Information Security Industry Predictions for 2014: Cloud

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	Cloud Security Takes Center Stage in 2014 Currently, most companies have either adopted a public, private, or no cloud strategy at all. One of the key drivers to the private cloud has been security related issues. As the potential for hybrid cloud solutions takes shape, enterprises will look to existing and new third party tools to ensure that the highest level of security is maintained. This space will heat up considerably in 2014.
Lancope CTO TK Keanini	2014 will be the year that businesses can move IT to the cloud and have better security than their traditional enterprise data centers. Leading cloud providers like Amazon's AWS offer state of the art encryption and operational visibility that is more cost effective than the traditional models. Especially for businesses that have seasonal and elasticity, cloud infrastructure in 2014 comes of age and just makes better business sense. Companies like Intuit and Netflix are pioneers and lead by example.
Steve Durbin, Global Vice President, Information Security Forum	While the cost and efficiency benefits of cloud computing services are clear, organizations will no longer delay getting to grips with their information security implications In moving their sensitive data to the cloud, all organizations must know whether the information they are holding about an individual is Personally Identifiable Information (PII) and therefore needs adequate protection. Different countries' regulations impose different requirements on whether PII can be transferred across borders. Some have no additional requirements; others have detailed requirements. In order to determine what cross-border transfers that will occur with a particular cloud-based system, an organization needs to work with their cloud provider to determine where the information will be stored and processed.
Catherine Pearce, security consultant at Neohapsis	The cloud will begin to show its unseen costs. We will see an increasing number of breaches of customer-specific cloud assets. This won't be due to weaknesses in the cloud service or its technology but on the integration, configuration, and operation of it by the customer. The burden of good cloud system management comes at a cost, but this cost is often downplayed in marketing or overlooked in business decisions. While the cloud can offer massive efficiency and cost gains, it's easy to see only the sticker price, and not the real costs. Cloud services can offer huge efficiency and cost advantages, however they can add operational security burden if not carefully (and knowledgably) deployed and integrated with the organization's existing systems. Just because something can be highly secure doesn't mean that it necessarily is in the way you're using it. Likely scenarios include the leakage of organization IP from poorly access-controlled cloud systems, attack pivoting via cloud services (where the customer has internal systems attacked via the cloud system's network link), and unauthorized access resulting from cloud-system accounts which are not synchronized with the central identity store.
Eric Chiu, president & co-founder, HyTrust	We will see a rapid growth in systems and services that provide additional control over privileged users, like the administrators that manage virtualized infrastructure. These super users have very broad controls, and a simple misconfiguration or malicious act can have catastrophic implications. We will also see growth in the tools and services used to protect the data itself, including strong encryption. Given some of the recent disclosures about government access to cloud service provider networks, we'll see further investment in key management systems that allow organizations to keep control of their encryption keys themselves vs. entrusting that critical security measure to the same vendor that holds their data.
Lior Arbel CTO of Performanta Ltd	New cloud security solutions to counteract the threat to corporate security posed by the NSA Given the recent revelations involving the NSA, GCHQ and other government organisations, companies are growing more wary of cloud solutions. There is now documented evidence that the NSA asked for the encryption keys to gain access to the entirety of a cloud providers database. This has led to a search for new-more security solutions. One which will become more popular in 2014 is split key encryption. A new start-up is offering a service whereby the encryption key is split in two, one half held by the provider and one by the customer meaning that the customer's database can only be accessed with their active participation (or at the very least make it harder for a government to access the data). An increase in direct attacks on cloud providers 2014 will also see a rise in attacks on cloud providers directly. These attacks are harder because unlike internal company networks there is constant monitoring of all incoming and outgoing data on cloud systems. However the target is lucrative which makes it worth the increased difficulty for cyber criminals. A well-executed attack on a cloud providers database can give access to the information of all of their customers and lead to further penetration from the cloud onto the internal intranet and LAN systems of customers.
Paige Leidig, SVP at CipherCloud	I expect to see compliance regulations and cloud continue to drive one another in 2014. The trend over the last year has been for various governments and standards bodies to strengthen privacy mandates around the world. From the ICO in the UK to PCI for retailers, a major compliance trend was that of regulators updating the rules to clarify security responsibility and to tighten the requirements for protecting information in the cloud. I think cloud adoption will continue to grow in 2014. This consumption of cloud services will feed data privacy, security and regulatory concerns for sensitive information in the cloud. The Snowden revelations have heightened awareness for these issues among consumers, enterprises and cloud providers. The recent moves by Google and Yahoo to upgrade encryption levels are just the beginning. In 2014, we'll see providers continue to fortify their networks. And I think specialist partners will play a crucial role because the ecosystem approach works best for certain security implementations. Encryption, for instance, gives customers the tightest control over their data when they hold the keys because this prevents third party access to the keys and encrypted information. To enable this for the cloud requires third party encryption software that the enterprise customers deploy.
Ron Gula, CEO of Tenable Network Security	Security concerns are heightened, and the BYOD market continues to develop The backlash against the security of cloud based providers who are suspected to be in partnerships with government intelligence and law enforcement agencies will continue to rise. Additionally, the mobile device management market will continue to stay vibrant, as more and more organisations start to tackle the BYOD problem. There will also be an increase in acquisitions of MDM vendors throughout 2014, leading to a continuously changing market landscape.
Phil Dawson, CEO of Skyscape Cloud Services	Significant progress has been made this year in helping a wide variety of public sector organisations realise the benefits of cloud computing. The Government's G-Cloud programme – which celebrated its first anniversary in February and the launch of the latest iteration of the Framework, G-Cloud 4, in November – has continued to change the way that the UK public sector uses and procures IT services. Yet there is still a way to go in eradicating the deep-rooted, excessively risk-averse culture. As we near 2014 (which, as we now know, will be the year of the first electronic car tax system!) more and more public and private sector services have moved, or are in the process of moving over to digital, and cloud adoption is sure to continue increasing. However, with data breaches seemingly par for the course, we can expect organisations to place a much greater focus on the security credentials of prospective cloud suppliers and whether or not these have achieved a credible accreditation status. This in turn is likely to increase competition among Pan-Government Accredited (PGA) providers, particularly those that offer services in the highest Impact Levels (ILs) – at IL3 and above. Currently, there are only a small number of suppliers that have achieved IL3 accreditation and so in 2014 we hope to see a rise in competition at this more secure end of the market via G-Cloud.

Seth Goldhammer, director of product management, LogRhythm	Cloud security will rise up the corporate agenda While users of cloud technologies have primarily focused on accessibility and productivity, next year will see security become a much bigger priority. This means a demand for better visibility of APIs to audit activities and events, such as Amazon Web Service's CloudWatch.
Paul Ayers, VP EMEA at Vormetric	A few months ago we were all oblivious to the US NSA's surveillance system, PRISM; however it is this one event that has already set the tone for cloud computing in 2014. The revelations on the whole have understandably aggravated data security and sovereignty concerns about information held in the cloud. While the fallout is expected to cost US-based providers of hosting services tens of billions of dollars internationally, it is fair to assume that EU-providers are equally unlikely to emerge unscathed as doubt sets in. In multi-tenant environments run by third-party providers, that may (or may not) have the proper security safeguards in place, it is ultimately up to the data owner to make sure they understand what controls are in place to protect their information. Controls that lock down data at its source and address who is accessing what data and for what purpose are integral. In turn, these controls will reduce the attack surface and mitigate the risk presented by the all-powerful 'privileged users' like sysadmins, cloud admins and Root who have all too often are able to read and copy data that they do not need to have access to.
Lital Asher-Dotan, product manager, Rapid7	Cloud security will continue to be increasingly important; however, it will not be sufficient as a stand-alone focus. Organizations will need to understand the complete context for user risk, incorporating cloud usage and security concerns along with other potential areas of risky user behaviour. We believe comprehensive behavioural monitoring across on premise, cloud and mobile environments will be needed to better indicate and manage potential threats.
Ian Lowe, senior product marketing manager, Identity Assurance, HID Global	NFC could hold the key to securing multiple cloud-based applications Enterprises and other large organisations that moved to cloud-based tools – including SaaS vendors like Salesforce.com and HR/Accounting tools like ADP – have lost secure access to their data along the way, and this is a big problem. Moreover, the traditional defences these organisations have spent, in some cases, millions of pounds setting up are no longer sufficient to protect them and their data. With sensitive information now residing beyond the company firewall, and multifarious threats like APTs on the rise, the focus is likely to shift to resolving challenges centred-on secure access and identity management across multiple cloud-based applications rather than merely securing the operating platform or device in use. The availability of NFC technology in smartphones, laptops and tablets enables them to communicate with each other for a variety of access control applications within a trusted boundary. NFC-based authentication has the potential to solve the security, convenience, cost and complexity problems of earlier solutions, while making it easier for enterprises to employ strong authentication not only on the desktop, but also to applications, servers and cloud-based systems as part of a multi-layered security strategy. NFC-based solutions will also provide a valuable platform for extending strong authentication to include a third factor in the form of something the user is (which can be ascertained through a biometric or behaviour-metric solution – templates could be stored directly on the smartphone, which would be presented for authentication to a camera, scanner or other biometric device).
Vijay Basani, co-founder, president and CEO, EiQ Networks	in 2014 we will see more enterprise data being moved to the cloud – public and private. Increased competition from Cloud ISaaS providers will make it lot more affordable for companies of all sizes to begin using the cloud. This will in turn attract the attention of hackers and cyber thieves / nation states to compromise cloud infrastructure and steal data. We will see several breaches in the cloud. Cloud Service Providers will begin to offer SLAs which will also include Security & Compliance.
Bala Venkat, CMO at Cenzic	The number of connected devices per user will multiply 5 to 10 fold by 2015. These devices will be managed via cloud posing new interactions and challenging security environment. Mobile apps and devices connecting individuals anyplace to anything will increase security risks both at the device and application level. New attack surfaces (smart meters, remote medical monitoring devices, smart cars, security cameras, etc.) will be managed in the cloud and pose complex threat vectors. More attacks via Supply Chain and Vendor Applications connecting to the parent networks as cloud becomes the norm!
Jason Hart, VP Cloud Solutions at SafeNet	Increase in account takeover on cloud applications. In 2014 we can expect cloud adoption to increase significantly across the UK, however the number of cloud applications that currently support the ability for two-factor authentication is very small. Without the traditional access controls that are implemented via the enterprise network, currently the only thing protecting the enterprise assets in the cloud is often a weak, static password. Therefore, in 2014 we can expect to see a rise in the number of account takeovers on cloud applications. We have already seen this start to materialise in 2013 and can expect this problem to intensify over the next 12 months. Cloud adoption will drive a fundamental shift in authentication to networks, applications and services. The adoption of cloud, along with changing user expectations around authentication, is creating a fundamental shift in awareness in how we – as end users and organisations – authenticate to networks, applications and services. 2014 promises exciting developments for the authentication market. I believe this will be a year in which we will witness the adoption of new authentication schemes that will further change the way we protect our accounts and identities in the cloud. At one end, having a seamless, portable identity and authentication tools that do not require us to remember dozens of passwords, will become possible. At the same time, more and more services will become secure by abandoning the reliance on passwords and moving to strong authentication, identity federation and single-sign-on technologies. Security risks will become more hybrid. Cloud adoption is galloping forward, as threat vectors continue to escalate and in 2014 we can expect security risks to become more hybrid as we are now between the corporate network and the cloud. As a result, enterprises will be more strident in their demands that cloud providers secure their offerings with HSM-based hardware-root-of-trust. Amazon has already taken a first step in this direction by offering Amazon Cloud HSM which secures their services and encryption keys. It will be these services that will provide customers with the confidence that they are creating the same level of security across the board.
Eddie Sheehy, CEO of Nuix	Many organisations will migrate their data from behind-the-firewall systems to the cloud. The big losers will be pure-play archive vendors such as Symantec and HP Autonomy, and the remaining Lotus Notes installations.
Jeff Jones, Director, Trustworthy Computing, Microsoft	In the wake of heightened concerns about unauthorized access to data, we will see the emergence and broad promotion of regional Cloud service offerings. The increased sensitivity to both legal data access and intelligence monitoring will be seen as a market opportunity that will be actioned in two ways – startups and existing providers. Regional start-ups will see a new opportunity to compete against global providers, while existing providers will develop and offer services delivered from regionally-based data centers in an effort to allay concerns and provide increased customer choice. We also anticipate continued levels of interest in the efforts of technology company support of principles to reform government surveillance practices
Kaspersky	'Clouds' are facing tough times. First, trust in cloud storage has been hit hard by Snowden's leaks and the newly discovered facts of data collection by various state-sponsored intelligence services. At the same time, the types of data being stored in these facilities are becoming ever more attractive to cybercriminals. Three years ago we assumed that in due course it would be easier for a fraudster to hack a cloud storage provider and steal company data from there, rather than hacking the company itself. It looks like that time is almost upon us. Hackers are targeting cloud service employees, seeing them as the weakest link in the security chain. A successful attack here could hand cybercriminals the keys to huge volumes of data. In addition to data theft attackers may be interested in deleting or modifying information, which in some cases may be even more valuable for those who commission the attacks.
Chris Harding, Director of Interoperability, The Open Group	Identity, access and entitlement management are crucial when cloud computing is used in conjunction with other new disruptive technologies such as social media, mobile communications, and big data. There will be important standardisation work in this area over 2014, which The Open Group will aim to adopt in

its definition of Open Platform 3.0, to enable enterprises to use these technologies effectively for business advantage.

Geoff Webb, Director of Solution Strategy, NetIQ	Cloud computing has taken a few hits of late. The security of the infrastructure of the internet has been called into question by revelations of the US government's work to undermine encryption technologies. It is likely that cloud computing companies will focus on re-establishing trust in their customers and in increasingly open discussions about the use of encryption to keep data safe.
Garry McCracken, VP Technology Partnerships, WinMagic	Many industry experts like to use the analogy that the cloud is really just a USB stick in the sky. Unencrypted data in the cloud is just as much or even more of a potential security risk as an unencrypted USB stick. IT must come to terms with the fact that more and more employees are moving away from the USB stick and are leveraging DropBox and other similar vendors for file-sharing needs. Instead of IT turning a blind eye, a top priority should be to find a way to properly encrypt company data without compromising user experience and productivity. Whether we like it or not cloud and BYOD adoption will continue to grow in 2014.
Richard Walters, CTO of SaaSID (an Intermedia company)	Cloud service providers will adopt SSO as standard and go beyond that to extend security controls to the browser Single sign-on (SSO) is often the starting point for organisations extending identity and access management to the cloud. Salesforce Identity was recently launched to extend SSO to third party web and mobile apps. Dropbox launched its SSO feature in May and rival cloud file storage company, Box, has been offering SSO since 2011. Google has instructed developers to use OpenID SSO for all apps uploaded to the Apps Marketplace. From a compliance perspective however, an audit trail is required. Auditors need to see how users interacted with corporate data in between login and logout. We anticipate that more cloud service providers will take the initiative to go beyond SSO and offer web application auditing to assist their customers in removing the blind spot between login and logout enabling them to benefit from using cloud-based services, without risking non-compliance with DPA and other information security standards.
Guy Bunker, SVP Products, Clearswift	Increased attacks on security vendors. We will see an increase in attacks on security vendors to introduce 'backdoors' into their customers. We have seen this in the past, e.g. RSA, but these will increase. The biggest targets will be the cloud security providers – as one backdoor there will open the door into (potentially) hundreds of customers.
Kevin Bailey, Head of Market Strategy at Clearswift	Cloud starts to fray at the seams In the simplest terms, cloud computing means storing and accessing data and programs over the Internet instead of your own computer, whereas a cloud is a visible mass of condensed watery vapour floating in the atmosphere, typically high above the general level of the ground. Why the education on terms? Well the recent disclosed activities of the NSA and GCHQ against Google and Yahoo has raised concerns that appear to challenge the way that cloud computing was intended to work. Security has always been a challenging subject for those deciding to move their operations into a cloud environment, with unauthorised access to business and personal data listing high on the concern list. Cloud providers in 2014 will need to visibly demonstrate how they have shored up their defences so they are able to identify breaches of access or as with the bi-product of a cloud, rain, when sufficient saturation (breaches) happens, precipitation (cloud providers) will fall to the surface, and evaporate (go out of business).
Fred Touchette, Senior Security Analyst, AppRiver	The "Cloud" used to be something that was somewhat of a niche. It was a thing that was unique and easily identifiable. Just a few short years after this buzzword was born, the Cloud is all around us, more like a fog. Personal Clouds are a thing now. The Cloud will continue to be the go to for businesses as people become more comfortable with outside security. Software as a Service will be a key component for businesses and the personal user alike. That's not to say that everyone providing these services will have a proper security model in place as we've seen recently many Cloud service providers have had a less than perfect track record with how they store and protect client data. So as is the case with anything that quickly becomes popular with the consumer, it will also remain popular with the cyber criminal.
Anaplan CEO Fred Laluyaux	Crowdsourcing to become crucial As well as collaboration between departments within an organisation, we also expect to see more collaboration across different businesses in the form of crowdsourcing. By sharing technologies, models and best practice across various sectors and non-competitive companies, we'll be able to dramatically improve how content is created, enriched and delivered. While many may be sceptical that businesses would want to share best practice models with competitors, we're already seeing this happen as industries look to improve processes and exchange information. Cloud first approach to computing The main objections to cloud adoption were traditionally concerns around the security of data and the perceived issues of data integration. During 2013, we hit a real tipping point around the world and across almost all sectors. IT teams started better understanding the value of cloud and began encouraging users to look to the cloud first in order to solve business issues. Next year, I predict that this trend will continue and all verticals, including previously slow adopting government and banking organisations, will be looking to the cloud to tackle IT and businesses challenges.
Nathan Pearce, Cloud/SDN Marketing Architecture, F5	2014 will see an explosion of XaaS markets. Software as a Service (SaaS) is already too broad and must now support sub-categorisation with clearer definitions. For example, Disaster Recovery (DRaaS), Security (SECaaS), Management (MaaS) have already been defined and we can expect to see further granularity of definitions appearing over the next 12 months. EMEA, in general, has been slow to adopt cloud computing, with concerns about security and regulatory compliance coming up again and again. However, with the growing popularity of cloud-based financial services like TEMENOS T24 showing how it can be done safely, we should expect this to now change. Volumes have been written about SDN in 2013, but in 2014 we will finally start to see it breaking into the mainstream – with more pilot projects maturing into production environments and an increased interest in the technology from a more diverse customer base. 2014 could very well be the year of Software Defined Anything (Application Services, Datacentres, Storage, etc.)
Matt Hines, Product Manager at FireMon	As use of cloud-based applications evolves every year, so have related concerns around security. When the cloud first emerged much of the concern was around whether services providers could be trusted to adequately protect sensitive corporate data, or maintain segmentation between customer databases to ensure that improper access or data collection wasn't a risk. Nowadays cloud security has certainly become far more accepted and some of those basic concerns have been abated. However, what we're seeing is greater demand from services providers themselves for methods of validating the security of their networks and operations on a continuous basis to provide assurance back to users in a consistent manner, to comply with regulatory standards and even use the strength of their internal security controls as a marketing tool in winning over new customers. There is also a lot of activity around security related to virtualisation among cloud providers and within organisations that build and maintain their own "internal cloud" services. With the continued expansion of virtualisation and the move toward newer paradigms such as software defined networking (SDN) there is a far more rapid pace of change and even greater complexity as underlying infrastructure is being continually optimised to support particular functions or services. With this change, much of which is becoming more automated, there is even greater need to assess the state of network security controls to ensure that as infrastructure is being adjusted, controls are being evolved effectively to ensure that related security gaps are not being introduced.
Sean Sullivan, security advisor at F-Secure	Location, location, location. And also, what is the core business of the cloud provider? Cloud computing from advertising companies based in the United States will face challenges. European companies have any opportunity – if they can act quickly enough. Even so, security and/or *privacy* (aka surveillance) concerns could hurt cloud computing growth in 2014.

Sean Power, security operations manager for DOSarrest	Companies need to recognise the gap in security that cloud offerings can pose. While business and financial benefits may look good on paper, often cloud services share infrastructure and are left fairly undefended against attacks with little or no consideration given to security in the small print. Because they use shared infrastructure, if one business is attacked, the rest will also be susceptible and the collateral damage can potentially be catastrophic. Companies need to be aware of this and make sure that their security strategies extend over the entire company architecture and into the cloud. It is also important to note that you can't box the cloud- meaning that once your business operates in the cloud, you cannot simply put a DDoS mitigation device (for example) at the front of it and call it a day. Cloud services call for protection in the cloud.
Alexander Gostev, Chief Security Expert at Kaspersky Lab	Attackers will increasingly focus on cloud storage facilities The cloud facing tough times. Firstly, trust in cloud storage has been hit hard by Snowden's leaks and the realization that our data is being collected by various state-sponsored intelligence services. At the same time, the types of data being stored in these facilities are becoming ever more attractive to cybercriminals. Three years ago we assumed that in due course it would be easier for a fraudster to hack a cloud storage provider and steal company data from there, rather than hacking the company itself. It looks like that time is almost upon us. Hackers are targeting cloud service employees, seeing them as the weakest link in the security chain. A successful attack here could hand cybercriminals the keys to huge volumes of data. In addition to data theft, attackers may be interested in deleting or modifying information, which in some cases may be even more valuable for those who commission the attacks.
Carl Leonard, Senior Security Research Manager EMEA at Websense	Attackers will be more interested in cloud data than your network Cybercriminals will focus their attacks more on data stored in the cloud vs. data stored on the network. This tactical shift follows the movement of critical business data to cloud-based solutions such as Google, Microsoft Office 365 and Confluence. Hackers will find that penetrating the data-rich cloud can be easier and more profitable than getting through the "castle walls" of an on-premise enterprise network. No doubt, attackers will still infiltrate enterprise networks to target users, steal information and compromise their systems. However, such attacks will serve as an intermediate step to gain access to third-party cloud services instead of an internal data store. It is vital for the organisation's IT team to understand how important the company's data is, in order to protect the information accordingly Implementing a comprehensive DLP solution can help you identify what data is in the cloud and where it resides and ensures your data is protected.
Chris Drake, FireHost CEO	The likes of Drop Box and Box are setting themselves up to IPO and this says a lot about changing attitudes towards the cloud. There's a general increase in cloud services available and clearly businesses are more comfortable using cloud applications than they once were. Organisations are willing to move more business processes to cloud models and, guess what, cybercriminals are going to be fully aware of that. 2014 will see larger volumes of sensitive data hosted online and organisations will need to ensure they take the necessary precautions to secure it. Just as cloud computing is providing new opportunities for business, it is also doing the same for hackers. Cybercriminals can now easily deploy and administer powerful botnets that run on cloud infrastructure and we'd expect to see further instances of this over the next twelve months. Unfortunately, many cloud providers don't adequately validate new customer sign-ups so opening accounts with fake information is quite easy. Once the account is created, application programming interfaces can be leveraged to deploy a lot of computing power on fast networks, giving a person the ability to create substantial havoc with minimal effort.
Garry Sidaway, Global Director of Security Strategy at NTT Com Security	Why is security still the blocker to cloud? Because again to look back at Microsoft it is security by obscurity. This is not acceptable to any business as they are responsible to their board and their clients to be able to ensure that they have put in reasonable measures to protect their information assets. Cloud providers need to demonstrate these controls are in place. We will also see greater use of Software Defined Networks and Software Defined Perimeters to transition businesses to the cloud and to maintain the security controls that are already in place within the traditional perimeter. We will also see the greater focus on services and embedded security. Services that focus on providing trusted domains within the cloud, such as an identity cloud. A focus on seamless services that don't simply manage a virtual firewall, but protect the whole business process.