Beat or prevent **occupational fraud**

The human factor is your weak spot when it comes to banking fraud.

Sergey Ozhegov

Any bank employee having access to useful data can put the power in the hands of fraudsters and create problems for a financial organisation – by evil will or mere negligence. Knowing what the danger is and where to soften the blow, you can significantly reduce insider risks. So who in a financial company creates risks, and why?

Top managers

Why? Because they don't have time for security. And this happens in every field, not only in banks. Top managers are aware of the importance of risk prevention on a business scale, but in real terms, they ignore security rules. For example, they agree to the default privacy settings or use weak passwords. I knew an executive who always used the same password, and when it had to be changed, he changed only the last number. It can be understood, time is short, and there is a lot of work to be done.

Mobility comes first! Nowadays, managers work less often from the office; they travel a lot and use gadgets. There is a lot of confidential information on these devices, and managers often ignore passwords and blocking. The device can be forgotten in the airport lounge and, before the company security department finds out about it, fraudsters will lay their hands on the information.

We should not forget that top managers, like other employees, are subject to social engineering and phishing.

What approach can be undertaken by security or risk management staff in working with a company leader? Make contact and communicate the importance of following the rules. It is difficult, takes a lot of time and is not always successful, but necessary.

IT personnel

The critical point is that these people manage the entire corporate infrastructure. In terms of information security, technical experts understand more than other employees, but they can also make mistakes or become victims of manipulation. And the price of such a mistake will be higher than the price of an incident caused by a staff member. Speaking about the practice of our clients, the most frequent cause of incidents due to the fault of an IT staff member was trivial negligence: not updated system or not deactivated account of an ex-employee. Sometimes such errors are very expensive.

Although we shouldn't forget about IT sabotage when system administrators abuse rights intentionally. Here is one of our client's cases. The system administrator quit because he wasn't promoted. But he decided to take revenge: he used remote access to connect to the infrastructure and upload a malicious programme with delayed launch. It was activated two weeks after the dismissal of the employee and erased the configuration of the network equipment. As a result, the work of the company was paralysed: employees could not send and receive emails or go online, and calls to sales-managers were forwarded to the company's CEO. It took a month to restore the system, and without recovery files it could take more time.

How to minimise the risks connected with IT staff? Evaluate not only professional competence; an employee in this position should be reliable and loyal, which can be assessed by HR as well as by risk management officers. For risk managers, there are technical tools like automated profiling, a system that performs classification of personality traits based on the analysis of correspondence.

It is also important to use advanced automated tools for monitoring: DLP, SIEM and other information security software. Basic DLP functionality will not be enough if a competent IT professional decides to bypass the system. All actions should be logged, including remote sessions.

Back office staff

These are the employees processing incoming requests for account statements and other transactions as well as the employees performing a variety of banking services and corresponding with customers, counterparties and third parties. Their email addresses can be an entry point for external scammers. For example, an email from a tax inspector to the accounting department of a company can be send by a fraudster who has created a mail box that would look like a valid inspector's address and would embed a virus in the email. The accountant worries, opens and reads carefully, meanwhile the spyware is being installed and starts to collect classified information. This is only one of the possible options.

Phishing, spoofing, social engineering and business email compromise (BEC) are the most popular external attacks that credit and financial institutions have to deal with today. This is the easiest and cheapest way for attackers, so banks will have to resist such attacks.

In addition to all technical tools for control, the main thing that can seriously reduce the likelihood of problems with back offices is regular training, as practice shows that 80% of the staff fall for a phishing email from top managers.

Clerks

These are the employees with a sufficient level of access to confidential information and relatively low salaries. This is an important moment, since some employees are not averse to earning extra money. There are ways to benefit from access to confidential financial data: cards and databases are in great demand on the black market and their prices range from five to 110 US dollars (ZAR75 to ZAR1,634). However, high-rank employees are far less likely to risk a place for a one-time gain.

By the way, video recording in customer areas is not a panacea. A camera records violations, but, to study a six-hour video, you need to spend about 12 hours. Moreover, this is reasonable only if there are suspicions collected in a different way – for example, complaints from customers, other employees or inconsistencies in bank documents.

Finally, let's be realistic: a huge flow of clients passes through the customer area. A violation due to simple fatigue is also a common practice. A few weeks ago, I visited a bank and I had to answer a huge amount of questions for identification, it took half an hour. Next time, the clerk checked the passport so fluently that almost anyone could present it to an employee. Here is another client's case: an employee collected data about deposits where there had been no movement for a long time. The employee changed personal data and transferred money to her own account, receiving confirmation of the operation from her colleague because they were friends.

To minimise such risks, it is necessary to elaborate security policies for the main types of sensitive data, which is accessible for clerks: customer databases, credit card data and transaction information. You can track all the operations with this information by implementing a DLP solution. Programmes can remember documents and compare them with the entire flow of information in a bank or recognise scanned copies of passports and cards. There are many search possibilities, and a detailed understanding of rules is a basis of timely notification of employees' suspicious activities.

As the experience of our customers shows, any employee can create problems for a bank. The damage from the actions of a clerk can amount to thousands of dollars, and the actions of top managers can lead to bankruptcy, however, you need to control both. The control methods will be different and, at the same time, a business can not only prevent deliberate fraud, but also protect the employees from accidental errors or from becoming victims of fraudsters. ■

Sergey Ozhegov is the Chief Executive Officer at SearchInform in the Russian Federation.