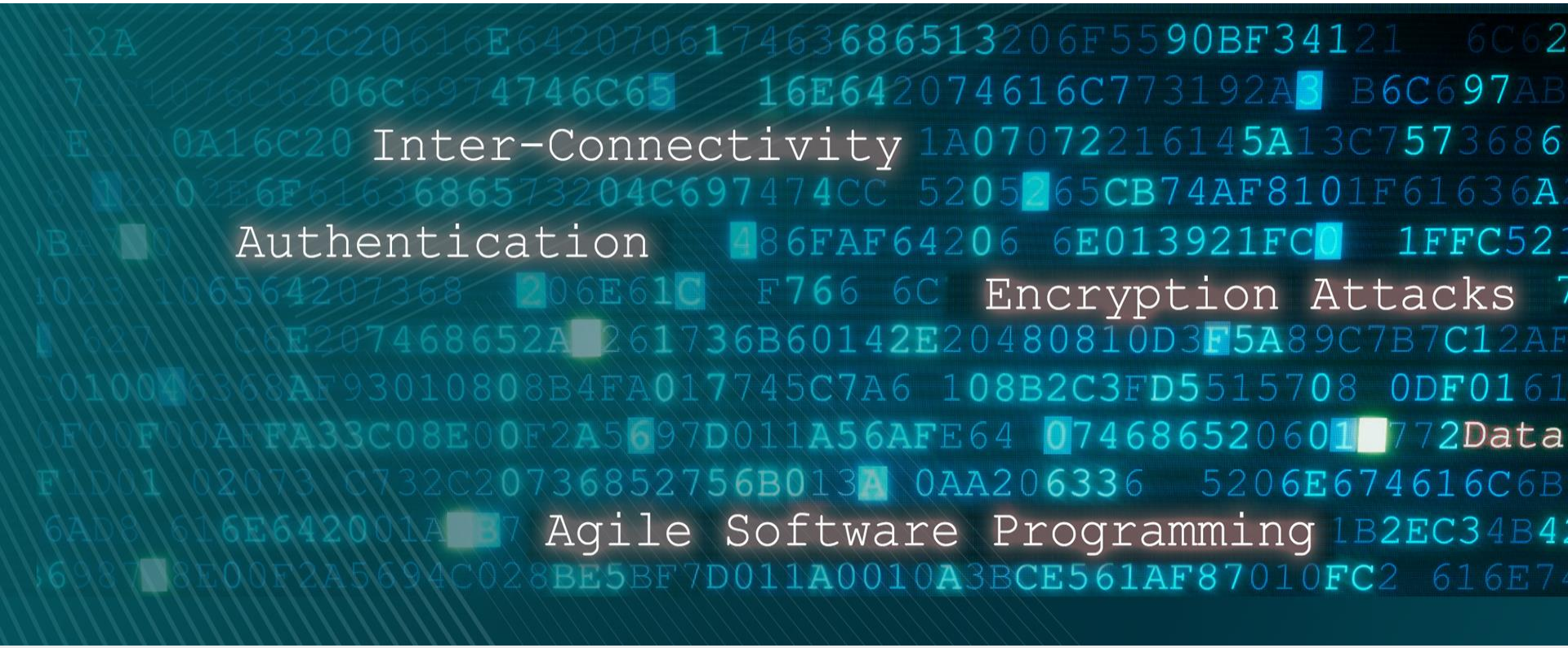
Elizabeth Terry

PCI DSS Roadmap – The Evolution of Payments

Growth of Payment Software

ControlCase
Compliance as a Service

Payment Security Themes for 2017



ControlCase
Compliance as a Service

Attacking the Interconnected World

World is becoming more connected every minute of every day with 30+ Billion Devices expected by 2020

- Third-party services
- Third-party software
- Crime-as-a-Service
- IoT access to data

ControlCase
Compliance as a Service

Authentication

The Evolution of Trust for Commerce

Multi-Factor

Card-not-Present

Enrollment credentials

Dynamic authentication

ControlCase
Compliance as a Service

Modern Payment Software

Code changing at a rapid pace

Extensive use of third-party software

Legacy code and modern threats

Newer security techniques

ControlCase
Compliance as a Service

Breadth of Opportunity for Encryption

Good

Encryption used throughout a payment transaction

Data breaches have limited exposure of data

Bad

Encryption leveraged by criminals for ransomware and obfuscation of activity

Migration from older cryptography a significant challenge for many

ControlCase
Compliance as a Service

PCI Themes for 2017

Better authentication

Better software design

Third party accountability

Improve education and collaboration

Technology and process to simplify compliance

More education on encryption and other technologies

Better Authentication

ControlCase
Compliance as a Service

Better Authentication Using 3DS

Three-Domain Secure (3DS) is a messaging protocol which enables consumers to directly authenticate their card with the card issuer

Three domains consist of:

Merchant/Acquirer domain

Interoperability domain

Issuer domain

Reduces fraud by preventing unauthorized uses of cards

ControlCase
Compliance as a Service

Software Attack Surface Increasing in Payments

IoT

Malware in Memory

Cloud-based

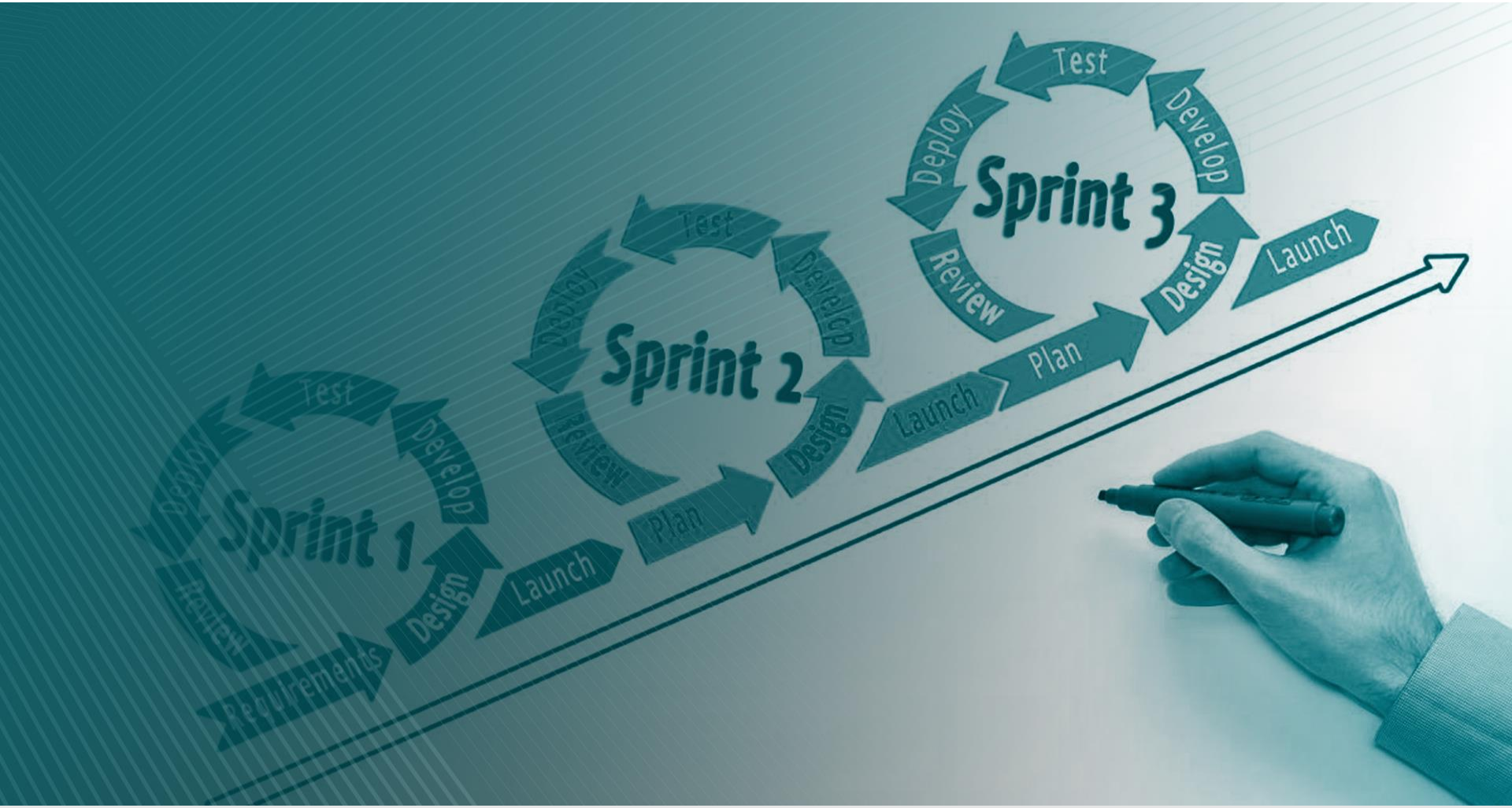
Legacy code

ControlCase
Compliance as a Service

Software Security Audit Challenges

ControlCase
Compliance as a Service

Secure Development Throughout Lifecycle



ControlCase
Compliance as a Service

App Developer Education

New coding platforms and developers

Need for app developer education

Accountability for due diligence

More investment required for software

Network security doubles AppSec

More incentive for good security

ControlCase
Compliance as a Service

Better Integration of Payment Technology

ControlCase
Compliance as a Service

Third Party Accountability

Qualified Integrator & Resellers (QIR)

DSS Service Provider Requirements

Third-party agreements

Software Developers

Third-party monitoring

Importance of Automation

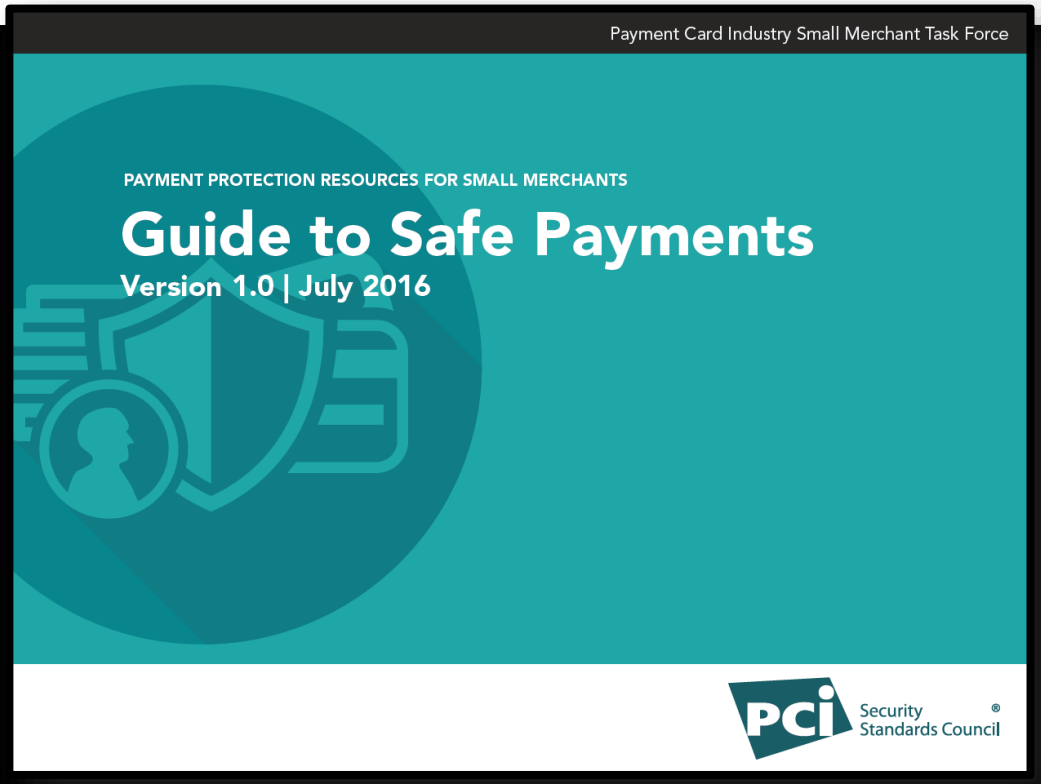
Ease security through automation for DSS

Machine learning advancements

PCI Security Standards Council

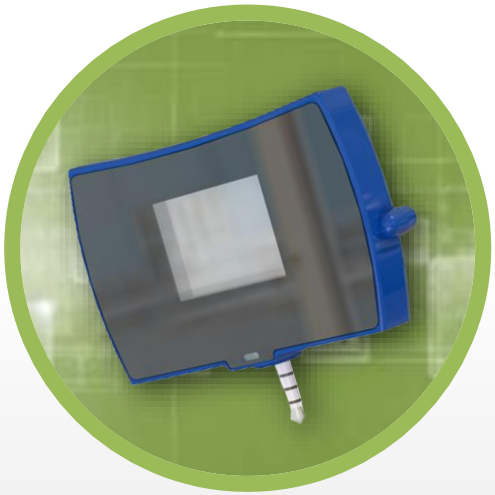
ControlCase Compliance as a Service

Security for Small Merchants



ControlCase
Compliance as a Service

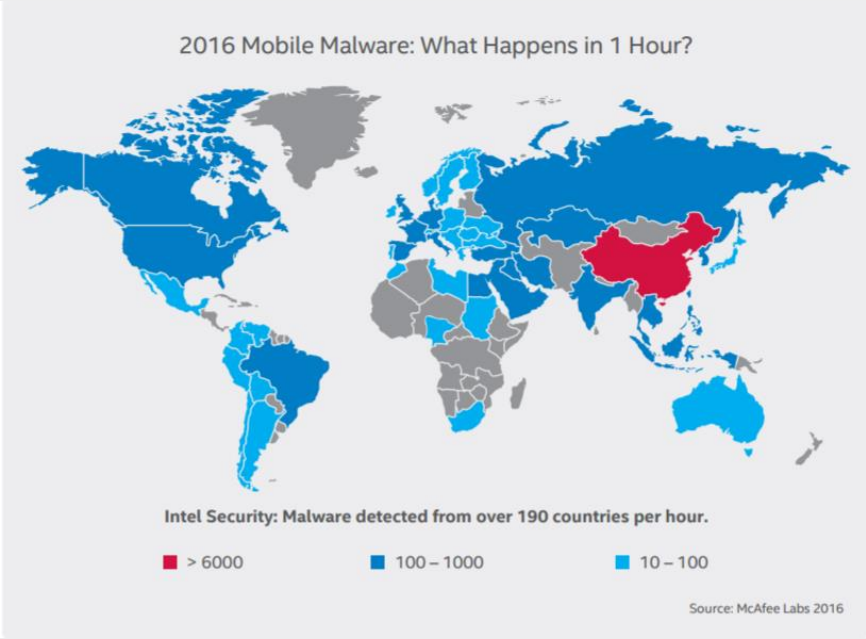
Mobile Payments



Bring It All Together

ControlCase
Compliance as a Service

Mobile Technology Attacks



As mobile becomes the new laptop and business access tool, it becomes "where the money is" for cybercriminals

25% of mobile devices were found to have some form of malware.
– McAfee Labs

More CVEs registered in first half of 2017 for mobile OS than all of 2016

ControlCase
Compliance as a Service

Recent PCI Updates

Growth of SCRs listed that perform encryption before entry into COTS

Over-The-Air (OTA) Provisioning

Token Service Provider Security

Updated Mobile Security Guidelines

PCI Mobile Payment Acceptance Security Guidelines for Developers (v2.0)

PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users (v2.0)

ControlCase
Compliance as a Service

How to Get Involved

PO members can contribute to:

- RFC for Software PIN-entry on COTS Devices
- Cloud SIG
- Software Taskforce
- RFC for Standards (PIN, Card Production)
- Feedback on existing standards (DSS, PA-DSS, P2PE)

Bringing it Together

Holistic Security Integration

Improved Authentication

Leveraging technology to simplify

Security accountability for third parties