IT Governance, Risk & Compliance

Coalfire Predicts: In 2015 the Cost of Cybersecurity and Risk Management Will Remain on Track to Double

Cost fueled by cyber-crime, cyber-ware, and cyber-terrorism

DENVER – Dec. 9, 2014 – Coalfire, the leading independent information technology governance, risk and compliance (IT GRC) firm, today released its top ten cybersecurity predictions for 2015.

"As 2014 ends, it is clear this was the year everything changed in the world of information security," said Rick Dakin, Coalfire's CEO and chief security strategist. "As high-profile data breaches were announced one after another, consumers stopped believing companies took protecting their information seriously. It's time for companies to start looking ahead at the next generation of threats and to step up their game to better protect consumer data. The threat landscape is continuously evolving. If you don't already have threat intelligence and response plans ready for implementation in 2015, now is the time."

Coalfire conducts more than 1,000 audit and assessments of systems containing sensitive data each year. Based on the trends in those investigations, Dakin predicts the following for 2015:

1. **Motivated Threat Actors** – The number and sophistication of cyber threats will continue to increase exponentially. Fueled by both geopolitics and economic incentives, international (and often state sponsored) criminal organizations will escalate their development of offensive cyber capabilities.

2. **Redefining the Defense** – The demands of cybersecurity are fundamentally changing IT. Cyber risk management and security compliance will take an equal weight to other design criteria like functionality, capacity and performance. Financial ROIs will be balanced by a new understanding of risk exposure for sub-par solutions.

3. **Three Heads vs. One** – In large organizations, there are technical roles that require the knowledge and experience of CIOs, CTOs and CISOs. While some have predicted the death of the CIO role, we see instead a balancing of responsibility between three peers.

4. **Investments Will Increase** – In the face of pernicious new threats, the cost of cybersecurity and risk management will remain on track to double over the next three years.

5. **New Fronts –** The expansion of mobility, cloud computing, bring-your -own - device (BYOD) policies, and the Internet of Things will provide new (and previously unforeseen) opportunities for cyber-crime, cyber-warfare, and cyber-terrorism.

6. **Universal Monitoring** – As a result of cyber-incidents, every organization (or person) will be using some form of continuous monitoring service (threat, scanning, identity or credit). These will be legislated, mandated by financials institutions or insurers, or acquired on their own behalf.

7. **Business Leadership on Policy Development –** Executive leadership will lead to further development and maturation of standards across private sector and governmental organizations. This approach to security and cyber risk management will reduce the potential for “unforeseen” damage from cyber-attacks, cyber warfare and cyberterrorism.

8. **New Threat Detection and Response Technologies –** There will be an increased use of crowdsourcing, machine intelligence, and cognitive/advanced analytics to detect and stay ahead of threats. Bounties for catching bad actors and advanced algorithmics will help the “good guys” identify and stay ahead of the hordes of malicious players.

9. **Improved Security –** New and better applications of authentication, EMV, encryption and tokenized solutions will increase the security of payments and other personal and confidential information. Apple Pay and other next-generation solutions will overcome anti-NFC inertia and lead to increasing adoption of mobile-based security technologies for both retail payment and other applications, such as healthcare, where critical and confidential information is exchanged.

10. **Back to Offense –** We will see the beginnings of a shift from cyber-defense to cyber-offense. From attempting to build impenetrable systems, to building systems that make it possible to identify attackers and provide the means to prosecute, frustrate or delay them.

About Coalfire
Coalfire is the leading, independent cyber security and risk management firm that provides audit, assessment, advisory and compliance management solutions. Founded in 2001, Coalfire has offices in Atlanta, Boston, Dallas, Denver, Los Angeles, New York, San Francisco, Seattle, Orlando, Washington D.C. and England and completes thousands of projects annually in retail, financial services, healthcare, government and utilities. Coalfire’s solutions are adapted to requirements under emerging data privacy legislation, the PCI DSS, GLBA, FFIEC, HIPAA/HITECH, HITRUST, NERC CIP, Sarbanes-Oxley, FISMA and FedRAMP. For more information, visit www.coalfire.com.

Contact:
Stephanie Vanderholm
303.883.8832
svanderholm@metzgeralbee.com

###