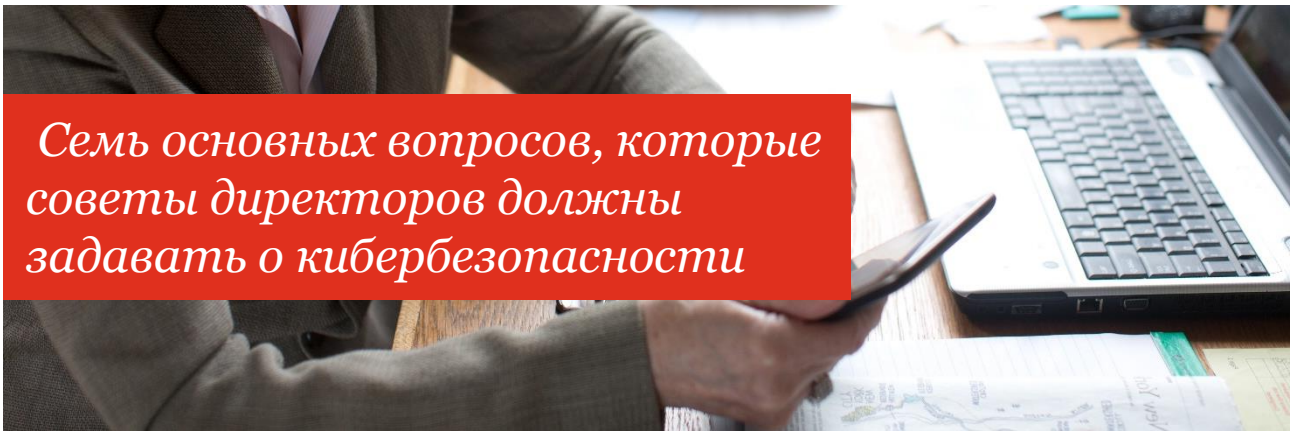
Центр по корпоративному управлению



Семь основных вопросов, которые советы директоров должны задавать о кибербезопасности

В связи с появлением все новых киберугроз советы директоров продолжают искать оптимальные способы контроля киберрисков. Советы директоров понимают потенциальную опасность, которую несут в себе нарушения системы безопасности, однако зачастую им не хватает специальных знаний и информации. Советы директоров не могут знать ответы на все вопросы, связанные с киберрисками, но они должны общаться с руководством и задавать им правильные вопросы, чтобы быть в курсе всех нюансов, связанных с этим сложным и непрерывно изменяющимся риском. Ниже приводятся семь основных вопросов, которые советы директоров должны задавать о кибербезопасности:

1. Знаете ли вы какие ваши информационные активы наиболее подвержены киберрискам?
2. Насколько эффективна наша стратегия кибербезопасности и управлении киберрисками?
3. Как мы защищаем конфиденциальную информацию, которой мы обмениваемся с контрагентами?
4. Есть ли у нас договор киберстрахования?
5. Есть ли у нас правильная стратегия управления данными, направленная на минимизацию рисков?
6. Как оставаться в курсе того, какие угрозы существуют в отрасли и на рынке?
7. Есть ли у нас проверенный план реагирования на киберинциденты?

1. Знаете ли вы какие ваши информационные активы наиболее подвержены киберрискам?

Советы директоров могут всегда быть в курсе того, эффективна ли программа кибербезопасности компании, если в повестку их собраний включены вопросы кибербезопасности и отчеты ИТ-директора (CIO) и директора по информационной безопасности (CISO). Также хорошей практикой являются регулярные встречи руководителя компании с руководителями направлений ИТ и кибербезопасности, на которых рассматривается текущее состояние и обсуждаются ключевые бизнес-инициативы.

Советы директоров также могут рассмотреть возможность проведения встреч с внешними экспертами, чтобы получать дополнительную информацию о последних тенденциях и соответствующих рисках. В ходе таких обсуждений советы директоров должны получать информацию о существующих угрозах, степени защищенности компании от кибератак, а также о соответствующих показателях в сфере безопасности.

Лишь 36 % CISO уверены в том, что руководство компании предоставляет совету директоров адекватную информацию и отчетность о соответствующих показателях в сфере безопасности[1].

[1] *Ежегодный опрос директоров компаний (PwC), 2016 г.*

pwc

2. *Насколько эффективна наша стратегия кибербезопасности и управлении киберрисками?*

Многие компании вкладывают средства в системообразующие механизмы обеспечения безопасности, чтобы повысить эффективность защиты от возникающих угроз. Некоторые компании увеличивают свой бюджет на кибербезопасность, другие реализуют стратегические инициативы по безопасности, такие как услуги по кибербезопасности на платформе облачных технологий или с привлечением третьих сторон, анализ данных для выявления угроз и более продвинутые системы защиты. Советы директоров должны задавать вопросы руководству компании и направления кибербезопасности о наличии комплексной стратегии по обеспечению безопасности данных, об эффективности и синергии этой стратегии с целями развития бизнеса, а также о том, включает ли программа обеспечения безопасности передовые технологии для мониторинга и выявления кибератак или инцидентов и для принятия необходимых ответных мер в случае их возникновения.

3. *Как мы защищаем конфиденциальную информацию, которой мы обмениваемся с контрагентами?*

Привлекаемые компанией сторонние организации и третьи стороны (поставщики, подрядчики, поставщики услуг и другие) могут иметь доступ к конфиденциальной информации компании, что создает потенциальную угрозу кибербезопасности. Советы директоров должны понимать, каким образом компания выбирает, проверяет и контролирует третьи стороны. Также необходимо знать, каким образом эти третьи стороны защищают конфиденциальную информацию компании. Кроме этого, советы директоров должны понимать юридические права компании в отношении третьих сторон, в частности в случае нарушения кибербезопасности.

В качестве источника нарушений безопасности, как и ранее, чаще всего упоминаются сотрудники компаний, при этом показатель инцидентов, связанных с действиями бизнес-партнеров, вырос на 22%[2].

4. *Есть ли у нас договор киберстрахования?*

Частые или серьезные кибератаки заставляют многие компании задуматься о киберстраховании. Это новый, быстро развивающийся вид страхования, поэтому важно, чтобы компании имели четкое представление о программе страхования: какие риски она покрывает и, что более существенно, какие нет.

Советы директоров должны понимать, что входит в их страховой полис (в случае его приобретения) и как меняется рынок киберстрахования, в частности по мере того, как страховщики приобретают опыт в этой сфере.

Ожидается, что объем рынка киберстрахования увеличится втрое и достигнет 7,5 млрд долларов США в 2020 году (в 2015 году он составлял 2,5 млрд долларов США)[3].

---

[2] *Глобальное исследование тенденций информационной безопасности (PwC), 2016 г.*

[3] *Там же.*

[4] *Страхование в 2020 году и в будущем: преимущества обеспечения устойчивости к кибератакам (PwC), 2016 г.*

5. *Есть ли у нас правильная стратегия управления данными, направленная на минимизацию рисков?*

Сегодня компании в рамках своей операционной деятельности создают и обрабатывают большие объемы данных и информации. Накопление и хранение такой информация сопряжено с рисками. Компаниям необходимо иметь эффективные регламенты, процедуры и средства контроля для управления информацией и данными, чтобы предотвращать нежелательное развитие ситуации и нарушение безопасности. Советам директоров следует обсуждать с руководством компании и информационной безопасности эффективность стратегии управления данными компании и необходимость ее обновления, чтобы повысить эффективность и пользу от хранения и обработки «больших данных» и минимизировать риски нарушения

Лишь в 51 % организаций ведется строгий учет данных[4].

6. *Как оставаться в курсе того, какие угрозы существуют в отрасли и на рынке?*

Информационный обмен – один из способов узнать больше о том, как другие компании обеспечивают кибербезопасность и с какими угрозами сталкиваются. Сегодня некоторые компании укрепляют деловое сотрудничество с другими участниками рынка и устанавливают регулярный обмен информацией о новых киберугрозах, способах защиты и реагирования на них, а также осуществляют глубокую аналитику и корреляцию данных для выявления сложных схем кибератак и их предотвращения.

Важно, чтобы советы директоров спрашивали свои компании, что они делают для того, чтобы укрепить устойчивость к кибератакам и повысить кибербезопасность, используя опыт других участников рынка.

7. *Есть ли у нас проверенный план реагирования на киберинциденты?*

Нарушение кибербезопасности может нанести серьезный урон репутации и финансовому положению компании. Советы директоров должны обсуждать с руководством компании план реагирования на киберинциденты, какие меры по обеспечению кибербезопасности он включает, как руководство тестирует план, а также возможности его совершенствования.

Лишь 29 % директоров утверждают, что они уверены в том, что их компания провела надлежащее тестирование плана реагирования на киберинциденты[5].

Кибербезопасность должна оставаться в центре внимания советов директоров компаний. Совету директоров следует активно обсуждать с руководством компании, что они сделали для защиты информационных активов своей организации в условиях постоянно усложняющейся цифровой среды.

Узнайте больше об актуальных вопросах и тенденциях в области корпоративного управления на сайте: www.pwc.com/governanceinsightscenter.com

[5] *Ежегодный опрос директоров компаний (PwC), 2016 г.*

Контакты

Тим Клау

Партнер, руководитель отдела
анализа и контроля рисков

+ 7 (495) 223-51-21
tim.clough@ru.pwc.com

Роман Чаплыгин

Директор, отдел анализа и
контроля рисков

+7 (495) 967-6056
roman.chaplygin@ru.pwc.com