Опыт управления ИБ
в условиях двойного кризиса в игорном бизнесе (экономического и отраслевого)

Алексей Чумаков

Эксперт по технологиям управления
в 2007-2009 – CIO в Storm International

alex@chumakov.ru

CSO Summit 2010

Storm International

- **Storm International** -- в 2007-2009 ведущий оператор верхнего сегмента игорного бизнеса в России
  - Казино **Шангри-Ла**, **Джаз-Таун**, **Нью-Йорк** и другие
  - Сеть **Супер-Слотс**
  - Более 5000 сотрудников, средний возраст менее 25 лет
  - 15 лет на рынке
  - Собственные программно-аппаратные информационные системы и развитые средства ИБ
  - Ключевая компетенция –- «атмосферное» клубное казино
- **Информационные системы** – идейно похожи на банковские
  - Система управления казино
  - Система управления сетью игровых автоматов
  - Система управления персоналом
  - Системы управления средствами безопасности
- **Подразделение ИТ** – около 100 человек, в том числе
  - Центр разработки программного обеспечения
  - Центр управления эксплуатацией
  - Проектный офис
- Автор – специалист по управлению, был приглашен в Шторм для целевой программы в роли CIO с 2007 по октябрь 2009 г.

Кризис отрасли

- **2006 – закон 244-ФЗ об игорном бизнесе**
  - Укрупнение операторов и реорганизация с 2007 г
  - Ликвидация ряда залов
  - Ликвидация всех действующих заведений 30 июня 2009 г.
- **→ Отраслевой шок**
  - «Потеря профессионального будущего» **около 500 тыс. чел.**
  - Отток ключевого персонала, снижение лояльности
  - Сокращение долгосрочного финансирования
  - Противоречивые ожидания (отмены закона, провокаций, …)
- Влияние на ИТ и ИБ:
  - Последствия экстренной централизации ИС
  - Смена приоритетов ИБ и направлений угроз
  - Фактор времени (долгосрочные программы не актуальны)
  - Технические средства есть, но теряют эффективность
- Дополнительно:
  - интернет и мобильная связь все больше открывают компанию со стороны сотрудников
  - + затем – мировой финансовый кризис

И на практике

- Нужно защищаться от инсайдеров
- Требуется сохранить существующие меры противодействия старым угрозам
- Резко изменилась инфраструктура, нарушена ее целостность
- Спроектировать и внедрить новую инфраструктуру «по уму» нецелесообразно (срок жизни, бюджет)

Отказались от подходов:

- *Традиционный аудит ИБ и последующее плановое выполнение рекомендаций*
- *Упор на вложения в технические средства (где гарантии?)*
- *Передача проблемы аутсорсерам (фактор времени, спекуляции и натяжки поставщиков)*

Потребовался эффективный подход для таких условий:

- *Времени мало («одна попытка»)*
- *Финансирования мало*
- *Текучка ключевых сотрудников*
- *Стратегия компании изменчива*
- *«Пугалки» несущественными угрозами мешают реальной ИБ*

Выбранный подход

- **Упрощение** (загрубление) картины мира в ИБ
  (меньше вариантов = меньше стоимость, меньше срок)
  - Цена риска
  - Категоризация объектов защиты и доступа
  - Категоризация субъектов защиты
  - Виды угроз
  - Меры противодействия
- Подтверждение догадок о потребностях в ИБ **реально полученным финансированием**
  («где не получен бюджет – риск признаем несущественным и не тратим время)
- Упор на **человеческий фактор**
  (противостоять невозможно – используем и опираемся)

Почему?

- В конечном счете, информационная безопасность --
  защита «хороших парней» (их интересов)
  от злоупотребления через информацию «плохими парнями»

- Защищаем всегда **людей**, а не **информацию как самоцель**
- Защищаем всегда **от людей**, как источник угроз (изучая и влияя на их мотивацию)
- Защищаем не «вообще», а **в рамках платежеспособного спроса**

Упрощенная картина мира на практике

- План информационной безопасности **на одной странице:**

- Категоризация данных – не более 5 строк, например:
  - Сильно защищаемые (…)
  - Служебные
  - Прочие
- Категоризация субъектов защиты – не более 5 строк
  - VIP
  - Потенциальные источники утечки (ИТ, ИБ, операторы…)
  - Клиенты …
- Доступ субъекта к данным – **да / нет**
- Цена риска утечки/утраты/злоупотребления – **катастрофический** или **игнорируется** (да/нет!)

- Меры противодействия – 5 вариантов
  - **Затруднить** (вывести в отдельную зону безопасности; ограничить доступ; подписать NDA; и т.п.)
  - **Наблюдать** (журналирование доступа и изменений)
  - **Отвлечь** (использовать данные или действия как ложные цели)
  - **Поддержать** (обеспечить положительную мотивацию субъектов)
  - **Доверять** (отключить не входящие в план средства защиты)

Реализация – точки приложения

- **Затруднить:**
  - Обеспечение **внешнего периметра** всего информационного поля
  - Изоляция в «островки» географических / административных подразделений
  - Сужение каналов связи, переход на терминальный доступ
  - Устранение способов «массовой выгрузки» (блокирование отчетов в приложениях, блокирование USB и т.п.)
- **Наблюдать**
  - Журналирование доступа к данным и изменений инфраструктуры
  - Изучение «пиковой нагрузки»
  - Технические средства прослеживаемости личной ответственности (трекер)
- **Отвлечь**
  - сохранить малоценные данные с их системой защиты
  - проводить аудит, расследования, пилотные проекты и т .п.
- **Поддержать**
  - Это – главное! См. следующий слайд
- **Доверять**
  - Убрать «тонкое разграничение доступа» между «соседними столами»

Поддержать!
(или опора на человеческий фактор)

- **Большинство угроз ИБ «замыкаются» на сотрудниках:**
  - меры противодействия внешним угрозам внедряют сотрудники
  - «тащат, что плохо лежит» сотрудники
  - разглашают по незнанию сотрудники
  - защищают – тоже сотрудники
- **При этом:**
  - Личные цели – у человека на первом месте
  - Работа = средство для реализации личных целей
  - **Человек стремится к признанию и самоуважению**
  - **Защищает свою территорию и близких**
  - **Не может быть нейтральным (поддерживает или мешает)**
- **Приверженный сотрудник:**
  - Сам приложит усилия для выявления и устранения угрозы
  - Обнаружит, осудит или воспрепятствует злоумышленнику
- Испуганный или «брошенный» сотрудник
  - Сломает или обойдет любой комплекс мер информационной безопасности, умышленно или просто опустив руки

Поведенческие особенности при кризисе

Два вида мотивации –

- **выгода** (рациональна, управляется рутинно для ИБ)
- **отчаяние** (эмоции, характерны для кризиса и наиболее опасны)

Сотрудник -

- Боится за свой достаток и будущее
- Если компания не заботится о сотруднике, он заботится о себе сам (и неизвестно, с какими последствиями)
- Сотрудник подвержен панике
- Сотрудник может «внутренне расстаться с компанией»
- Сотрудники выбирают стратегию («присоединиться к сильному», «выжить слабого», «сбежать»)

Без специальных мер ситуация подобна эффекту лавины.

Если не заручиться поддержкой сотрудников в кризисе, они, следуя своим страхам, используют компанию как средство для выживания, которым можно пожертвовать.

И тогда никакие технические меры ИБ не помогут!

В сфере ИБ потенциально наиболее опасные сотрудники – это сотрудники ИТ и ИБ (максимальный доступ, отсутствие прямой личной ответственности за угрозы бизнесу)

Как заручиться поддержкой сотрудников?

Потребовалось заручиться поддержкой *разделяющих цели* и предотвратить вред *не разделяющих цели*. (и отличить одних от других)

- **Объявление намерения, целей и ценностей** (собрания, программа действий, образцы для подражания) –
- **Личная ответственность и публичная оценка каждого сотрудника** (матрица; трекер для регистрации всех задач с единым критерием оценки для всех)
- **Изменение системы вознаграждения** (равная зарплата для равных должностей; уровень оплаты зависит от уровня ответственности / возможного ущерба)
- **Гарантия корректного сокращения** при необходимости
- **Вовлечение сотрудников в целесообразность** («выживая, мы имеем право голоса, как именно»)

- **«Не умеешь – научим, не можешь – поможем, не хочешь – уходи»: все не разделяющие цели и ценности – могут уйти по сокращению, но в ограниченный срок** (поддержка HR и бюджет на выходные пособия, премии и обучение;
после срока – выдавливание за несоответствие утвержденным требованиям и премирование за эффективность)

Результат

- **Обеспечена информационная безопасность в 2007-2009 г**
  - 24/7 доступность и целостность
  - 0 реализованных приоритетных рисков
  - Единицы инцидентов, предотвращены и обнаружены сотрудниками
  - 2 каскадных сбоя (без нарушения работы бизнеса)
  - 1 утечка (уже после успешного завершения программы)
  - Ряд «показательных проникновений» с целью продать услуги в области информационной безопасности (второстепенные риски)
  - Ряд «ложных тревог»
- **Сотрудники ИТ и ИБ, оставшиеся к концу 2007 г., были на 2/3 сокращены в 2009 г, и, зная о предстоящем сокращении, на 100% выкладывались**
- **Бюджет на ИБ ограничился**
  - компенсационными выплатами
  - премиальными выплатами
  - бюджетом на обучение
  - необременительными традиционными затратами на ИБ
  - загрузкой имеющихся сотрудников

Резюме

Программа, которая сработала:

- **«Упрощение картины мира»** в ИБ (отказ от всего сложного и частного)
- Технические меры – **играют вспомогательную роль** («дверные замки и ограда»)
- Верим в значимость заявленных потребностей в ИБ **только после подписания бюджета**

И главное:

- **Заручиться реальной поддержкой персонала – значит, сэкономить средства и не дать человеческим страхам разрушить ситуацию**

Без этого прочие меры бессмысленны.

Вопросы?

Обеспечение ИБ выполнялось как часть проектной программы реорганизации и перепрофилирования ИТ, для которой автор был приглашен в Шторм в роли руководителя ИТ.

Использовались технологии позитивного управления, практикуемые и внедряемых автором в роли топ-менеджера или наставника в различных организациях.

Алексей Чумаков

Эксперт по технологиям позитивного управления
в 2007-2009 – CIO в Storm International

Звоните, пишите!

alex@chumakov.ru

+7 903 200 11 80