When your good guy goes bad

One of our clients recently ousted one of its most trusted employees, who had been using the company's clients intellectual property and contacts to run his own business, in direct competition with his current employer. Using company time and resources, the employee had been offering the same services as the company, even using the company's name, but was invoicing 'off the books' and being paid directly into his own bank account. This has cost our client vast sums of money in lost revenue and will now take up valuable time while the criminal case is investigated.

By John Mc Loughlin 17 Sep 2014

The company's owner first realised something was amiss when she received a call from a supposed client complaining ab bad service.

"It was a shock," she told us. "I had no idea who the company was or that we were even working with them, but the irate 'client' assured me not only had they been using our services, they had been paying for them. Yet I had no record of thes claims."

Upon further investigation, we found that because he was a senior member of staff, he had privileged levels of access to information that was a requirement of his position. This access then provided him with the knowledge to stop certain monitoring tools we had installed - but not everything. A rogue employee will do everything he can to deter detection. We h consulted and ensured that our client had more than a single layer of security to protect its information and while the nasty insider made it tougher to find, we had ensured that he could not escape.

Incidents are growing

I cannot stress this enough - the insider threat is not only real, the incidents are growing in frequency and severity. It is a sad truth that as times become more difficult people are trying to find different ways to take home extra money to live beyc their means. No matter how illegal their methods are, we hear so many excuses on how the perpetrators justify their actior

I would like to point out some key points to consider:

- Firstly, I would like to commend the smart leadership of my client for listening to our advice and choosing J2 Software's solutions and services to provide a multi-layered approach to protect its information. Data security does not stop at the pol creation, you need then to monitor and enforce compliance. We have ensured that solutions were in place to cover agains the unthinkable - the insider threat. It is remarkable how many organisations still adopt the 'it won't happen to me' attitude. one imagines that a trusted employee in a position of power will turn against the company, but this case proves that it is a very real threat to any organisation, and this is exactly the reason why stringent security measures and solutions should b put in place;

- Secondly, of course, is that we had all the evidence to prove fraudulent activity when we needed it. This is a major point is important for business owners (big or small) to realise that all too often it is the most trusted users that cause the most damage. Even being in a long-standing senior position should not indemnify employees from being scrutinised.

This case raises the age old question - who manages the managers? Or who administers the administrators?

In this case, having access to sensitive data was a requirement for the rogue employee to perform his daily job. And track where this data went and who it was sent to, was what allowed us to catch the culprit red handed. This kind of tracking alsc made it easier to take corrective steps much faster than would normally be the case. Remember, a trusted individual can r only cause losses, but can destroy businesses.

React to the warning signs

Another important lesson to take way from this experience is to ensure that other senior management members and the Cl take note of and react to the warning signs. If something seems out of the ordinary with an individual, it probably is. You cannot turn your back on the signs. The first warning sign that the rogue employee was 'hiding something' was when a particular security solution had been repeatedly removed from his machine. Being a senior employee, he would have knov how to remove the solution as part of the post-implementation training.

The initial suspicion caused us to start looking early and the unknown client calling to report bad service provided the final piece of the puzzle. As soon as we checked our multi-layered defences we quickly built a vast amount of solid evidence without wasting excessive time or spending more money.

I always say that a comprehensive, yet easy to understand information security policy is your starting point. From there it imperative that you monitor and enforce compliance to these policies by your staff. I believe visibility is the key and even i you think you don't want to check up on somebody, it is an essential part of modern business to do so, just as this client's story has shown us. It is not a case of 'if' you will need to use our solutions, but rather a case of 'when'.

As far as I am concerned, there are two types of businesses - those that have suffered a loss due to the trusted insider ar those that will. The key is having tools and mechanisms in place to ensure that the effects of this are mitigated as much as possible.

ABOUT JOHN MC LOUGHLIN

John Mc Loughlin is a visionary entrepreneur that has been involved in the setup and management of a number of start-up businesses. For the past seven years, he has been working towards changing the security landscape for SMEs in South Africa through his company, J2 Software, which provides solutions around reducing risk and improving compliance. John industry specialist and thought leader in the security space, and his particular areas of expertise lie in planning and strategising.
View my profile and articles...