BANK OF ENGLAND

Speech

Remarks to the City Week conference

Speech given by

Will Brandon, Chief Information Security Officer, Bank of England

City Week 2016 Conference, London

10 May 2016

Thank you very much for the opportunity to speak. I'm going to start by qualifying my response to the question. I honestly don't know whether or not cyber is the biggest threat to the Financial Services Industry. I am sure that individual businesses could cite all kinds of other big threats, from legacy IT to political uncertainty, to disruptive technology.

But you don't have to be one of the recent, high profile corporate victims of a cyber attack to realise that cyber is a clear and present danger – even if the threat is often unclear and perpetrators notably absent. Or that the corporate consequences – including for the careers of senior executives – can be extremely serious.

I am not in a position to say to any individual firm which risk, out of the many risks they face, is the biggest. And I don't think I can offer a one-size-fits-all blueprint for defence. But I hope I can at least suggest a way of positioning this cyber risk that may help you work out where it fits in your overall risk framework, and what you can do about it.

The first thing is to get away from the perception that cyber is just a technology problem that can be solved entirely through engineering solutions. There is a tendency for boards to look at it, fear that it's too technical to understand, and then delegate the whole issue to technologists – who duly deliver some technological fixes.

The trouble with that is that most cyber-attacks are not exclusively – or even mainly – technical in nature. People and processes are every bit as important.

This is because attackers tend to exploit the credulity or laxity of their targets to achieve their ends. And while some can and do develop highly technical attacks, for the most part these are facilitated in some way by people or process weaknesses in their victims' defences.

Most cyber-attacks start with social engineering: sending emails with tempting but malicious links or attachments, compromise of websites that targets might visit, and so on. In doing so, they exploit people: the culture, training, and integrity of your staff.

Most attackers then take advantage of the initial opening by installing malware that exploits known technical vulnerabilities. Vulnerabilities that could have been patched had the target had the right procedures in place. Arguably, what is being exploited is the weakness in a necessary process.

Working out what to patch isn't difficult – in 2015, the top 10 vulnerabilities accounted for 85% of breaches. It's a matter of having the necessary systems – and the collective corporate will – to actually do the patching.

Once they are on a system, hackers move inwards, generally by guessing or stealing credentials and using them to access the more sensitive parts of your system. How do they do it? Surely all organisations have policies mandating strong, frequently changed, strictly confidential passwords? Well, they do. But according to Verizon's 2016 Data Breach Investigations Report, 63% of confirmed data breaches involved weak, default or stolen passwords. So in other words, hackers exploit yet another people and process issue – this time, endemic poor compliance.

People need to be led. Processes need to be managed. So it seems to me that cyber is, to a great extent, a leadership and management issue.

Leadership that needs to be applied from the top – not just from the IT department. And felt throughout the organisation. The prominence given to this issue in the Bank of England's 2015 Annual Report reflects our leadership's focus on ensuring that that security-conscious staff play an active role in the defence of the organisation.

Processes need to be managed holistically, via the same governance approaches most of us use in all the other parts of our businesses. That will mean, among other things, clear policies and standards, good management information, and a sensible approach to compliance.

You may also need oversight: a formal means for the business to assess and manage risk. And a requirement that managers take ownership of information security risk as they would any other.

So how do you balance cyber risk against other risks? I suppose the first thing is to quantify it, at least to the extent you can. That might involve assessments or testing, but it probably starts with working out who might do what to which part of your estate. Or to put it another way, breaking the risk down into threats, vulnerabilities, and assets.

Threats derive from the capability and intent of people who might attack an institution. The trouble is, defenders have limited control over this: they tend to attack because of who or what you are, and most of the time you can't help that. What you can do is develop or buy in a threat intelligence capability that allows you to assess and address the specific threats you face. Threat is one area that differentiates cyber form other risks because cyber is adversarial: the attackers are constantly evolving in response to your defence. And there are a lot of potential threats, for example:

- Criminals. They have industrialised their processes. Last year, official statistics showed that fraud and cyber crime had become the most prevalent crimes committed against victims in England and Wales. Those criminal activities, including cyber crime and cyber-enabled fraud, may damage confidence in, for example, mobile banking, and more widely, internet commerce.

- Larger institutions are repositories of market sensitive information that could allow manipulation of the markets: last year, nine people were indicted in the US for their part in a scheme whereby information gleaned through cyber attacks was used to trade illegally on financial markets, reaping more than $100 million in illegal proceeds
- Hacktivists and other interest groups may take action against financial institutions for political or ideological reasons.
- Nation states may be interested in supporting their own institutions competitively, or attacking critical infrastructure in countries they perceive as hostile.

Vulnerabilities are what you can definitely do something about. They are the weaknesses that the threat actors exploit. All Financial Services companies are attractive to attackers, because that's where the money is. And attackers are opportunistic. So they target on the basis of vulnerability, not just size or security spend – and vulnerability is more a matter of culture than of technology.

Outdated operating systems, poor patching, untrained staff, unsegregated networks, weak security monitoring. And so on. These are susceptible to both measurement and testing. More importantly, they can be fixed. Less obvious, but as important, may be an institution's wider ability to respond to a critical incident: if you don't have a plan, or you haven't rehearsed it at all levels, an incident is unlikely to go well.

Assets are the systems or information which underpin your critical business processes. You need to know what they are, and have a clear view on the impact on your business if the confidentiality, integrity or availability of those assets is compromised. Successful attacks may have a range of consequences, including financial loss, loss of customers, loss of confidence in firms or markets. You should also be clear that the owners of those information assets are the owners of the business processes they support: they own the risk. Not the CIO, not the CISO: it is the owner of the business process who should be accountable.

If you have that view of the components, you then have some way of assessing the likelihood and impact of the risk crystallising. And you will a have good idea of what controls you might need to apply to reduce vulnerabilities or to mitigate impacts.

You may also be able to work out what the cost would be – whether in financial or business terms – of implementing those controls. Some may be cheap but unpopular – for example, ensuring compliance with policy. Others might be expensive but effective, for example, segregating your corporate network from core systems.

And that should, I suggest, give you a way forward in balancing risks. Managers, as risk owners, should be able to take account of cyber as they would any other risk that could cost them their profits, their reputations, or their jobs. If that means balancing cyber risk against other business or risks, good. That's what risk-ownership means.

So, to sum up, cyber risk is one of many risks. It is certainly serious, but it can be understood, and it can be quantified. So it needs to be managed like anything else that could damage a firm's business - by understanding it, and then by balancing investment in mitigation against similar investments that are needed across the business. Thank you for listening.