



## PRESS RELEASE

### **BYOD Survey: 47 Percent of Users Lack a Password on Smartphones Accessing Company Files**

*Coalfire survey reveals 84 percent of respondents use the same mobile device for personal use and work; more than half report their companies have no mobile device usage policy*

**Louisville, Colo. – August 14, 2012** – Gone are the days when employees only used a company-issued phone or laptop for work. Today, employees bring personal smartphones and tablets to the office and often have access to sensitive company information on these devices.

Coalfire, an IT governance, risk and compliance (IT GRC) services company, recently conducted a survey on the Bring Your Own Device (BYOD) to work trend. The findings reveal many companies are not discussing mobile device cybersecurity issues with their employees and lack policies to protect sensitive company data.

The survey was conducted last month among 400 individuals in a variety of industries across North America that do not work in IT departments.

“The BYOD trend is not slowing down, and while it has many benefits, it’s also introducing a number of new security risks that may be foreign to many companies,” said Rick Dakin, CEO and chief security strategist with Coalfire. “The results of this survey demonstrate that companies must do much more to protect their critical infrastructure as employees work from their own mobile devices, such as tablets and smartphones, in the workplace. Companies need to have security and education policies in place that protect company data on personal devices.”

The results of this survey highlight that as the BYOD trend continues to rise in popularity [cybersecurity awareness training](#) needs to improve

between employers and employees. The majority of individuals are still using “unsafe” methods when it comes to mobile device security, especially when it comes to how they store passwords. By not providing the proper training for employees, companies are leaving themselves vulnerable to cyber attacks and data breaches.

Key findings of the survey include:

- 84 percent of individuals stated they use the same smartphone for personal and work usage.
- 47 percent reported they have no passcode on their mobile phone.
- 36 percent reuse the same password.
- 51 percent of respondents stated their companies do not have the ability to remotely wipe data from mobile devices if they are locked or lost.
- Despite the growing awareness, 60 percent of respondents are still writing down passwords on a piece of paper. There is progress, however, as 24 percent reported using a password management system, 11 percent are saving an encrypted document on their desktop and 7 percent have a document saved on their desktop.
- Nearly half of all respondents - 49 percent - stated their IT departments have not discussed mobile/cybersecurity with them.

To review more of the survey’s findings [click here](#).

### **About Coalfire**

Coalfire is a leading, independent information technology Governance, Risk and Compliance (IT GRC) firm that provides IT audit, risk assessment and compliance management solutions. Founded in 2001, Coalfire has offices in Dallas, Denver, Los Angeles, New York, San Francisco, Seattle and Washington, D.C. and completes thousands of projects annually in retail, financial services, healthcare, government and utilities. Coalfire has developed a new generation of cloud-based IT GRC tools under the Navis™ brand that Coalfire clients use to efficiently manage IT controls and keep pace with rapidly changing regulations and best practices. Coalfire’s solutions are adapted to requirements under emerging data privacy legislation, the PCI DSS, GLBA, FFIEC, HIPAA/HITECH, NERC CIP, Sarbanes-Oxley and FISMA/FedRAMP. For more information, visit [www.coalfire.com](http://www.coalfire.com).