

# PCI DSS в Украине

## К чему готовиться?

**Александр Смычников**

Консультант департамента ИТ консалтинга  
ООО «БМС Консалтинг»



[Alexander\\_Smychnikov@BMS-Consulting.com](mailto:Alexander_Smychnikov@BMS-Consulting.com)

- PCI DSS увядает?
- Динамика стандарта
- Новые вопросы и мифы
- Наши прогнозы



## PCI DSS увядает?

Динамика стандарта

Новые вопросы и мифы

Наши прогнозы



# Повод задуматься?



БМС консалтинг



# Heartland

PAYMENT SYSTEMS™

The Highest Standards | The Most Trusted Transactions

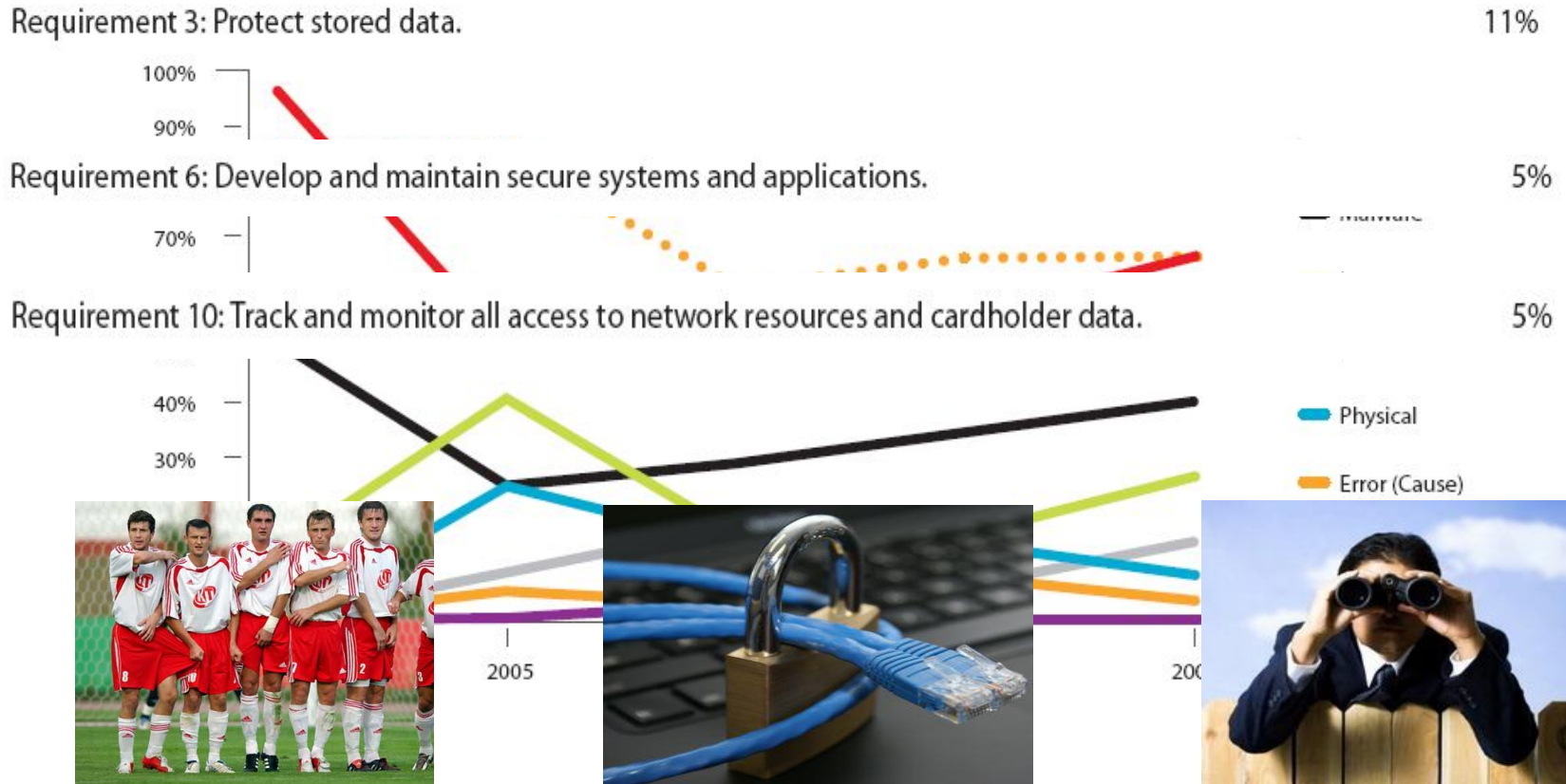
**Вопрос: Что дает соответствие PCI DSS?**

\*



# Голые факты

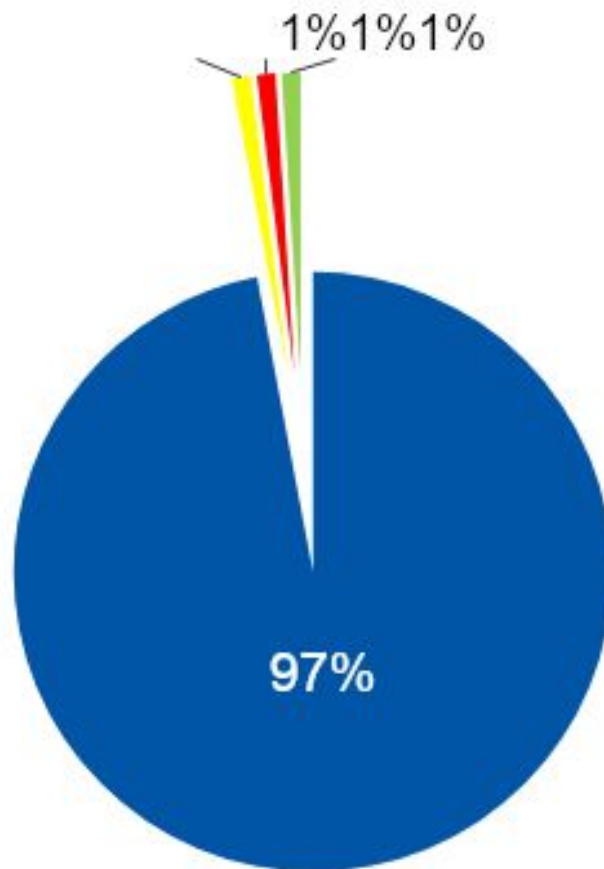
Figure 14. Threat categories over time by percent of breaches



2009 Data Breach Investigations Report, Verizon Business RISK team

\*

# Голые факты - 2



- 1 Персональные данные
- 2 Государственная тайна
- 3 Ком. тайна, Ноу-хау
- 4 Не установлено

2009 Глобальное исследование утечек информации за 2008 год, InfoWatch

\*

# В чем ошибка?

## Ошибки пользователей

- Антивирус и обновления
- Запуск непроверенного ПО
- Установка обновлений безопасности системного и прикладного ПО
- Отказ от резервных копий и их тестирования
- Нарушения регламента использования сети

## Ошибки безопасности

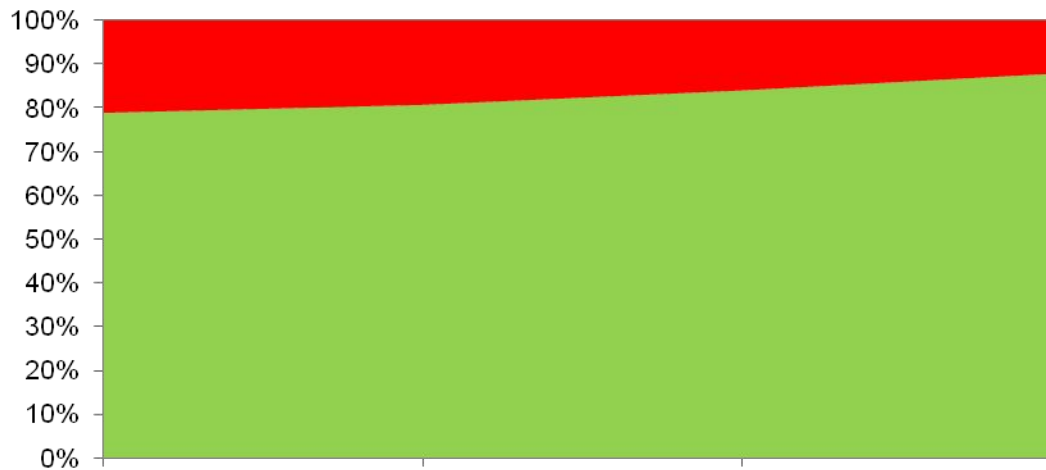
- Безопасность работы в Интернет
- Использование систем после обнаружения уязвимости
- Использование протоколов не поддерживающих шифрование
- Разглашение пароля пользователей по телефону без авторизации
- Запуск небезопасных сервисов, которые не требуются в работе
- Некорректная настройка межсетевых экранов
- Обновления антивирусного ПО
- Отсутствие обучения пользователей в сфере ИБ
- Допуск неквалифицированного персонала к обеспечению ИБ



# PCI DSS учитывает это!



БМС консалтинг



- Угроза не учитывается
- Угроза учитывается

\*



PCI DSS увядает?

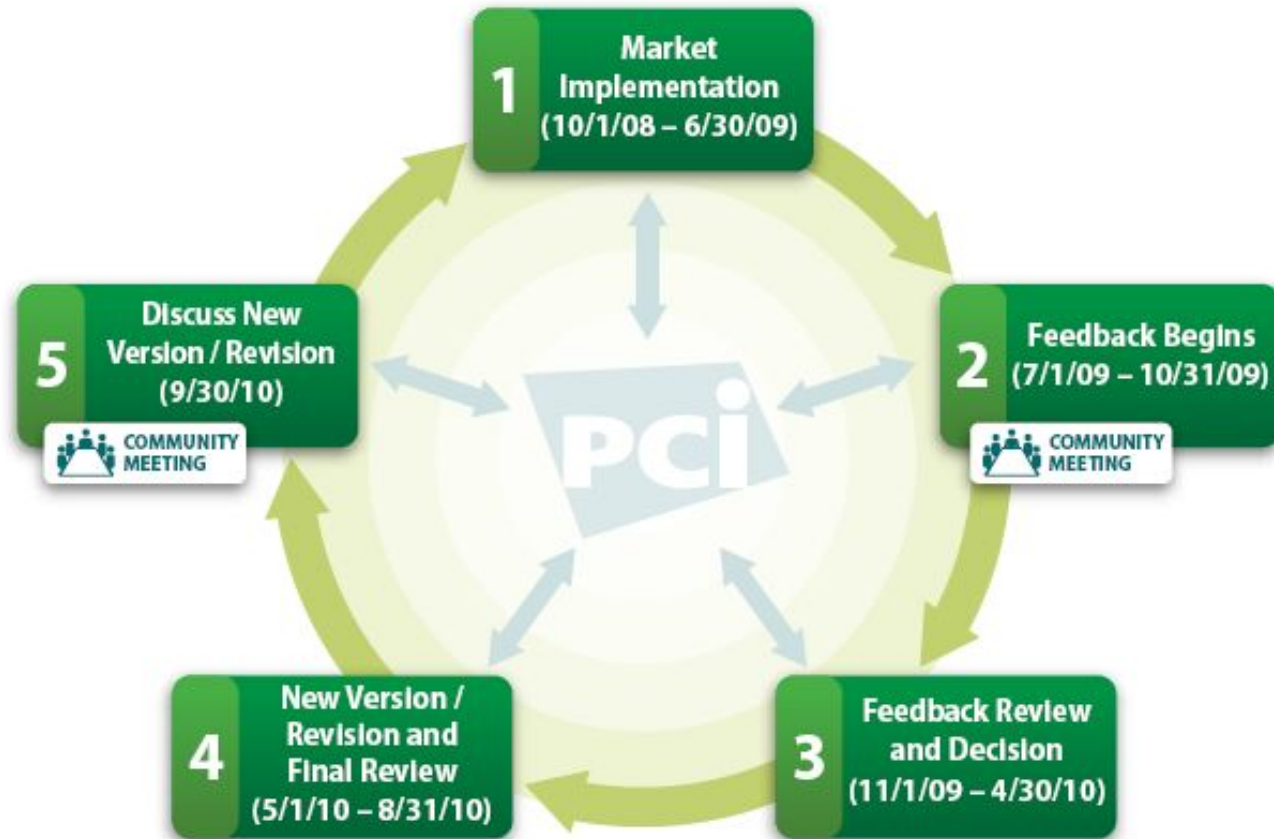
**Динамика стандарта**

Новые вопросы и мифы

Наши прогнозы



# Жизненный цикл стандарта БМС консалтинг



© 2008 PCI Security Standards Council LLC.

\*

PCI DSS увядает?

Динамика стандарта

Новые вопросы и мифы

Наши прогнозы

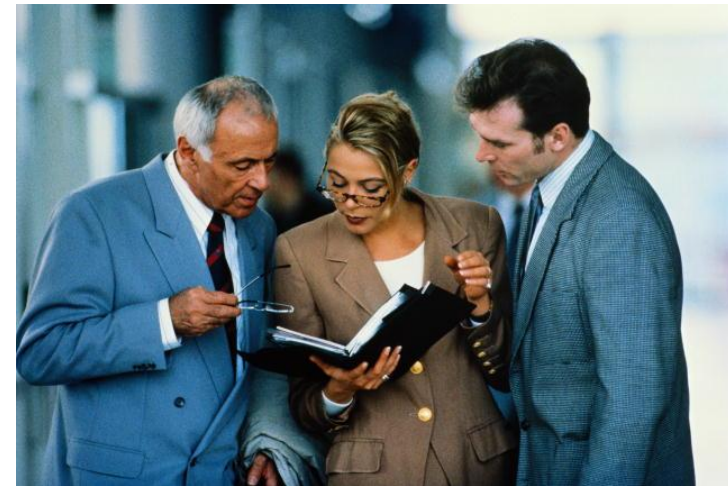


# Кто нам ответит



# Вопрос 1.

## Так что же дает стандарт?



\*



# Вопрос 2.

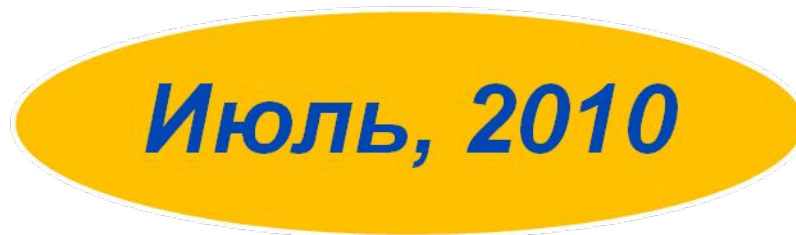
## Кому верить?

- Санкции PCI к QSA
- Некачественная работа
- «Медвежьи» услуги



# Вопрос 3.

## Июль 2010 года?!



# Вопрос 4.

## Как быть с приоритетами?



БМС консалтинг



PCI DSS PRIORITIZED APPROACH

- Первая стадия разработки
- Не инструмент аудита
- Нужен «новичкам» и SMB retail
- Подготовка к SAQ



\*

# Вопрос 5.

## Аутсорсинг или его «дети»?



\*

PCI DSS увядает?

Динамика стандарта

Новые вопросы и мифы

Наши прогнозы







# Наши прогнозы

---

- Безопасность баз данных
- Управление уязвимостями
- Аутсорсинг
- Борьба за качество аудита
- PA DSS



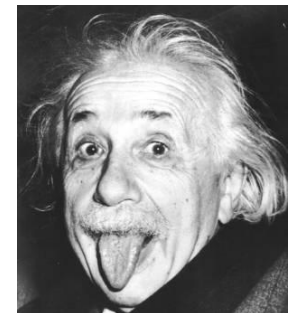
# Добрый совет

- **Надежный партнер**
- **Квалифицированная консультация**
- **Меры «внешние» и «внутренние»**
- **Процессы, а не проекты**

*Внутренние меры*



*Внешний опыт и знания*



\*

**Спасибо за внимание!**

**[www.bms-consulting.com](http://www.bms-consulting.com)**

