy of a fine from the ICO.
Steve Durbin, Global Vice President, Information Security Forum	We will see further regulation around the collection, storage and use of information along with severe penalties for loss of data and breach notification Most governments have already created, or are in the process of creating, regulations that impose conditions on the safeguard and use of Personally Identifiable Information (PII), with penalties for organizations who fail to sufficiently protect it. As a result, organizations need to treat privacy as both a compliance and business risk issue, in order to reduce regulatory sanctions and commercial impacts such as reputational damage and loss of customers due to privacy breaches. Furthermore, we are seeing increasing plans for regulation around the collection, storage and use of information along with severe penalties for loss of data and breach notification particularly across the European Union. Expect this to continue and develop further imposing an overhead in regulatory management above and beyond the security function and necessarily including legal, HR and Board level input.
Catherine Pearce, security consultant at Neohapsis	We'll see a cyberwar redux. Details on nation-state cyber capabilities and activities of countries other than the known big players will begin to be revealed. Geopolitics has many fronts, and it's to your advantage to play in every event. So, it's fair to assume there are players as yet unknown - whether smaller countries or larger ones that haven't been exposed yet. In addition to political battles over the internet's fate [see prediction 4 below], countries will continue to covertly gain advantage over each other via the internet. We will begin to see more details on the activities of countries other than the USA (and allies), China, Russia or Iran. While you can probably guess the obvious players, those that come to mind as likely undertaking cyber activity under the public's radar include: India, Indonesia, Brazil, Pakistan, Japan, Mexico, Germany, France, Italy, and South Africa. And that's only going through the top 25 countries by population! Privacy will continue to lose out to opposing parties in US Legislature. In response to public awareness and outcry, we will see a failed attempt to pass electronic privacy protection regulation in the USA, attempting to follow the lead of countries such as Germany. This will target private companies under the guide of protecting teenagers, and will exclude government programs. However, irrespective of voter support, market forces and lobbying by interested parties will quash this. The Internet governance battle will continue. There will be yet another showdown between the US and the rest of the world on control and regulation of the internet. In recent years, questions and concerns have been raised about US dominance in the Internet's governance. These concerns have been raised in international bodies (e.g. IETF, ICANN, the United Nations), and some parties have pushed for changes to limited success so far. Nevertheless, these concerns have resulted in some countries attempting to reduce their reliance on US benevolence by either strict internet controls (as in China) or through a "parallel internet" (as Iran has discussed). The USA has generally stood on the side of online freedom – except where copyright is concerned – but those pushing for change are largely seeking to restrict freedom of communication or information. Any change away from online freedom is concerning. Whether IETF, ICANN, or the United Nations, the internet will continue to be a space for political forces to battle. However, US adversaries will begin to form a more coherent opposition.
Lior Arbel CTO of Performanta Ltd	Planned EU legislation will require necessary changes to be effective in 2014 The biggest change to government security we will see in 2014 is the planned introduction of privacy regulations across the EU. A clause of this will make it mandatory to report a security breach within 24 hours, however, many companies do not currently have the technical support to match this requirement. Under current plans if a company is unaware of the attack then they will not be liable for the damage, meaning certain companies can take an attitude that it is "better not to know" to avoid the costs. This legislation needs to be changed so it has the force to make companies liable for the data they gather and force them to deploy necessary safeguards. Organisations that don't follow suit may find themselves subject to actions by regulators and other legal repercussions. 2014 will be the year when a decision is made about the level of regulation that governs company data.

Ron Gula, CEO of Tenable Network Security	Cyber security rises up the government agenda, and the return to a more balanced spend on compliance and threat software National cyber security will remain high on the agenda next year. Over 2013 and 2014, the UK cabinet office will invest £180 million in cyber security, increasing this amount to £210 million in 2014-2015. The US Department of Homeland Security's $6 billion procurement of IT security tools, known as Continuous Diagnostic Monitoring, will be watched closely by other countries, causing more governments to invest in similar monitoring strategies. Furthermore, while 2013 saw the height of investment in threat solutions, 2014 will see this start to swing back to a more balanced spend between threat and compliance software, with the development of new sets of real-time and scalable technology.
Seth Goldhammer, director of product management, LogRhythm	Increased action from government and regulatory bodies We have seen government take both a carrot and a stick approach to regulatory compliance this year. For example, we saw HIPAA violation penalties increase in 2013 as well as changes to the EHR Meaningful Use programme, with the addition of financial incentives. We do not expect any slowdown in breaches during 2014 that expose customer data, patient data, and credit card data among other things. This will lead to an increase in penalties and creation of financial incentives as governments and regulatory bodies look to be responsive to these security events. Businesses will no longer take a check-box approach to compliance In 2014 companies will need to adhere to much more stringent security regulations. Guidelines such as version 3.0 of the PCI SSC Data Security Standard, which comes into force in January, will see all businesses take a much more proactive approach when faced with today's cyber threats. It will essentially change the way organisations view compliance, which will start to be seen less as a one-off obligation and more of a day-to-day, continuous activity. Stricter standards such as these will ultimately ensure businesses are properly prepared for cyber attacks, which is now key, because it really is becoming a case of when, not if, you will be targeted – even if you look 'compliant' on paper.
Paul Ayers, VP EMEA at Vormetric	Lawmakers around the world are actively engaged in enhancing existing compliance requirements and designing new legal frameworks around data security. This is hardly surprising given it's no longer a case of if a business will suffer at the hands of hackers or insider threats, but when. Notably, this autumn we witnessed the revised E-Privacy Directive come into force. This law mandates that in the event of a data breach all telecoms operators and ISPs must notify the appropriate national authority within 24 hours. While it applies only to this sector for now, it certainly sends a warning shot to all organisations processing personal data. Indeed, clauses in the impending revised Data Protection Legislation Act means all businesses will inevitably have to follow similar rules. It is only by taking steps now to implement policies and technology solutions that are simple and powerful enough to adapt to compliance variations – and by ensuring that data is sufficiently obfuscated in the event of a breach – that a business will be able to shield themselves from the financial and reputational penalties at stake.
Michael Yaffe, Director of Product Marketing, BeyondTrust	2014 will be the year people move beyond just doing compliance and start doing real security. Compliance is already king and one of the main reasons why people buy security technologies. In 2013 complying with requirements has become a more streamlined process there will continue to be a high demand for products that support directives to comply with FISMA requirements such as FDCC, SCAP and DIACAP.
Vijay Basani, co-founder, president and CEO, EiQ Networks	We'll see a Cyber Security Framework released in early 2014. Its adoption will be minimal in dues to lack of sufficient punitive damages, lack of industry enthusiasm, and clear guidelines. It may turn out to be whole lot of nothing as more focus is on risk management and less on security. Expect continued movement towards more prescription controls implemented in regulations/compliance in general. Security Best practices such as SANS Critical Security Controls will gain traction as they begin to deliver tangible cost savings and meaningful improvements in security posture / visibility.Government contractors, consultants and 3rd parties will become the major sources of IT Security infiltration in the government. While DHS CDM (Continuous Detection and Mitigation) project implementation starts, most agencies will not implement it in time to prevent uber attacks and data loss.
Morey J. Haber Sr. Director, Program Management, BeyondTrust	Regulatory standards like the PCI DSS are advocating switching from quarterly assessments to more of a real time approach and conducting assessments as a part of normal business routines. This strategy, in itself, is not surprising since government bodies have promoting real time assessments and continuous monitoring for the last few years. What will change in the next year is the technology used to conduct assessments and provide a real time, continuous views, of when new applications and configurations violate this requirements. With vulnerability scan engine technology becoming a commodity, and cost of assessments decreasing, organizations will continue to have multiple sources for vulnerability data. Business intelligence tools that consolidate this information, much like a SIEM, will become more important and relevant in the next year. With the end of life for Windows XP, allowing administrative rights on the desktop will take a center stage. There will be no logical reason to allow administrative access to desktop for Windows 7 or 8.1 as tools and procedures allow for least privileged to maintained on every system and help organizations obtain security best practices and comply with regulatory initiatives.
Bala Venkat, CMO at Cenzic	Companies will need to develop programs to monitor and report on security compliance on critical assets and interactions that touch security at the national and global level.
Jason Hart, VP Cloud Solutions at SafeNet	Customer demands for ease of use and frictionless authentication will drive improvements. Customers' expectations for seamless trusted authentication and the continued dominance of smart phones and smart devices will accelerate the move from legacy hardware One-Time-Password tokens to mobile friendly, embedded security and contextual access controls. These methods will rely on security elements built into devices, and leverage device sensors to authenticate users. We can already see early examples in Apple's iTouch for biometric authentication, and investments by vendors such as Samsung to bake enterprise grade security controls into their KNOX platform. Shift in focus from breach prevention to breach protection. With hacking attempts becoming almost a daily occurrence, it's clear that being breached is not a question of "if" but "when. Therefore, in 2014 we can expect to see companies move away from the traditional strategy of focusing on breach prevention, and move towards 'secure breach' approach. This means accepting that breaches happen and using best practice data protection to guarantee that data is effectively useless when it falls into unauthorised hands, so we can expect to see an increase in the use of encryption that renders any data useless to an unauthorised party.
Sam Maccherola, VP Sales, General Manager EMEA & APAC , Guidance Software	Surveillance Revelations - Encryption will be key The heightened awareness of, and revelations on surveillance will be a driver for companies to tighten up security and develop ways to protect their data from decryption. Next year could see more changes in the way that new encryption technologies are deployed; Yahoo recently announced that it is to encrypt users' data and most recently tech giants including Yahoo, Google, Apple and Facebook have joined forces to call for reforms that would allow them to resist unreasonable demands for customer data.
Neil Cook, Cloudmark CTO	Governments will clamp down on this spamming and fraud with increased regulation especially in the mobile messaging arena. Developing markets will likely exemplify this with harsher positions against messaging abuse. In the US, intervention by the FTC has resulted dramatic decreases in various SMS campaigns. Other regions have not fared as well though, stumbling over less effective legislation in attempts to curb SMS spam, for example by setting limits on the number of SMS that can be sent from a single SIM. We expect regulators in 2014 to start concentrating on clarifying regulations for operators to enable them to effectively police their own mobile messaging streams, as well as ensuring that law-enforcement and other agencies have the appropriate "teeth: to deal with the perpetrators. Premium rate texting specifically will rise to be a paramount concern in the coming year for those regions that have lenient rules around the service. The implications of such an easily-exploited service will only gain popularity.

Eddie Sheehy, CEO of Nuix	Companies are going to pay significantly more attention to their privacy obligations in the face of tightening laws in Europe, Australia and the United States. We can thank Edward Snowden's leaks, even more than stricter legislation, for making the public more aware of how organizations handle their private data.
Paul Nicholas, Senior Director, Global Security Strategy, Trustworthy Computing, Microsoft	The US Government will release its Cybersecurity Framework and this will begin a more detailed conversation between what can be accomplished by leveraging voluntary efforts, standards and tailored regulatory actions. Similarly, the directive on Network and Information Security (NIS) discussions in the European Union (EU) will continue to evolve and examine how to improve security, including raising more detailed discussions of incident reporting. The US and EU efforts will not happen in isolation. It will be important to ensure that we do not end up with hundreds of different approaches to cybersecurity. This type of approach would begin to erode the base of the global ICT industry. In 2014, I predict that policy makers, private sector companies and vendors of all sizes will begin to see the imperative for harmonization and begin to align risk-based approaches to managing cybersecurity.
Eddy Willems, Security Evangelist at G Data	Cloud storage services as a gateway for malware Dropbox and other storage services in the cloud are popular among users for backing up or storing data. To criminals, such services are worth cash. G Data experts have already seen attacks aimed at intercepting data this year. In 2014, the German IT security provider expects to see attacks in which criminals are not only spying on data in hacked accounts, but are also placing malware there camouflaged as PDF, image or text files. These will then be able to infect PCs via manual or automated downloads. Such attack methods will be seen mainly in the business environment.
Kaspersky	Amazing things have happened to the Internet. Many experts, including Eugene Kaspersky, are talking about the need to create some kind of parallel "safe Internet" which won't allow anonymous users to roam, with potentially criminal intent. Meanwhile, cybercriminals have created their own Darknet based on Tor and I2P technologies allowing anonymous cybercriminal activity, commercial activity and communication. At the same time, the Internet has begun to break up into national segments. Until recently this only really applied to the Great Firewall of China. But the People's Republic is no longer alone in its efforts to separate and manage their own Internet resources. Several countries, including Russia, have adopted or are planning to adopt legislation prohibiting the use of foreign services. Snowden's revelations have intensified the demand for these rules. In November, Germany announced that all communications between the German authorities would be fully locked within the country. Brazil has announced its plans to build an alternative Internet channel so as not to use the one that goes through Florida (USA). The World Wide Web has begun to break up into pieces. Individual countries are no longer willing to let a single byte of information out of their networks. These aspirations will grow ever stronger and legislative restrictions will inevitably transform into technical prohibitions. The next step will most likely be attempts to limit foreign access to data inside a country. As this trend develops further it will soon lead to the collapse of the current Internet, which will break into dozens of national networks. It is possible that some of them will prove unable to communicate with each other at all. The shadowy Darknet will be the only truly world-wide web.
Peter Armstrong, director of cyber security, Thales UK	DCPP - The Ministry of Defence (MoD) last year launched the Defence Cyber Protection Partnership (DCPP) in conjunction with other Government Agencies and nine UK defence and telecoms firms including GCHQ, BAE Systems, BT and Thales UK. The DCPP will be defining and applying a new standards framework that will protect investments already made in cyber security whilst ensuring a proportionate response that matches the threat: this will eventually be rolled out to the whole defence industry the intention being to mandate compliance through contracting. This is a positive step in further ensuring that the UK is a safe place to do online business. 2014 will also see the DCPP address the cyber challenges that higher threat environments face in defence, but also critical national infrastructure sectors like nuclear, or power water distribution. From this, we'll see substantial take-up of BIS foundation level improving basic cyber husbandry and CSMM across all of the Defence Supply Chain and through some of the CNI regulatory bodies into the utilities environments meeting higher level cyber defence needs. Smaller and medium-sized businesses will see government and security requirements affect them in the coming year. In 2014 we will see the DCPP extend its compliance models to include smaller businesses in the supply chain and the DCPP partnership will open up its membership to other firms and eventually other firms in the industry. This will enable greater collaboration across the country to tackle the growing threat of cyber attacks on the supply chain.
Jim Hietala, VP Security, The Open Group	In 2014 we can expect to see more regulation aimed at ensuring data security and privacy as a result of the Snowden breach revelations. In the US, we'll see the final publication of the US NIST Cybersecurity Framework, which while technically a "voluntary standard" should have broad impacts on US private companies in critical infrastructure sectors. Expect most companies in critical infrastructure areas to treat this framework as their de facto standard for information security compliance.
Geoff Webb, Director of Solution Strategy, NetIQ	Next year will definitely be the year of privacy. European governments will move to focus heavily on defining and enforcing privacy regulations, and will work to outline the types of information that can be shared between services. This has become a special priority in the light of the recent disclosures about the US government's widespread data gathering, which includes ordinary citizens and world leaders too.
Garry McCracken, VP Technology Partnerships, WinMagic	As regulatory security requirements like the NIST framework and Obama's Cybersecurity Executive Order add teeth to the punishment dished out (i.e. fines and public shaming,) government organizations must look closely at the ways they protect their data. User education for government sector is vital and should reinforce simple things employees still often forget. In the case of the forgetful employee, government entities can mitigate user error by enabling encryption capabilities on all of their employee-issued devices. As a result, exposed (but encrypted) critical data will be NOT be deemed a security breach.
Richard Walters, CTO of SaaSID (an Intermedia company)	General Data Protection Regulation will never be enforced By the middle of 2014, EU Justice Commissioner, Viviane Reding, hopes to push through the European General Data Protection Regulation (GDPR). This proposes a single set of data protection rules binding all twenty eight member states. Key parts of the GDPR proposals include the requirement for data controllers to inform the relevant Data Protection Authority within twenty four hours of becoming aware of a breach and penalties of up to 5 per cent of a company's global revenues. A central proposal is the creation of a 'one-stop-shop' to reduce companies' administrative burden when complying with multiple countries' privacy laws. However, the head of the European Council's own legal service has challenged the 'one-stop-shop', arguing that citizens must be able to bring privacy cases in their own country. http://www.ft.com/cms/s/0/6930c9a6-5e8a-11e3-8621-00144feabdc0.html?siteedition=uk#axzz2mvBY4Cvb). This legal delay, coupled with the low level of investment behind the GDPR, indicates that this regulation will never actually be enforced.
Guy Bunker, SVP Products, Clearswift	Information Governance becomes a recognised buzzword. There will be increased call from legislators for organizations to better understand where their critical information is. We have seen issues in the past where backup tapes etc. have been known about, but unable to be located – and the result has been fines for not producing the information. Inadvertent loss. This granularity will reduce, such that even copies of information on memory sticks will become part of the reporting. Critical information will need to be better understood, before it can be managed – what is the information, where is it stored, who has access. Information Governance (IG) is the term for this understanding and ultimately management of critical information. Solutions will start to come to market to address the IG challenges. 2014 the year for global identity? Every year I wonder if this will be the year identity gets turned on its head – and become 'person' centric rather than 'company' centric. I don't think it will happen in 2014... but, you can but hope!
Kevin Bailey, Head of Market Strategy at Clearswift	Regulators become the new bankers and utility providers! As regulations of all types are being introduced across organisations for industry, national, regional and function purposes, these will weigh heavily on businesses still recovering from the economic downturn. Organisations are still focusing their budget spend on [high return] business growth rather than 'zero return' costs projects such as regulation policies that may never be required. With increased [enforceable] penalties integrated within the new regulations, will 2014 be the year that the regulators be despised as much as bankers or our gas and electricity suppliers or will organisations find the holes in the regulations to reduce their exposure, albeit like off shore banking?
Fred Touchette, Senior Security Analyst, AppRiver	I think the biggest arena to be hit will be in the medical industry. It may be difficult for many of these practices to become compliant with new HIPAA compliance regulations, thereby leaving large gaps in network security and the security of patient information. This leaves a lot of opportunity for thieves to get a hold of unsecured patient records and because of the strict rules regarding the reporting of such breaches, we will most certainly be hearing about a

	good deal of these in the coming year.
Ashley Stephenson, CEO of Corero Network Security	There is generally widespread agreement amongst security practitioners regarding the fundamental need for stronger legislation around cyber threat protection. The overall initiative stemming from the President's executive order earlier in 2013 is certainly a positive step towards reducing the cyber security risk to the Nation's critical infrastructure. We believe that mandated controls will allow the US to take positive steps towards regaining control of the battle against cyber activists. The flexibility that the proposed framework offers is welcome. At a minimum, baseline guidance that smaller organisations can take advantage of while larger organisations can utilise the framework as a strong compliment to existing business continuity plans, adding cyber-attack defense planning and more. The framework is moving in the right direction in allowing for a consistent and iterative approach to identifying, assessing and managing the evolving cyber threat landscape. The framework was not designed to be an exhaustive checklist of activities; it does provide a very solid structure and organisation around the areas of concern and the recommendations for improving upon an organisation's current state of cyber security readiness. Every Internet connected organisation, from Small to medium enterprises, large Enterprises, Government, Internet Service Providers, Hosting Providers and the burgeoning Cloud, needs to have a defense in depth strategy, for protecting themselves and their customers. I think the framework lends itself nicely to this approach. If properly executed, the five core functions that are outlined, Identify, Protect, Detect, Respond and Recover, can exponentially increase an organisation's resilience and ultimate level of protection against cyber-attacks. Additionally in the UK and across Europe, The proposed EU directive, will allow for better information sharing across borders, to help combat the cyber threat. With a desired result of achieving cyber resilience, reducing cyber-crime, and allowing for better development for cyber defense policies in the future, it is really about taking a cooperative stand against these attacks, and collectively learning from them. DDoS attacks have been around for more than a decade. These attacks are continuously evolving, the more sophisticated types of attack can wreak havoc on organisations large and small across the globe. With greater visibility and access to more reporting, the analysis of attack data and impact will help us to understand the true extent and costs, both financially and from a reputation perspective, of these attacks. A by-product of this global effort could even drive additional legislation related to the punishment of these crimes. Overall it's a win-win in a global stance against cyber warfare for 2014.
Matt Hines, Product Manager at FireMon	It's always difficult to predict just how government activities will play out with evolving legislation and enforcement, and changing administrations, but overall worldwide it does appear that there will continue to be greater emphasis placed on automation of controls and assessment of those controls, as well as use of security-related analytics and metrics to understand performance over time. As we've seen in the US and now more so in the EU, government security management leadership is working hard to maintain visibility into the current state of affairs and get their hands on more real-time, accurate data on the effectiveness of IT security controls through more continuous, automated assessment to increase so-called "situational awareness." An example of this can be found in the United States Dept. of Homeland Security Continuous Diagnostics and Mitigation (CDM) Program, which mandates that U.S. federal government agencies constantly assess the state of their network security device infrastructure to ensure that forces of complexity and change are not leading to less effective protection of critical assets. In the EU there are similar elements aimed at increasing use of automation, centralised reporting and standardised security metrics, as with those suggested in the European Parliament resolution of 2012 on critical information infrastructure protection.
Sean Sullivan, security advisor at F-Secure	If governments didn't realise the scale to which they are targets at the beginning of the year, they certainly do now. There have been numerous disclosures made this year that are already having a large impact on security requirements and policies. These requirements will cost money (and time) to implement – it's something that governments and companies should have sorted out long before now.
Ken Parnham, Managing Director, EMEA for TRUSTe	Whether the proposed EU Data Protection Regulation is introduced in 2014 or not, privacy will be increasingly important consideration for businesses next year. The rise of dual-screening, facial recognition technology, wearable tech and smart devices are likely to give rise to new privacy and security challenges for consumers, businesses and regulators. The challenge will be to find ways to use new technology in a privacy-savvy manner and to be transparent about the data you're collecting, what you're doing with it and provide people with a way to opt out if they wish. Addressing potential privacy concerns from the start will be one of the best ways to ensure your business is well-prepared for any potential government and regulatory requirements that may be introduced in 2014 and beyond.
Adrian Culley, Global Technical Consultant, Damballa	Banks and Beyond The Prudential Regulation Authority's more exacting requirements around cyber resilience, coupled with an increased awareness of these matters from the Bank of England itself, will change the landscape for Banks and Financial Bodies throughout the year. This comes as Cyber defences at banks have continued to be called into question following high profile incidents such as the resurgence of the Caphaw malware which has attacked major European banks. It's likely that other Regulators, particularly those concerned with Critical National Infrastructure will follow and up the ante in terms of existing cyber security frameworks. Social Media and the general election As we move into the second half of 2014 both the Government and the people of the UK will realise the impact of Social Media upon the forthcoming May 2015 election, and how vulnerable this will be to manipulation. It will arguably be the first election swayed, not by that morning's Headline, but by that day's Twitter and Facebook. This makes it highly vulnerable to coercion. Much blood, sweat and tears will be shed over this.
Elad Sherf, Senior Security Researcher at Websense	Government regulations will encourage companies to report attacks The new cyber security standard to be created and enforced in the UK by the Department of Business, Innovation and Skills (ISO27000) in 2014 will encourage businesses to improve their security services in order to comply with the regulations. As the government continues to proactively protect its infrastructure from cyber-attacks, companies that receive recognition of compliance with the new requirements will see an increase in trust, reputation and customer confidence. Due to more companies being compelled to report attacks and share the details with government departments, we will see a gradual and slow increase in co-operation between businesses resulting in an overall long term increase in security protection, faster identification of security trends as well as a reduction in regulatory fines.
Matt Middleton-Leal, regional director, UK & Ireland at CyberArk	In 2014, expect to see increased regulation of insider privileged accounts and new encryption standards emerge 2013 has provided a number of significant wake-up calls to organisations with regards to proactive security. The now infamous Edward Snowden leak provided a high-profile example of the fallout that can be caused by a 'rogue insider', all political viewpoints aside. The insider threat is ever present and the Snowden incident continues to reverberate across industries worldwide. As a result of the heightened awareness around unrestricted insider privileges – given Snowden's background as a former NSA contractor – we can expect compliance and regulatory requirements to evolve to reflect this, by placing an even greater emphasis on individuals and the powerful access rights in use within all organisations. Added to which, I expect the global repercussions of the Snowden leak to lead to increased encryption and as a result, we're highly likely to see new encryption standards emerge and new methods developed next year. As we reach the end of 2013, business decision makers should carefully consider the following questions: If an attacker has successfully infiltrated your corporate network – and frankly it's wise to assume that if they haven't already, it's only a matter of time – are all the core assets locked down? Is privileged access monitored and would this be immediately revoked if deemed suspicious? In 2014, we hope to see businesses spend more time and resources on securing from within and ensuring a system is in place to manage, monitor and control any suspicious access or activity, with the option to terminate a

	session in real-time if needed.
Kurt Hagerman, director of information security at FireHost	I won’t be alone in predicting that 2014 will see more stringent regulations than ever before. No doubt people say this every year of course. It’s no surprise that regulations seem to get stricter and more complex each year, it’s how industry bodies and governments keep pace with developments in business and technology. If compliance controls remain the same for too long they will always run the risk of becoming out-dated, ineffective and can even become more difficult for organisations to meet, especially if they’re no longer aligned to modern-day business operations. Tightening compliance controls is a necessary evil. Although new regulations may force companies to find additional investment in resources and personnel, if this means reducing risk and improving security, it must be considered as a positive step. For example, compliance with regulations like PCI DSS is often mandatory for businesses that, for example, handle payment card data. The arrival of the updated 3.0 standard in 2014 is undoubtedly making the process of achieving compliance a growing challenge for businesses and there is no denying that the new standards will mean an increase in time and costs for organisations to remain compliant. However, the revisions made for the latest version of the PCI standards will go a long way to improving the quality of assessments and reducing overall risk. As such it’s a change that the security industry should fully support.
Garry Sidaway, Global Director of Security Strategy at NTT Com Security	Governments have to play, and are playing, an increasing role in highlighting the concerns over the cyberthreats, but they also have to move with the times and not impose compliance and regulations on companies that simply don’t work in the 21st century. Compliance has always looked back, and governments and businesses need to start to look forwards and work towards embedding security into the services that they provide and not simply bolting on technology to protect against the latest threat. Compliance and governments have to realise that businesses are now more and more reliant on cloud providers and these are global entities and not restricted by traditional borders. Compliance will fail if it continues to restrict businesses and impose controls that simply do not allow business agility. As I have said before compliance should be the result of good security and not the other way round, but also good security needs to be based on an understanding of risk. Governments need to work with businesses to put these risks in context and define what is acceptable in the age of the cloud. They also need to work together to define global initiatives that ensure that complying to one set of standards is acceptable to businesses, consumers and governments.
Andrew Avanessian, VP Professional Services, Avecto	Gen Y Revolts, Bringing Increased Risk Organizations today are struggling to balance security with user flexibility and empowerment. Though they want to use IT as a business enabler, the weight of current endpoint security systems is often limiting employee productivity. If organizations don’t learn how to strike this elusive balance, I predict that savvy “Gen Y Techies” will circumvent the burdensome security policies in place, finding their own ways to and access the documents, files and tasks they need and therefore potentially introducing the organization to new attack vectors. Recent research even shows that 80% of Gen Y employees admit to not obeying IT policies. Many organizations will take the easy road out and let employees dictate the security agenda, opting for convenience over security and gradually softening security policies and reintroducing local admin access. This should not be allowed to happen. In fact, according to Gartner, by year-end 2014, 70% of large enterprises will permit access to external social media sites, compared with 50% in 2010, which will open up a whole new attack vector. There are many solutions that mitigate risk without suffocating employees at the endpoint and organizations that put these into place with grant their users the flexibility they demand without needing to compromise on security.
Greg Hanson, Senior Director EMEA Technical Operations at leading data integration provider Informatica	Privacy The days when customers refused to share any information about themselves are now behind us. However, we will see an end to the era of unfettered sharing too. In 2014, I predict, customers will start to expect something in return for their data, be it a simpler life, special offers or even cash. This is borne out by Forrester research, which states that over a third of UK online shoppers would be willing to sell all of their digital data[5] to the right brand at the right price – and half of them would be more likely to buy from a retail brand if they did so. In order to capitalise on the monetisation of data, companies need to make sure that they offer tangible benefits to those whose data they hold. Businesses should take care of this data and only use it in ways that simplify their customers’ lives and provide real value. What’s tricky is how to determine what constitutes “value” to each individual customer and ensure that the offer is something that they can truly appreciate.