

What should be the main 2012 trend? Mobile Security

With all the predictions of what's coming for 2012 floating around, one really should stand out: Increased mobile security.

For example, it is extremely rare when any politician goes out on a limb, so it's important to take note when they do. Case in point: Rep. Dutch Ruppersberger (D-Md.) said the following at a trade group's round table in December:

"As a member of the House Intelligence Committee, I am often asked what keeps me up at night, and one of the key issues is cyber threat. Some of our top officials predict, and I agree, we will have a catastrophic cyber attack within the next year. Whether it's an attack on a banking system or a grid system, it is going to happen and we need to be sure we protect ourselves."

Ruppersberger and Committee Chairman Mike Rogers (R-Mich.) introduced a bipartisan bill, passed by the committee 17-1, that gives the federal government new authority to share classified cyber threat information with approved American companies. ABA supports the bill, Doug Johnson, senior policy analyst, tells Tech Topics. In fact, the committee reached out to the association for advice in drafting it, he says.

The limb-sitting goes on. "There are two types of companies in this country: those who know they've been hacked, and those who don't know they've been hacked. Economic predators, including nation-states, are blatantly stealing business secrets and innovation from private companies," Rogers says in a release.

From there it is a short leap to the newest but fastest growing banking channel, including payments—mobile. A study by Deloitte found that "Information security threats have increased on multiple fronts over the past 12 months including hackers, cyber criminals, and state-sponsored actors intent on targeting intellectual property, customer information, and increasing business disruption. Coupled with the increased use of emerging technologies, such as the cloud, mobile devices, and social media, it's not surprising that information security breaches were reported by 75% of the 138 global organizations surveyed."

Observers from mobile central, namely Verizon's annual data breach investigations report, say much the same.

"We witnessed highly automated and prolific external attacks, low-and-slow attacks, intricate internal fraud rings, country-wide device tampering schemes, cunning social engineering plots, and much more," its executive summary says.

Eight out of ten incidents were targets of opportunity, Verizon says. "Unfortunately, breaching organizations still doesn't typically require highly sophisticated attacks...The majority of data is stolen from servers, victims usually don't know about their breach until a third party notifies them, and almost all breaches are avoidable (at least in hind sight) without difficult or expensive corrective action."

Meanwhile, KPMG just issued a report that concludes a greater number of consumers today "are embracing mobile banking, and many others might do so except for privacy and security concerns."

"Consumers are clearly open to using their mobile devices to conduct everyday transactions and will steadily move in this direction for years to come. With mobile banking now gaining widespread acceptance, the challenge for banks will be to develop a mobile payment solution that effectively allays security and privacy concerns," says Mitch Siegel, a KPMG principal.

A formidable challenge indeed, when a survey just released by the National Cyber Security Alliance is taken into consideration. It finds that 72% of Americans have never installed data protection applications or security software on their smartphones in order to protect against data loss, viruses, and malware.

"While mobile internet users may feel their devices are safe, data thieves and hackers continuously evolve their operations to take advantage of user vulnerabilities. Mobile malware incidents are still relatively low in number, but with smartphones and tablets eclipsing unit sales of desktop and laptop PCs, cyber criminals will continue to set their sights on mobile," the alliance says.

All of which places banks dead center between providing customers hungry for mobile banking/payments, while highly sophisticated cyber criminals work to break in, and customers themselves inadvertently open themselves to exploitation.

Conclusion: Finding ways to increase mobile security must be a top priority in 2012.

#

Sources used for this report include:

Holiday Mobile Device Shoppers Take Heed: New Study by National Cyber Security Alliance and McAfee Reveals Lack of Cyber Safety Among Mobile Users

Privacy, Security Issues Hamper Wider Growth of Mobile Banking, Despite Increasing Consumer Acceptance: KPMG Survey

Broader Security Threat Landscape, Increased Use of Emerging Technologies Require More Information Security Investment by TMT Companies: Deloitte Survey

Government Official Predicts Catastrophic US Cyber Attack

Verizon 2011 Data Breach Investigations Report

Bipartisan Cybersecurity Bill Clears Key Hurdle

Ruppersberger, Rogers Introduce Cybersecurity Bill to Protect American Businesses from "Economic Predators"

About the Author

John Ginovsky is contributing editor of ABA Banking Journal and editor of the publication's TechTopics e-newsletter.

For more than two decades he has written about the commercial banking industry. In particular, he's specialized in the technological side of banking and how it relates to the actual business of banking. He previously was senior editor for Community Banker magazine (which merged with ABA Banking Journal) and was a staff writer for ABA's Bankers News.