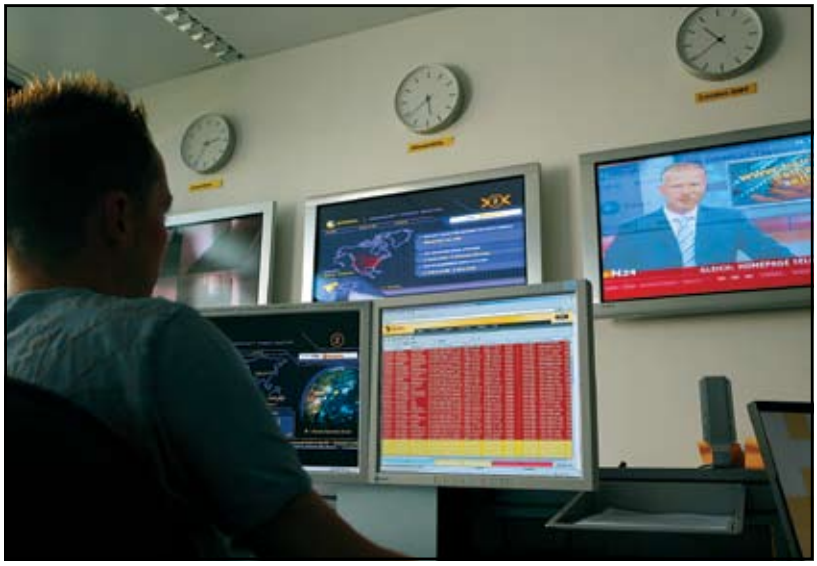
Управление ИТ-рисками: взгляд Symantec



В современных условиях крупным компаниям, имеющим сложно организованную информационную инфраструктуру, практически невозможно обеспечить необходимый уровень информационной безопасности без организации эффективного риск-менеджмента, учитывающего наряду с традиционными бизнес-рисками также и ИТ-риски предприятия. Неправильное отношение к вопросу управления ИТ-рисками может привести к серьезным авариям ИТ-систем и нанести весьма существенный ущерб бизнесу. Корпорация Symantec провела международное исследование об отношении организаций к управлению ИТ-рисками и выпустила итоговый отчет (Symantec IT Risk Management Report Volume II), из которого следует, что уровень осведомленности организаций о важности управления ИТ-рисками повышается и что руководители ИТ-подразделений стали придерживаться более взвешенного подхода в данном вопросе, учитывающего риски готовности, безопасности, производительности и соблюдения нормативных требований. Вместе с тем, этот отчет, составленный на основе анализа более 400 углубленных систематических опросов ИТ-профессионалов во всем мире, показал, что 53 % всех ИТ-инцидентов связаны со случаями утечки данных и вызваны проблемами технологического характера, напрямую вытекающими из уязвимостей информационной системы предприятия.

В этой связи исследование Symantec выявляет и анализирует ряд распространенных заблуждений, или мифов, связанных с управлением рисками в сфере информационных технологий:

1. Управление ИТ-рисками сосредоточено только на вопросах ИТ-безопасности.
2. Управление ИТ-рисками представляет собой локальный проект.
3. С ИТ-рисками можно справиться исключительно с помощью технологии.
4. Управление ИТ-рисками является научной дисциплиной.

Миф первый: ИТ-риск – это риск ИТ-безопасности

Несмотря на традиционное восприятие ИТ-рисков, связывающее их главным образом с рисками безопасности, результаты исследования указывают на существование более широкого взгляда в среде ИТ-профессионалов на данную проблему. 78 % опрошенных оценили как "критический" или "серьезный" риск готовности информационных систем – при том, что для рисков безопасности, производительности и соответствия нормативным требованиям эта оценка составила соответственно 70, 68 и 63 %. Тот факт, что разница в оценке рисков по типам составляет всего 15 %, указывает на то, что ИТ-профессионалы склоняются к более взвешенному отношению к ИТ-рискам, в меньшей степени сосредоточенному на проблемах безопасности.

"Вывод отчета Symantec о том, что организации признают важность управления ИТ-рисками не только в сфере безопасности, но и в таких областях, как готовность и производительность ИТ-систем, обнадеживает, – считает старший аналитик Enterprise Strategy Group Джон Олтсик (Jon Oltsik). – Предприятия начинают понимать, что в современном взаимосвязанном мире на деятельность организации и ее результаты могут повлиять неполадки в широком спектре систем".

Выводы отчета подтверждают, что рискам безопасности и соответствия нормативам часто придается большее значение ввиду того, что инциденты данного типа бросаются в глаза и имеют далеко идущие последствия – 63 % респондентов оценили как оказывающие серьезное влияние на их бизнес инциденты, связанные с утечкой данных. Однако и по отношению к рискам готовности наблюдается все более серьезное отношение: как показывает проведенное исследование, руководители отдают себе отчет в том, что даже мелкие проблемы производительности могут распространяться по стоимостной це-

почке и приводить к потерям, измеряемым миллионами долларов. Недавно ученые Дартмутского колледжа и Университета штата Вирджиния установили, что гипотетический отказ системы диспетчерского управления и сбора данных (SCADA) на нефтеперегонном заводе может привести к последствиям, ущерб от которых оценивается в 405 млн долларов, причем поставщик понесет убытки только в 255 млн, тогда как остальные потери лягут на плечи других участников цепочки поставок.

Миф второй: управление ИТ-рисками – это проект

Мнение о том, что управление ИТ-рисками можно осуществлять в рамках единого проекта или даже ряда отдельных мероприятий, проводимых в течение определенного бюджетного периода или года, игнорирует динамическую природу внутреннего и внешнего управления ИТ-рисками. Чтобы идти в ногу с динамично меняющимися условиями, в которых приходится работать современным предприятиям, менеджмент в области ИТ-рисков должен быть организован как непрерывный процесс. Отчет выявил следующие цифры, указывающие на частоту ИТ-инцидентов разного типа:

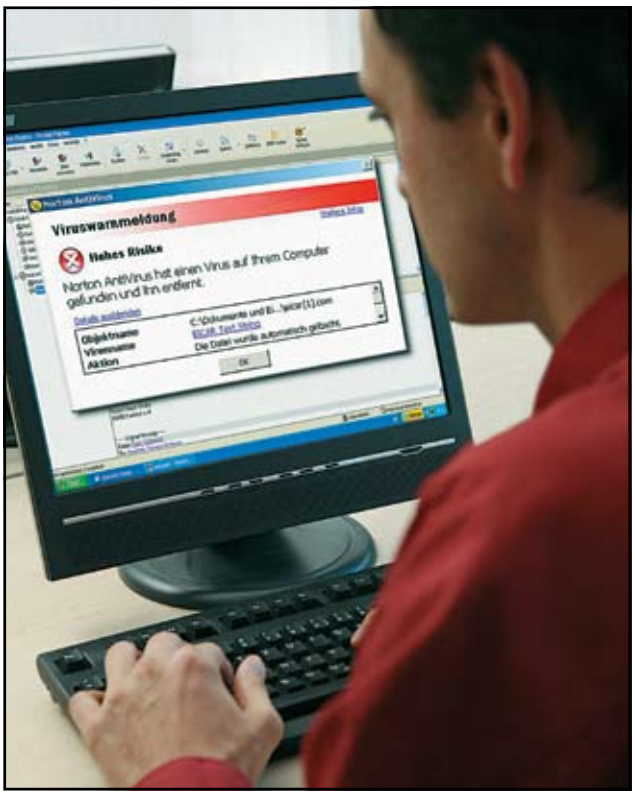
- 69 % респондентов ожидает мелких ИТ-инцидентов раз в месяц;
- 63 % респондентов ожидает серьезных ИТ-инцидентов каждый год;
- 26 % ожидает как минимум раз в год инцидентов, связанных с несоблюдением нормативных требований;
- 25 % ожидает как минимум раз в год инцидентов, связанных с утечкой данных.

Согласно иследованию Symantec, наиболее эффективные организации придерживаются систематического подхода. При этом многие из них не уделяют должного внимания таким фундаментальным мерам по управлению рисками, как классификация ресурсов и управление ими: всего 40 % участников исследования оценили свою эффективность по этому показателю в 75 % или выше. Так, только 34 % участников убеждены, что они располагают актуальным реестром своих беспроводных и мобильных устройств, без которого в современном деловом мире не обойтись.

Миф третий: ИТ-риски можно уменьшить при помощи одной лишь технологии

Хотя технологии играют важную роль в предотвращении ИТ-рисков, эффективность программы управления ИТ-рисками определяют также люди и процессы, обслуживаемые этой технологией. В соответствии с отчетом, 53 % ИТ-инцидентов вызваны проблемами, связанными с технологическими процессами. Обеспокоенность вызывает также снижение рейтинга некоторых факторов по сравнению с предыдущим, прошлогодним, отчетом (Symantec IT Risk Management Report Volume I). Например, с 50 % до 43 % снизилось число респондентов, оценивающих эффективность своих программ обучения и информирования на 75 % и выше.

Данные последнего отчета демонстрируют очень незначительный прогресс в отношении оценки фактора классификации ресурсов по потребности в защите от ИТ-рисков. Между тем, пренебрежение этим фактором, предполагающее одинаковое отношение ко всем ресурсам, вследствие чего одни системы, процессы и объекты будут излишне защищены от ИТ-рисков, а другие недостаточно защищены, ведет к экономической и производственной неэффективности.



В отчете подчеркивается, что число участников, считающих "эффективной более чем на 75 %" разработку безопасных приложений, увеличилось на 10 %. Отчет указывает также на повышение рейтинга фактора дисциплины управления ИТ-проблемами.

Миф четвертый: управление рисками – научная дисциплина

Исследование Symantec приближает руководителей к пониманию того факта, что управление ИТ-рисками не является областью научной деятельности, а представляет собой развивающуюся бизнес-дисциплину, которая опирается на практический опыт, накопленный отдельными людьми и организациями в процессе развития деловой и технологической среды, и которая, помимо анализа и контроля операционных рисков, рисков качества и рисков производственного и ИТ-менеджмента, включает специфические организационные и технологические факторы, уникальные для области ИТ.

Ситуация с ИТ-рисками в различных отраслях

Отчет дает представление о состоянии проблемы управления ИТ-рисками в отдельных отраслях экономики. Так, например, больше всего инцидентов ожидают представители здравоохранения. Учитывая сложность и высокоиндивидуальную природу услуг в сфере здравоохранения, а также строжайшие требования по соблюдению нормативов, это вызывает определенную обеспокоенность. Активнее всех средства управления ИТ-рисками внедряют в индустрии связи, за которой близко следует сфера банковских и финансовых услуг, что, по-видимому, вызвано растущим числом нормативных актов и строгостью требований по их соблюдению для перечисленных секторов, а также заботой о защите информации частного характера.

"Второе издание годового отчета об отношении организаций к управлению ИТ-рисками обеспечивает ИТ-профессионалов и руководителей высшего звена беспрецедентным по глубине взглядом на проблему управления ИТ-рисками – от понимания того, что работает, а что – нет, до практических рекомендаций и действенных советов по эффективной реализации соответствующих программ, – комментирует результаты исследования вице-президент отделения Symantec Information Technology and Services Group Дэвид Томпсон (David Thompson). – Лучшее понимание практики управления ИТ-рисками позволяет организациям с уверенностью брать на себя точно рассчитанные риски и использовать ИТ для достижения конкурентного преимущества".

Основные выводы отчета международного плана

Исследование впервые анализирует обширный материал по Азиатско-Тихоокеанскому региону, что позволило вскрыть более широкие географические различия в управлении IT-рисками. Географический охват исследования включает 16 % респондентов из региона EMEA (Европа, Ближний Восток и Африка), 28 % – из Азиатско-Тихоокеанского региона и 55 % – из Северной Америки.

Вывод 1

Существует заметная разница в оценке степени угрозы для бизнеса различных видов ИТ-рисков между респондентами из Азиатско-Тихоокеанского региона, EMEA и представителями Северной Америки:

- В 2007 году респонденты выше оценили, по сравнению с 2006 годом, ИТ-риск, связанный с управлением цепочкой поставок (в 2007 году 34 % респондентов оценили этот ИТ-риск как высокий или критический против 27 % в 2006 году). Это изменение объясняется увеличением в 2007 году числа организаций из Азиатско-Тихоокеанского региона и производителей промышленных/потребительских товаров, для которых управление цепочкой поставок имеет существенное значение для бизнеса.
- Респонденты из Северной Америки в большей степени, чем их коллеги из Азиатско-Тихоокеанского региона и EMEA, озабочены ИТ-риском, вызываемым требованиями, предъявляемыми к хранению данных

Выводы отчета Symantec применительно к ситуации, характерной в этой области для российских компаний, комментирует **Максим Ничипорович**, руководитель отдела инфраструктурного программного обеспечения компании OCS.

Несмотря на то, что формально Российская Федерация принадлежит к региону EMEA, если бы по России проводилось отдельное исследование, то, как мне представляется, выводы были бы ближе к результатам Азиатско-Тихоокеанского региона. По уровню развития ИТ-рынка мы отстаем от стран Европы и США на три–пять лет, соответственно, можем проанализировать опыт внедрения множества новых продуктов и технологий и выбрать лучшее из того, что появилось на западном рынке за это время. В результате мы имеем более высокий уровень оснащенности и подготовленности российских компаний в техническом отношении к ИТ-рискам. Хотя в плане восприятия комплекса вопросов, связанных с управлением ИТ-рисками, как целостной концепции, отставание все же сохраняется.

Если говорить о российской специфике, то риски, связанные с нарушением интеллектуальной собственности, в России так же велики, как и в Азиатско-Тихоокеанском регионе. Однако в области "тяжелого" инфраструктурного программного обеспечения, которым занимается, в частности, компания OCS, ситуация выглядит лучше, чем с пользовательским софтом. Во-первых, в связи с изменением законодательства в корпоративном секторе идет активный процесс легализации ПО. А во-вторых, тяжелое ПО, как и все прочее в ИТ-индустрии, с течением времени становится все сложнее, и без оперативной и высококвалифицированной технической поддержки сейчас уже, как правило, не обойтись.

Кроме того, нельзя не отметить возрастание, в связи с изменением с 1 января 2008 года порядка налогообложения на передачу прав на результаты интеллектуальной собственности, рисков соответствия нормативным требованиям.

Что касается положения дел по отраслям, то в России наиболее продвинутыми в плане работы с ИТ-рисками также представляются предприятия банковской сферы и индустрии связи. В этих областях ситуация характеризуется наличием достаточных средств и необходимостью работы с очень большими объемами постоянно обновляющихся данных. Так что здесь мы не отклоняемся от общемировых тенденций.

(68, 58 и 49 % соответственно оценили этот ИТ-риск как высокий или критический). По всей видимости, данные цифры отражают существующие между регионами различия в уровне законодательных норм и опыте организаций по их соблюдению.

- Участники опроса из Азиатско-Тихоокеанского региона продемонстрировали более высокую озабоченность по сравнению с их коллегами из региона EMEA и США ИТ-риском, связанным с нарушением интеллектуальной собственности (60, 48 и 43 % соответственно оценили этот ИТ-риск как высокий или критический). Очевидно, что данное расхождение является следствием разницы в опыте национальных культур в сфере соблюдения международных стандартов защиты интеллектуальной собственности.

Вывод 2

Ожидания в отношении вероятности наступления тех или иных ИТ-инцидентов заметно различаются между географическими регионами:

- 44 % респондентов из Азиатско-Тихоокеанского региона полагают, что им никогда не придется столкнуться с обвинениями в нарушении нормативных требований, тогда как в Северной Америке таких компаний всего 29 %, а в EMEA – 35 %. По мнению аналитиков компании Symantec, такое соотношение обусловлено более высоким уровнем требований, предъявляемых к организациям в западных странах по сравнению с появившимися недавно подобными требованиями в странах Азиатско-Тихоокеанского региона.
- 76 % респондентов из региона EMEA и 74 % из Северной Америки ожидают как минимум десять мелких ИТ-инцидентов в год по сравнению всего с 58 % респондентов из Азиатско-Тихоокеанского региона. Более низкий уровень ожиданий незначительных ИТ-инцидентов в странах Азиатско-Тихоокеанского региона отчасти объясняется новизной оборудования и отсутствием сложных унаследованных систем в некоторых странах Азиатско-Тихоокеанского региона, что способствует повышенной стабильности систем.

Вывод 3

В большинстве случаев респонденты из Азиатско-Тихоокеанского региона оценили успехи своих компаний в сфере внедрения средств управления выше, чем их коллеги в западных странах. Такая оценка с определенностью объясняется более высоким процентом респондентов из Азиатско-Тихоокеанского региона, представляющих отрасли с наиболее развитым управлением ИТ-рисками, включая телекоммуникации и банковский/финансовый сектор:

- Респонденты из Азиатско-Тихоокеанского региона сообщили о более успешном по сравнению с их коллегами из Северной Америки и региона EMEA внедрении средств управления ИТ-рисками всех четырех основных групп: стратегическими, рисками поддержки, снабжения и безопасности.
- В отдельных областях управления респонденты из Азиатско-Тихоокеанского региона чувствуют себя значительно увереннее, чем участники опроса из Северной Америки и региона EMEA, а именно: в управлении жизненным циклом данных, управлении уровнем обслуживания, управлении непрерывностью бизнеса, а также в области проектирования, разработки и тестирования приложений на безопасность.

Второй том отчета об отношении организаций к управлению ИТ-рисками доступен на веб-сайте компании Symantec по адресу: www.symantec.com.

По материалам компании Symantec