



HOPKINSON, NELSON, SUMMERHAYES, NESBITT

ATTENDEES

FRANK NESBITT

Tait Walker

STEVE NELSON

Calibre Secured Networks

DAN HOPKINSON

Lockton

NEIL STEPHENSON

Onyx Group

DAVID ARTHUR

Tait Walker

PAUL HUGHES

Crutes

DAVID SUMMERHAYES

Crutes

ALAN COTTOM

Stonesoft

Securing your business

Insider gathered together some of the North East's top business security and fraud prevention specialists to discuss how secure North East businesses are and what precautions need to be taken

What are the biggest business security and fraud risks for the region's businesses?

Frank Nesbitt The biggest risk is that businesses don't accept fraud as a real risk. Admitting that you have been a victim of fraud is very difficult for a business. There are lots of issues to consider – businesses don't want to make an admission that they are at fault. Fraudsters are very good at gaining entry into a business whether it be from within or from outside. If businesses don't have measures to protect themselves ultimately they will find a way in.

Dan Hopkinson A lot comes back to brand. The damage that a security breach can do to a company's reputation is the biggest factor to businesses. The Information Commissioner is moving more to the way they are in the US, they are going to start notifying now of incidents where there is a breach or attack or personal data has been compromised.



"Admitting that you have been a victim of fraud is very difficult for a business. There are lots of issues to consider."

Frank Nesbitt

Steve Nelson Information security as a whole should be a concern to businesses. We're talking about online and offline activity. Individuals aren't necessarily looking to defraud the business out of assets, but to get a foothold into the business electronically for various purposes. They may use the infrastructure of the business to launch an attack on another business or to use it as a cover.

David Arthur It comes back to a HR issue, where the real problem gets buried (sacked) and is never really dealt with.

David Summerhayes We see a lot of that – people within the business at all levels having access to information and using that information for their own means.

STEPHENSON, NELSON, COTTOM





What can businesses do at a basic level to protect themselves?

Nesbitt The most important thing is not to engage a fraudster from the very beginning. Screening and vetting are very important. I see numerous examples where at high levels applicants claims are being accepted at face value.

Hopkinson Processes are also very important. We see a lot of examples of simple precautions not being taken. We often see senior staff passing the buck, saying business security isn't their problem. But it has to be filtered down from a senior level. Simple risk management can be straight-forward and it can be free, but people don't seem open to even do the basics. For example, is stock monitored in and out of the building, are people signed in.

Alan Cottom IT infrastructure in a business is extremely important, but unless companies have the policies in place and senior managers don't back security policies, they never get implemented. There's almost a false sense of security in a lot of organisations. Most businesses will protect the perimeter of their network – they will have a firewall and so on to stop attackers getting in – but year on year the biggest threat to security is from the inside, whether it is a malicious user who has a grievance or whether it is accidental. Time and time again we are seeing big companies such as Sony being caught out. There is technology available that will help to form part of your underlying security, but if your security systems aren't being monitored they can usually be bypassed.

Arthur For organisations, it takes a lot of time to stress test these systems. How many businesses can shut down their systems and do a real stress test on them to see whether they are secure?

Nelson You're quite right David. We're finding that it's as much about education as well as having the tools and specialists to do the job. The education element of what we do is making clients realise that there is an issue. Statistics show that if there is an unpatched machine in your organisation accessible from an

external source it will be compromised by an external attacker within six minutes. We're not talking about weeks and weeks to define a policy, this is happening now. A further problem is that quite often businesses don't know they have an issue, or they don't want to address it for fear of being seen to have a perceived weakness in the system.

Hopkinson Another issue is outsourcing. When you outsource, how much pressure do you put on your provider to mirror what you do. I'd say the majority don't put any pressure on. They hand it to a third party and say it is their responsibility. But in terms of data, it's your data, your customer, your responsibility – you can't pass the buck on that.

Neil Stephenson If you take real life examples and controls – it's often someone who has physically let you down. No matter what the level of the person, you have to give trust to people. Without controlling them like a robot there is always scope for fraud.

Nesbitt But if you have a fraud prevention culture in place in the organisation you have a better chance of staff noticing and reporting changes in behaviors in fellow staff members.

Summerhayes You can't put technological processes in to stop every fraud, and it is impossible to stop every fraud. It is a question of risk; minimising it, and having a culture that helps you do that.

Stephenson It's a tricky one because if you have a person employed who commits fraud, when you find out, you just want rid of them as quickly as possible. Does anyone know a company that has been in that situation and has made the situation public? I don't know of any.

What else should companies be doing to protect themselves?

Nelson We live in a technological world; everyone's got a mobile phone and an email account, everyone has a laptop, even kids. The breach that happened to Sony, which is going to cost in the billions of dollars, wasn't an insider, it wasn't someone who particularly had a grudge against the company. It was



STEPHENSON, SMITH, COTTOM, ARTHUR



“How many businesses can shut down their systems and do a real stress test on them to see whether they are secure?”

David Arthur

a directed attack at Sony's infrastructure because of a weakness in technology. Not because a person wanted to steal the information, but because some kid in the Shetland Islands did it because he could. Here's an example: I stuck up a box on our network on Monday and we had a sustained attack on that box from Monday night until I turned it off the next morning. These attacks were from countries all over the globe, Japan, Russia, Chechnya – we're not talking about some small risk, this kind of vulnerability is widespread and is a massive risk to businesses.

Stephenson It all comes back to culture. To see a change in this I think we need to see tougher penalties. The deterrents need to be from a management point of view. We've had the Data Protection Act for quite some time, but there have been very, very few prosecutions. It's just starting to become more of an issue now but the fine levels have dropped so there is no real deterrent.

Nelson To make business security work, businesses need a combination of the human element of getting the culture within the business right and the technological element of having the right systems in place. Only then will businesses become properly protected.