Financial Cybercrime Perspectives

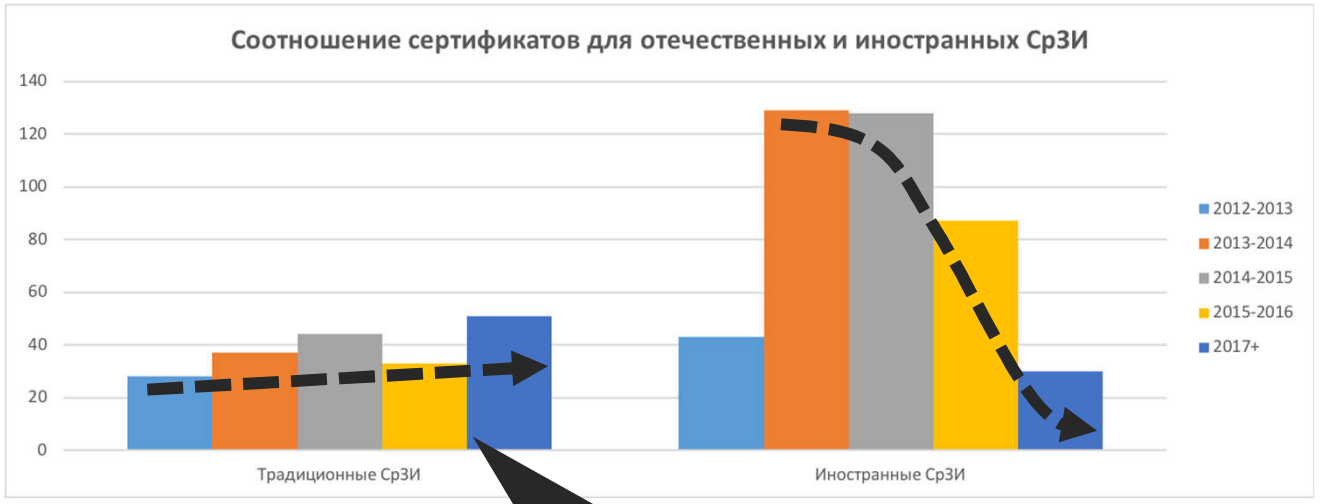
Compliance / Digital Sovereignty / Awareness Lesson Learned

Alexey Lukatsky
Business Security Consultant
February 4, 2019

Three pillars of financial cybercrime future in Russia

Digital Sovereignty	Compliance	Awareness
• US / EU sanctions • RU Digital Sovereignty Direction	• New anti-cybercrime laws • New regulations from Central Bank • New critical infrastructure protection legislation	• Lack of cybersecurity awareness • Inability of security awareness control

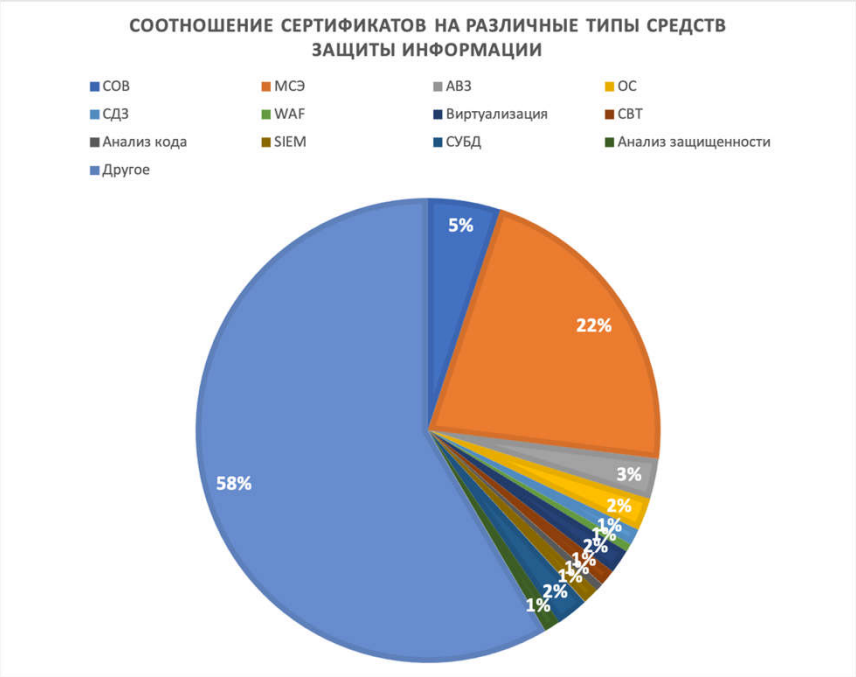
Decreasing foreign security vendors in Russia



Real digital sovereignty in cybersecurity ☹

- Reducing the number of foreign vendors by 4 times
- Tightening security requirements
- The practical absence of growth of domestic vendors

Russian cyber security vendors



- Focus on network security
- Lack of cybersecurity R&D
- Active use open source software as a base for domestic products

New compliance

New GOST 57580.1 and other standards

Base level of cybersecurity measures

FZ-187 about CI protection

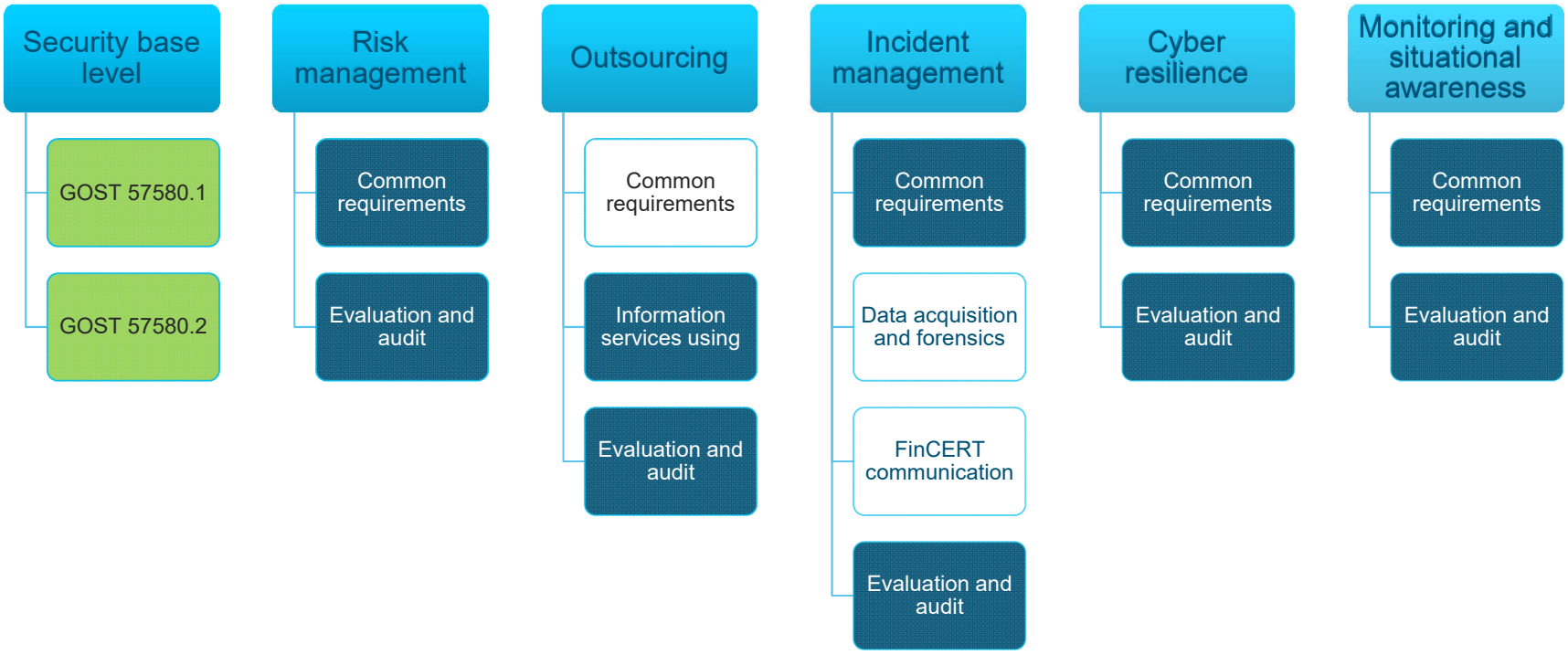
Mandatory security monitoring, incident notification and GosSOPKA joining

FZ-167 about antifraud

Mandatory fraud notification and using fraud criteria from Central Bank

Increasing of cybercrime security legislation

Security standardization by Central Bank



Continuous monitoring and incident notification

- Immediate notification about incidents and fraud attempts to FinCERT of Central Bank

- Immediate notification about incidents to GOV-CERT of FSB

Lack of security awareness

- We have enough compliance
- We have immediate notification about incidents and fraud
- We have security solutions so far
- BUT **lack of security awareness among users and judges**

Questions?