Faronics U.S. and U.K. Survey Reveals BYOD, Unstructured Data, Check and Credit Card Fraud Most Critical Threats

Organizations Frequently Fail to Understand Repercussions of Data Breaches,
Continue to Underinvest in Data Protection

VANCOUVER, B.C. and SAN RAMON, Calif. November 13, 2012 – Faronics, a global leader in simplifying, securing and managing multi-user computer environments, today announced the results of its *State of Cyber Security Readiness* survey, which examines the cyber threat and data breach experiences of small and medium-sized businesses (SMBs). The research was completed by The Ponemon Institute.

When asked about a range of threats most likely to affect their organization's ability to achieve its business objectives, more than three quarters of respondents in both the U.S. and U.K., 76 percent and 77 percent, respectively, consider check or credit card fraud either "likely" or "very likely." Respondents included executives from many levels of these organizations, ranging from the owner/partner to outside consultants, but were heavily weighted toward the director, manager, supervisor and technician levels.

The top three threats to their organizations listed by U.S. respondents included "proliferation of unstructured data," (69 percent), "unsecure third parties including cloud providers, (65 percent) and "not knowing where all sensitive data is located, (62 percent). U.K. respondents had a slightly different set of concerns: 62 percent believe "proliferation of end-user devices" is a key issue, as well as "lack of security protection across all devices," (cited by 56 percent) and "unsecure third parties including cloud providers," (53 percent).

"Although organizations have become more aware of potential threats, they do not seem to accurately perceive the repercussions associated with data breaches," said Dmitry Shesterin, vice president of product management at Faronics. "Findings indicate that organizations do not understand the full costs and damages they will suffer as a result of a data breach. These organizations need to become more proactive about their security programs in order to minimize the damage they will inevitably experience from one, if not more, data breach."

A common belief labels IT departments and managements as too complacent with security and data protection, leaving their organizations vulnerable to cyber threats. However, Faronics' survey found otherwise. Just 9 percent among U.S. respondents and 4 percent in the U.K. admit "security is not taken seriously because our organization is not perceived as being vulnerable to attacks." Among other key survey findings:

- 64 percent of U.S. respondents and 75 percent of U.K. respondents cited "insufficient people resources" as a primary barrier to achieving effective security
- 62 percent of U.K. respondents consider "the complexity of compliance and regulatory requirements" as a key barrier.
- 55 percent listed "lack of in-house skilled or expert personnel"
- 50 percent of U.S. respondents noted "lack of central accountability" and 41 percent listed "lack of monitoring and enforcement of end users"

When queried about the impact of data breaches on their organizations, more than half of U.S. and U.K. respondents cited the loss of time and productivity most frequently. Both U.S. and U.K. respondents also listed damage to their organization's brand second most frequently. According to the findings among companies that experienced a data breach:

- 42 percent of U.S. respondents and 38 percent of U.K. respondents stated they "lost customers and business partners"
- 41 percent and 34 percent of U.S. and U.K. respondents, respectively experienced an increase in the "cost of new customer acquisition "
- 35 percent of U.S. respondents and 31 percent of U.K. respondents "suffered a loss of reputation"

"This is the first study to investigate what smaller companies in North America are doing to prevent and detect cyber attacks," said Dr. Larry Ponemon, chairman and founder of Ponemon Institute. "Results indicate that companies tend to seriously underestimate the potential damage to brand and reputation, revealing a great data breach perception gap. Misconceptions about the consequences associated with a data breach are preventing organizations from implementing the necessary financial tools, in house-expertise and technologies to achieve cyber readiness."

Survey findings uncover that IT managers made security and data protection investment decisions based on ease of deployment and ongoing operations as well as low purchase costs. The majority of respondents, 73 percent in the U.S. and 78 percent in the U.K., seek products and solutions that enable easy deployment. U.K. teams further indicated the importance of minimal maintenance effort with 62 percent of respondents listing the "ease of ongoing operations" as a key factor influencing security investments, followed by 58 percent seeking "low purchase cost" and 52 percent seeking low total cost ownership (TCO). U.S. teams indicated a greater concern with costs, as 65 percent of respondents listed "low purchase cost" as a primary influencer over the 60 percent who listed "ease of ongoing operations" and half who listed "low TCO."

Among the data protection solutions respondents most frequently employ today; 65 percent and 75 percent, respectively of U.S. and U.K. respondents employ firewalls and other perimeter security technologies. Thirty-six percent of U.S. and 53 percent of U.K. respondents turn to blacklisting and/or whitelisting tools to identify content with vulnerabilities. A significant plurality of IT teams relies on enforcing strict data policies, cited by one-third of U.S. and 45 percent of U.K. respondents.

For further information, the full survey report can be found www.faronics.com/ponemon.

About Ponemon Institute

Ponemon Institute conducts independent research on privacy, data protection and information security policy. The company's goal is to enable organizations in both the private and public sectors to have a clearer understanding of the trends in practices, perceptions and potential threats that will affect the collection, management and safeguarding of personal and confidential information about individuals and organizations. Ponemon Institute research informs organizations on how to improve upon their data protection initiatives and enhance their brand and reputation as a trusted enterprise.

About Faronics

With a well-established record of helping organizations manage, simplify, and secure their IT infrastructure, Faronics makes it possible to do more with less by maximizing the value of existing technology. Their suite of products ensures 100% workstation availability, and frees up IT teams from tedious technical support and software issues. Incorporated in 1996, Faronics has offices in the USA, Canada and the UK, as well as a global network of channel partners. Faronics solutions are deployed in over 150 countries, and are helping more than 30,000 organizations worldwide.

Additional information about Faronics can be found on www.faronics.com.

###

Press contacts:

North America
Cathy Goerz., Alexis Murray-Merriman
Stearns Johnson Communications
T: +1 415.397.7600
E: faronics@stearnsjohnson.com

Europe
Hannah Townsend or Richard Scarlett
Johnson King
T: +44 (0)20 7401 7968
E: faronics@johnsonking.co.uk