ЭФФЕКТИВНОСТЬ ИНВЕСТИЦИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Никита Кожокару

Молдавская экономическая академия

Abstract: Technology has become the central nervous system of a business, supporting the flow of information that drives each business process from product development to sales. Many organizations failed to survive the information technology revolution. Many more will not survive the current wave of technology-driven innovation—and the threats and vulnerabilities that come with it.

На сегодняшний день информационные технологии активно проникают во все сферы деятельности человека, значительно упрощая ему жизнь. Между тем именно они неизменно привносят новые угрозы информационной безопасности. Бороться с новыми угрозами безопасности в вечном информационном противоборстве может помочь правильный подход к управлению рисками.

Риск - сценарий инцидента (события), в результате которого цели организации не будут достигнуты (в полном объеме). Если мы говорим о коммерческих организациях, то их основная цель - получение максимальной прибыли. Соответственно, риски снижают прибыль, за счет потерь от реализации этих самых рисков.

Риски бывают разные. В больших организациях различные группы рисков обрабатывают отдельные подразделения, зачастую координируя свои действия. Общая схема классификации рисков выглядит следующим образом:

Рисунок 1. Классификация рисков

Источник: http://www.securitylab.ru/bitrix/exturl.php?goto=http://1.bp.blogspot.com/-7Lhsq9eFw7U/VhZrMFnOLJI/AAAAAAAAHqk/AHT9E2u8R9E/s1600/risk-taxanomy.bmp

Количественную величину риска, связанного с осуществлением конкретной угрозы безопасности, можно выразить при помощи простой математической формулы:

$$\mathbf{R} = \mathbf{P} \cdot \mathbf{L}, \qquad (1)$$

- R – Вероятность успешной реализации угрозы с использованием уязвимости и причинения ущерба организации;
- P – Вероятность того, что угроза будет реализована;
- L – Вероятность того, что в случае реализации угрозы, безопасность будет нарушена и организация понесёт определённый ущерб.

В настоящее время выбор подходов управления рисками ограничен существующими методиками, которые непрерывно совершенствуются. Основной задачей специалистов информационной безопасности стало развитие данных методик, оценочных показателей и анализ эффективности инвестиций.

Попытка оправдать расходы на обеспечение информационной защиты всегда была проблемой для специалистов информационной безопасности. Несмотря на то, ряд академических моделей всё же были разработаны, они не пользуются популярностью и не применяются на практике.

В любой государственной или коммерческой организации инвестиции должны быть оправданы, но непосредственно эффективность зачастую оценивается после вложения инвестиций. В финансовой сфере оценка эффективности называется окупаемостью инвестиций или ROI (Return on Investment). Окупаемость инвестиций рассчитывается следующим образом:

$$\text{ROI} = \frac{\text{Прибыль от инвестиций} - \text{Стоимость инвестиций}}{\text{Стоимость инвестций}} \qquad (1)$$

В процессе оценки инвестиционной деятельности зачастую применяются следующие категории:

- ROI,” Return on Investment” или возврат инвестиций
- TCO, “Total Cost of Ownership” или совокупная стоимость владения
- PB, “Payback” или окупаемость

Окупаемость инвестиций в информационной безопасности

Стоит учитывать, что концепция расчета ROI относится к любому виду инвестиционной деятельности, включая, также, и информационную безопасность. Для вычисления необходимых затрат на обеспечение информационной безопасности, нужно определить: во-первых, как влияет низкий уровень информационной безопасности на бюджет организации и, во-вторых, как выбрать самый выгодный способ его повышения.

В области информационной безопасности расчет окупаемости (ROSI) может дать конкретные ответы на важнейшие вопросы экономики:

- Достаточно ли средств тратит организация на обеспечение информационной безопасности?
- Какое влияние окажет низкий уровень безопасности на финансы и производительность организации?
- В какой момент целесообразно приостановить инвестиционную деятельность?
- Достаточно ли полезен внедряемый продукт (набор организационно-технических средств безопасности)?

Основная формула расчёт ROSI выглядит следующим образом:

$$\text{ROSI} = \frac{\text{Материальный ущерб} - \text{Стоимость решения}}{\text{Стоимость решения}} * 100 \qquad (2)$$

При расчете ROSI используется подход, аналогичный расчету окупаемости инвестиций в области страхования, то есть, ситуацией возникновения риска считается ситуация, аналогичная наступлению страхового случая. В свою очередь, к «страховым случаям» может относиться любой инцидент информационной безопасности– несанкционированный доступ и изменение информации, утечка информации, взлом, компрометация, заражение системы и так далее.

Необходимо анализировать факторы, выступающие источниками эффективности ROSI:

- снижение рисков в рамках модели угроз
- рост эффективности процессов обеспечения информационной безопасности (выбор политики, администрирование).

Для того, чтобы упростить процесс расчёта ROSI, профессионалы в области информационной безопасности разделили процесс управления решениями безопасности на 3 категории:

НАЗВАНИЕ КАТЕГОРИИ	ПРИЕМУЩЕСТВА ДЛЯ КЛИЕНТОВ
Эффективность безопасности	Снижение цен на внедрение и использование различных инструментов информационной безопасности в пределах одной организации или сети
Снижение рисков	Защита человеческих ресурсов, снижение рисков информационной безопасности, обеспечение непрерывности бизнеса, улучшение репутации организации.
Эффективность бизнеса	Инвестиции клиентов на улучшение системы информационной безопасности помогают улучшить процесс производства самого бизнеса, снизить затраты и увеличить доход.

Таблица 1. Уровни безопасности в процессе управления

Источник: https://www.sans.org/reading-room/whitepapers/modeling/modeling-security-investments-monte-carlo-simulations-35457

Планирование и анализ жизненного цикла процессов информационной безопасности, являются неотъемлемой частью расчёта ROSI. Понимание жизненного цикла может увеличить производительность организации и улучшить применяемые в ней меры информационной безопасности. Жизненный цикл описывает хронологическую последовательность восьми событий, свойственных фактически любой среде безопасности, начиная с определения целей и заканчивая подробным анализом. Каждая стадия представляет собой часть механизма по постепенному улучшению системы информационной безопасности бизнеса. На различных этапах жизненного цикла профессионалы в области безопасности могут ответить на жизненно важные вопросы безопасности и гарантированно улучшить защиту организации.

Рисунок 2. Жизненный цикл системы безопасности

Источник: https://www.sans.org/reading-room/whitepapers/modeling/modeling-security-investments-monte-carlo-simulations-35457

Заключение

В настоящее время расчёты окупаемости инвестиций в области информационной безопасности затруднены “лавинообразным” ростом угроз, причём, как в количественном, так и в качественном отношении. Поэтому сам процесс инвестиционной деятельности должен соответствовать современным стандартам безопасности (семейство ISO/IEC 27000, семейство ISO 9000, ISO/IEC 24762:2008, NIST и др.), базироваться на известных и доступных данных, описывающих статистику угроз и уязвимостей. Расчёт ROSI включает в себя процесс моделирования, требующий больших объёмов разнообразной информации. Эта информация должна характеризовать различные стороны не только деятельности самой организации, но и системы информационной безопасности. Кроме того, необходимо внедрять системы самообучения по управлению рисками и формированию ROSI.

Литература

1. *Астахов А. "Как управлять рисками информационной безопасности?" CISA, 2006,* http://iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/kak-upravlyat-riskami-informacionnoi-bezopasnosti
2. *Аугрьянов И. "Таксономия рисков", 11 октября, 2015* http://www.securitylab.ru/blog/personal/aguryanov/152951.php
3. *Harkins M. "Managing Risk and Information Security", 2013 by Apress Media, LLC, ISBN 978-1-4302-5114-9 (eBook)*
4. *Плетнев П., Белов В. "Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса", УДК 004.056 июнь 2012*
5. *Астахов А. «Искусство управления информационными рисками», http://xn----7sbab7afcqes2bn.xn--p1ai/content/kolichestvennoe-opredelenie-velichiny-riska*
6. *Lyon D., "Modeling Security Investments With Monte Carlo Simulations", September 16, 2014,* https://www.sans.org/reading-room/whitepapers/modeling/modeling-security-investments-monte-carlo-simulations-35457
7. *Magnusson C., MoIvidsson J. and Zetterqvist S., "Value creation and Return On Security Investments (ROSI)", 2007, in IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, eds. Venter, H., Eloff, M., Labuschagne, L., Eloff, J.. von Solms, R.. (Boston: Springer), pp. 25–35.*
8. *Introduction to Return on Security Investment, Helping CERTs assessing the cost of (lack of) security; European Network and Information Security Agency (ENISA) 2012*
9. *"Как считать ROI для средств защиты информации?" http://habrahabr.ru/company/securitycode/blog/136172/*