ИБ — функция или процесс?

Роман Семенов
Начальник отдела консалтинга и аудита ARinteg

В крупных банках, входящих в ТОП-30 (или 50, не суть важно), подразделение ИБ является неотъемлемой частью процесса жизнедеятельности банка.

Инициировать процесс появления в структуре организации подразделения ИБ можно по разным причинам и разными способами, но — рано или поздно — оно появится. И тут как для топ-менеджмента, так и для рядовых сотрудников банка, не понимающих задачи данного направления, начинаются неприятные сюрпризы. Руководству ИБ видится как бездонная бочка, от финансирования которой нет очевидной отдачи, а сотрудникам — как неприятные люди, которые запрещают писать пароли на бумажках и рассматривать котиков в Интернете. Это непонимание создает как для ИБ-подразделений в банках, так и для самой этой информационной безопасности целый ворох проблем, сказывающихся во всем, начиная от сложного процесса согласования и внедрения какого-то «ненужного документа» (например, «Политики информационной безопасности») и заканчивая финансированием по остаточному принципу. Источник этих проблем прежде всего следует искать в главном «безопаснике»: зачастую руководитель ИБ просто не умеет общаться с бизнесом на понятном тому языке. Сложно перевести на язык цифр все те вопросы и обстоятельства, с которыми на регулярной основе сталкивается информационная безопасность. При этом любой руководитель ИБ осознает бизнес-ориентированность своего подразделения в банке.

Банковские службы ИБ обычно строго централизованы: в подразделении сосредоточен практически полный цикл по реализации и контролю политик информационной безопасности. И это правильно… Или нет? Подобный подход повышает риск ошибки руководителя ИБ ввиду его абсолютного приоритета в выстраивании политики ИБ. При таком подходе к процессу обеспечения безопасности что-то приносится в жертву в сложных взаимоотношениях между ИБ и бизнесом: бизнес либо будет вынужден подчиняться политике ИБ, снижая свою продуктивность и доходы, либо бизнес добьется неприятия политики ИБ. При этом в силу того, что ИБ и бизнес изначально говорят на разных языках, дискуссии не получится.

Каков же выход? Инициировать диалог и сократить издержки на финансирование подразделения информационной безопасности вполне реально в случае передачи части функционала ИБ непосредственно в бизнес-подразделения. Аргументированно защитить интересы бизнес-подразделений и выработать действительно общую политику ИБ можно путем создания института security officers, которые являются сотрудниками бизнес-подразделений. Им следует поставить задачу нахождения баланса между вечно конфликтующими ИБ-требованиями и бизнес-целями. Тогда можно будет убить двух зайцев одним выстрелом: ИБ обретет понимание бизнес-целей, а бизнес получит прозрачную картину затрат на информационную безопасность. В приложении к информационной безопасности как к процессу издержки автоматически снизятся, если удастся перевести операционную деятельность ИБ в подразделения-заказчики. Впрочем, вероятность того, что бизнес-подразделениями попрежнему будут игнорироваться риски ИБ, остается. Но эту проблему можно решить использованием некоторых несложных механизмов: внутренним аудитом, привязки бонусов security officers к КПЭ, а также возложить выбор кандидатов на должность ответственного за ИБ в подразделении на руководителя ИБ банка.

Получается, что службу ИБ можно организовать достаточно компактным штатом из нескольких человек, которые будут отвечать за взаимодействие с регуляторами и анализ рисков. Подобного рода службы ИБ могут состоять из двух-трех человек: аналитик, технический эксперт и руководитель, который осуществляет взаимодействие ИБ с руководством и представителями бизнес-подразделений. Весь остальной функционал, привычный для этой ригидной области, вполне может уйти в другие подразделения.

Конечно, можно возразить, что в нашей стране это работать не будет. Но подобного рода механизм существует у мировых лидеров банковского рынка. В России эти лидеры вполне себе присутствуют, и вряд ли их корпоративная политика делает исключение для региональных представительств. Конечно, при инертном подходе к обеспечению безопасности подобный процесс не только трудно реализуем, но и практически недостижим. Сейчас модно говорить, что кризис — подходящее время для оптимизации процессов. У нас так любят внедрять ITIL и семейство ISO 27000, эксплуатировать COBIT и т. д. Так, может быть, следует перенять и этот работающий опыт, не идти в очередной раз особым путем развития? Почему нельзя отказаться от догматов, осознав, что информационная безопасность прежде всего процесс, а не функция? Только из-за понимания, что этот процесс реализуем исключительно в организациях со зрелым менеджментом, где есть понимание вопроса? Наверное, так, ведь у нас очень особый путь развития.