Asam Malik

Director – Risk Assurance, PwC

In our latest executive interview, PwC Director Asam Malik tells us why all companies need to do more to protect their data as they become increasingly dependent on complex IT systems and threatened by ever more sophisticated cyber attacks.

Could you start by giving a brief overview of your current role at PwC? How has the role of the Risk Assurances team changed during your 13 years with PwC?

As a Director with the firm, my role is to lead the risk assurance practice in the North East. My team offers a broad range of services such as IT and project assurance, commercial assurance, performance assurance, internal audit, business resilience and data assurance. I personally specialise in technology and I generally assist clients with IT strategy, cyber security, ERP systems, IT project assurance, IT disaster recovery as well as helping clients choose new IT systems. Since starting at PwC, the service we provide has changed massively. A lot of the services that we offer now didn't exist when I joined and I think as a firm, we have been good at evolving to meet our clients' needs. We used to focus a lot on IT controls but today the big focus is on cyber security and data. Generally, clients have more complicated IT issues today and there is also a much greater reliance on technology which means there has been an increase in demand for our skills.

How important is cyber security for businesses today? Is everyone at risk, or are some businesses more attractive targets than others?

Because the majority of organisations are online and far more dependent on technology, cyber security is one of the biggest threats they will encounter today. Many businesses, for example, haven't fully considered the risks associated with IT systems and often leave data insecure and easy to compromise. Quite often, clients ask us to test the security of their systems and using 'ethical hacking' techniques, we have often been able to gain access to sensitive data within a few hours. There's still a prevailing attitude of 'it'll never happen to us', but the reality is that everyone is a potential target. Each year we are commissioned by the department for Business, Innovation and Skills (BIS) to conduct an Information security breaches survey and in 2013 we found 65% of companies in North East & Yorkshire suffered attacks by an unauthorised user. It's not just financial data that people target either. Some organisations hold data on people's medical records or even details of vulnerable children, for example. The problem is much broader than simply 'protecting your card data'

Typically, who are the culprits? How does PwC keep up to date with new 'vulnerabilities'?

Often, it is just opportunists doing it for fun but if you go further up the food chain you will find cases of organised crime and even state-backed hacking. A lot of smaller organisations are guilty of thinking 'what have we got that's interesting?' but they're often victims of hacking from people doing it for fun. Hackers often look for organisations with known vulnerabilities in their security and target them because it's easy. We've got a huge pool of expert resources that we can draw upon but, keeping up to date with all of the vulnerabilities requires a significant investment that all organisations are not able to make. Smaller organisations can find it hard keeping up to date with it all. It is a constant battle; as soon as a new patch is released, a new vulnerability suddenly emerges and I don't think it will ever end. As such, it's vitally important to invest in security because the more complex you make your IT systems, the more you will depend on them.

Has this led to a clamp-down on employee freedom in the workplace?

Yes, organisations have certainly made it more difficult for employees to take data 'off-site' but I think there is still an awful lot more to do actually and many organisations still aren't where they need to be. Awareness levels have been raised due to high profile leaks and breaches which is a good thing, but organisations need to do more to identify where their sensitive data is, who has got access to it and also do everything they can to protect that data. Quite often you have one person who has got access to sensitive data, such as employee details, in a secure system then what happens is they download it and put it on a spreadsheet and then suddenly it's on a local machine, or it's on a USB stick or it's printed out. Most organisations will have some safeguards against this happening, but need to invest much more to tackle this.

What technologies have been the most 'disruptive' to current business practises in recent years?

The emergence of smart phones and tablets has had a massive impact on organisations. The biggest change is that employees are no longer bound to the office and can work remotely, at any time of the day. A knock-on effect of this is that customers and clients now have an expectation to be able to interact with organisations 24/7, via a multitude of digital platforms. So, while in the past, organisations simply had an IT strategy that was very internally focused, today, more outward focused digital strategies are required to determine how an organisation will interact with its customers from a web perspective, mobile perspective, a social media perspective, or a CRM perspective. Crucially, managing digital security also needs to be considered and for most businesses, there's still a lot to be done in developing that area. So, it's not just about securing your traditional hardware and software within an application anymore, but having the capability to authenticate who is trying to access your systems via remote devices.

What technologies do you anticipate being the most 'disruptive' to current business practises over the next few years?

One area that is growing at a rapid rate is cloud computing. It's made a huge difference to the speed at which organisations can outsource IT systems because you don't need to have a big in-house IT department. We're really beginning to see some impressive developments in that space. BYOD (Bring Your Own Device) in another growing trend. Employees are increasingly expecting to be able to access to their work emails, documents and tools on their own devices. While this saves money for the company as they don't have to supply separate work devices for staff, the issue of data security needs to be carefully considered.

You joined PwC as a graduate. What are the current graduate career opportunities for IT professionals at PwC in the North East? Why should other people consider joining the business in the region?

PwC has been voted number one in the Times Top 100 Graduate Employers for the last ten years. So, in terms of our graduate program, it's very well established. In the North East, we offer a range of different opportunities such as graduate vacancies, summer internships, placement years and experience days. Having leading universities on our doorstep, and offering a leading graduate scheme, enables us to keep a strong pool of talent here in the region. Last year our Newcastle office took on 20 new graduates and three school leavers, including four in my team. In terms of working in the North East, for me personally, I found that you get the opportunity to work on a broad range of areas. For my personal development, that was fantastic. We also give our staff the opportunity to work overseas in other offices and bring back the knowledge and skills they have gained, which is vitally important, certainly during the early stages of your career.

You're a relatively young leader who has ascended fairly quickly into a senior role at a major consultancy; what aspects of your career to date have helped you to climb the ladder? What advice would you pass on to other young aspiring leaders?

Doing a quality job is essential, not only to help and support our clients, but to also be recognised internally. If you want to progress, you must make time to develop your team because, at the end of the day, you are only as good as the team behind you. The other thing I would say is that you need to evolve your skills and your experience and go outside your comfort zone, try something new and push yourself to work on more complex or different engagements.

> "Because the majority of organisations are online and far more dependent on technology, cyber security is one of the biggest threats they will encounter today."