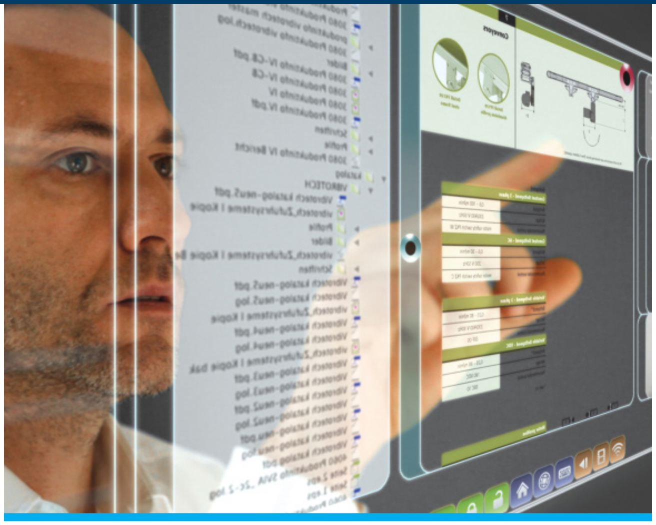
2014 Cyber Security Forecast

December 2013



Experts predict that heightened expectations among consumers, advocates and regulators will require organizations to step up cyber measures in the year ahead

Kroll, the global leader in risk mitigation and response solutions, today released its third annual Cyber Security Forecast, a prediction of the most significant cyber issues organizations will confront in 2014. The latest forecast highlights seven trends identified by Kroll and suggests that a changing tide in cyber standards, both social and legal, will require organizations to take stronger actions and safeguards to protect against reputational, financial and legal risks.

Predictions

1. NIST and similar security frameworks will become the de facto standards of best practices for all companies.

Between the Snowden fallout and increased scrutiny by the FTC and other regulators in the U.S. and around the world, cyber security strategies that were largely designed for companies that were part of the "critical infrastructure" will become more of an expectation for everyone, from conducting an effective risk assessment to implementing sound cyber security practices and platforms. Whether compulsory or unstated, these standards will drive organizational decision-making with regard to cyber security. Organizations that don't follow suit may find themselves subject to shareholder lawsuits, actions by regulators, and other legal implications.

"This trend will move the U.S. in the direction of the EU, where there is a greater recognition of privacy as a right," said Alan Brill, senior managing director at Kroll. "As new laws evolve that reflect the NIST guidelines and look more like the EU privacy directive, some U.S. companies will find themselves ill-prepared to effectively respond to the regulations. To minimize their risk, organizations will have to get smart on these standards and make strategic business decisions that give clients and customers confidence that their information is protected."

2. The data supply chain will pose continuing challenges to even the most sophisticated enterprises.

It is not unusual for companies to store or process the data they collect by using third parties. However the security that these third parties use to safeguard their client's data is frequently not understood until there is a breach. Additionally, companies may believe that their subcontractors will notify and assist them in the event of a breach. Unfortunately, this is often not the case. Companies will need to vet their subcontractors closely and get specific as to the technical and legal roles and responsibilities of their subcontractors in the event of a breach.

"Kroll has responded to breaches where subcontractors not only failed to provide timely notice that they were breached, but also refused to cooperate with the investigation. Companies should know who they are giving their data to and how it is being protected," said Tim Ryan, managing director and Cyber Investigations practice leader. "This requires technical, procedural, and legal reviews."

3. The malicious insider remains a serious threat, but will become more visible.

“Et tu, Brute?” Whether it was Shakespeare’s Caesar or America’s Benedict Arnold, we have long known the pain of betrayal by those we trust. Information technology simply made the betrayer’s job easier. In 2014, a significant number – if not almost half – of data breaches will come at the hands of people on the inside. However, as the federal government and individual states add muscle to privacy breach notification laws and enforcement regimes, the hidden nature of insider attacks will become more widely known.

“There’s a tremendous amount of data compromised today where the act is never discovered or disclosed. People discount the insider threat because it doesn’t make the news. Instead, we see headlines about external credit card breaches and theft of personally identifiable information, because regulations mandate accountability and punishment is expensive. The insider threat is insidious and complex. Thwarting it requires collaboration by general counsel, information security, and human resources. SEC breach disclosure of “material losses” may be the model for rules requiring a company to be more transparent and answerable for allowing bad actors to go unpunished,” said Ryan.

4. Corporate board audit committees will take a greater interest in cyber security risks and the organization’s plans for addressing them.

With more and more data breaches – from theft of trade secrets to loss of customer information – in the headlines, corporate audit committees are beginning to focus on the connection between cyber security and an organization’s financial well-being.   As such, they will expand their attention beyond the financial audit process to the organization’s strategic plans for protecting non-public information and risk mitigation plans for responding to a possible breach. CIOs and IT leadership should prepare accordingly.

“Organizations recognize that it’s their duty to protect against the loss of information and its associated risks,” said Brill. “As corporate boards carry out their fiduciary responsibilities, they must also protect the company from possible shareholder lawsuits that allege the company's cyber security wasn't at a level that could be reasonably viewed to be ’commercially reasonable’ and that incident response plans weren't in place to mitigate the risk. The challenge they face is determining what is a reasonable level of security and response, and who should make that call – is it their IT team, an industry expert, an independent third party?”

5. Sophisticated tools will enable smart companies to quickly uncover data breach details and react faster.

Companies realize that even the best firewalls and intrusion detection systems cannot stop all attacks; the most secure firms experience computer security incidents. But technological progress over the last 12 months will enable companies to unravel events and see with near-real-time clarity what’s happened to their data and how much damage has been done. That is, if companies choose to change.

“Most organizations have invested in preventative security technologies, but remain unprepared to launch an effective response to a leak or intrusion. Without the right tools and policies in place beforehand, they find themselves suddenly under intense pressure to investigate, track, and analyze events,” said Ryan. “It takes more money and time to scramble at the last minute. We’ve seen a dramatic improvement in response technology over the last year. Companies have never had a better opportunity to enhance their existing protocols with a methodology that can mean an informed and timely response. There’s no reason not to be prepared.”

6. New standards related to breach remediation are gaining traction and will have a greater impact on corporate data breach response.

Credit monitoring will no longer be the gold standard in breach remediation in 2014, as lawmakers, consumer advocates and the public at large continue to raise questions about the relevancy and thoroughness of this as a stand-alone solution and demand a more effective alternative. While no legal guidelines currently exist for consumer remediation, the FTC and states like California and Illinois are already offering guidance that suggest a risk-based approach to consumer remediation – one that matches remedy to individual risk based on the unique circumstances of a breach – will be the way of the future.

“The notion that credit monitoring is a panacea for all data breaches is misguided. When you couple the myriad types of sensitive information with the multitude of ways an identity can be stolen and used fraudulently, there are many instances where credit monitoring will not be helpful to a breach victim at all, including medical identity theft, criminal impersonation, employment and tax fraud, etc.,” said Brill. “That’s not to say that credit monitoring is useless because it’s a valuable tool when it aligns with the type of data exposed. Rather, companies will need to gain a better understanding of their actual breach risks, how the breach could actually affect their customers, and the best way to remedy those specific risks and provide better protection to the affected consumers."

7. As Cloud and BYOD adoption continues to accelerate, greater accountability will be required for implementing policies and managing technologies.

The development and evolution of Cloud services and BYOD has moved at a whirlwind pace, leaving IT departments scrambling to get out in front of the technologies and employee usage. In 2014, IT leaders will need to work closely with senior leadership and legal counsel to adapt corporate policies in a way that addresses changing legal risks, while effectively meeting the need of the organization.

"Up until now, cloud and BYOD adoption has been like the Wild West – uncharted, unregulated, and few restrictions. However, we're seeing courts issue rulings that include significant penalties where discovery, disclosure and other legal obligations aren't being met because of the use of these technologies," said Brill. "While it's implausible to anticipate every possible risk presented by the use of the cloud and BYOD, companies that have integrated these technologies into their corporate policies, IT security, and risk management plans will be much better prepared to fulfill their legal obligations. Organizations must realize that even if they don't want to deal with this, they're not going to have much choice."

About the Experts

Timothy P. Ryan is a Managing Director with Kroll and the Cyber Investigations Practice Leader for North America. Tim joined Kroll's Cyber Investigations Practice after a distinguished career as a Supervisory Special Agent with the Federal Bureau of Investigation (FBI), where he supervised the largest Cyber Squad in the United States and also led one of the FBI's largest computer forensic laboratories. An expert in responding to all forms of computer crime, attacks, and abuse, Tim has led complex cyber investigations involving corporate espionage, advanced computer intrusions, denial of service, insider attacks, malware outbreaks, Internet fraud and theft of trade secrets. Tim is an adjunct professor at Seton Hall University School of Law.

Alan Brill is a Senior Managing Director for Kroll and founder of Kroll's global high-tech investigations practice. With more than 33 years of consulting experience, Alan has assisted firms with a wide range of technology security issues. He has worked on many large-scale reviews of information security and cyber-incidents and has extensive experience developing methodologies for collecting evidence from corporate information systems and consults on everything from computer intrusions to the misappropriation of intellectual property. Additionally, Brill served as an instructor for the FBI, Secret Service, Federal Law Enforcement Training Center, AICPA, and many others.

About Kroll

Kroll, the global leader in risk mitigation and response, delivers a wide range of solutions that span investigations, due diligence, compliance, cyber security and physical security. Clients partner with Kroll for the highest-value intelligence and insight to drive the most confident decisions about protecting their companies, assets and people.

Kroll is recognized for its expertise, with 40 years of experience meeting the demands of dynamic businesses and their environments around the world. Headquartered in New York with offices in 45 cities across 28 countries, Kroll has a multidisciplinary team of nearly 4,000 employees. Learn more at http://www.kroll.com.

Certain Altegrity companies provide investigative services. State licensing information can be found at www.altegrity.com/compliance.

Kroll®