The Magnificent Seven

Seven 2012 Trends in Bank Technology that will Affect 2013

2012's Magnificent Seven

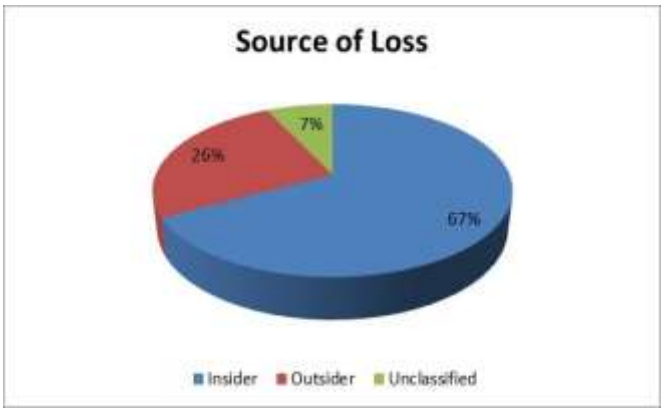
It's that time again! Time to define the seven most important trends we've watched over the past year. This means that, in most cases, these trends are still trending, and should drive our 2013 tactics.

This year's top seven trends are (drum roll please):

1. Continued Breaches Due to Unawareness
2. Compliance with the Supplement
3. Corporate Account Takeovers
4. Orchestrated Attacks Against American Banks (still ongoing)
5. Mobile Banking (and look for virtual wallet and NFC in 2013)
6. Increased likelihood of Pretext Calling
7. Smishing Scams on the Rise

Number One: Continued Awareness Breaches:

Our number one 2012 trend is the fact that even now, after all our efforts, banks are still losing data thanks to a lack of awareness on the part of our own employees. It's the same old number (67%) we've always seen, but digging into the data might enlighten us a bit.

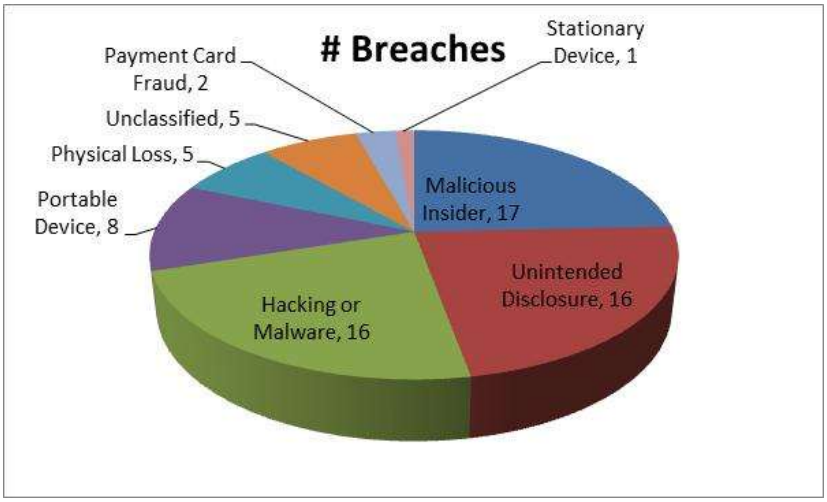


According to our analysis of the publicly known breaches ***of financial institutions*** listed at privacyrights.org, 70 data breaches at United States Banks were made public in 2012. Seventeen of those breaches were caused by a malicious insider, meaning that someone with legitimate access intentionally breaches information - such as an employee or contractor. We think banks need to be realistic that 24% of breaches came from malicious users.

Sixteen of those breaches were "Unintended Disclosures," meaning that sensitive information was posted publicly on a website, mishandled, or sent to the wrong party via e-mail, fax, or mail. This is what we usually think of when we hear about insider breaches.

Eight of the breaches were due to lost, discarded, or stolen portable devices (laptops, PDAs, Smartphones, etc.). Again, these were at US Banks. More than 10% of the breaches were due to bankers losing their portable device.

Five of the breaches were "paper loss," where an employee discarded sensitive information in a manner that does not comply with our Destruction of NPI policies. They didn't use the shred box, and they embarrassed the bank.



That leaves 26% of the breaches due to external threats . . . . the threats we most worry about, the hackers and the corporate account takeovers. Maybe our strategy this year should focus on awareness training . . . not at the expense of protecting ourselves against the external threats, but in addition to that protection.

Number Two: Compliance with the Supplement:

Most of our Clients continue to implement actions to bring themselves into compliance with the FFIEC's June 2011 Supplement to the 2005 Guidance on Authentication in the Internet Banking Environment. The theme of the supplement is "layers of security." The layers called for are robust authentication, anomaly detection and response, and customer education.

While they have been forced (yet again) to rely upon (and wait for) their vendors for answers to the authentication layer component of the supplement, most of our Clients are still investigating effective methods for implementing Detect and Response, and are at least talking to their marketing people about the marriage of security and marketing, in the form of Customer Education. We think most community-based banks will be listing Customer Education as a high priority in 2013.

Number Three: Corporate Account Takeovers

The reason Supplement Compliance will be a high priority in 2013 is because of the fact that corporate account takeovers are part of a trend that has bank's realizing real monetary losses. We have at least three clients who are dealing with this very issue right now. The good news? The supplement was right.

Number Four: Orchestrated Attacks Against American Banks (still ongoing)

The fourth trend we are witnessing in real time is the Distributed Denial of Service attacks on American banks. We've all read the press on this. It can happen to us too. We predict that this trend will continue, and we should dust off our incident response plans in case our providers are attacked. I agree with the skeptics that these organized criminals are probably not going to target a small bank in the middle of Indiana. Instead, they will target your provider. So dust off your incident response plans. How are you going to communicate to your on-line banking customers that your system will be "off-line" until further notice?

Number Five: Mobile Banking

The use of SmartPhones only quickened in 2012 and we all agree this will continue long past 2013. All the risks we predicted in 2009 related to mobile banking are alive and well. The difference in the near future will be a result of near field communication (NFC). Look for virtual wallets to not only cause irritating breaches and fraud, but also a loss of market share. Maybe 2013 is too early for your sized community. MAYBE NOT.

Number Six: Increased likelihood of Pretext Calling

2012 was the year that our phone rang off the hook with bankers looking for someone to implement some pretext calling tests. Most of our Clients are experiencing pretext calling on a regular basis. Unfortunately privacyrights.org does not list pretext calling as a source of a breach. Furthermore, most pretext calling breaches go unnoticed, and are one record at a time. But we see them being used not just by the nosy neighbor, but also as part of malicious attacks on banks and bank customers.

Number Seven: Smishing Scams on the Rise

Smishing is the text-message version of phishing, where the bad guys send a text (SMS) to your customers, asking them to either click on a link or, in the cases we've seen, call an 809 area code where they can unlock their locked account. While we've only seen one smishing scam in 2012, we were struck by how easy it was to pull off, and how difficult it would be to trace evidence back to a perpetrator. With SMS banking becoming more popular, and all we've already stated about awareness, customer education, and portable device risk, we see this trend in 2012 being a big driver of issues in 2013.

Note: Privacyrights.org (www.privacyrights.org) is an excellent source of information about information breaches that were made public. The search capabilities on this site make it a great tool for information security officers to help their employees understand WHY controls exist.