JEL CLASSIFICATION: C60, C67, L81, L86, M15

QUANTITATIVE MODEL FOR ECONOMIC ANALYSES OF INFORMATION SECURITY MEASURES IN INTERNET-PAYMENT SYSTEMS

Oksana V. KLYUVAK

Lead Specialist of the Scientific Department Lviv Institute of Banking of the University of Banking of the National Bank of Ukraine (Kyiv)

Summary. It is proposed quantitative assessment approach of security measures cost-effectiveness in internet-payment systems. It is analyzed the effectiveness of authentication methods in internet-payment systems within this approach in USA.

Information security was traditionally considered as a technical discipline, whose purpose was to provide the maximum level of security. In the last decade, a major economic component was considered in the related research as investments in information security are rapidly increasing. Knowledge about investments in information security requires quantification of costs and benefits of the investments. IT security solutions was previously oriented exclusively on search of technical tools and methods, without any consideration of the financial costs. The optimal level of information security investments is treated on the basis of the expected cost/benefit investment trade-offs.

In case of a security incident, merchants, customers and banks suffer financial loss L, which is measured in monetary units. It can be defined by the formula 1:

$L = L_{m\_chargeback} + L_c + L_{m\_indirect} + L_{b\_indirect}$, where $L_{m\_chargeback}$ – merchant's losses, for example from «chargeback», L_c – customer's losses equal to the cost of purchased goods and services provided by swindler, $L_{m\_indirect}$ – indirect merchant's losses, $L_{b\_indirect}$ – indirect bank's losses.

There are multiple strategies available to treat each security risk in internet-payment systems: reduction of security risk by implementing an appropriate technologies and tools (such as firewall, antivirus systems etc.) or adopting appropriate security policies (like passwords, access control, port blocking etc.); transfer of security risk to either outsourcing security service provision bodies or insurance agency; avoidance of security risk by eliminating the source of risk or the asset's exposure to the risk; acceptance of security risk as a part of business operations.

Internet-payment systems can be protected from potential security attacks by implementing security measures that can be classified into three categories according to their impact on the parameters R (risk), ρ (probability of a security incident) and L (financial loss): preventive security measures s_p, which reduce the probability of a security incident ρ (e.g., firewall, antivirus protection); detective security measures s_d, which reduce the time needed for an incident detection t_d (e.g., IDS systems, athentication methods, SMS, athentication datas hashing); other security measures s_o, which reduce the loss L in the event of an incident (SMS, blocking funds in the account, good merchsnts logistics systems). Each security measure s is defined by two quantitative parameters productivity of measure α and cost of measure C. Cost of measure C is a monetary investment in security measure. Return on Investment (ROI) as a popular accounting metric for comparison of investments is defined for three categories of security measures. Formulas for ROI, which are given in the article, are reconstructed into Formula 2:

ROI = (Pm – Lm – Sa)/Sa, where Pm – average merchant revenues; Lm – average amount of losses from online fraud; Sa – average spending on authentication technologies. Using this formula and USA statistical data it is demonstrated the authentication technology cost-effectiveness of American merchants. USA merchants mostly use typical verification authentication methods of international payment systems (Visa, MasterCard), that's why the costs

of these technologies are not significant and indicator ROI has a positive value.

A part of merchants' costs should be directed into effective risk management, logistics system and risk insurance. From customer's side – banking services cost, for a example SMS-banking. For banks – costs can be related to risk insurance, transaction technical support, special software. Besides the cost of security measures and other economic indicators, it should be focused on the reliability and resistance to attacks at the programming level. From this point of view it is advisable to apply authentication data hashing during the transaction realization.

References

1. Bojanc R., Jerman-Blazic B. (2012). Quantitative model for economic analyses of information security investment in an enterprise information system. Research papers Organizacija, Volume 45, Number 6, 276-288

2. Odarchenko R., Lukin S. (2012) Ekonomichna efektyvnist vprovadzhennia system zakhystu stilnykovykh merezh 4G [The economic efficiency of security systems in 4G cellular network. Information processing systems]. 4 (102), 2, 51-55.

3. Advantages of a risk-based authentication strategy for MasterCard SecureCode. mastercard.com. Retrieved from http://www.mastercard.com/us/merchant/pdf/rba_secure_code_HR.pdf

4. CEB (The Corporate Executive Board Company) TowerGroup Retail Banking and Cards Pract. Retrieved from http://www.executiveboard.com/.

5. True cost of fraud study. Merchants struggle against onslaught of high-cost identity fraud and oline fraud. Annual Report LexisNexis, September 2013, 1-35.

6. Card-Not-Present Fraud: A Primer on Trends and Authentication Processes. smartcardalliance.org. A Smart Card Alliance Payments Council White Paper. smartcardalliance.org. Retrieved from http://www.smartcardalliance.org/publications-card-not-present-frauda-a-primer-on-trends-and-transaction-authentication-processes.

7. Visa e-commerce merchants' guide to risk management. Tools and best practices for building a secure internet business. usa.visa.com. Retrieved from http://usa.visa.com/download/merchants/visa-risk-management-guide-ecommerce.pdf