Разведка и контрразведка во враждебных поглощениях

Генеральный директор ООО «Р-Техно»
Директор интернет-проекта «Технологии разведки для бизнеса» - www.it2b.ru
Роман В.Ромачев
roman@romachev.ru

Данная статья доказывает необходимость комплексного подхода к организации системы безопасности предприятии с использованием технологий разведки и контрразведки, которые должны выявить и не допустить потенциальные и реальные угрозы благополучного процветания бизнеса. Статья адресована в большей степени руководителям, top-менеджерам, чья функция принимать управленческие решения на основе аналитически обработанной информации полученной от подразделений службы безопасности.

Безопасность – система

В одном из отчетов о результате работы управления экономической безопасности правительства Москвы, ее руководитель Александр Корсак заявил об участии (в период с лета 2002г. по октябрь 2003г.) в решение более 110 корпоративных конфликтов, связанных в большей степени с попыткой враждебного поглощения[1], и это только на территории Москвы. По данным журнала «Слияние и поглощения» за 2002г. в России произошло 1870 поглощений, из которых более 1400 (76%) были недружественными. Как мы видим, враждебное поглощение это не миф, а реальная угроза для бизнеса.

Такой вид корпоративного конфликта как враждебное поглощение, способен решить ряд ключевых задач для компании агрессора:

- возможность завладеть ценными активами (для Москвы это в первую очередь объекты недвижимости – земля, здания)
- дальнейшая приватизация объекта нападения
- уничтожение конкурента и т.п.

Анализ количества враждебных поглощений, показывает значительный рост их, год от года. Но увы, многие top-менеджеры не до конца понимают механизмов этого процесса, а некоторые об этом и не задумываются, считая враждебное поглощение слишком нереальным для их бизнеса. Однако, некоторые директора уже попали в такую ситуацию, когда придя с утра в офис, заставали в своем кресле абсолютно постороннего человека, предъявляя при этом решение собрания акционеров о назначении его генеральным директором. Еще более распространенный случай, когда у входа в офис, теперь уже бывшего директора не пускают люди в масках. Как же быть? Как не допустить такого поворота событий? Ответ один – необходимо уделять внимание вопросам безопасности. Да, именно безопасности как системе, а не только физической охране объекта путем выставления «шкафоподобных» охранников на входе в офис. Существует и другое распространенное заблуждение – говорить о защите предприятия от враждебного поглощения, как только о юридической безопасности. Только комплексный, системный подход к безопасность предприятия позволит уберечь его. Нельзя выбрасывать из системы такие ее элементы как кадровая безопасность, информационная безопасность, защита коммерческой тайны, разведывательные и контрразведывательные мероприятия. Совет по безопасности предприятия должен проанализировать все возможные угрозы, и выстроить такую систему, которая позволит создать адекватную защиту, еще до появления потенциальной угрозы на горизонте.

Еще в 511 г. до н.э. в своем трактате «Искусство войны» Сунь Цзы сказал: "...умелый боец находит для себя такую позицию, которая делает его поражение невозможным, не упуская при этом момент для поражения противника". Именно для того, чтобы принять «правильную позицию» для обороны, руководство предприятия должно обладать информацией о

[1] Враждебное поглощение (hostile takeover) - попытка овладеть контролем над компанией путем скупки ее акций на рынке (т.е. против воли руководства или ведущих акционеров).

готовящемся нападении, либо информацию косвенного характера свидетельствующую подготовительные действия со стороны агрессора. Здесь на помощь должна прийти разведывательная и контрразведывательная служба предприятия.

Ни одно поглощение не проводится без серьезного изучения жертвы. Во время изучения агрессор буквально «выворачивает все предприятия наизнанку», все для того, чтобы отыскать слабые места, на которые в дальнейшем давить. Задача подразделения безопасности выявить такие действия агрессора как вне, так и внутри компании.

Разведка агрессора

Сбор и анализ информации о цели, позволит компании агрессору разработать стратегический план нападения. Задача плана – быстро и дешево поглотить предприятие. В свою очередь, зная какая информация необходима агрессору, контрразведывательные службы предприятия смогут по возможности максимально защитить эту информации, либо дать агрессору дезинформацию, и тем самым направить его по ложному пути.

И так, агрессора интересуют:

- учредительные документы
- документы, касающиеся приватизации
- сведения из реестра акционеров
- протоколы совета директоров, общих собраний акционеров
- показатели финансово-хозяйственной деятельности
- информация о руководстве компании
- криминальная ситуация вокруг предприятия
- отношения с акционерами
- трудовые договора и соглашения
- взаимоотношения с трудовым коллективом и возможные конфликты

Часть информации можно получить из открытых источников, в том числе из: СМИ, интернет, регистрационных баз данных и т.п. Для получения оставшейся информации нападающей стороне необходимо будет прибегнуть к хитростям и уловкам, которые управление безопасности компании обязано не упустить.

Глухая оборона

Одно из первых действий которое предпримет нападающая сторона, это получение реестра акционеров, именно получив информацию об акционерах предприятия, можно начать захватывать его. Законодательством четко установлены рамки получения информации об акционерах компании, для этого достаточно 1% акций. Но были случаи когда реестр получали за бутылку водки, либо под предлогом организации отдыха для акционеров. Агрессор может воспользоваться юридической неграмотностью персонала компании реестродержателя[2], так на моем личном опыт был случай, когда реестр получал акционер владеющий менее 0,01% акций. В связи с этим при выборе реестродержателя управление безопасности должно обратить внимание на следующие моменты:

- связь реестродержателя с конкурирующими, противоборствующими компаниями;
- связь регистратора с криминальными структурами;
- участие компаний держащих реестры у данного реестродержателя в процессах враждебного поглощения
- участие реестродержателя в судебных делах по факту корпоративного конфликта вызванного оспариванием купли-продажи долей акций.

[2] Реестродержатель либо регистратор – юридическое лицо обладающее правами ведения реестра владельцев ценных бумаг.

Разведывательным подразделениям желательно наладить хорошие контакты с сотрудниками регистратора, для того чтобы те в свою очередь докладывали о попытках получить реестр, о фактах купли-продажи долей. Не мало важно информировать СБ о том, кто пытается это получить! Именно обладая такой информацией можно оперативно спланировать метод защиты, а порой и сделать «ход конем» - перейти в наступление.

В свою очередь подразделение контрразведки тоже не должно дремать, а вести работу с сотрудниками компании. Не редкость, когда агрессор начинает действовать через шантаж, уговаривание простых рабочих компании продать свою долю. Здесь, желательно иметь информаторов, которые рассказывали об обстановке, докладывали о малейших колебаниях, недовольствах в коллективе, о проблемах. Это все необходимо и для поддержания внутренней безопасности, для предотвращения мошенничества, воровства и т.п.

Однако воздействовать на простого сотрудника можно и путем черного PR, например закидываю дезинформацией о скором банкротстве предприятия. Такое мероприятие можно провести как через СМИ, так и «заслав казачка», либо завербовав нелояльного сотрудника компании, который бы пускал на предприятии слухи о скором прекращении его деятельности. Для недопущения подобного, органов безопасности предприятия должны осуществлять:

- постоянный мониторинг СМИ:
    - на факт враждебных поглощений в данной отрасли, в регионе, это позволит спрогнозировать дальнейшую обстановку вокруг предприятия;
    - на факт появления дезинформации о деятельности компании;
    - на факт подозрительных действий конкурентов, которые могли бы привести к потере контроля над предприятием, и т.п.
- тщательная проверка сотрудников при найме на работу (на факт связи с конкурентом, криминалом);
- постоянный мониторинг персонала.

Все вышесказанное необходимо и должно проводиться управлением безопасности и в повседневной жизни, а не только при появлении потенциальной угрозы быть поглощенным.

Не стоит забывать и о создании (совместно с пресс-службой) положительного имиджа предприятии через СМИ, как о очень большом значении предприятия для всей отрасли, региона, страны. Это позволит «поднять шум» при появлении захватчика, и не даст ему оперативно осуществить свои замысел.

Еще одна из важнейших «точек пересечения» это банк. Здесь необходимо действовать также как и с реестродержателем (производить проверку банка на связи с конкурентами, криминалом …), ибо именно в банке концентрируется вся финансовая информация о деятельности компании, и все денежные активы.

Контрагенты

Другой способ поглощения, который также распространены у нас в России, это поглощение через банкротство. Признать предприятие банкротом используя современное законодательство и поддержку судебных органов не так уж и сложно, достаточно организовать через подставное лицо поставку той или иной продукции на пару тысяч долларов, и исчезнуть на несколько месяцев так, чтоб поставщика невозможно было отыскать. Данным методом не побрезговала воспользоваться одна московская компания, поимев тем самым большие торговые площади. Задача подразделения деловой разведки здесь, в составлении достаточно полной бизнес-справки с указанием всех выявленных аффилированных лиц контрагента, и последующая проверка их на факт связи с конкурентами, криминалом.

Провести банкротство, можно также скупив долги предприятия. Задача разведывательного подразделения здесь, такая же, как и раньше – мониторинг открытых источников информации (именно в средствах массовой информации, интернет публикуются объявления о купли - продажи долгов предприятия, например - http://rusdolg.ru), проверка всех поставщиков на связь с конкурентом, криминалом, потенциальным захватчиком.

Фантазии агрессора нет границ, порой приходится аплодировать тому, кто придумал тот или иной способ завладеть чужими активами.

К сожалению, многие руководители понять не могут, что вкладывая в безопасность, они инвестируют в развитие бизнеса!

19.06.2004г.