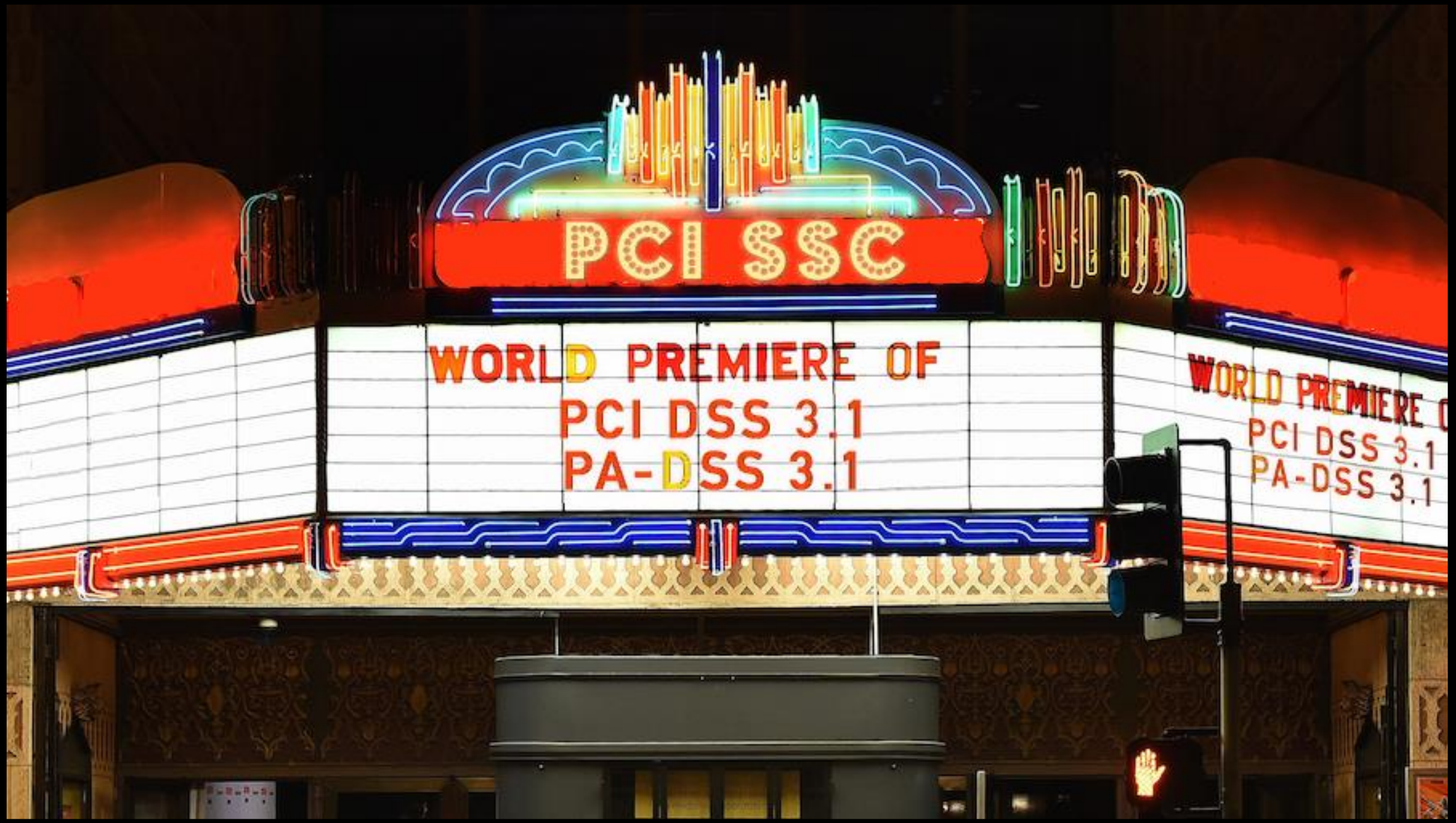
Digital Compliance

Последние изменения в стандартах безопасности платежных карт

Андрей Гайко,
QSA


PCI SSC
WORLD PREMIERE OF
PCI DSS 3.1
PA-DSS 3.1
WORLD PREMIERE O
PCI DSS 3.1
PA-DSS 3.1

PCI DSS 3.1

- **2.2.3.c, 2.3.f, 4.1.i** Компании, использующие уязвимые протоколы, должны составить план миграции на новые протоколы (такие планы должны быть в наличии и при аудите они будут проверяться), разработать и выполнять процедуры по мониторингу новостей об уязвимостях в используемых протоколах
- **2.2.3.b, 2.3.e, 4.1.h**. POS (POI), использующие SSL или TLS 1.0 и которые могут быть проверены на предмет невозможности их компрометации, могут и дальше использовать эти протоколы после 30 июня 2016 года
- Разрабатывая или внедряя новые системы необходимо исключить использование SSL всех версий и TLS версии 1.0
- После 30 июня 2016 года все компании обязаны отказаться от использования протокола SSL и TLS 1.0 и закончить миграцию на более безопасные

Обязателен к применению с 1 июля 2015 года

PA-DSS 3.1

- **8.2, 11.1, 12.1-12.2.** Из примеров безопасных протоколов удалены SSL и TLS 1.0
- Сертификация по PA-DSS v3.0 возможна до 31 августа 2015 г.
- После 1 сентября все приложения должны проходить оценку соответствия по PA-DSS v3.1
- Приложения, находящиеся в процессе сертификации, должны быть сертифицированы до 30 ноября 2015 г.

Обязателен к применению с 1 июля 2015 года

«На основании статистики по расследованию инцидентов (собранной за 10 лет), связанным с компрометацией ДДК, на момент инцидента ни одна компания, не соответствовала требованиям PCI DSS»

*согласно данным, представленным в отчете VERIZON 2015 PCI COMPLIANCE REPORT


Контроль работы СЗИ
Отслеживание изменений в ИС
Внутренние аудиты
Контроль статуса поддержки ПО и железа
Отслеживание изменений в организации
Business as Usual

PCI DSS Designated Entities Supplemental Validation

Что это?

- Дополнительные обязательные к исполнению требования для отдельных организаций, постоянное соответствие (BAU)

Для кого?

- Для компаний с высоким риском копрометации данных (например, обрабатывающих большое количество ДДК) или часто подвергающимся атакам

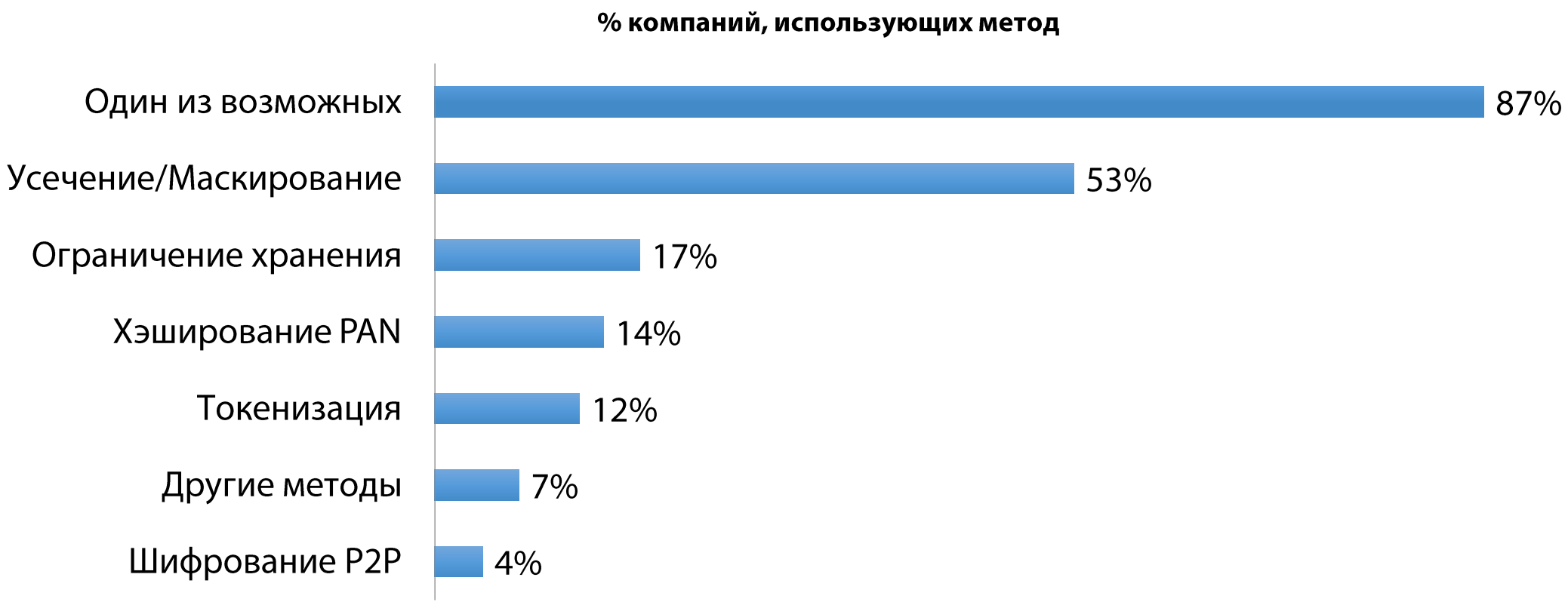
Требования PCI DSS DESV обязательны к исполнению для всех компаний?

- Только если об этом попросит эквайер или МПС

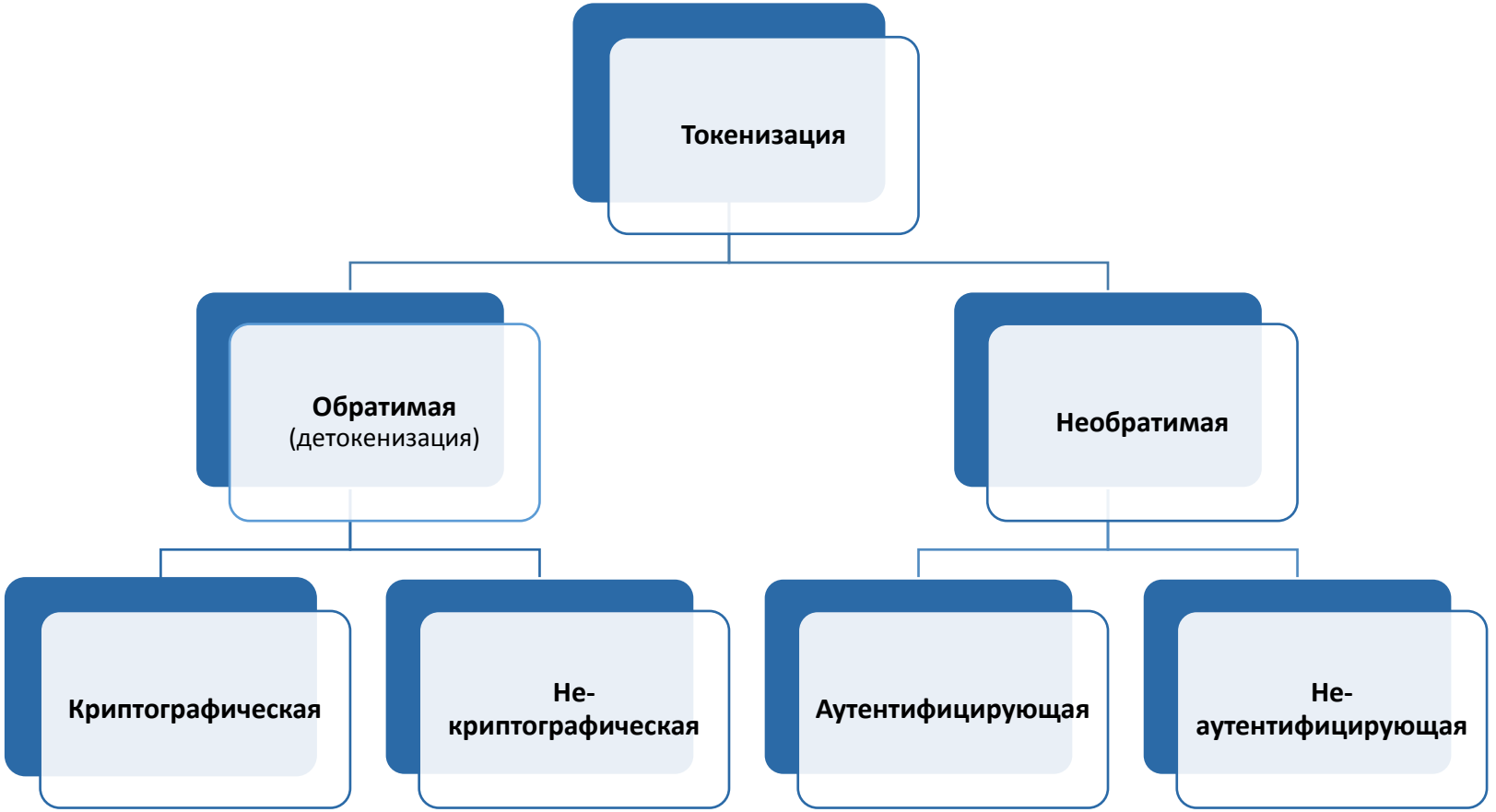
У меня есть сертификат PCI DSS. Мне надо сертифицироваться еще раз?

- Аудит по требованиям PCI DSS DESV выполнятся в ходе аудита по PCI DSS

Последние изменения в стандартах безопасности платежных карт



*по результатам анализа RoC за 2012 – 2014 год (Verizon)


Токенизация
Обратимая
(детокенизация)
Необратимая
Криптографическая
Не-
криптографическая
Аутентифицирующая
Не-
аутентифицирующая

Алгоритм	3DES	AES	RSA	Эллиптические кривые	DSA/D-H
Минимальная длина ключа в битах	Использование не допускается	128	3072	256	3072/256

Алгоритм хэширования
SHA-256
SHA3-256
SHA3-384
SHA-512
SHA3-512

Вероятность угадывания PAN из токена должна быть не менее 1 в 10^6 (как и вероятность угадывания усеченного PAN)

Digital Compliance

Последние изменения в стандартах безопасности платежных карт


msi
http://conference.hitb.org
HITBSecConf2015
AMSTERDAM

Digital Compliance

Последние изменения в стандартах безопасности платежных карт

Digital Security

Методика проведения теста на проникновение ООО «Диджитал Секьюрити»

Оглавление

Методика

Digital Security

КОНФИДЕНЦИАЛЬНО

Экспертное заключение по проведению тестирования на проникновение в инфраструктуру ООО «.....»

Оглавление

Отчет

Чего ожидать в 2015 году

Ежедневный анализ журналов событий

- Руководство по анализу событий и выявлении потенциальных проблем безопасности
- Руководство по инструментам/техникам агрегации и просмотра событий

Разделение ответственности между компанией и поставщиками услуг

- Руководство по предоставлению отчетности
- Руководство по разделению области ответственности, сервисов

Information Supplement: Penetration Testing Guidance	https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf
Tokenization Product Security Guidelines: Irreversible and Reversible Tokens	https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf
PCI DSS Designated Entities Supplemental Validation	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_DESV.pdf
Verizon 2015 PCI Compliance Report	http://www.verizonenterprise.com/resources/report/rp_pci-report-2015_en_xg.pdf

Digital Compliance

Спасибо за внимание!

115054, Россия,
Москва, Партийный пер.,
д. 1, корп. 57, стр. 3

197046, Россия,
Санкт-Петербург,
Петроградская наб., 16 А

+7 (812) 703-15-47
+7 (495) 223-07-86
info@digitalcompliance.ru