



# Three audits

Foto: Ivan Dimitrov

## at a stroke

*Three successful audits, more security, optimised processes; BORICA Ltd., the central organisation for credit and debit cards in Bulgaria, has an excellent opinion of SRC services. SRC Security Research & Consulting GmbH helped BORICA implement the MasterCard Logical Security Audit concurrently with a PCI DSS Security Audit and a RINGS-environment audit.*

||-- Most of the credit and debit cards in Bulgaria depend on BORICA systems. The "Bank Organisation for Payments Initiated by Cards" (BORICA) is owned by Bulgarian National Bank (BNB) and twenty two local banks and it is the central national organisation for all matters relating to card-supported cashless payment transactions. BORICA also issues the leading Bulgarian debit card with the same name (comparable with the German Girocard). BORICA is Bulgaria's third party processor for Visa International and MasterCard Worldwide and their local partner banks. BORICA also produces and personalises Bulgarian debit and credit cards for both card organizations.

### *Strong requirements*

-- The Payment Card Industry Security Standards Council (PCI SSC), of which MasterCard and Visa

are also members, helped formulate the PCI Data Security Standard (PCI DSS) specifications, with which all companies have to comply who store, process or transfer card data within international payment systems. In addition, MasterCard and Visa also require any issuing operations to pass an annual Logical Security Audit and a Physical Security Audit. Logical Security provides MasterCard with the confirmation that logical security requirements are complied with during the card personalisation process. This audit reviews for example roles and responsibilities, analyses security planning, takes a close look at encryption, monitors observance of double-checking and also considers building factors like how and where are cards produced? How and where are they destroyed? Logical Security is complemented by aspects of physical security: what is the situation in terms of data and

*"That was no normal audit. We also benefited from the high level support provided by SRC and collaborated very intensively."*

**Christo Kostov**  
Head of Information Systems  
BORICA Ltd.

network security? How does user management and access control function? What is the software and hardware security situation? And last, but not least: what is the condition of buildings in which credit and debit cards are produced and personalised? SRC also has MasterCard accreditation for such audits.

#### *Idea to combine audits*

-- BORICA was established in 1993, and had previously passed all audits and requirements specified by the credit card industry with the aid of a major international business consultant. In 2007 the Bulgarian card processor put the audits out to international tender. SRC, based in Bonn, won the tender, beating many big players. "SRC met our requirements exactly and also put in low priced bids thanks to its efficient and integrated procedures," is how Christo Kostov, Head of Information Systems at BORICA explains the Bulgarian's choice. SRC also convinced the Eastern Europeans in other ways: SRC proposed combining the MasterCard Logical Security Audit with a PCI DSS security audit and an independent audit of the link and operations of BORICA with the Real Time Gross Settlement System (RINGS) that performs the settlement of interbank card transactions which is managed and operated by the Bulgarian National Bank, in accordance with the requirement of BNB regulations. The big advantage: all three reviews could be implemented concurrently to cut costs. SRC was also the only company world-wide able to offer all three audits from a single source. In the future, MasterCard's Physical Security Audit will also be integrated into the combined audits at BORICA. Christo Kostov: "It was this kind of integrated approach which we found so persuasive." Today, MasterCard only approves those auditors who, like SRC, have the capacity to execute both audits – the logical and the physical. SRC remains the only operation world-wide which has approval for MasterCard logical and physical audits and PCI DSS security audits.

#### *Providing Consulting services*

-- During the course of work in Sofia, it quickly became apparent that BORICA's choice of SRC was the right one, for another reason as well: during the analyses it was soon obvious that implementing the security specifications in Sofia was not going to be a 1:1 transfer. SRC therefore also provided BORICA with consulting services. The German-based firm was able to advise its Bulgarian client, drawing on experience and knowledge gained from a large number of previous projects: "That was no normal audit",

says Christo Kostov, "we also benefited from the high level support provided by SRC and collaborated very intensively." As an example, BORICA also runs a mainframe system in which the encryption of card numbers is not possible using classic procedures. It was thanks to SRC's mainframe know-how plus a considerable level of technical finesse combined with some security measures developed specifically for BORICA that SRC was able to help BORICA comply with encryption requirements, reports Manuel Atug, Consultant at SRC. This included, BORICA experts travelling to Bonn to join SRC staff to study firewall regulations and security concepts, giving them key knowledge to take back with them on their return to Bulgaria. The BORICA network was restructured with the help of SRC so that it is now fully compliant with the higher security specifications. Christo Kostov's overall impression: "SRC has experienced people with lots of background information in the banking and payments sectors. They are invaluable for us."

Because SRC knows what auditors want, they were able to support BORICA at several levels and stations in satisfying requirements. Advice included tips on software tools available from SRC's neutral software listings. The German experts also provided practical help: because the payment systems require all audit documentation to be in English, but because BORICA only had the documents available in Bulgarian, SRC helped in translating/interpreting and acting as intermediary between the company and the auditors. And since BORICA is also planning a move, SRC also reviewed the plans for the new building to ensure they accorded with the international payment systems' specifications.

#### *BORICA exceeded requirements*

-- Thanks to solid preparation, the actual audits took place without any problems or complaints. According to Christo Kostov, the auditors were very impressed that BORICA had even exceeded requirements in a number of places. The new password management process adopted at BORICA is well above the standards required by PCI. The audits plus the additional consultation components have ultimately helped upgrade the Bulgarian card processing and card issuing organisation: it can now not only document its compliance with international specifications, it also benefits from extra security, lower risks and optimised processes. Head of IT Kostov likes the bottom-line. He has negotiated a long-term contract with SRC and has also signed up with the Bonn-based security consultants for more audits and consulting services. --||



Christo Kostov  
**BORICA Ltd.**  
 117 Tzarigradsko Chaussee Blvd.  
 Sofia 1784  
 Bulgaria  
 Tel: +3592 9707 613  
 kostov.ch@borica.bg  
<http://borica.bg/>



Detlef Kraus  
 Thilo W. Pannen  
**SRC Security Research & Consulting GmbH**  
 Graurheindorfer Str. 149 a  
 D-53117 Bonn  
 Germany  
 Tel: +49 228 2806-0  
 sales@src-gmbh.de  
<http://www.src-gmbh.de>