Alex Keetch and Tim Roberts discuss the current information security environment, and ways in which company boards should be considering and managing the risks to their businesses. Tim coordinates Promontory’s global teams focused on information security, cyber security risk management, data protection, and privacy. Prior to joining Promontory, he was chief operating officer at Ignis Asset Management, a major UK-based asset manager. While at Ignis, Tim successfully merged the operations and support functions of two businesses, led a major operational transformation, and had board-level responsibility for risk management, information security, compliance, and regulatory relationships. Before Ignis, he enjoyed a 16-year career at McKinsey & Co., where he was head of the UK financial services practice. He served major financial institutions around the world, and was one of the founding partners of McKinsey’s global risk management practice.

For the uninitiated, what is information security and why does it matter?

Information Security is the process of protecting the information a company or any organisation holds, or that which flows through it. InfoSec has always mattered, but it matters increasingly these days as more and more businesses are ‘going digital’. Previously, security was more ‘physical’ – stopping people stealing customer records and paper money was a matter of having bank vaults and so on. Nowadays, it’s not just banks that possess and manage valuable information. Retailers have big customer databases, and indeed, are currently trying to use ‘big data’ to enhance their marketing activities. All of that information needs to be protected. To put it another way, there are many more opportunities to steal from a company these days than there used to be. Stealing data takes value away from the customer, but it also damages affected companies’ reputations at the same time.

At an individual level, who specifically do information security issues affect?

It’s an issue for all of us: all consumers and all businesses. We all give our details to any number of different organisation types, whether to travel companies, online retailers, government organisations etc. This information can be exploited through identity theft, making fraudulent payments, or similar. It also affects all businesses – it’s hard to imagine any business these days that doesn’t have sensitive information flowing through it. Proprietary product information is also at risk. Another form of information security risk is industrial espionage, conducted by competitive companies, and even governments looking to give their countries an advantage.

Would you say financial services companies are more likely to be targeted than broader industrials, because they deal with money as their core ‘product’?

The first wave of security breaches mainly hit banks because that’s where the money is. As the banks became more secure – spending a lot of money on protecting themselves, so as to become harder to rob – the attention shifted, and the retail sector became a big target. That said, we’ve seen breaches across a number of sectors, including gaming companies, air travel companies, hotel groups etc. Anyone who has a large global online customer database is going to be vulnerable and a target.

Organisationally, where does the Information Security function tend to sit within large firms?

Historically, InfoSec sat within IT, and was thought of as ‘IT security’ – a purely technical discipline.
Nowadays, whilst there clearly is a huge technical element – because the architecture behind things like the access policy for company staff has got to be well managed – the concept is becoming of relevance to the whole organisation. The more a business gathers and holds customer data, the more likely you are to be using that data in different parts of the organisation, whether CRM in marketing, or salespeople analysing data to determine business development strategies. Therefore, there needs to be an enterprise-wide approach to managing data-related risks. Firms who are vulnerable are those who continue to see InfoSec as a narrow technical discipline, because they will get attacked in ways for which they are not prepared. The firms who seem to us to be best prepared are those that think about the technical controls, and about policies relating to data and customer information to be adopted across the organisation.

**Do these issues have sufficient visibility at boardroom-level?**

Information security is increasingly seen as a board-level priority, especially amongst firms that have been breached and have suffered the resulting negative publicity. We at Promontory strongly believe it should be a board issue, given the level of risk involved. That said, some boards can struggle with the technical details, and most boards don’t include a dedicated InfoSec expert as it stands. They will need to in future, in the same way that regulated financial firms’ boards are being encouraged by their regulators to increase IT expertise. Boards really need to ask themselves, do we understand the threat facing our business? Do we have sufficient ‘risk appetite’ for it in order to continue our activities? This is to acknowledge that you’ll never have ‘zero-risk’ as it’s impossible to protect yourself completely. To use a physical analogy, a fully ‘burglar-proof’ home would be so prohibitively expensive as to be economically unattractive. Boards also need to define roles and responsibilities beyond the IT function. These might include HR’s responsibility for research and training, the legal function’s accountability for data protection legislation compliance, and the role of facilities in terms of monitoring physical security.

**Indeed, the element of InfoSec that gets the most attention is the ‘cyber’ security side, i.e. hacking, but there are other substantial risks as well.**

That’s right. When you say ‘cyber security’, you’re not really talking about teenagers in their bedrooms. You actually need to think about organised crime, or governments, externally attacking you. You need to think about the internal threat as well – malicious attacks and accidental slip-ups by company insiders have been behind some of the most high-profile breaches on both sides of the Atlantic in recent years. We’re currently working with a large financial institution who accidentally sent a batch of customer data to the wrong customers. That’s a breach, even though it doesn’t involve anyone intentionally seeking to damage the company. These incidents still get a lot of publicity and can damage customer trust.

**It sounds like ‘fat-finger’ trades and payment network failures we’ve seen recently would also sit within the InfoSec stable. Is that right?**

Indeed, information resilience is a very closely related topic. Academic definitions of InfoSec have three components: first is confidentiality, or data protection. Second is availability, ensuring the systems don’t go down because of an internal issue or an external attack. For example, one of the most common forms of attack is the Distributed Denial of Service (DDoS), flooding a company’s website with requests so that the systems collapse. And the third element is integrity – the data has to be valid. If someone can tamper with the data a company holds, either by changing credit limits, or removing records, it’s not going to be of much use to the company in question, and may damage the customer in some other, unforeseeable way.

**The real issues at stake seem to come down to protecting customers and company reputation in a lot of cases. How are global banking regulators currently approaching information security?**

That’s a good question, and one that we are being asked a lot. For the last two years, global financial
regulators have become aware that this is a major new risk that needs a specialist approach. The US regulator started benchmarking firms two years ago, sending out questionnaires in order to assess existing capabilities. They are now starting to publish guidelines around their specific expectations in relation to various international standards. Additionally, about a year and a half ago, the Bank of England issued a questionnaire to regulated firms, and earlier this year started issuing ‘Dear CEO...’ letters to banks, identifying areas of weakness, asking to see plans, asking for detailed timetables of InfoSec upgrades, understanding governance arrangements, and asking questions around board awareness and involvement. Earlier this year the ECB and the Singapore regulators have both issued questionnaires as well. As a result, you see large, global, regulated firms in many cases appointing new, more senior CISOs, from outside the firm or even outside their industries, or even the Intelligence community. People who have government and/or military experience, and a commensurate degree of familiarity with the threat environment, are in demand. As an aside, a common notion among CISOs is, if a nation state wants to get into your network, they will. That’s not really the biggest threat. What you need to devote attention to is elsewhere. If you’re a midsize company, you probably won’t get attacked by a nation state. However, there is a whole range of organised crime elements, large and small, against which you need protection of this kind.

The ecosystem seems to be taking shape: attackers, targets, and regulators. An interesting consideration would be when regulators themselves become the target of attacks; they hold a lot of data, after all. This leads to my next question – what are the ‘X-factor’ issues here? What might potential target firms be missing?

There are a couple of key things. Firstly, this is a new risk, and people are generally not good at handling new risks. Most banks’ board-level risk committees spend their time looking at economic risks, which are nice and familiar. They will not spend a lot of time thinking, ‘what is the nature of the cyber threat to our business? How vulnerable are we to a system collapse?’ Human beings are good at analysing familiar patterns, but very bad at analysing new and unfamiliar threats, so we need to be aware of and protect against that natural shortcoming. The other factor, and I mentioned this earlier, is that boards in general don’t have a great deal of IT literacy, so it’s difficult for them to discuss highly technical issues. As discussed, these issues affect the whole organisation. Everyone should understand and be aligned to set IT policies, and it’s the board that has to lead that process. You can’t just delegate it to IT and hope that’s sufficient.

Someone needs to be accountable, is what you’re saying. It’s not just large firms that are facing down these threats, either; an individual at a small hedge fund was recently tricked into fraudulently transferring funds to criminals, and is now being sued by his former employers for negligence. What can individuals do in order to protect themselves?

Well, a lot of breaches that have taken place have been facilitated by individuals not following policies, or not being alert to risks around them. One major breach of a British company took place because an auditor asked for some data, which was provided, but intercepted by a malicious individual. You could respond by saying there’s nothing you can do if a malicious element is intent on wrongdoing. However, in the first place, the data shouldn’t have been provided in an unencrypted format, it shouldn’t have been provided in its entirety, it should have been ‘anonymised’, and it shouldn’t have been possible for this individual to intercept it. At least four things went wrong, beyond the fact that there was a malicious individual. There’s also a significant ‘common sense’ element, beyond putting processes in place. Ask questions, don’t just supply information, test and verify why it’s needed. Another thing we should be alert to is ‘phishing’. Everyone needs to know about and be on the lookout for suspicious email attachments, and avoid clicking on suspicious links. There’s a certain level of literacy and scepticism that we all need to develop in order to protect ourselves as consumers, let alone as company employees.
It feels as though that awareness is evolving, although not everyone is as aware as they should be that ‘the individual’ is such an obvious target. You hear about elderly people, for example, taking calls during the day from people asking them to turn on their computers and send out information.

Yes, and these campaigns are specifically designed to target vulnerable people. It’s almost guaranteed that someone in their anxiety will click on the link or the attachment, and that’s all an attacker needs in some cases in order to deposit malware on a computer, and the threat spreads from there.

To revisit an earlier question, which industries do you feel are furthest forward in terms of their preparations?

Well, the banks have done a lot of work on this because they historically always invested the most in physical security. They were also among the first companies to computerise all of their processes. I hesitate to be too emphatic that the banks are in the lead though, because there is always a risk of complacency. Banks are very porous organisations. The sheer number of employees and customers of some banks also facilitates the ‘numbers game’ for attackers. Also, spending the most money is not the same as being best prepared, as has emerged in public recently. A major global retailer had invested in expensive monitoring systems, however, these throw out lots of ‘false positives’, especially when first installed. You need to calibrate them, so you can screen out the noise and detect breaches. In fact, they neither detected a major breach when it was underway, nor after it had happened. As often happens, it was a third party that notified them that they’d been breached. Like any security system though, the more layers you have, the harder it is for someone to get in. A medieval castle is a nice analogy. You are on a hill, with a cleared ground, a moat, a high outer wall, an inner wall with very small spaces, and then you have an inner keep. In the same way, banks have multiple security layers: well-designed network architecture to begin with; access controls; network monitoring; employee checks; employee monitoring; data movement monitoring etc. That constant multi-layer vigilance is what typifies the best set-ups. Additionally, humility is a characteristic of all effective security arrangements – you need to be constantly alert, constantly expecting an attack of some kind.

It’s an additional challenge that whilst the Edward Snowden affair has incited a highly charged democratic debate amongst law-abiding citizens and democratic institutions about privacy of data and freedom of information in the modern age, organised crime groups don’t have anything like the same scruples. For them it’s business as usual, and they’re grateful for the distraction from their nefarious activities, such as identity theft or fraud.

That’s right – they are looking dispassionately at the data they have acquired, and thinking ‘how can we make ourselves some money out of this?’

In a roundabout way, that brings us to the ‘business end’ of the InfoSec ecosystem. What’s the commercial opportunity here for consultancies, programmers, and other providers?

InfoSec is very much a nascent industry, so there are lots of opportunities for companies to establish themselves and make a contribution, Although I suspect this is another challenge for company boards, as it is quite difficult to get your head around who you should be getting help from. There are companies who will help you design robust, bespoke business systems; there are people who will help secure your network; there are firms that will help you monitor what you have in place – the equivalent of selling you a burglar alarm for your house. Additionally, there are specialist firms who can help companies with remediation after a breach. Their market are the companies who acknowledge that they can’t fully avoid a breach, but can at least be set up to recover quickly after an incident, by providing system back-ups, system redundancy, forensic investigations etc. One of the fastest-growing service lines is running outsourced security operations centres for large firms. There are also firms like Promontory, who take a holistic view of both the client’s wider business, the threat environment and the range of solutions on offer, and will help clients to develop risk management
frameworks based on all of these. The thinking is, clients need various specialist technology services, but also need advice on behavioural guidelines and policies to complement that technology.

There’s a huge amount of movement in the space from the sound of things. Resourcing challenges are no doubt on the horizon; what trends are you seeing in the InfoSec talent acquisition space?

Well it certainly feels like a busy recruitment market. Anybody in a role with a job title including the word ‘cyber’ seems to be getting a lot of attention. There is also a skills shortage: there are training programmes being set up, and increasing numbers of degree programmes being established. You also see companies rushing around trying to recruit and strengthen their teams. We see some companies creating an InfoSec team within their risk function, outside of the pure IT domain. This is about trying to create a second line of defence, that’s able to oversee and challenge the activity of IT and other departments. The combination of risk and IT experience is in high demand, in order to test and challenge and improve existing assumptions. Additionally, banks are calling on consultancies to help them create, install, and monitor IT risk frameworks, whilst they build their teams. The best consultancies will factor in ‘skills transfer’ into their offering as a matter of course. Clients need someone to show them best practice and leave the components in place and permanently effective.

Returning briefly to an earlier issue, would you say it’s easier to hack into an organisation than it is to protect an organisation against hacking?

Definitely. It’s much harder to wear a ‘white hat’ than a ‘black hat’, as they say in hacking circles. The enemy is well-trained, well-funded, and persistent. Metaphorically speaking, as a ‘white hat’, you need to be checking and securing every window, every door, in a very large building – and these companies are not houses, they are skyscrapers, with a lot of windows! A ‘black hat’ only needs to find one access point. This is a world of continuous improvement and constant testing and learning, on both the attacking and security sides.

That continuous improvement in itself is enough to get professionals enthused at the prospect of being at the vanguard of an evolving field. Do you think there is sufficient ‘evangelism’ amongst the information security population to keep ‘defending the realm’?

I think so. This is not a fad; it is a ‘step change’ in the vulnerabilities of all sorts of businesses and the affairs of individuals, so it’s going to keep lots of people busy for a long time. I hesitate to use the term ‘gold rush’, but anyone in this field can tell this is a busy space offering some great career opportunities. Information security is now a true ‘discipline’. We’re running our own training programme internally for colleagues to acquire the CISSP (Certified Information Systems Security Professional). if you’re going to university now and you’re looking to do computer science, this is a great area in which to specialise. Getting a broad grounding at first but then potentially choosing this as a specialist topic would guide you to a great first job in an expanding field.

One of the advantages that information security teams might have in the fight against cyber attacks is that there are lots of opportunities for collaboration with other firms, in the spirit of levelling the playing field. Is it fair to say groups of ‘blackhats’ might be less collaborative, or am I being overoptimistic?

Well, unfortunately the wrongdoers are more collaborative than you might think. The organised crime ‘industry’ that is attacking you is disaggregated, and increasingly sophisticated, because the pay-offs can be and have been so large. You can buy malware from crooked programmers, you can pay people to test companies’ vulnerabilities, and you can pay someone else to insert the malware. You can even try different forms of malware and have them all competing with one another. On the positive side, companies are increasingly collaborating in order to share details of threats and potential solutions. Firms need to stand united to fight off these threats, and industries need to adopt technical standards and regulations that will protect everybody. One thing
that undermines the collaboration element is that as a pragmatist, your attitude may be that you needn’t make your firm completely impregnable, only a less easy target than the majority. The lion on the savannah isn’t going to eat all the antelope, only the slowest ones.

That sort of thinking is how ‘arms races’ start, isn’t it?

That’s right. Companies really are beginning to see that this is more than just a hygiene factor – it’s becoming a competitive advantage. If you have a series of breaches (and there are a couple of major brands out there that have been hit more than a couple of times in differing parts of their business), you start to look accident-prone. New customer propositions, involving customers signing up with their personal and financial details, might invite a bit more scepticism than before. These firms might be bulletproof thanks to their learnings from past experiences, but the brand may be irretrievably damaged in the mind of the customer.

With all the above in mind, what’s the profile of the ideal CISO in this day and age?

Building on the points we’ve made, I’d argue that it’s not a pure technologist. A CISO is someone who is highly technology-literate. It’s someone who is adept in the field of risk in a broad sense. Additionally, a CISO will have a strong understanding of how to change an organisation. Making a firm more secure is not going to happen overnight – it will often involve a major, group-wide programme. Finally, a good CISO will be someone who can engage with the board, for reasons we’ve discussed. The CISO for one of our clients, who was hired 18 months ago, has attended and spoken at every board meeting since they joined. Interestingly, this firm hasn’t yet had a breach, but they recognise it as a possibility, and recognise that robust security is a competitive advantage. The CISO’s team should be made up of similarly versatile people as well, and will need to operate globally. For example, if you’re a US company with substantial operations abroad, and your CISO team is very US-focused, you are going to be vulnerable outside the US, which means you’re going to be vulnerable everywhere. Additionally, a major US retailer suffered a damaging attack recently from a hacker who found a way in through a supplier network, demonstrating that you need to manage and monitor your entire supply chain, not just your own company. The enemy is looking for the weakest link, and if you’re not sufficiently prudent, if your framework is not sufficiently robust, they will find it.