Putting Trust at the Heart of Your Brand Identity

Posted by MHB in IT Peer Network on 02-Mar-2015 10:41:43

We're all familiar with bank security, and it's no wonder. We want our banks to take security seriously — after all, it's our money and our personal information they're protecting!

Indeed, security touches every aspect of a financial organization. You need your customers to trust your brand because, if they don't, they'll take their business elsewhere.

Risking the Breach

It's not just the loss of business from a few unhappy customers that you're risking if you get this wrong; lapses can quickly spread alarm. We've all seen the high-profile headlines about security breaches. Unfortunately, when it comes to banking, trust is won in drips and lost in buckets. And then there's the financial cost. In a report published in 2015, our security partner McAfee estimates that around $400 billion is lost to cybercrime every year. At a more local level, I learned at the Sibos conference that the average loss for a U.S. bank from a cyberheist is estimated around $1.3 million, compared to just $6,000–8,000 for a physical bank robbery. According to the Symantec Intelligence Report, between November 2013 and October 2014, 583 million identities were stolen online.

There's already a lot of great work being done to combat cybercrime, but unfortunately, fraudsters are clever, and are constantly changing their approach to try and beat the latest countermeasures. Financial institutions are the best defended against attack though, meaning cybercriminals typically go after softer targets such as retail and hospitality industries. Financial organizations are vulnerable in that they sometimes rely on industries that may not have the same level of security as they do. For example, a recent McAfee infographic estimates that we can expect 50 billion internet-connected devices by 2019, each of which presents an opportunity for a fraudster.

How to Combat the Onslaught

So, privacy and security are as important as performance in financial services. They've been a concern for a long time, and remain vital even as we adopt exciting developments like the SMAC stack, cloud business transformation, and big data analytics. At Intel, we're developing ubiquitous security and identity protection solutions across all our computing platforms (both on the client and in the data center/cloud) to ensure that robust security is always there. For example, we've worked with major banks and payment providers in Europe to implement a two-factor authentication solution that minimizes friction for the bank's customers and reduces cost.

To summarize: the third Industrial Revolution has started, and to remain competitive you need to be agile, innovative, and open to change as an organization. Do this by embracing new technology platforms, adopting the cloud, understanding your data through analytics, promoting cultural change internally, and staying ahead of cybercrime with effective security. Keep these points in mind, and you'll be a revolutionary leader. Further developments in the European banking security space will be discussed in the next blog. I'll explain how we are building on existing technologies with biometrics and additional levels of authentication for both enterprise and consumer use cases.

To continue the conversation, let's connect on Twitter.

Mike Blalock

Global Sales Director

Financial Services Industry, Intel

This is the fifth installment of a seven part series on Tech & Finance. Click here to read blog 1, blog 2, blog 3, and blog 4.