Link to Article

Managing data breaches

Top IP & Technology lawyer Sheena Jacob highlights simple precautions to sidestep information security woes.

CYBER ATTACKS AND INFORMATION SECURITY breaches have become more regular as hackers devise new ways to access private information from firms both great and small, with prime targets being banks, investment firms and government departments.

As the number of cyber attacks escalate, both governments and the private sector are taking urgent measures to combat the threat, with various countries, including Singapore, setting up cyber security departments.

Jacob emphasises that the first few hours after a cyber attack has been discovered are the most critical from a damage limitation stance. "The most critical decisions come in the first few hours. The very large financial institutions have protocols in place but maybe the smaller ones don't. What is absolutely important is to have a plan now for what you are going to do if you do have a security or data breach. Waiting for it to happen to react is likely to result in much greater damage.

"In the instances that a breach has occurred, some clients were very well prepared, very well organised, with all the vendors in place. I came into the system on the legal side, we had an independent computer forensics expert to look at the breach, and there was also a PR firm to deal with crisis management. The important thing is that there is a plan and that everyone knows what they need to do."

"On the other hand, there are examples where clients are just not prepared and have left internal IT to deal with the situation. Often IT spends hours trying to deal with the technology problem without realising that the information has already left the premises; they were just trying to contain the situation, but not dealing with the immediate consequences of the actual breach. I think this is natural, because the IT organisation will focus on the infrastructure, but the business needs all the other elements in place. Because of legal regulations, you may have to notify multiple regulators in more than one country. You may also, in some circumstances, have to notify the individuals immediately concerned, because they need to make sure they take appropriate steps to protect their data before further damage is caused, especially if the data compromised is credit card information."

SHEENA JACOB
JurisAsia

Pragmatic Jacob is pragmatic when it comes to giving advice on how to put measures in place to avoid or

minimise cyber security breaches, with advice ranging from the simple to the sophisticated.

"One basic security step for individuals and small businesses is to ensure they regularly change passwords. People tend to use the same passwords for different platforms and it's quite important to realise that just using a password alone is insufficient security; you want to have a second level of authentication. It would be preferable to use some form of two factor authentication, even for tools like WhatsApp. Businesses should look at encryption of their laptops and USB drives so that the loss of these devices does not compromise the data on them.

Jacob also sees various governments regulating cybersecurity for fear of losing valuable information and

PEOPLE DON'T NECESSARILY APPRECIATE HOW IMPORTANT SECURITY IS UNTIL SOMETHING GOES WRONG ESPECIALLY IN FINANCIAL SERVICES OR IN PRIVATE BANKING

critical infrastructure. "Governments are very concerned, especially if you are holding information that they consider to be critical. They are concerned about the offshoring of data and systems if that results in less control. However, data localisation requirements go against the grain of central hosting or using cloud service providers to be able to consolidate all information into a data center somewhere else in the world," she said.

"China has introduced a cyber security law to localise data if you are a key infrastructure provider, but even if you are not, if you just have a network, probably by the end of 2018 you may have to localise that data in China. That's been a big issue for companies because they are suddenly having to revise their infrastructure."

Safety over convenience Jacob freely admits that this will call for people to log in every time they want to use a device or application, but she stands by that in the interests of safety.

"While it might sound like security can require a lot of additional work, people need to adapt in terms of their technology and internet behaviour. No matter what level of security you have, people must understand that there is always some risk to any information you share or collect. For example, if I was a private banker, I would not maintain client information in one document. I would not, for example, put all of my client's names next to some of their other personal information. In other words, try to assume that some of this information might be compromised and think about the risk of having it all in one spreadsheet should that document be compromised. The key is to keep your information as segregated as possible and minimise the collection."

Jacob also warns against closing the gate after the horse has bolted, and the effect that could have on a company's standing within the community. "I think there are reputational issues, and unfortunately many firms don't understand why cyber security is so important. People don't necessarily appreciate how important security is until something goes wrong, especially in financial services or in private banking.

The clients' information is sacrosanct, and the bankers or IFA's are the guardians of that information and need to make sure that everything possible has been done to protect it. From a reputational point of view, it's hard to recover from a data breach; you are going to lose client trust. If you can't look after their data, how are you going to look after their money, surely the two are inextricably connected." ■

Cyber catcher

SHEENA JACOB IS A LEADING intellectual property (IP) and technology lawyer with more than 25 years' experience in the IP and technology field. With a strong international client following, Jacob is qualified to practice in Singapore, New York and England and Wales.

Considered an expert in her field, Sheena works with technology companies and innovative businesses to help them build and extract value from their global IP assets.

She also has extensive experience in the privacy field in Asia Pacific, having previously headed the Asia Pacific data protection practice at an international firm. She works with clients to review their privacy policies and processes as well as being appointed in advance to advise on any data breach. She is the only Singapore lawyer on the global board of iTechlaw and sits on the Asia Advisory Board of the International Association of Privacy Professionals She holds both Certified Information Privacy Management and Certified Information Privacy Professional (Asia) qualifications. Her deep knowledge of IP & technology has been described by her peers as "truly remarkable". ■