

## TRANSACTION SECURITY IN AN ALBANIAN FINANCIAL INSTITUTION HAS BEEN BREACHED – WHAT TO DO NEXT

**Enida Puto**

Bank of Albania

ALBANIA

enidaputo@yahoo.com

**Kozeta Sevrani**

Faculty of Economy - UT

ALBANIA

kozeta.sevrani@unitir.edu.al

### ABSTRACT

The question for a financial institution is not if they will suffer a cyber-attack, it's when. We focus this study on Albanian financial institutions and potential cyber-incidents that involve fraudulent transactions, as this is the main focus for attackers nowadays. When financial transactions are compromised, a cyber-incident plan helps to minimize the effects of the cyber-attack, the time to bounce back to normal business and also helps minimize financial harm. Although every financial institution should take very strict measures of defense in all the parts of information technology infrastructure, including perimeter, people, policies, procedures, network, PKI, hosts, applications and databases, part of the whole process should also be a plan of what to do in case of a cyber-attack that may or has led to fraudulent transactions. We performed a study in Albania, in order to understand where Albanian financial institutions stand in regard to a cyber-incident plan when financial transactions were compromised. We found out what procedures Albanian financial institutions had in place and what lacked for managing a cyber-incident involving fraudulent transactions. In this paper we analyze the case of a severe cyber-attack, where the institution's data have been breached and possibly stolen, modified or used to impersonate this institution by sending fraudulent transactions. In this perspective, we analyze several Albanian financial institutions on how they deal with it, and what plan do they have in place in case of such a cyber-attack. We suggest a detailed and customized cyber-incident plan according to institution's infrastructure and type of attack and compare this plan against the findings in financial institutions that we examined. Then we come to conclusions of what should be the best way or plan on dealing with these kinds of cyber-attacks.

**Keywords:** Cyber-attack, defense, data, breach, security, financial.