Politically motivated cyber-attacks now a reality

Following last year's much publicised Sony cyber-attack, in which Sony executives were left red-faced following the leak of sensitive company information into the public domain, Richard Keymer, Head of Pre-Sales of SecureData Africa, is predicting a marked increase in politically motivated attacks in the year ahead.

Richard Keymer

"Up until now, hackers tended to be driven purely by financial gain. Here, through the use of sophisticated malware, they would steal intellectual property such as banking or credit card details, gaining access to bank accounts or credit facilities without necessarily engaging with their victims.

"What differed in the Sony attack is the fact that the hackers not only engaged with their 'victim', but held them to ransom where the attack was motivated by a political or ideological agenda. Here, Sony execs found themselves in a situation where if they did not comply with the hackers' demands, they would pay the price in the form of sensitive information being leaked into the public domain as opposed to any type of financial loss," he commented.

No organisation or entity is un-breachable

Although Keymer emphasises implementing standard good practice when it comes to preventing these kinds of cyber-attacks, he stresses that no organisation or entity is un-breachable, with organisations required to adopt the mindset that a breach is inevitable and implement plans to best respond to these kinds of attacks.

"Among the lessons learnt from the Sony attack is the need for organisations to move from a proactive to an ongoing reactive approach, where having an incident response plan in place can no longer be regarded as a 'nice to have'.

"A response plan to any form of cyber-attack is critical in preventing both financial and reputational damage. Sony's response demonstrated a clear lack of planning. With data breaches or hacks now an inevitable part of daily life, not having a clear incident response plan in place will see many organisations paying the ultimate price from both a financial and

reputational perspective," he stressed.

In terms of incident response plan best practice, Keymer said that disclosure should be top of the list. "Prompt disclosure serves to mitigate not only reputational, but also potential financial, damage. For instance, should data pertaining to banking information or credit card details be leaked, organisations cannot afford to be on the back foot.

Heavy penalties

"Not only can heavy penalties be imposed for not having sufficient measure in place to secure sensitive information adequately, but the cost of clients opting to close accounts or publically voicing discontent can have both financial and reputational impact from which few organisations will be able to recover unscathed," he explained.

For Keymer in the reactive cyber response scenario, time is money and having measures in place to monitor and mine data from both networks and non-intrusive internal systems are invaluable to both proactively preventing as well as successfully recovering from breaches.

"Statistics show that malware often sits undetected on systems and networks for up to six months before it is picked up. This means that hackers have ample time to gain access to whatever data is needed to achieve their goal whether it be financially or politically motivated," he added.

Going forward, Keymer predicts not only an increase in these politically motivated attacks, but also an increase in attacks by hackers backed by deep pockets with access to big budgets. "This is a concern as, in reality, it means that there is not a lot that a targeted organisation can do in terms of their response plan as chances are the attackers have access to the manpower and technology to achieve their overall goal.

"However, with this in mind, some organisations have more to lose than others and, again, it comes down to weighing up the risks of a potential data breach and implementing appropriate security investment to adequately address these risks," he concluded.