

Ten PCI DSS Common Myths



John Elliott

PAYMENTS, SECURITY, PRIVACY AND RISK SPECIALIST

@withoutfire www.withoutfire.com



Myth #1

If you don't store data, PCI DSS doesn't apply

Fact

PCI DSS applies if you **store, process, or transmit** cardholder data



Myth #2

PCI DSS is a legal requirement and should be treated as such

Fact

It's normally a contractual requirement and should be viewed like any contract



Myth #3

Encrypted cardholder data doesn't count

Fact

Requirement 3 says all cardholder data has to be encrypted

Encrypted cardholder data = cardholder data

Key management can take encrypted data out of scope



Myth #4

PCI is a technical issue so there's no need to involve the rest of the business

Fact

Protecting cardholder data requires everyone. Projects led from the finance department are usually the most successful



Myth #5

There is a silver bullet. Product X or software Y will make us compliant

Fact

There is no silver bullet :-)



Myth #6

Everything is outsourced so we don't have to do anything

Fact

It's still your responsibility. Is the outsourcer compliant?

Do you have anything you need to do?



Myth #7

We're compliant because we are using compliant terminals

Fact

Often this isn't the case: remember a 'PCI compliant' thing doesn't exist



Myth #8

I'm too small for the criminal to take an interest

Fact

Sorry. Criminals attack anywhere they can



Myth #9

Now that we've just been certified, we're fully PCI compliant for the next year

Fact

You have been assessed as compliant at a snapshot in time. To remain compliant you have to keep every requirement working every day (and that's almost impossible)



Myth #10

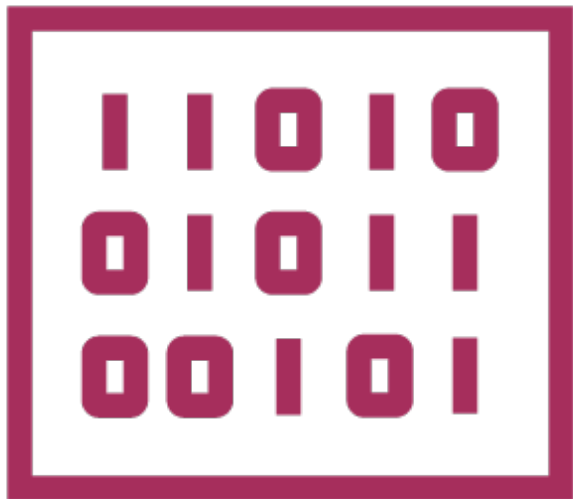
A breach of a PCI DSS requirement is the same as a data breach

Fact

It's not. Remediate it. Document it. Learn from it. Make sure it doesn't re-occur



Myth #11



The Big Picture



PCI DSS is a prescriptive technical standard

Twelve requirements,
about 280 sub-requirements

Every organization that stores, processes
or transmits cardholder data will be
contractually bound to comply

There is one standard

There are multiple compliance programs

