



SafeNet, Inc. Survey Sheds Light on the State of the Data Breach; 66 Percent of Security Professionals Believe They Will Suffer a Data Breach within the Next Three Years

1 out of 5 of Enterprise Security Professionals Would Not Entrust Their Personal Data to their Own Networks

BALTIMORE – February 12, 2013

- 1 out of 3 (35 percent) security professionals surveyed stated that their security investments are being deployed to the wrong technologies
- However, 95 percent continue to invest in and employ the same data security strategies
- While almost 3 out of 4 (74 percent) security professionals believe that their perimeter defenses are effective, 1 out of 2 (59 percent) said that if a network perimeter breach were to occur, their high-value data would not be safe.

SafeNet, Inc., a global leader in [data protection](#), today announced results from a survey conducted by SafeNet of 230 United States security professionals, revealing that, despite continued investments in network perimeter technologies, respondents are not confident that they are employing the right technologies to secure their high-value data.

This became abundantly clear when more than 74 percent of respondents indicated that while they believe network perimeter defenses are effective at keeping unauthorized users out, 31 percent of those same respondents acknowledged that their network perimeter defenses have been breached in the past. What is more concerning is that 20 percent said they were not even certain whether or not they had been breached, indicating that the respondents may not have the right technologies in place to detect whether an internal or external security breach has occurred. The security breach survey results raise numerous questions as to whether the enterprise has the sufficient data protection technology to record accurate audit trails, enforce compliance, and maintain control of their data, whether it is on premise or in a cloud or virtual environment.

Survey Reveals that While a Breach Prevention Strategy is Necessary, It's Not a Panacea for Today's Threat Environment.

Ninety-five percent of respondents state that they have either maintained or increased their investment in network perimeter security; however, more than half (55 percent) of those respondents felt that their company was not spending enough on security. These statistics appear contradictory, but in questioning the respondents further, it became clear that current threat mitigation technologies are undermining confidence in the entire industry that supplies them.

When asked if they were confident in the security industry's ability to detect or prevent security breaches, only 19 percent were confident, 49 percent remained unconvinced that the industry can thwart current threats, and 33 percent have become less confident in its ability to do so.

Corporate Headquarters:

4690 Millennium Drive
Belcamp, Maryland
21017 USA
Tel.: +1 410 931 7500 or 800 533 3958,
Fax: +1 410 931 7524,
Email: info@safenet-inc.com

EMEA Headquarters:

Tel.: +44 (0) 1276 608 000,
Email: info.emea@safenet-inc.com

APAC Headquarters:

Tel: +852 3157 7111
Email: info.apac@safenet-inc.com

Media Contacts:

Michele Loguidice
Tel: 443 327 1409
Email: michele.loguidice@safenet-inc.com



Investments in network perimeter technologies continue to rise even in the face of a growing data breach epidemic, which they have failed to adequately address.

Security Professionals Believe Their Organization Will Experience a Breach but Remain Uncertain on the Best Way to Prevent It

When asked if the recent spate of security breaches caused respondents to rethink their security strategies, more than half (52 percent) stated that high-profile data breaches have indeed caused them to adjust their data security strategies. However, when survey respondents were asked if they believe a security breach could happen, over 65 percent believe they will suffer a data breach within the next three years.

In addition, 35 percent of the survey respondents admitted that they believe their company is investing in the wrong security technologies and, as a result, when asked if their data would remain secure if the perimeter was breached, over 59 percent said that their data would not be safe. As budgets remain tight, security officials are confronted with how best to allocate their resources to ensure the security of their high-value data in an increasingly perimeter-free world.

The data breach survey results further underscore the difficulties security professionals face in identifying the technologies that will keep their data safe as that data transitions from the datacenter to the cloud.

Dave Hansen, President and Chief Executive Officer, SafeNet, stated, "While the overall IT and threat landscape has dramatically changed over the past several years, the security industry has been slow to adapt to those changes. Today's threat landscape demands a mindset that moves beyond attempting to achieve absolute breach prevention. Organizations must accept that a breach will happen and implement strategies such as encryption that secure the breach by making the data useless to anyone but its rightful owner. Threats to vital infrastructure and high-value data have outgrown traditional breach prevention strategies, such as network perimeter security and anti-malware, and it is clear that maintaining the same approach of years past is antiquated and dangerous. As an industry, we know what needs to be done, and the time for change and action is now."

SafeNet has adopted a [new approach to security](#) that is built around the assumption that the perimeter has been breached. The company has published a Secure Breach Manifesto that outlines the current state of the data breach epidemic and the roadmap security professionals can follow when implementing a strategy that "Secures the Breach".

SafeNet will be in attendance at the RSA Conference USA 2013 later this month in booth #1825 to demonstrate the strategies and tools necessary to "Secure the Breach".

Supporting Resources:

- **Secure Breach Manifesto:** http://www2.safenet-inc.com/securethebreach/downloads/secure_the_breach_manifesto.pdf
- **Blog Post:** Security Industry: The Sanity Test, Tsion Gonen, Chief Strategy Officer <http://bit.ly/U5PHTx>
- **Follow SafeNet** on [Twitter](#), [Facebook](#), [YouTube](#), and [LinkedIn](#)

Corporate Headquarters:

4690 Millennium Drive
Belcamp, Maryland
21017 USA
Tel.: +1 410 931 7500 or 800 533 3958,
Fax: +1 410 931 7524,
Email: info@safenet-inc.com

EMEA Headquarters:

Tel.: +44 (0) 1276 608 000,
Email: info.emea@safenet-inc.com

APAC Headquarters:

Tel: +852 3157 7111
Email: info.apac@safenet-inc.com

Media Contacts:

Michele Loguidice
Tel: 443 327 1409
Email: michele.loguidice@safenet-inc.com



About SafeNet, Inc.

Founded in 1983, [SafeNet, Inc.](#) is one of the largest information security companies in the world, and is trusted to protect the most sensitive data for market-leading organizations around the globe. SafeNet's data-centric approach focuses on the protection of high value information throughout its lifecycle, from the data center to the cloud. More than 25,000 customers across commercial enterprises and government agencies trust SafeNet to protect and control access to sensitive data, manage risk, ensure compliance, and secure virtual and cloud environments.

Corporate Headquarters:

4690 Millennium Drive
Belcamp, Maryland
21017 USA
Tel.: +1 410 931 7500 or 800 533 3958,
Fax: +1 410 931 7524,
Email: info@safenet-inc.com

EMEA Headquarters:

Tel.: +44 (0) 1276 608 000,
Email: info.emea@safenet-inc.com

APAC Headquarters:

Tel: +852 3157 7111
Email: info.apac@safenet-inc.com

Media Contacts:

Michele Loguidice
Tel: 443 327 1409
Email: michele.loguidice@safenet-inc.com