Оценка возврата инвестиций в информационную безопасность

написано Александр Астахов | 11 июня, 2023

Основной целью обработки риска является выбор наиболее эффективных мер, обеспечивающих сокращение среднегодовых потерь организации от инцидентов информационной безопасности при максимальном возврате инвестиций. Величина возврата инвестиций представляет собой разницу между полученной выгодой и вложенными средствами. В качестве полученной выгоды выступает оценочное значение сокращаемых среднегодовых потерь, а в качестве вложенных средств – денежные средства, прямо или косвенно затраченные на механизмы безопасности и обеспечивающие такое сокращение потерь.

[Возврат инвестиций]= [Уменьшение среднегодовых потерь] – [Стоимость защитных мер].

Максимизация возврата инвестиций – основная экономическая задача информационной безопасности. Бюджет на безопасность всегда ограничен, поэтому стоит задача выбора наиболее эффективных контрмер, т.е. таких контрмер, которые дают наибольший возврат инвестиций при наименьших вложениях.

Для определения того, насколько эффективно защитные меры сокращают потери, используется *коэффициент возврата инвестиций (ROI)*, который определяется как отношение величины возврата инвестиций к стоимости реализации контрмер, которая включает в себя расходы на их планирование, проектирование, внедрение, эксплуатацию, мониторинг и совершенствование.

[Коэффициент возврата инвестиций (ROI)]= ([Уменьшение

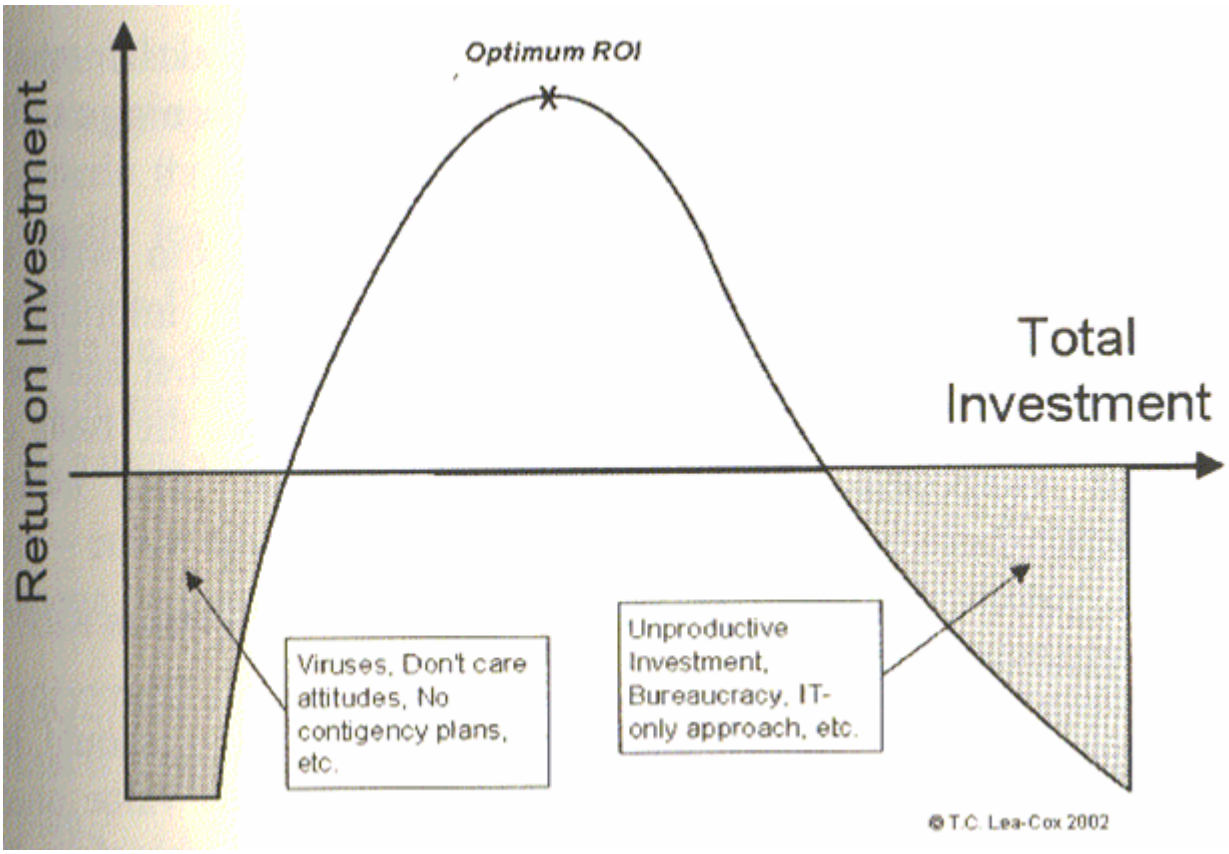
среднегодовых потерь] – [Стоимость защитных мер]) / [Стоимость защитных мер].

_____

ROI показывает, во сколько раз величина возврата инвестиций превышает расходы на безопасность.

График изменения ROI в зависимости от объема инвестиций в информационную безопасность показан на рисунке.

Мы видим, что сначала ROI находится в отрицательной области (области недофинансирования). При увеличении вложений в безопасность, начиная с определенного уровня инвестиций ROI выходит в положительную область (область оптимального финансирования) и постепенно достигает своего максимального значения, а затем начинает уменьшаться и опять входит в отрицательную область (область избыточного финансирования).



Отрицательный возврат инвестиций (ROI < 0) означает, что организация тратит на безопасность больше, чем получает от этого выгод. В этом случае безопасность является затратной

статьей для организации, а предпринимаемые защитные меры обходятся дороже приобретаемых выгод либо только ослабляют реальную защиту и приводят к возрастанию рисков.

На схеме закрашены проблемные области с отрицательным возвратом инвестиций: область недофинансирования и область избыточного финансирования. В первом случае деньги на безопасность выделяются в недостаточном объеме по остаточному принципу. Предпринимаемые фрагментарные меры не дают желаемого эффекта. Для этого случая характерны проблемы с вирусами, отсутствие планов непрерывности бизнеса и легкомысленное отношение персонала к вопросам безопасности.

Во втором случае осуществляется избыточное финансирование безопасности, но большая часть средств расходуется впустую. Для этого случая характерно процветание бюрократии, избыточная формализация, приобретение дорогостоящего оборудования и/или программного обеспечения без принятия необходимых организационных мер.

При выборе способов обработки рисков для каждого рассматриваемого механизма безопасности (способа обработки риска) производится оценка ROI. При этом надо учитывать, что многие механизмы безопасности взаимосвязаны и в отрыве от остальных не дают требуемого эффекта, т.е. не обеспечивают желаемого возврата инвестиций. Так, политики безопасности или технические средства защиты не работают без соответствующего обучения и контрольных процедур. Поэтому при оценке ROI чаще всего рассматривается сразу группа взаимосвязанных механизмов безопасности, которые поддерживают и дополняют друг друга, обеспечивая максимальный эффект.

Поясним концепцию использования ROI для оценки эффективности контрмер на примере системы антивирусной защиты. Для этого оценим затраты на внедрение и эксплуатацию системы антивирусной защиты для организации, в офисе которой имеется 1000 рабочих мест. Эти затраты складываются из следующих составляющих:

- первоначальной стоимости лицензий на антивирусное ПО (единоразовый платеж – 100 тыс. долл.);
- стоимости подписки на обновление антивирусных баз (ежегодный платеж, начиная со второго года, – 30 тыс. долл.);
- стоимости серверного оборудования (единоразовый платеж – 10 тыс. долл.);
- стоимости трудозатрат технических специалистов на внедрение и администрирования системы (~50 человекодней в год – 10 тыс. долл. и еще 10 тыс. долл. – в первый год на внедрение);
- стоимости обучения и повышения осведомленности пользователей и администраторов антивирусной защиты (разработка антивирусной политики и инструкций, проведение обучающих семинаров для пользователей и администраторов обойдется ~ 10 тыс. долл. единоразово и 4 тыс. долл. – в последующие годы).

Таким образом, *средняя ежегодная стоимость эксплуатации системы антивирусной защиты* корпоративной сети на 1000 рабочих мест на пятилетнем периоде составляет 100000 + 30000 × 4 + 10000 + 10000 × 4 + 10000 + 4000 × 4) / 5 = 59200 ~ 60 тыс. долл.

В случае если корпоративная сеть организации подключена к Интернет, построена на платформе Windows, содержит конфиденциальную информацию, утечка которой может нанести значительный ущерб репутации и прочим интересам организации, а также реализует информационные сервисы, критичные с точки зрения доступности, тогда оценочный среднегодовой ущерб может быть очень значительным, вплоть до того, что организации вообще не сможет нормально работать, со всеми вытекающими отсюда последствиями. Среднегодовой ущерб (ALE) в этом случае вполне может исчисляться миллионами долларов.

Предположим, что по результатам оценки рисков мы получили ALE ~ 1 млн. долл. В этом случае ежегодный возврат инвестиций в

систему антивирусной защиты составит:

Δ ALE = 1000000 – 60000 = 940000 долл.

Коэффициент возврата инвестиций для системы антивирусной защиты будет равен:

ROI = 940000 / 60000 ~ 15,7.

Конечно, наша оценка возврата инвестиций (ALE) может принципиально различаться в зависимости от следующих факторов:

- оценки возможного ущерба для организации в случае антивирусных инцидентов, определяемой ценностью ее информационных активов;
- наличия механизмов безопасности, оказывающих влияние на реализацию данной угрозы, например, использования шифрования конфиденциальной информации, наличия системы автоматической установки программных коррекций и т.п.;
- наличия подключения к Интернет и разрешенных сетевых протоколов;
- используемой программной платформы (для UNIX-систем вероятность вирусной угрозы во много раз ниже);
- квалификации пользователей и технического персонала, возможности использования мобильных устройств и носителей и т.п.

Совокупность всех этих факторов может давать совершенно различные значения ROI. Кроме этого, надо учитывать, что наши оценки угроз, уязвимостей и ценности активов являются весьма приблизительными и допускают весьма существенные погрешности. Минимальное и максимальное значения ALE могут различаться в несколько раз (но все же не в десятки раз при условии, что оценку рисков проводят квалифицированные эксперты).

Поэтому значения ROI, не превышающие 10, как правило, являются не самыми лучшими решениями для информационной безопасности (т.к. с учетом возможной погрешности оценки реальный ROI при

этом может оказаться близок к 0). Эффективные механизмы контроля как правило должны иметь более высокий коэффициент возврата инвестиций.