

Pay Now or Pay Later: Obtaining ROI from Security Solutions

In the aftermath of Hurricanes Katrina and Rita, the headlines read: "Hurricanes rain on risk insurance industry." Insurance rates for the oil and gas operators in the Gulf of Mexico are soaring as much as 400%. On the contrary, the same oil and gas operators can enjoy information security solutions that are more efficient, more robust, and at the same or lower rate than a year ago. Why do companies realize that buying insurance is inevitable for a healthy business, yet they invest little in IT preventive measures? The answer lies in the maturity of the insurance industry in measuring risk and pricing mitigation, while the young IT security industry struggles in delivering similar mechanisms.

Security analysts or IT leaders at Credit Unions should adopt a risk management methodology to make security plans and set security budgets. Many methodologies can be adapted from the insurance or trading industries. Risk management encompasses three processes, risk assessment, risk mitigation, and risk evaluation. The risk assessment process includes identification and evaluation of risks and risk impact and recommendations for risk-reducing measures. Risk mitigation includes prioritization, implementation, and maintenance of the recommendations. Finally, the continual evaluation process ensures that an effective risk management program is implemented.

In the risk assessment phase, you should calculate a security ROI. A simple method is to answer the following key questions:

1. What key information assets are most critical to the Credit Union? What is their value?
2. What security incidents are of concern? What is the incident cost?
3. What is the total cost of a security solution? Capital and O&M cost over 3-5 years?
4. How does the total cost compare with new risk assumptions?

Regardless of how robust of a plan you produce, resources will always be limited in staffing, skills, and Dollars. The best Dollar spent starts with a sound employee acceptable use policy that is implemented and enforced. It may take you a while to fight cultural resistance to change, but it requires no technology, implementation cost or risk of project overruns. Next, you should spend your Dollars on perimeter security. Perimeter security stops problems at the gate and provide the best ROI from a rollout and maintenance standpoint.

To ensure your ROI analysis is complete, do not underestimate the soft returns, such as damage to the brand or loss of trust by members. Your analysis should not be stacked with only soft ROI. In addition, with some careful research and analysis, you can assign hard numbers to such dimensions.

At Network Box USA, we found that the unified threat management perimeter security solution coupled with managed security services and push technology provides one of the lowest total cost as compared to integrated solutions. The reason lies in lowering the cost of integration, narrowing the timeframe from virus outbreaks to protection updates, while conforming to NCUA examiner scrutiny.



Fadi Kanafani
COO



Fadi Kanafani is Chief Operating Officer of Network Box USA. As COO, Fadi is responsible for day to day operations and management of Network Box USA, Inc. Fadi is one of the founders of Network Box USA, Inc., the US distributor of the all-in-one Network Box internet threat prevention and security appliance. Fadi is a skilled management consultant bringing to the table over 20 years of experience derived from senior level appointments with energy and chemical related organizations. His knowledge is diverse and spans the entire value chain of natural gas and energy distribution as well as information strategy and software manufacturing. A speaker at pertinent industry conferences, Fadi holds Bachelors of Science degrees in Chemistry from Western Illinois University and in Computer Science from the Colorado State University.