БРИФИНГ ПАРТНЕРСТВА РИСК-ДОКТОРА

УПРАВЛЕНИЕ РИСКАМИ КИБЕРПРЕСТУПНОСТИ

© Май 2014, Ben Rendle

ben.rendle@rioscaconsulting.co.uk

Киберпреступность - быстрорастущая угроза для мировой экономики. Определение киберпреступности недостаточно хорошо сформулировано, и ее часто путают с кибер-войнами или кибер-терроризмом. Профессионалы в области управления рисками должны хорошо разбираться в киберпреступности и ее влиянии на управление рисками, так как они могут оказать ценную помощь в борьбе с этой серьезной угрозой для бизнеса и общества.

Некоторые специалисты в области рисков считают, что киберпреступность касается только технических сотрудников, и этот вопрос должен решаться в рамках ИТ-отделов. Но киберпреступность представляет значительный риск для всей организации, так как влияет на ее способность к достижению стратегических и оперативных целей. К сожалению, многие предприятия не осознают, что такое киберпреступность, насколько велика ее угроза и степень воздействия, а также как лучше управлять ею.

Перечислим возможные виды негативного влияния киберпреступности на организацию:

- онлайн кражи или мошенничества
- похищение личных данных
- вымогательство
- кража данных клиентов
- кража интеллектуальной собственности
- промышленный шпионаж

Воздействие киберпреступности связано с уровнем интернет-деятельности, осуществляемой организацией, в том числе с масштабом ее присутствия в Интернете, с объемом хранения ценных активов и информации в сети, эффективностью служб онлайн-безопасности и степенью осознания риска в организационной культуре организации.

Для управления рисками киберпреступности мы должны сначала определить уровень нашей деятельности в Интернете и установить, какие активы и показатели могут быть затронуты в связи с этой угрозой. Тогда мы сможем выявить наши риски и управлять ими. Будут полезны следующие действия:

- **Четкое понимание и определение целей организации при деятельности в Интернете.** Распознавание разнообразных и конкретных онлайн-окружений заинтересованных сторон и оценка их склонности к онлайн-риску.
- **Работа как с культурными, так и с техническими факторами.** Такие факторы включают в себя культурные барьеры, трудности в общении и последствия предубеждений в отношении рисков киберпреступности.
- **Признание как внутренних, так и внешних угроз киберпреступности.** Внутренние угрозы могут возникнуть из-за ошибок сотрудников, случайной потери данных или вредоносных утечек конфиденциальной корпоративной информации. Внешние угрозы могут исходить от хакеров, групп давления, конкурентов или даже недружественных иностранных государств, а также вирусов, червей, Троянских коней и т.д.
- **Установление собственности, подотчетности и стимулов для борьбы с рисками киберпреступности.** Все руководящие сотрудники должны нести ответственность за управление рисками киберпреступности в своей зоне ответственности, и нам следует оспорить позицию заинтересованных сторон, считающих, что это «не их проблема».
- **Управление рисками киберпреступности в рамках Системы управления рисками на предприятии.** Риски киберпреступности могут повлиять на организацию в таких областях, как репутация, обеспечение непрерывности бизнеса и вызвать эффект домино для дочерних организаций и поставщиков. Вот почему необходимо согласованно работать с такими рисками в рамках общей стратегии реагирования.
- **Построение глобальной перспективы в отношении последствий рисков киберпреступности.** Многие организации зависят от зарубежных стран в области торговли, экспорта и создания материальных благ, что подвергает их рискам зарубежной киберпреступности, которые также нельзя игнорировать.

Как специалисты в области риска, мы не должны забывать о киберпреступности, так как в наших силах предложить практические и конкретные рекомендации нашим организациям для уменьшения угроз и защиты нашего бизнеса.