Data breach security… Where’s Plan B?

“Hacked” used to be a term that referred to one’s anger over a situation. In today’s context, hacked means another system breach and a lot of upset (hacked) customers. The alarming part has to do with the fact that these events are becoming more and more common.

• • •

The latest big example came when Sony announced that its PlayStation database was hacked including the potential compromise of 70 million users of the PlayStation network. In other words, the personal information, including credit and debit card numbers, of their customers was exposed and potentially stolen.

The story of system breaches is being replayed over and over again. (The ramifications from the RSA Security breach in March are still being felt.) It is as though vendors only have one line of defense and they never expect that their respective security systems will be penetrated.

Where was Sony when its system was being probed? Did system alarms go off notifying managers of an attack? Was this an inside job? Was the Sony security controller asleep at the console?

Given these constant announcements of electronic security breaches, it would appear to me that security is not being taken seriously in a global sense. There are a lot of questions I could ask here, and I am sure that someone closer to the situation will ask them, but let’s take a moment to establish a few common practices when it comes to systems and security that you should take very seriously.

The Wombat’s Security Standards

1. Any system should expect attacks at all times and from multiple entry points!

2. You should assume that your security system will be breached at some point.

a. From outside the firewall.

b. From inside the enterprise.

3. All systems should have secondary and tertiary lines of defense growing in strength and complexity at each level. We refer to these as Plan B and Plan C!

4. System monitoring should be 7 x 24 and real time (not month end, end of week or tomorrow morning), and should cover both external (firewall) and internal (changes to the network and system access) threats.

5. Identified events should receive immediate intervention (virtual and immediate) and be fully investigated even though they have been thwarted, to determine potential vulnerabilities.

6. Customer data should be compartmentalized, with separate security and access, and be encrypted (with separate access to the encryption keys).

7. Executive management must be actively engaged in understanding security and risk.

8. Risk is always increasing—treat it that way!

It is naïve to assume that security, once established, will always be effective. It is also naïve to assume that attacks will always come from outside the enterprise. Vigilance must be a constant in today’s organization; always looking for weakness as opposed to reacting to it.

Furthermore, when you ask and receive customer information, be it email or financial, the responsibility to protect your customer’s trust and their information just moved into an entirely different realm. Let’s not forget, the internet and technology can be as dangerous as it is convenient.

The Wombat!

About the Author

Dan Fisher is president and CEO of The Copper River Group, a consulting firm headquartered in Fargo, N. D., that focuses on technology and payment systems research and consulting for community financial institutions. For nearly 30 years, Fisher has worked in the financial industry using technology to improve the bottom line. He was CIO of Community First Bankshares (now part of BancWest), has served as a director of the Federal Reserve Board of Minneapolis, the chairman of the American Bankers Association Payment Systems Committee, and was a member of the Independent

Community Bankers of America Payments Committee. Fisher has written numerous articles on banking technology and the payments system. He has authored or co-authored six books and recently published a book titled, "Capturing Your Customer! The New Technology of Remote Deposit." You can contact Fisher at dan@copperrivergroup.com.

P.S. To understand Dan's nickname, check out "About the Wombat" on his website, www.copperrivergroup.com