

## Osborne joins Interoute

© Communications News 2005

Mark Osborne launches into a Peter Kay tirade as soon as you meet him. For those that know the comedian – Mr Kay, that is – Osborne disarms you with offers of ‘tea?’ with the requisite tea-drinking hand movements, then follows up with a quick burst of loud exclamations of ‘garlic...bread?’ amid lots of chuckling.

Osborne is the new director of information security at pan-European carrier, Interoute. Despite the serious job role, expensive suit and austere pedigree, he is one of the most charismatic and blatantly funny people you could hope to meet.

“A lot of this job is being a suit; it’s not all glamour and hacking into firewalls at banks,” Osborne states. “But I did used to get on stage and tell the audience that I’ve broken into more banks than Jessie James. For the last 11 years at KPMG, hacking into banks was part of my job.”

The pedigree of this man is impressive. Osborne began in the industry as it was developing, so his knowledge and career has grown with it. Today, he works as a government security advisor. He has also appeared as an expert witness in a number of high profile legal actions. Over the past decade, he has worked at KPMG as director of security. Here he bought together the company’s security engineering and technical assurance teams.

Osborne has had a busy career. He was the horn-blower for many of the flaws in the WAP and WiFi protocols; authored a major intrusion detection system and many proof of concept security tools, including the renowned open source WIDZ wireless intrusion detection system; developed a number of ZERO\_DAY vulnerabilities; and released the Fata-jack 802.11 vulnerability that could disrupt any 802.11 network. He also has a plethora of acronyms behind his name: CISSP; CISM; CCSP; CLAS; CCSA; CCSE; and MBA.

The company now known as US Steel, formerly called Marathon Oil, is where Osborne began his career. He says: “There was a fraud at the company I worked at and the guy that came in to investigate it was like Norman Wisdom; he didn’t have a clue. At the time I was a technical support manager. I saw this was an area with a future and at the time, computing was becoming a commodity, so I decided to move into something more specialised.

“At Marathon, I did a very technical job,” he continues, “I knew about routers and security sub-systems. I worked my way up from fixing them to watching over the guys that did. Fundamentally, security is about understanding how it works.”

Osborne then joined KPMG as its only technical consultant in the practice. “At the time in the 1980s, there wasn’t a technical aspect to security in general. The senior security personnel wrote a security policy, while the junior personnel looked after a big mainframe and added user IDs to the computer. The big thing when I joined KPMG was Unix, which was very insecure then.”

His first year at KPMG was rocky, he says, thanks to his lack of a Cambridge degree which reduced his credibility. Huddersfield Polly was the place for him, as it was one of three places of further education recommended by IBM, which meant more money for a graduate. However, when the IT director of a major bank client requested more people like Osborne and no more fresh faced university graduates, the snobby situation at work changed.

“The bank was going from a mainframe system to Unix, and none of its security infrastructure applied any more. It needed someone to go in and sort it out, plus communicate with a very traditional security team that was trying to put mainframe security policies onto Unix and then NT. So I wandered in and fixed it.”

After that, he helped the bank provide the first online banking service in the UK, after he had at first refused and they had tried then given up with a so-called expert in that area. That was 1996.

“It’s all about practical common sense,” Osborne says. “That’s the story of my career. But common sense is amazingly uncommon. I was employed to give a level headed opinion on new technologies, then I moved onto installing and reviewing online banks, and trying to catch hackers.”

He continues, misty eyed: “It was a little like being a rock star. Going up to senior people, saying that I didn’t know what this problem was but I’d seen something similar before, so trust me. There was a level of theatrics about it. People made a big fuss about security, so it made the senior management feel more secure and comfortable about there being problems.”

Although he adds that he feels security issues have been a little over-dramatised in the past, to the point where now little is done by many organisations who suspect that the media, vendors and security consultants are just crying wolf for their own gain. “Hackers and viruses

are not out there to get you," Osborne explains. "If you treat the threat as a normal affair instead of an extraordinary event, you can get through it, feel comfortable to take advantage of new technologies and get away from FUD – fear, uncertainty and doubt – as companies that don't try to take advantage of new technologies, fail."

Osborne is glad that regulations such as Sarbanes-Oxley are forcing companies to consider security through the legal implications of ignoring it. "We need to take security seriously. IT and network managers have to behave responsibly. You still see people with no adequate disaster recovery, who still aren't backing up their systems and data, who don't have adequate systems, who aren't looking after their firewall, and who aren't updating their antivirus."

The key for the vast majority of businesses out there is mundane and simple, Osborne says, but the following procedures will keep security tight. "For the top 20% of companies, the challenges are de-perimitisation through partners, collaborative deals and home workers; the mobile nature of security; and growing regulation.

"But for everyone else, it's staying on top of viruses, malware and spam; patch management; maintaining your firewalls and routers; looking at governance controls; and managing your environment, by making sure you have the right users on the system, making sure the users have the right level of access to systems, and deleting the users when they go," Osborne states. "This is not a sexy message, but it's important."

For Interoute, things are looking good. This company has recently expanded with its acquisition of Via Networks. Adding the security heavy weight in the form of Osborne to the mix proves to customers that this is a serious business with exciting propositions for the industry. And the future is going to be great, Osborne adds, with the development of voice over IP services and the creation of a new, corporate-friendly version of Skype on the cards. Watch this space.

ends