IT Security Roundtable

Late last year, *FSTech* and Symantec gathered bankers and insurance professionals to discuss the very topical issue of IT Security. Conversation flowed from mobile devices, iPads and desktop PCs, to virtualised desktops and fraud.

SJ: Everyone has been talking about the consumerisation of IT for the last two or three years. Every year, we have stood up at our vision conference and said consumerisation of IT is the future to what we are seeing at Symantec. Luckily now we have been proven right this year with the iPad which has been a different gear. It has gone from having a mobile device which you can walk around with but has got a tiny little screen, to suddenly having a device that is usable and big. What we are seeing at Symantec is that it has gone from being the techy who wants the latest little gadgetry phone to the senior executive walking in saying 'I have got my iPad, I want to be able to read a merger and acquisition document on it; I want to be able to prepare my PowerPoint; I don't want to carry a laptop on the plane I want to have an iPad'. That is what we are seeing really, both not just in the industry but outside Symantec too. Our rollout of iPads started top down – definitely with our executives from the top down, from our chief technology officer across all these sorts of guys: our CEO and our COO, they are the first people that have iPads. The big problem we are seeing is that the people that are walking around with the iPads and the next tablets or whatever technology (iPad is the big thing today, tomorrow it could be the Galaxy tablet or some other bit of technology), but it is finally becoming functional and the guys that want it are the guys at the top. And they are the people that have got sensitive information on it.

We have seen an explosion of device and internet connectivity. There are already almost as many internet-connected devices and mobile devices as there are PCs today. A Morgan Stanley report says that by 2012 there will be more mobile devices connected to the internet than actual laptops and PCs – you can control a laptop, you can control a PC, but how do you control a mobile device? And the next thing to be concerned about is a mobile device – people want to buy it, they want one of their own, they want to get the latest and they tend to have a year or a two-year cycle and this destroys the controls – how to sort out that? A report came from the Enterprise Security strategy group recently and they said 40 per cent of smartphone users that they interviewed hold confidential company data on their devices. Thirty-eight per cent hold personally identifiable information on customers, and 36 per cent hold sub data that is subject to security and privacy regulations. So it is not just a case of basic contacts – things are going onto these devices now that are really sensitive and they really control. We have lots of technology, but we need to consider things like control.

So many people have talked about how on a laptop and on a work station, control is definitely the way to go and that will happen on the mobile device, but today it is about people actually taking information and choosing to put it on devices that are so much easier to lose. People lost the plans to Operation Overlord in the back of a taxi. The problem is the smaller it gets, the easier it gets to lose, the easier it gets to be picked up by somebody else.

So how do you control it? There is obviously technology that provides control, but what about the policy around it? If it is a corporate device, it is a Blackberry historically or a Nokia running Good Link, you have got full control, you have got full

Attendees:

Attendees:

Adam Dawson – former Programme Manager, Office of IT Strategy, Credit Suisse (AD)
Tony Gee – Information Security Analyst, Friends Provident PLC (TG)
Rob Holman – Datacentre troubleshooter (RH)
Philip Harrison – Executive Director, Morgan Stanley (PH)
Sian John – Distinguished Engineer, Symantec (SJ)
Ramzi Musallam – Information Risk Consultant, Greatpark Consulting (RM)
Derek O'Carroll – Head of Security Practice EMEA, Symantec (DO)
Minal Popat – London Victoria (MP)
Matthew Ford – IT Manager, Sarasin & Partners (MF)
Mark Shephard – Symantec (MSh)
Guest Panellist – insurance services manager (GP)

policy on that. But what if people want to bring their own iPhone or iPad – at the moment do you let people use their own devices? Do you enforce corporate devices? At the moment there is maybe a point where you can still enforce corporate, but we expect it is going to become much, much more. People are going to want to bring their own devices, to use the same device for work and home. At that point what is the policy round it? If I am going to let you put company data on that device, I need to have the ability to wipe it if you lose it. I need to be able to put policies around it, to be able to say what applications you can use, what things you can connect to, what data you can use, but then that means I am controlling your own device.

So what do you do with the policy around that? How do you make sure you have got the right policy in place, that you track the people, the fact that people accept those policies before you let them onto the network, and how do you manage taking things away if they leave if it is their device? So there are really two things here: one is obviously mobile devices and a corporate approach of locking down; and then the extension of mobile devices – do you see the threat of people wanting to bring in their own device and connect it? Even at Symantec we have very strong policies around 'you know I am not allowed to connect my own personal device through the corporate network'. We have adjusted, we are a technology company so we have put iPhones and iPads on our supported list because we have got technology to control them, but corporate only. We have had to turn off a wireless network in our office that you could access just with your Windows credentials because people were connecting their iPads and their iPhones to it – their own iPads and iPhones that we couldn't control. From a technology perspective we can control that but how do we set the policy to allow us to say that if we let you connect to this we effectively have the right to brick your device? We have the right to take your device that you bought and make it unusable because you have got data on there that we want.

The other problem then is how do I ensure that anything on that mobile device is protected? Is it encryption, certificates, proving who you are? It is not just about identity now, it is who are you, where are you and what device are you using? So I might give you more access on your corporate laptop than I would give you on your mobile device – how do we manage that? How do we control that, how do we put the pressure in place? We know ourselves across the finance industry of a few companies have jumped very much onto this mobile device train. Their executives are taking them, they have got to go, they are rolling out iPhones to everybody and then suddenly they have got traders doing trades on an iPhone. How do you prove the non-repudiation of that? How do you prove the security around that? These are the problems and issues that we are seeing. Obviously we are developing our strategy, we have technology, we have things to control it. But is this a policy and a problem that is being seen by everyone?

And then finally this thing about automation. If you have got mobile devices, how do I automate bringing them on? How do I make the manageability of that easier to do? How do I let someone say 'I just bought a bright new shiny iPad, can I get connectivity?' What is going to be the thing tomorrow? It used to be 'we support this, this is our corporate standard device'. We are seeing that it is about breadth of support of devices now. It might be Apple today, it will be android tomorrow, it will be something else in a year or two years' time, because the technology moves so much faster in this particular area – a policy that lasts for five years will probably not last for that in the future. Those are the things that we are seeing that we feel the need to control.

Symantec are experts in malware going back 20 years. Malware is not yet sophisticated on mobiles. It is very sophisticated on desktops, laptops, servers on the Windows and the Linux platforms, but on the other systems it is not yet there, but we will see that coming because of things like Android that are open to it.

So, how do you manage devices, how do you control them against theft, and against data going onto them? How do you look at the policies, formal devices and deal with that exposure and the fact that it is being led by the business at top-down, and it is a lot harder to say no to those guys – but at the same time they are much more likely to have sensitive information, and how do you manage the life cycle of devices.

WC: So I heard a couple of themes there. I heard productivity, expectation, policies, standards – do they actually hold back self productivity? What are the big mobile security issues?

RH: I think application springs to mind. Look at mobile phones, iPhones, iPads – how many applications are there? Over 100,000. It is pinning that down and just disallowing people from installing something that could actually have nefarious reason for being installed in the first place.

AD: I guess segmentation probably would be the area that I would be looking at. There is a lot of pressure from senior execs

as well as fairly large number of normal users to basically be allowed to use their own devices and the only real way that we can facilitate that is by owning a section of the device. So, that feels like kind of an achievable technology so you should, but I think you have highlighted that the major issue is what happens when that person leaves how do you reclaim that portion of the device, how do you prevent them from taking information where they shouldn't. So for me it is more of a compliance, HR, legal headache than a technology headache.

"For me it is more of a compliance, HR, legal headache than a technology headache" – Adam Dawson

TG: I think there has to be two different types of mobile device. There has got to be what I think is the future, which is personally owned mobile devices – and that includes personally owned laptops connecting onto your network and your systems and corporately owned devices. At Friends Provident we have recently started trialling some mobile technology for mobile phones called Good, and we use that on personally owned devices because we feel it is a sensible way to segregate the network, or the data I should say. We can leave the user to do what they want with their device – there is a small concern as you say about what happens if there is a rogue application which comes out which can break into that system. And ultimately I don't think we have got much control there, it is a small risk we just have to accept to provide a more flexible solution. But we do limit where they can be used, and at the moment we only provide them to iPhones and iPads. But for a corporate device whilst it is an acceptable way to get email and calendar on that device, it is not really as flexible as the proper built-in mail client that you can use for editing documents and really working on the go. From my perspective, I am interested in how we can enable the entire device securely rather than going through an application. For personal devices I think it works fantastically well – you can do a remote wipe of just the data and leave the phone in perfect stead, but how do you do it corporately and how do you securely enable someone to bring in their personal laptop and use that as a primary device?

Conversely, although it controls that section of the device, one of the great advantages is that you can make the rest of the device usable and so from a corporate point of view what we want to try and do is we want to try and avoid locking down devices to such an extent that they are no longer a Smartphone, but are just simply a phone with email on them. We don't want to make a Blackberry; we have got Blackberries that work very well for that section of users, but we want to make something which is a little bit better and that is really what is interesting me with corporate iPads.

GP: In general, if you are trying to on-board a lot of different systems, a lot of different kinds of applications, sometimes it is very difficult to run processes and do normal IT work when you have got firewalls.

DO: Are there other considerations? I mean, we have talked about locking down the device, widening the device, maybe having a policy angle in terms of what data is on that device and using that to control wipe and so forth. But there is the enterprise, there is the carrier and then there are the people who are manufacturing the mobile device, and the people who are supplying the apps onto the mobile device. So what are the issues to be considered?

WC: I think we are in a situation where the technology is getting so far ahead of the policies and historic standards that it will take a very visible error or even a catastrophe before standards are going to catch up and I haven't seen that many mobile catastrophes so far. But you know it is going to come because it always comes when technology gets ahead of standards and some policies.

RM: How feasible is it to really have a basic rule that all company data can only reside on a company-owned product?

MF: It limits you – you either allow them to bring in a facility or you don't. It has to be one or the other.

Where is your data?

MSh: It would be interesting to do a poll of how many organisations think they are actually in control of all their data, irrespective of whether it is on a mobile device or whether it is within an organisation. We speak to people about what data is important to them, what data is sensitive, the fact that people don't classify data because it is all too hard, that they can't rely on end users to do that; but how many organisations can put their hand on their heart and say we know where all our sensitive data is and we can control it? I would probably say that 99.9 per cent of organisations can't do that.

GP: You have got to treat every remote access request fairly, and you have got to have remote access IT security policies that allow for back-up and other crime. The other consideration is making sure you are compliant with all laws and standards at all times.

Customer data is another thing that I think should have graded levels of security. So for customer data you know you need non-disclosure agreements and a lot for things, which an employee or consultant must sign up to before taking customer data off-site. I think there must be a higher test and a more graded approach to security and more graded forms of authentication, and if someone is doing its clients data off site, I think there needs to be more restrictions.

MP: I think the point on customer data is really important as well in terms of an equal framework, especially when we are dealing with contractuals and we are outsourcing information or services. We really need to make sure there are robust controls in place or there are contractual indemnities in place so that we can mirror and have a hold on what they are doing.

Contracts

SJ: With outsources you can set it into the contract – when you take that to a cloud provider they have one standard contract.

AD: So when your outsourcing provider is also outsourcing to another outsourcer and it could be four or five providers deep. The kind of due diligence process is just massively complex.

WC: So how about the technology supporting that? I am a great believer in policies and standards but I know people break the rules, you know just because people are people. So how does the technology prevent that?

MF: I have a point to make here. Generally speaking, most people believe the military is very good at keeping its own military secrets. They have a system in place which allows them to protectively mark their documents, and everyone knows how to appropriately handle that data, even though they don't understand the written contents. I have a military background myself, and when you encroach on this issue with a commercial company that has never classified any of their data – as most have not – and they store that data into a single repository or drive, they are highly likely to lose that control of that data eventually. Everyone has access to it, and no one in the company can clearly separate what is sensitive, and what is innocuous. What people often fail to articulate is the simple reasons for classifying data, is so you don't need to understand the contents of the file, only that it is secret and it should be handled accordingly. However, even with the military system, as water tight as it may be, the weakest link always boils down to the individual member of the company, charged with handling it in the first place. We have seen this with Wiki leaks, and the massive amount of open disclosure that has occurred, irrespective of all the controls an organisation puts in place. Nothing stopped that person from just physically walking out with the data in the first place. I don't see any current level of technology ever preventing this for the time being.

AD: I would be interested to hear with that in mind whether everybody agrees or not that it is very difficult to control data – you have mentioned that one of your aims is to promote the use of people's own devices. Do you feel that the two are completely at odds with each other and therefore not necessarily?

TG: Consumerisation is not necessarily the direction we wish to go in, corporate data is likely to be more secure on corporate devices, but ultimately the business are our employers and if they want to go in a particular direction you have to find ways of doing it securely. Information Security has often got a bad name for saying no, that is not how we like to do our security at Friends Provident. We like to say yes, but let's put in these controls to mitigate or to manage the risk.

WC: I think we are agreeing round the table that the Pandora's Box is going to be opened in terms of technology and the technology is out there, but you are talking about ways of employing that technology to make it safer because we can't put the lid back on the box again. So what are other people doing to control this new technology then in terms of security?

RM: There is a real vacuum because in the past the technology hasn't got too far ahead of the regulations and policies and controls that they are trying to put in place, but the real concern is I think that there has been such an escalation in the number of people that do want mobile devices.

PH: I think one thing we are missing out here is the onus on the manufacturers to do a better job of securing those devices. If the iPad had the same security model as the Blackberry, we probably wouldn't be having this conversation around this table.

The problem is there are a lot of devices, a lot of operating systems, a lot of applications out there that don't have that control, haven't had security designed in to the application.

MF: There is a trend to try to connect the technical device with the biometric signature we all have. You know, whether it is a key token or a personally owned device, the industry is shifting towards making this feasible for everyone. However, the use of biometrics involves too much trust, and to much understanding of purpose by its user base.

MSh: Most people always carry a mobile phone with them, and one idea is to have some auto via Bluetooth authentication with something you are looking at. So, as long as you have got that device with you, it will seamlessly authenticate without you knowing. I have just come back from two weeks in India. That country has gone from having fixed landlines, lots of people queuing outside to use a telephone, to virtually every single individual in India having a mobile device. And there are masts the size of skyscrapers scattered all about India. I never once lost signal in Rajasthan. I was permanently connected in what was effectively a third world country ten, 15, 20 years ago. It has got to be one of the most densely, pervasive mobile populations in the world. China is probably going to go exactly the same way if it hasn't already.

Fraud

GP: There is enormous susceptibility to fraud. One thing that I thought was interesting was when some of the governments of the world tried to crack down on research and motion and the use of Blackberry devices because it is so encrypted, and that is why it has become a corporate standard. It represents an intrusion step that I suppose is very good for corporate.

AD: I think one of the factors in that is that most retail banks as far as I am aware, kind of inherit the risk and the profile of their customers to a degree. So if the customer is prepared to use a mobile device for example without an appropriate level of authentication, if there is an incident, it tends to be the bank that takes the financial hit for that rather than the end customer. So there is a level of risk involved for the customer, but actually from a financial risk perspective, it tends to be the institution.

WC: Who is accountable for actually delivering that security strategy for these mobile devices?

AD: For me I think that needs to tie to the business case, because I appreciate what you are saying, that security needs to be seen as an enabler and generally I agree, but if there is no business case other than the fact that somebody wants to play with a new toy and that opens up an enormous amount of risk in an otherwise risk averse organisation, then that needs to be a difficult conversation. If there really is a business case and productivity will go through the roof or you enable access to new markets, then at that point you need to start looking at the people versus technology aspects.

Tradition

WC: How will banks and enterprise convince the consumer to move away from the traditional banking, online banking to use their mobiles? Is there any other reason why your customer might move away? What is in it for them?

TG: I don't think banks and enterprises are going to convince consumers to move away from traditional banking, I think it is the other way round. The consumers are going to influence banks to work in better ways. A key example of this, a personal example actually, I used to have a bank account with a online only bank. I like working online.. But then a bank brought out an app for the iPhone. I have changed bank accounts because I can check my balance on my iPhone very, very simply. The iPhone is a consumer product and I am believe that Bank x's desire for an iPhone app was driven out of consumer demand rather than the business saying let's go and do this.

WC: Not a lot of functionality there I suspect.

RH: No, dead simple. All I want is be able to view my balance – it works perfectly as an app. I don't want to transfer money, that is a bit too risky for my phone.

Corporate

WC: So what about this risk of corporate data loss? What technology still needs to be built up?

TG: Surely it comes back to accountability: if an individual loses it, they need to be responsible until such time as they report it missing, then the company can take over by remote wiping it or doing whatever they need to do.