

Safety culture

In October, *FStech* held a retail banking/IT security roundtable, in association with EMC, Stroz-Friedberg and F5, looking at such issues as compliance with security regulations, online banking and the mobile security threat. Highlights as follows

TH: I'll kick things off by running through the main discussion points this evening: compliance with security regulations; online banking and protection against infrastructure attacks; data integrity; and the mobile security threat. Starting with compliance with security regulations, perhaps we could get an idea of the security regulations that those of you around the table have to comply with: stuff around FSA, PCI DSS, SOX and so on.

JPM: I think that a corporation has to deal with all of those things. One of the challenges lies in the fact that you can say, this is PCI DSS and it's credit card processing but where does that credit card processing lie? SOX applies to America, then you need to look at the systems which service America.

TG: That raises the worldwide nature of this discussion. I guess there are three categories: legislation which we all have to abide by (data protection and so on); regulation, whether that's from the FSA or organisations in the US; and there's contractual stuff, which is where PCI DSS falls. I wonder whether there's any real difference other than the enforcement mechanisms - you break the law, you could go to prison. PCI DSS, you get fined.

SM: That's very true. The interesting difference with PCI DSS is that the consequence of that can be much faster than the other two, much more immediate. You might not just get fined, you might be put out of business because they (PCI) have that power

and much more quickly than any national regulator. Then there's the fact that it is not a law, or a regulation derived from some enabling law, it is a voluntary law in the sense that you opt into it. And it's international so there are no borders. That's an interesting development, almost disintermediating governments, which may not be a bad idea.

TG: Do you really opt into it though? Your acquiring bank demands it of you - you don't have a choice.

SM: That's true. Although you could choose not to do that and be a cash only business, for instance. Having said that, you might not be in business in this day and age.

MC: We're a PCI DSS QSA and the only accredited accountancy firm in Europe who provide these services. I only know of a handful of businesses who have been advised that they are no longer able to process payments using cards and/or who have been fined, which is somewhat surprising given how long the standards have been in force. It comes back down to what was being said earlier - there are so many regulations, so much compliance required, that no one ever steps back and takes a holistic view, they spend too much time considering the verticals and invariably end up with a controls framework which is not fit-for-purpose. People tend to look at the individual pieces of the regulation and not at what that regulation is saying.

GS: I think that nowadays there is good support. There are some solutions that provide a library, mixing all the different regulations so you have a unique approach to this. If you have these types of tools in place, you at least have a better understanding of the business requirements and the security objectives and where investment should go, trends in your company and so on.

MC: One of the challenges that I increasingly see as a QSA and which really concerns me and you'll appreciate this if you have reviewed PCI DSS in detail, that businesses are considering compensating controls and alternative control mechanisms and it's ultimately down to the QSA to attest against their effectiveness or otherwise. There is a therefore a considerable risk

Attendees:

Tim Holman, President, ISSA-UK (Chairman)
Simon Burrows, Director, PricewaterhouseCoopers
Stephen Murgatroyd, Business Systems Designer, BCS
Ramzi Musallam, Consultant, Greatpark Consulting
 Representative of JPMorgan Chase
Tony Gee, IT Security Consultant, Friends Life
Mark Child, Partner - IS Risk, Kingston Smith Consulting
Nathan Pierce, Solutions Architect, F5
Vijay Rathour, Vice President, Stroz-Friedberg
Giampiero Saracino, EMEA Security & Risk Management
 Consulting Director EMC



that the standard is being interpreted differently between one QSA to the next. We've engaged clients whereby the standard states the requirement and whilst this isn't necessarily being strictly adhere to, the controls they have in place are entirely appropriate and the card holder environment entirely secure. The QSA is then required to document and attest against these controls, but it's down to interpretation and I don't think it's a coincidence that we've seen a large number of QSAs put into remediation or struck off, perhaps there is a compromise to be had? We have spoken with the PCI DSS Council to relay some of these concerns, and our view remains that a number of QSAs probably don't have all the core prerequisite skills required to adequately pull together a thorough Report On Compliance (ROC). I was a practitioner for circa 20 years and would suggest that you require 10-15 years practical experience to complete a ROC for a PCI level 1 business coupled with prerequisite expertise across all the platforms which are in scope.

TH: The big problem with PCI DSS is, if we look at the UK on its own, you have probably got close to 250/300,000 merchants but the issue is how do you regulate such a vast number of people?

TG: There are thresholds, aren't there?

MC: We always run into the classic question from merchants..."Is my acquirer and bank compliant?" My response is always - no comment! But the merchants themselves are pushing back and I think rightly so. I think this is particularly evident with Small to Medium Enterprises (SMEs), who are really struggling to interpret and subsequently apply the requirements.

TG: There are organisations that have been PCI DSS compliant and they still get fined, so they think what was the point of that?

MC: The liability resides with the QSA. I can understand why the Big Four haven't particularly engaged on PCI DSS QSA. To be honest, it's the only piece of legislation I have encountered which "scares me". To a degree it is inevitable that a Level 1 business is never going to be entirely complaint first time round and is likely to have to "rely" on a number of compensating controls to achieve compliance. As a practitioner it's somewhat of a daunting undertaking when you sign the ROC off.

SM: Talking about the merchants, it strikes me that Europe is more compliant to PCI DSS than North America because America doesn't have chip and PIN and further more has no plans for it, as it's afraid of retailers' reaction to the cost. So, we are safer by definition, but not completely safe as chip and PIN isn't perfect, but it's a lot better than nothing.

GS: The standards adopted in Europe are definitely stronger than elsewhere. The digital signature, for instance, our regulations are highly advanced when compared with the rest of the world. It's a matter of culture, there has been a strong emphasis on security for years.

RH: In terms of the States, over here we have around 12 acquiring banks and in the US they have over a thousand and there is a big problem getting the message out and getting everyone to adopt the PCI standard.

SB: It's interesting that PCI DSS gets such a high profile. A lot of the banks I work with see it as one of their biggest challenges whereas the raft of other requirements and regulations they are subjected to, relatively speaking, are taking a back seat. From an FSA point of view, the largely principles-based approach is somewhat at odds with the PCI approach. There must be a lesson there for the regulators around the fact that PCI now has some teeth, it has some traction and is making people do things, something which the principles-based approach often hasn't achieved.

VR: The principles-based approach, by its nature, is unpredictable and ambiguously defined. As a consumer it's probably desirable to have a regime that can take effect quickly and which has teeth as well. Enterprises are generally aware of the need for prompt action and customer redress when data breaches occur, and private actions, compensation claims and reputational damage are just a few of the problems that can cause. But external standards like PCI certainly help bring focus.

RM: It's about having a robust system of control in place rather than just being able to tick all the boxes. The key should always be to ensure the business has good practice and the right controls and attitudes to the risks as opposed to simply thinking, we'll do this as it's the cheapest option.

VR: There are many overlapping regulatory environments that we have to be conscious of. The FCPA and the Bribery Act, for instance. It can be helpful to have a hybrid approach which ticks the boxes for those regulations that can be boiled down to black and white, but as a contrast you have the principles-based approach where if you do drop the ball it's going to be a very useful defence if you can say that your business had effective systems and processes in place to minimise the risks of such breaches.

GS: There are many organisations who are not taking into account that this is a daily task and not just something that happens when the third party comes in.

MC: It never ceases to amaze me how many organisations still haven't got their risk frameworks right and how much money they've invested in them.

VR: On many occasions I have been asked to assist large, multi-national corporations that have been the victim of an internal or external attack. Organisations of every size can be at risk, and it is vital to seek advice on how to pre-empt and prevent security breaches.

TH: I see compliance officers who are completely independent of the risk officers. Something's broken - they should be brought together. It saves money for starters.

SM: There's an interesting concept called the Swiss Cheese Theory, which was invented by James Reason. What it means is that all the holes in the Swiss cheese have to line up for the incident to occur. The list of holes in some of the companies mentioned is very long. In SocGen, it was a catalogue of things which has just been repeated at USB in shocking detail according to early indications and analysis.

GS: The technology is there. The Federation of Management was supposed to sort this issue out because, by means of a federation creating a circle of trust, you could have a trusted authority managing these kind of situations for the third party.

MC: It's interesting you talk about SocGen and UBS, ultimately they were probably straightforward control failings. Typically nothing clever with no one having gone to great lengths to circumnavigate the systems.

SM: One of the things picked up was audit controls, reports passed over and deferred by management so that at each board meeting concerning the audit control the report gets passed over for the next meeting.

TG: It's easy to point the finger at HR or control frameworks but there are consequences of not doing things by the rules, and it's also a case of aggregating responsibility. Things like access to social media from your work desktop, turning it off for security reasons, which is absolute nonsense. It should be turned off because people are wasting huge amounts of time on Facebook etc when they should be working. That's a line manager's job to spot if someone is wasting hours on social media sites.

GS: There are tools available that can allow you to assess this and look at who is passing what information out of the organisation.

TG: All this talk of banning it from the workplace, people have smartphones anyway and there's actually a vast amount of benefit for an organisation in using social media.

VR: There are so many disparate areas of a business which are responsible for risk and so many different bodies. There are examples like social media but other areas as well, such as allowing employees to bring their iPads into work. From an FSA point of view, principles-based, so much of this comes down to, who can we make accountable? Who should be the highest person up the chain to take the fall? How many people do we actually encounter in our jobs as security advisors who can adequately understand all these areas and have a sufficient overview to be held accountable? Few can, or perhaps should need to. But regulators will rarely see ignorance as a defence: it is vital to be prepared.

MC: : Even the so called "specialists" don't know!

VR: To use the Swiss Cheese analogy, dedicated hackers can very often find a way to get the "holes to line up" and find a way to penetrate your hardware and software defences. In the banking environment, and many other enterprise scenarios, few have implemented end-to-end, demonstrably defensible security infrastructure. A holistic approach from the outset is best, but it's never too late to get a handle on the strengths and weaknesses of your infrastructure.

GS: You can have all the right tools in place, but then the end users are still opening emails and clicking on attachments where they don't necessarily trust the origin. It's a matter of people. There is less and less budget dedicated to end user awareness.

SM: You're talking about safety culture which exists in various industries and it exists in the banking environment but not as strongly. For example, it's my understanding that it's a disciplinary offence at British Gas to go up a stairway without using a handrail! This is because some of these premises are actually drilling rigs and their safety regime is imposed across the business to reinforce the culture. Can you imagine a bank imposing a similar culture around security or improper behaviour?

VR: This is all about relative risk. But consumers and customers are unlikely to be satisfied with anything less than a robust risk approach.



TH: Let's steer the conversation to retail banking and online banking and protection against infrastructure attacks.

NP: It's an interesting one. I was reading at lunchtime today some Gartner stats: 95 per cent of technology security investment goes into network secure firewalls and 75 per cent of attacks are at the application level. Encryption is the cloak of invisibility for the hacker - they go through things. Simply investing in dual layer/vendor firewalls is irrelevant because the information still flows through.

TH: Some banks, however, still have that policy in place.

NP: Yes and they open a tunnel right the way through to the application. The only alternative is to unplug the system from the internet but you have to provide access.

VR: You can have all the firewalls in the world, but if your database is outward facing and going to grant hackers access to all your information, it doesn't matter. You must assume someone will try to hack you: how do you intend to prevent and react to it?

NP: There are solutions to that - web application firewalls. However, people don't know where they fit, who manages them.

GS: Proper application testing is key here.

SM: I've seen a demonstration where in effect you had a legitimate access with an illegitimate request built onto the access - this was a vendor presentation which had been developed by an academic to protect the application, rather than the server or network. So the access into the estate is legitimate but that application will only accept requests that have been programmed by another box, based in the middle, and that box is under the control of the security people so they tell that box what kind of messages are acceptable to that application.

JPM: The problem is implementation.

SM: Yes, it looked pretty complicated to implement. But this was a big vendor so they would claim otherwise. It was interesting that it had been developed by an academic and purchased by the vendor.

MC: What I'm hearing here is a lot of "old school" to be totally honest. This is not where the real vulnerabilities lie. We all know what the issues and exposures are. I used to be a global

head of IT audit and a CIO, I would say - tell me what I don't know. What we're talking about here is what we know. I've read some articles around intelligently engineered malware that blows a great deal of current thinking out of the water. You can't see it and don't even know if it's there, no matter what controls you've got. We've been working with a vendor and I have seen them undertake work for the military and large corporates and they are going through their current security provision like a dose of salts. The security people are sitting there and saying "wow, we thought we had everything covered, but obviously not."

GS: Of course. A single injection is something you cannot monitor in a standard monitoring tool.

NP: This is what I was talking about, looking at the dynamic stuff. You say old hat, you mean layer four stuff. I'm actually talking about layer seven stuff, the unknowns. It amazes me how many companies are still investing in web application firewalls.

TG: Too few organisations, so far as I can see, use intelligence to inform their protection strategies. There's an awful lot of open source out there and intelligence to be gained from government agencies, trying to identify - are you likely to be the subject of an attack? You can find that stuff out. If we are, by who and for what purpose and when? How many organisations are gearing up for 15Oct.net which is aligning with Occupy Wall Street and London and worldwide action? Allied with people, hacktivists I guess, who are using low level stuff like DoS and they don't care if they get caught. The whole threat environment is changing and intelligence and counter intelligence is key to finding out where you're likely to be hit. Too few organisations do that stuff.

SB: One of the big spend areas for retail banks at the moment revolves around rolling out two factor authentication to the customer. I'd be quite interested in peoples' thoughts on that because to me as a customer and a consultant in the field, I think it's quite misguided.

SM: I heard about a report today which said that online banking fraud is down on the previous year, though the banks are very much concerned about one of the other areas we're talking about today, mobile fraud. The price of a full identity on the black market has gone down from \$20 to \$5 so the market is saturated.

RH: Online fraud has certainly gone down but alarmingly attacks on individuals are shooting up.

MC: It's the same as when you get into a system. It's not about what you take today; it's what you take in two or three years time. It's just stockpiling.

SM: One of the things that has helped is out of bounds communications. Whenever my bank makes a payment I get a text. Now my bank knows my phone number but the hacker doesn't. It can conceivably be compromised but it is pushing down fraud, as the fraudsters would have to know my mobile number and then compose a false text to me.

GS: There are solutions being installed on mobiles which mean that you no longer need these text messages.

TG: In most consumer environments the majority of us would acknowledge that the mobiles we're using are less secure than worktop devices. HSBC has to factor that into their security protocols knowing that they have to make such a service available, knowing they have to make the end-to-end food chain as reliable as possible or less likely to be hacked by the obvious entry points. But as we all saw with the RSA issue, two factor authentication is not necessarily any stronger. On screen keyboards, two factor authentication, one time passwords, SMSs, is this picture your's? - all of these issues are about displacing the attack surface into a position where the bank has more control over it.

SM: There was a recent article in The Times about the Rapport software, which many of the banks make available to their customers - it has been compromised.

MC: Hacking involves attacking the weakest point. People invariably don't understand where their weakest points are.

SM: There's an issue with the myriad of websites that you have to log into. There is software that can save your passwords but then you're at the mercy of the software. The whole problem is that all of these systems are not identifying the user, they're identifying some token of the user.

GS: If anything it has swung too far the other way these days, where you need 16 character passwords and you just end up writing them down somewhere and the weakest point becomes the end user.

RH: Well, we've touched on data integrity and mobile security but sticking with data integrity. It's been said that all the data in the world doubles every xx days. So I tried to get some substance

to that claim and I came across some statistics released by IBM in 2006 saying that the amount of data in the world would double every 12 hours.

NP: They also said there wouldn't be more than six computers in the world.

RH: Then I saw some statistics from EMC showing that in 2010 the amount of data in the world would double every two years.

GS: That's about right. The challenge is the evolution of collecting data along the different systems.

MC: I've taken an in-depth look at metadata repositories and people say you can't get these to work; well contrary to belief I have seen working examples and very good ones at that. If you can get it to work it can potentially save your organisation a great deal of money and at the same time dramatically reduce their risk exposures.

SM: : One of the FSA's requirements is that the banks have a single view of the customer, i.e. a single database, but well protected. A lot of banks used to have that and they've lost it due to mergers and acquisitions. But now one of the things that's happening is switching the focus from the banks to the insurance companies. Solvency II is causing them to have a huge rethink on their work practices and insurance companies are even worse than banks at having fragmented data. It has become an ingrained habit amongst insurance companies to use a myriad of spreadsheets and access databases on an individual's machines. This is proving to be a nightmare for developers of new systems, according to the briefings I've been to.

MC: I implemented SOX for a large global financial organisation and when we ran our first scan, of .fin spreadsheets, we found 1.6 million. Do you know how many we finished with that were critical to SOX? 36!!

SM: A lot of those would have been duplicates.

VR: It's surprising how many companies are reactive rather than proactive. Many companies are spending millions or billions of pounds trying to put the cat back into the bag, after the damage has been done. But harm to the brand can be irreparable. And these attacks are so often preventable.

NP: It's human nature. It's the same reason why so many Mac users don't have antivirus installed.