RISKY BUSINESS

How good is your security?

Recent events in the financial services world have shown how vulnerable even the largest players can be. They've also shown that the smartest techies can be fooled.

Risk Vector 1

In the US on December 19th, Target confirmed a credit card data breach compromising personal or payment information for what is now believed to be as many as 110 million people – about 45% of the U.S. adult population. Target's CEO, Gregg Steinhafel, was quoted as saying that profits "softened meaningfully" (*sic*) after the theft, by which he probably had in mind that they had fallen 40% in the quarter.[1] To rub salt into the wound, it's been claimed that the hackers penetrated Target's POS system easily enough by using the credentials of an air-conditioning contractor[2]. The lawsuits are just starting.

All of which rather raises the question of "How much will US business be prepared to lose to card fraud before it gives up on mag stripe and invests in Chip and Pin?"

Unfortunately, even Chip and Pin isn't a complete protection against ineptitude: in South Korea, personal information (but not Pin numbers or CVCs) on some 20 million credit card holders – over half the working population – was stolen from three prominent card issuers. Allegedly, the culprit was an IT contractor who simply loaded the data on to flash drives, which he then sold to marketing companies. As a direct result, on January 20th the issuers' CEOs resigned, followed by 20 high level executives. Within three days, their companies received 2.6 million customer requests to reissue or cancel existing cards.

IT contractors running free, live customer information rather than dummy data, memory sticks ad lib – the mind boggles. As in the US, the lawsuits in South Korea are just starting.

Risk Vector 2

Last month's piece took a passing swipe at "all the babble about the 'Internet of Things' and its cousins in the ranks of stratospherically-priced solutions seeking a problem". Some readers took issue with the comment, arguing that technology is a powerful driver of progress.

Partly, of course, it's a matter of personal choice. Take web-connected home appliances for example: do you want your fridge to remind you that you're out of orange juice? Do you want to use your mobile to switch on the burglar alarm? Some of us would find those possibilities empowering and exciting. Others would be unnerved, or at least unmoved, by the prospect.

But we now learn that this whizz-bang functionality has a further dimension: risk.

---

[1] *New York Times*, February 26, 2014

[2] http://www.itnews.com/retail/74142/target-breach-happened-because-basic-network-segmentation-error?page=0,0&source=ITNEWSNLE_nlt_itndaily_2014-02-06

Because it turns out that it may not be just you who's controlling these clever gadgets. Just like any other computer hooked up to the Internet, they can be accessed by the bad guys. Already, a computer security firm has identified a group of around 100,000 so-called "smart" devices that have been built into a network sending out spam e-mails.[3]

In recent demonstrations, hackers have shown they can slam on a car's brakes at freeway speeds, jerk the steering wheel and even shut down the engine — all from their laptop computers.

Apparently, the web-enabled little computers inside your fridge and washing machine in fact aren't so smart: they're standardised, off-the-shelf, bought on price, rather than security. That means they could be used to do much more damage than promote doubtful on-line pharmacies.

Such as, for example, hacking into Bitcoin exchange computers….

Risk Vector 3

The Germans have a splendid word for it: *schadenfreude* – "pleasure derived from the misfortunes of others". Many of those who toil in the payments industry would have felt precisely that on hearing about the troubles at Mt Gox and Flexcoin: the nerds out-nerded, the Internet libertarians finding out just what Internet liberty can mean.

In the light of the failures in Japan and Canada, consider the claims made on a leading website:

"Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network. Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part. Through many of its unique properties, Bitcoin allows exciting uses that could not be covered by any previous payment system."[4]

To an "All Government is bad" believer, that platform probably sounds a passionate call to action. To the sceptic, precisely the same words say "Don't touch it with a bargepole".

Which of them is right? Will events at Mt Gox and Flexcoin sound the death-knell of virtual currencies? It's too soon to tell. But perhaps we can be forgiven a sense of unholy joy at the discomfiture of the current crop of Bitcoin boosters.

Risk Vector 4

Finally, consider the likely reaction of a lender to a borrower looking to finance a mortgage with a loan to valuation ratio of 97%. In today's cautious climate, the reception isn't likely to be enthusiastic.

And yet, this is precisely the leverage ratio – more precisely, of equity to assets – proposed by the Basel Committee of worldwide banking supervisors. To put it another way, what the regulators have

[3] *The Economist*, 25 January 2014
[4] https://bitcoin.org/en/

in mind is that investors' capital should be able to absorb a loss in value of bank holdings of up to 3%. Not a huge ask, the layman would have thought.

Yet many banks have found it a difficult challenge to take on. No doubt, assets have different risk profiles: at this time, a German Government bond is probably a good deal less problematic than a loan made to a Ukrainian property developer. Proper allowance should be made for such differences. Even so, it's not necessary to have the memory of a Methuselah to recall that it was precisely these much-vaunted risk-adjusted ratios that set in motion the collapse of 2008.

As so often, The Sage of Omaha has it right: "Risk comes from not knowing what you're doing".

Roy Stephenson

Background

- With more than 20 years of experience in the payment card industry, Roy was previously with American Express, where as VP and General Manager, he launched the highly successful commercial card business in the UK, going on to lead product rollout across EMEA and latterly Latin America/Caribbean.
- As a consultant, Roy works with banking and payment card clients around the world, identifying and advising on best practices in customer marketing and relationship management. He has also undertaken assignments in media, utilities, airlines and retail.
- He has developed and audited coalition and bank loyalty programmes in the UK, Ireland, the Netherlands, Spain, Canada, Dubai, Kuwait, Australia, Singapore, Spain, Israel, Turkey, Saudi Arabia, Brazil, Chile, Venezuela and Mexico.
- Roy has also advised on airline FF programmes, and has been the rewards lead in the MasterCard Advisors pool.
- He speaks fluent Spanish, reasonable French and is the author of *Marketing Planning for Financial Services* (Gower Publishing). He has a B. Com, holds an MA in Management Studies and is a Fellow of the RSA.
- For further background, client list, articles and sample engagements, please visit www.roystephenson.co.uk