



Kroll Announces Top Ten Cyber Security Trends for 2012

Nashville, TN - December 14, 2011

The Cyber Security and Information Assurance Division of Kroll Inc., today released its annual security forecast, highlighting key areas of risk and trends that will impact how organizations and governments combat and respond to cyber threats.

“The events of 2011 suggest that the cyber security landscape will find public and private organizations are still on unsteady footing,” said Karen Schuler, practice leader of the Cyber Security and Information Assurance Division. “Traditional pain points for organizations including mobile technologies, incident response and regulatory requirements will intensify as new and developing challenges surface in 2012.”

“We frequently see organizations with protective measures based on the assumption that they are not a target,” said Alan Brill, senior managing director of the Cyber Security and Information Assurance Division. “Yet 2011 taught us that no one is exempt from attack. Companies need to take a strategic and aggressive approach to cyber security. Ignoring a problem is no guarantee that the problem will ignore you.”

Kroll’s 2012 Cyber Security Forecast includes:

1. Mobile technology security threats will be at an all-time high. Mobile technologies are changing so rapidly that in some organizations the demand and pressure to deploy new technologies (e.g., tablet computers) will outstrip the organization’s existing capabilities to secure them. This unfortunate dynamic is no secret to thieves who are ready and waiting with highly targeted malware and attacks employing mobile applications. Similarly, the perennial problem of lost and stolen devices will expand to include these new technologies and old ones that previously flew under the radar of cyber security planning. For example, digital cameras used by medical facilities to document patient treatment are becoming increasingly attractive to potential thieves. The loss of this type of data represents a potential HIPAA privacy law violation and could have serious ramifications for the health care industry.

2. Social media will increase in popularity as a conduit for social engineering attacks. Social media adoption among businesses is skyrocketing and so is the threat of attack. In 2012, organizations can expect to see an increase in social media profiles used as a channel for social engineering tactics. Thieves will utilize clever tactics to coerce end-users into disclosing sensitive information, downloading malware or both. To combat the risks, companies will need to look beyond the basics of policy and procedure development to more advanced technologies such as data leakage prevention, enhanced network monitoring and log file analysis.

3. Small businesses (SMBs) will enter the crosshairs of cyber attacks. “Hacktivism” may make headlines, but the fact of the matter is that data thieves are simply looking for the path of least resistance. Of late, that path has been leading directly to SMBs that house large amounts of valuable data but lack the data security budgets of their big business peers. Common modes of attack include everything from social engineering to SQL injection. In addition, ongoing use of legacy systems – weakened by postponed or overlooked upgrades and replacements – put SMBs at heightened risk.

4. As cloud services gain in popularity, related breach incidents will flourish. If we were meteorologists, we’d definitely be calling for overcast with a chance of storms. Companies are smartly embracing the cloud for the associated cost savings and ease of use. Unfortunately, current surveys and reports indicate that companies are underestimating the importance of security due diligence when it comes to vetting these providers. As cloud use rises in 2012, new breach incidents will highlight the challenges these services pose to forensic analysis and incident response and the matter of cloud security will finally get its due attention.

5. Business and government cooperation will be mission-critical for economic and infrastructure health. Cyber crime has the capacity to cripple almost every aspect of commerce from the largest corporation to the individual consumer. Similarly, the security of U.S. infrastructure is being called into question in disturbingly real ways. For these reasons there is a growing sentiment among both private organizations and the U.S. government about the increased need for information sharing. Improved communication between the private and public sectors will not only give government the ammunition needed to take down major threats, it will also increase private entities' capacity to respond to large threats more effectively.

6. Privacy concerns will keep geolocation technology in a white-hot spotlight. Geolocation technology is the quintessential double-edged sword. On one hand, consumers love the convenience of innovative mobile apps and services utilizing this technology. On the other, the backlash against surreptitious tracking or disclosure can be swift and strong. In fact, two federal bills were introduced in 2011 dealing specifically with the protection of geolocational information. It's doubtful either will become law in 2012, but we can expect to see privacy advocates urging businesses to adopt an opt-in or consumer consent model.

7. Management and analysis of logs will gain more respect for its role in incident preparedness and response. Security incidents have increased in sophistication and frequency in recent years and one of the most effective modes of response involves maintaining complete logging for the network and key applications. While historically undervalued, logging provides vital information that can be utilized for analysis of network activities and documentation of security incidents. As companies begin to see the error in their ways in 2012 they will begin to implement formal risk assessments to look for security weak spots.

8. Incident Response Teams will get a permanent seat at the table when it comes to standard business operations. Historically, incident response teams were made of employees from across the organization tapped to mobilize only if and when security incidents occurred. But to remain competitive in today's market companies need to upgrade incident response teams from contingency plan status to day-to-day operations. Effective incident response teams can include a group of full-time employees designated as incident responders or a team of outside consultants (via a third party) hired for 24/7 incident response support.

9. Companies will overlook key vulnerabilities, as regulatory compliance continues to drive organizational security. Let's face it – state and federal regulations remain the yardstick by which the comprehensiveness of data privacy and security are measured. But using such a “checklist mentality” to drive security initiatives is dangerous because a number of data security regulations overlook basic IT security controls. Certainly there are regulations that address the need for encryption or the development of an incident response plan but few require a wide range of best-practice controls such as up-to-date anti-virus software. As more breaches occur as a result of security gaps, we should expect to see governing agencies offer specific guidance on risk assessment and standard IT security controls.

10. Breach notification laws will gain traction outside of the US. While the U.S. Congress struggles to reach consensus on a federal breach notification law, internationally the idea is gaining momentum. Germany began requiring breach notice in all sectors in 2010 and several other EU nations have expressed interest in putting similar requirements in place. Meanwhile, Canada is also considering mandatory breach notice as part of proposed revisions to PIPEDA, which governs how Canadian businesses collect, use and disclose personal information. Companies with a global presence should watch these developments closely because they could have significant impact on their operations abroad.

About Kroll

Kroll, the world's leading risk consulting company, provides a broad range of investigative, intelligence, financial, security, technology and supplier management services to help clients reduce risks, solve problems and capitalize on opportunities. Headquartered in New York with offices in 52 cities in 29 countries, Kroll has a multidisciplinary team of approximately 2,800 employees and serves a global clientele of law firms, financial institutions, corporations, non-profit institutions, government agencies and individuals.