



Leveraging Technology to Ensure Compliance with Cyber Security and Data Privacy Regulations and Threats

Interview with Ann Marie Keim
Assessment & Authorizing Official and IT Security Official at NASA

Certain regulations mandate that companies maintain reasonable security procedures and protocols to protect sensitive information and be able to demonstrate their compliance with regulatory security mandates. In this interview, Ann Marie Keim, Assessment and Authorizing Official and IT Security Official at NASA, shares some insights on how companies can implement reasonable technological safeguards.

Legal IQ: Your session at the upcoming Cyber-Risk and Data Breach Management Summit will feature a presentation on technological safeguards an organization can implement to provide better data protection and superior control over identity protection. Can you give us an overview of what some of these safeguards are?

Ann Marie Keim: So far this year there have been over 550 reported breaches and while 95 of those are a result of outside hacks, a good portion of these are a result of lost or stolen portable devices such as laptops, smartphones, PDAs, thumbdrives, even SD cards that were in possession of the employees, while outside the work environment. People leave phones in cabs all the time, laptops disappear from airports, buses, trains, and coffee shops daily. Consider the types and amount of data that can reside on these devices, confidentiality becomes a key concern. Data at rest (DAR) should absolutely be a consideration for any mobile device. There are products available for enterprises as well as small and mid-sized businesses and prices range from free to 'if-you-have-to ask...'. In the case of businesses covered by HIPAA, hefty fines can be levied for portable devices that AREN'T encrypted!

User awareness is also key – do your users know how to safeguard data? And maybe more importantly, do your users understand WHY it's important to safeguard it?

And there are the obvious technical solutions: antivirus, antispymware, and antimalware software should be in place.

Legal IQ: Companies differ greatly in resources, and the nature of the business conducted – how does a company determine the level of technological safeguards they need to have in place?

Ann Marie Keim: The role of IT Security is NOT to implement controls or even to audit...it's to protect the business, no matter WHAT that business might be. The level of safeguards is determined by a business impact assessment...what would the impact to the business be if something went 'boom', if there was a successful breach? Would it be an inconvenience or a major negative event? Some people use the term Risk Assessment. It's determining the likelihood of an event, and the resulting impact if that event happened. What is the likelihood that a threat will become a reality? Many times managers, especially of small businesses, think they are too insignificant to become a target of attack. There IS no one too small. Hackers are indiscriminate, and anyone with a web presence is a target. Once you have a clear picture of your risks, likelihood and impact, you can dedicate your resources to the ones that will give you the most bang for your buck, and protect your most critical assets.

Legal IQ: What is the scope of the biggest risks organizations are currently facing, and can expect to encounter in the future?

Ann Marie Keim: Obviously the outside threat continues and will continue to be a major threat. The economics of cybercrime is just too great to ignore, and often it's a state or nation sponsored activity. As many resources as a company can dedicate to cyber security, you can bet that there are more of 'them' than there are of you. APT stands for 'advanced' (they have more skills than you), persistent (they have more time and resources than you), and threat (they are a very real threat to you). Many local economies, particularly in some developing parts of the world, RELY on cybercrime and if it's not openly encouraged, it's at least not discouraged.

The other major threat is, again, mobile devices. As the lines between business and personal use blurs, and the app markets flood with malware, more corporate data will be exposed and compromised.

Botnets will continue to be an issue, with millions of employees home computers compromised and guess what happens when they bring that company USB drive home to work on papers over the weekend? The malware copies itself and when introduced to the corporate network, allows a window into your internal and private network.

Legal IQ: What defenses are organizations employing to counteract and anticipate these threats?

Ann Marie Keim: Best practices deal with 'defense in depth', starting with perimeter defenses, both physical and logical via firewalls, and intrusion detection and intrusion prevention appliances. Many of these have come a long way in terms of pricing and ease of installation, use and ongoing maintenance.

User awareness will play a big part. We are only as secure as our least secure person, and the actions of one can affect many! I'm sure the executives who have fallen victim to a social engineering ploy or phishing email that resulted in leaked documents or information breached wished they questioned before answering that email or clicking on that link.

More companies, especially those bound by regulations that require a pro-active role in keeping information confidential, are adopting data at rest, encrypting data on the servers, and enforcing identity and access management solutions.

Legal IQ: You have an upcoming show on the Nasa IT security channel on "traveling safely with mobile media". Can you give us a preview of the insights you have on this topic?

Ann Marie Keim: Sure! As I mentioned, hackers are constantly coming up with new ways to capture our identities and information, and have even resorted to setting up rogue wifi hotspots in airports, hotels and public places, with similar sounding names as the legitimate spots. They're relying on us not paying attention to what we're doing and attaching to their networks, logging onto facebook to tell all our friends that we're not home! Many people still use the same password for multiple sites and their email. Once thieves get one, they have access to a lot of things!

The new passports have an RFID chip in them that is easily monitored from several feet away. If you don't have one of the RFID blocking wallets, get one.

And don't forget that not all identity theft is technical – shoulder surfing is not dead, and any Sunday morning in a coffee shop can garner a lot of information.

Ann Marie Keim is a speaker at the upcoming Cyber-Risk and Data Breach Management Summit in New York City, November 30 to December 2, 2011. For more information or to register visit www.cyber-riskmanagement.com or email info@iqpc.com.

