

November 29, 2011

published by [mar.com](#)

## Top ten cyber security trends for financial services in 2012

29 November, 2011  
By Mark Cox

2012 will be a pivotal year for banks and investment firms as they try to stay ahead of the IT security curve, says Booz Allen Hamilton, a strategy and technology consulting firm

"These trends highlight the fact that cyber security today is about living with and managing the risk in your network. It's more than just preventing security violations," said Bill Wansley, senior vice president at Booz Allen Hamilton.

"Every day, it's essential that the financial services industry -- from small community banks to large Wall Street institutions -- know what cyber security threats are on the horizon, and how the cyber and technology industries are meeting these concerns," Wansley said. "Today's business environment requires financial institutions to be more creative in meeting the demands of their customers, shareholders, and regulators.

"As the list of companies victimized by hacking grows, it is clear that no network is completely impenetrable, but there are effective solutions that can help" said Wansley. "To thwart these attacks, one must embrace a dynamic defense that embodies the same aggressive, nimble, and methodical approach as our cyber adversaries use against us today. As the daily headlines remind us, cyber security isn't something on which anyone can declare victory. Cyber security is now a relentless operational risk issue for every organization that develops or delivers value."

Booz Allen Hamilton sees ten cyber security trends being important for financial services.

1. The exponential growth of mobile devices drives an exponential growth in security risks. Every new smart phone, tablet or other mobile device, opens another window for a cyber attack, as each creates another vulnerable access point to networks.
2. Increased C-suite targeting. Senior executives are no longer invisible online. Firms should assume that hackers already have a complete profile of their executive suite and the junior staff members who have access to them.
3. Growing use of social media will contribute to personal cyber threats. A profile or comment on a social media platform -- even by the CEO's son or sister -- can help hackers build an information portfolio that could be used for a future attack.
4. Your company is already infected, and you'll have to learn to live with it-- under control. Security should remain a priority, but today's risks and threats are so widespread that it will become impossible to have complete protection-- the focus of cyber security tactics increasingly must be to analyze, detect and expunge threats inside your system.

5. Everything physical can be digital. The written notes on a piece of paper...

### PROMOTIONS

PromoPipeline Exclusive Channel Promotions  
Find Out How You Can Make Money Today!  
ENROLL FREE! >>

### BLOGS

Please join me on MSPTv  
Robert M. Cohen - Integrated  
[mar.com](#)

To Write or Not to Write Hasnt that Always Been the Question?  
Beth Vanni - Amazon  
Consulting

Borders Bites the Dust a Prediction for IT Integrators in the Wake of Cloud?  
Beth Vanni - Amazon  
Consulting

Navigating in a Channel-Less World  
Diane Krakora - Amazon  
Consulting

Getting Carried Away in the Channel  
Diane Krakora - Amazon  
Consulting

5. Everything physical can be digital. The written notes on a piece of paper, the report binder and even the pictures on the wall can be copied in digital format and gleaned for the tools to allow a hacktivist-type of security violation, and increasingly this will be a problem.

6. More firms will use cloud computing. The significant cost savings and efficiencies of cloud computing are compelling companies to migrate to the cloud. A well designed architecture and operational security planning will enable organizations to effectively manage the risks of cloud computing.

7. Global systemic risk will include cyber risk. As banks and investment firms continue on the path to globalization, they will become increasingly inter-connected. A security breach at one firm can create negative ripple effects that greatly impact systemic risk in financial markets.

8. Zero-day malware (malicious software) and organized attacks will continue to increase. Like a vicious, insidious virus that mutates, the tools of cyber criminals adapt and change constantly, rendering the latest defenses useless. Firms need to be prepared to adapt quickly as well to zero-day malware and the tactics of organized crime and foreign adversaries that are increasingly used today.

9. Insider threats are real. The accidental insider breach will continue to be the primary source of compromise for the Advanced Persistent Threat (APT) and other attacks. Organizations need to focus on security awareness training and internal monitoring to detect intentional and accidental insider access.

10. Increased regulatory scrutiny. Recently, the Securities and Exchange Commission introduced guidelines that require companies to report incidents that result, or could possibly result in, cyber theft or a risk of compromised data considered material.

[home](#) | [feedback](#) | [printer friendly version](#) | [email this article](#)

©2009 Integrated mar.com Corporation | 1.800.465.2059