



Security in knowledge

LESS IS MORE

PCI DSS SCOPING DEMYSTIFIED



Lauren Holloway

PCI Security Standards Council

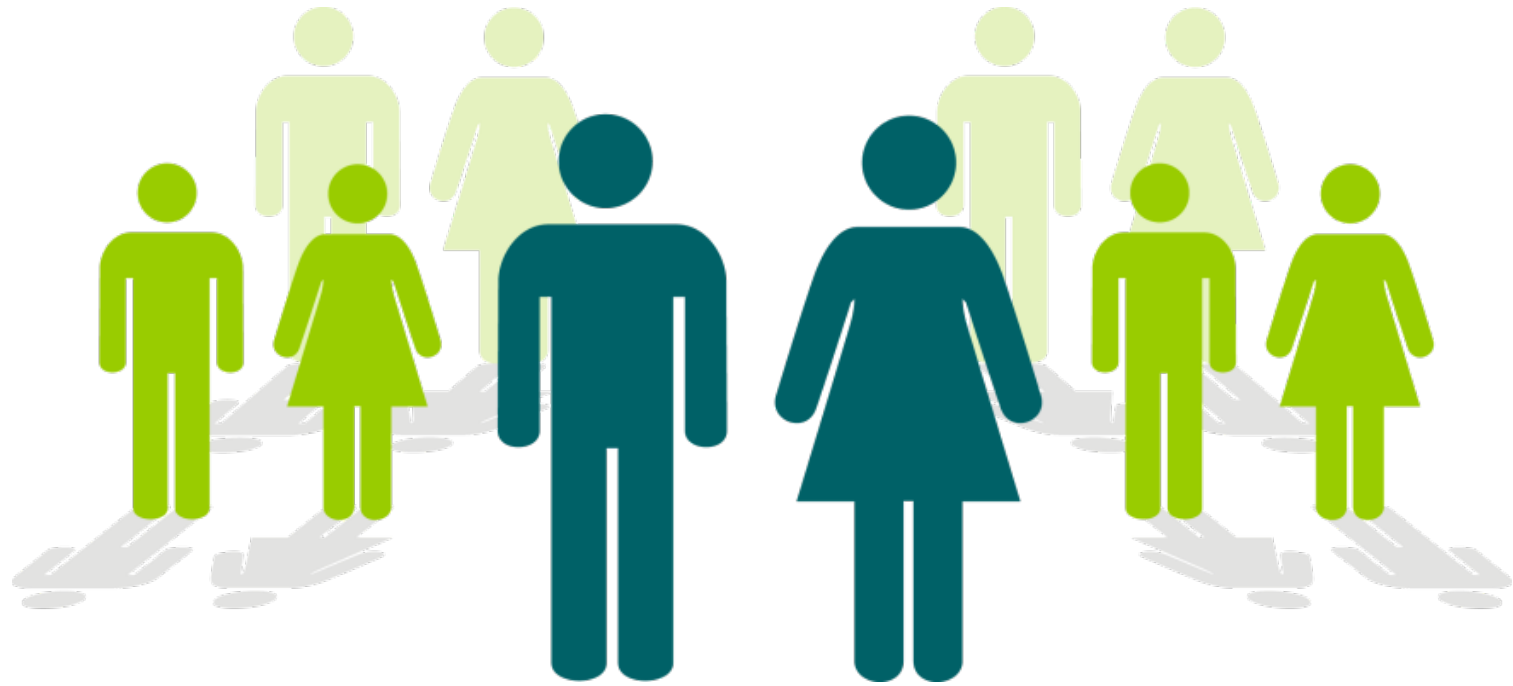
Emma Sutcliffe

PCI Security Standards Council

Session ID: DSP-W21

Session Classification: Intermediate

Who's Here Today?



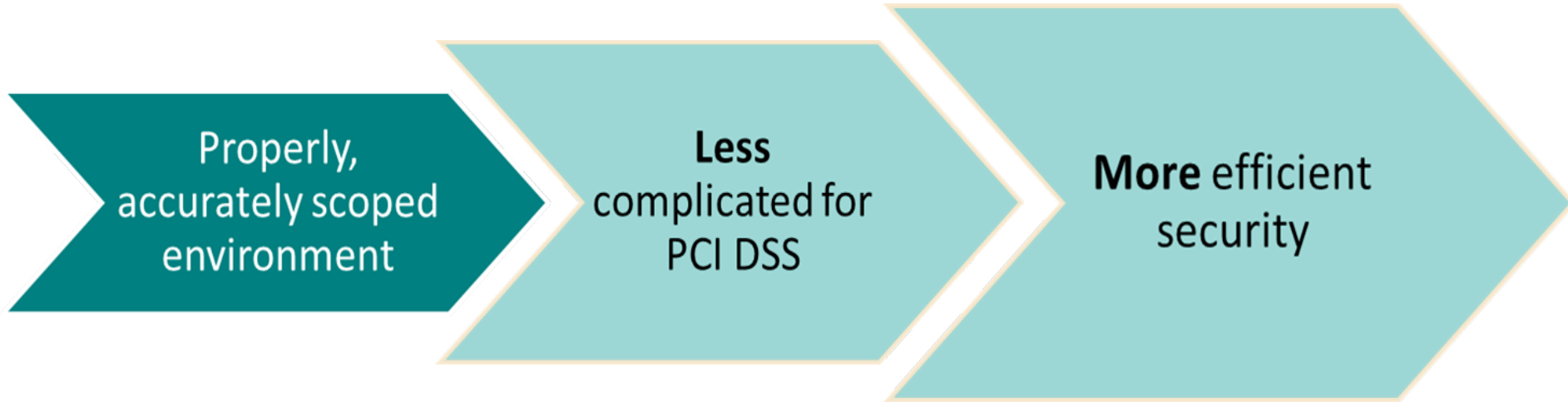
Agenda

- ▶ Why PCI DSS Scoping is a Hot Topic
- ▶ Scoping Scenarios, Misconceptions and Clarifications
- ▶ Top Tips for PCI DSS Scoping
- ▶ Wrap-up and Questions

Key Points to Remember...

- ▶ Improper scoping puts your business at risk
- ▶ Focus on security, not compliance
- ▶ Scoping is not a one-time activity
- ▶ Understanding segmentation is key

Less is More



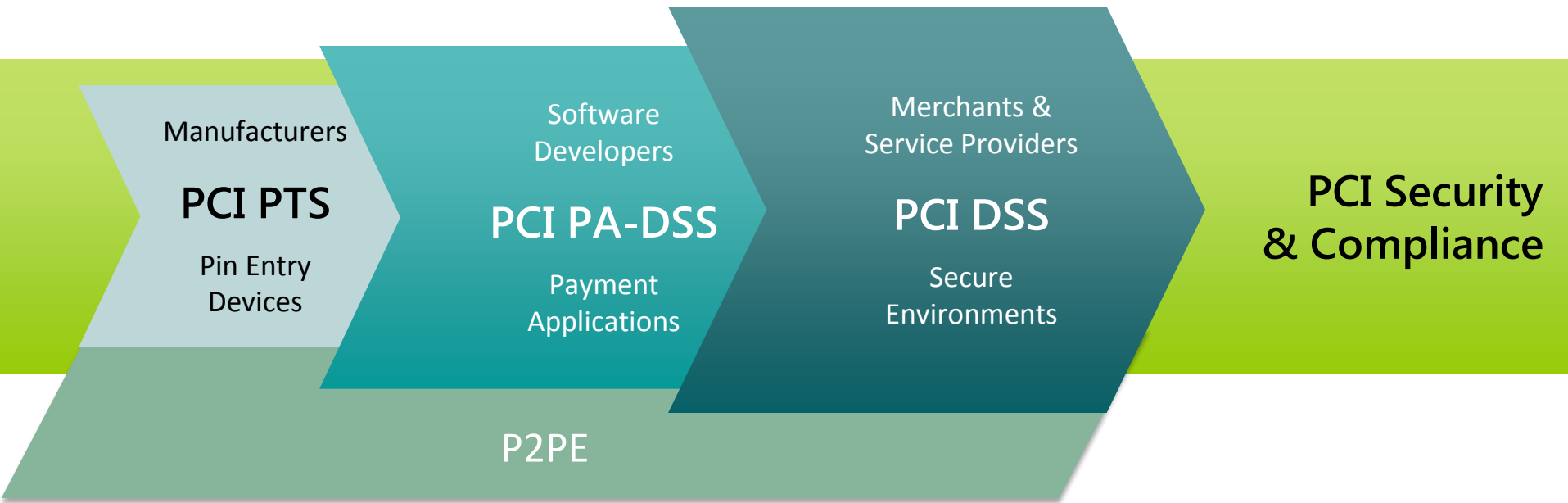
Why PCI DSS Scoping is a Hot Topic



Security in knowledge

PCI Security Standards

Protection of Cardholder Payment Data



Ecosystem of payment devices, applications, infrastructure and users

What Does PCI DSS Say?

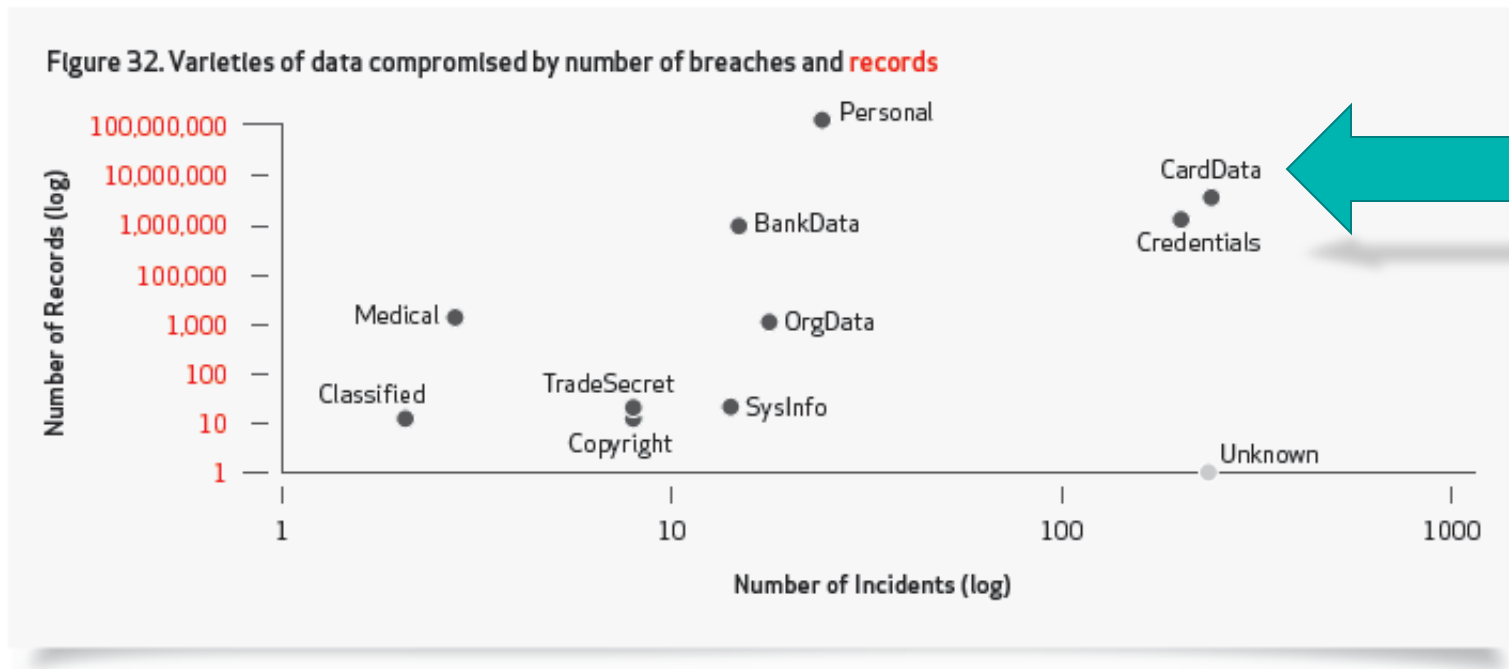
- ▶ PCI DSS requirements apply to all system components included in or connected to the CDE
- ▶ If network segmentation is used, the assessor must verify it is adequate to reduce PCI DSS scope
- ▶ Adequate network segmentation isolates systems that store, process, or transmit cardholder data from those that do not
- ▶ Specific implementations of network segmentation are highly variable

Why PCI DSS Scoping is a Hot Topic

- ▶ There are many interpretations of “adequate network segmentation”
 - ▶ Not all are accurate
- ▶ There are many motivations for wanting to reduce scope
 - ▶ Not all motivations are in the best interests of security
- ▶ Improper scoping choices are contributing to compromises
 - ▶ Cardholder data is still a very desirable target for hackers

Why PCI DSS Scoping is a Hot Topic

In 2011, payment card information was again involved in more breaches (48%) than any other data type



Verizon 2012 Data Breach Investigations Report

Why PCI DSS Scoping is a Hot Topic

- ▶ Bad interpretations and/or motivations can lead to
 - ▶ Aggressive or accidental under-scoping
 - ▶ Ineffective segmentation controls
- ▶ Which can have disastrous consequences
- ▶ Bad interpretations can also lead to unnecessary over-scoping
 - ▶ Can result in ineffective allocation of security resources

Scoping Scenarios, Misconceptions and Clarifications



Security in knowledge

Common Misconceptions & Misunderstandings

1. I am “compliant” therefore I am secure
2. My data is out of scope because *<insert “silver bullet” here>*
3. I know where all my CHD is – it’s in my CDE
4. Controlled access = segmentation = isolation?
5. General scope confusion
6. My vendors do my compliance for me

Compliance vs. Security

Lessons learned from a high-profile breach (published):


“In <company’s> experience, qualified security assessors (QSAs) repeatedly rated <company> as being PCI compliant without detecting the existing SQL injection vulnerability <that lead to the breach>.

Even though the method of attack had been used many times in the months preceding <company’s> breach, XXXX emphasized that it went unidentified during QSA audits.”

Compliance vs. Security

- ▶ What did a finding of “compliant” mean in this scenario?
 - ❑ The assessor detected all vulnerabilities present at the organization being assessed

OR

-  The assessor verified that the organization had solid processes in place for detecting and addressing vulnerabilities

Compliance vs. Security

- ▶ A “compliant” result means:
 - ▶ Policies and processes are in place
 - ▶ Personnel are aware of the processes
 - ▶ Systems were verified to be secure
- ▶ A compliance validation does not mean:
 - ▶ There will never be vulnerabilities in the future
 - ▶ All personnel will follow the processes at all times
 - ▶ All systems will continue to be maintained securely
 - ▶ The environment will continue to be secure
- ▶ Security involves maintaining compliance and includes:
 - ▶ Understanding of environment and associated risk
 - ▶ Controls to meet PCI DSS requirements are appropriate for the level of risk
 - ▶ Checks and balances help to ensure people follow processes at all times
 - ▶ All systems are periodically verified as secure



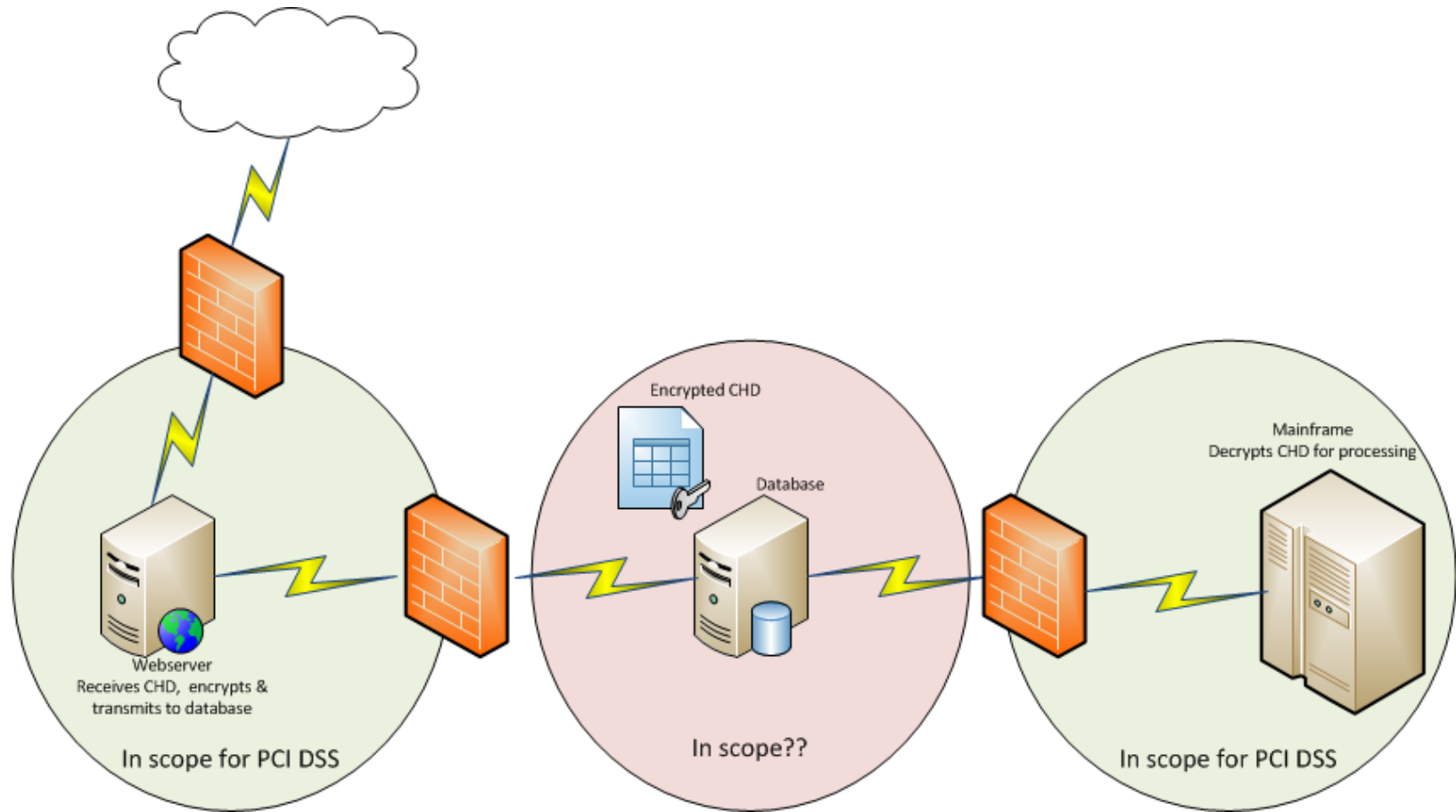
Compliance vs. Security

More often than not, entities claiming to be “PCI DSS compliant” are basing this assertion on the fact that, at one point in time, they underwent and passed a PCI DSS assessment.

However, compliance is the continuous state of adhering to the regulatory standard.

*VERIZON 2011 PAYMENT CARD INDUSTRY COMPLIANCE
REPORT*

Isn't my data out of scope because...?



Is the database with encrypted data out of scope?

Isn't my data out of scope because...?

Don't start with the assumption that encrypted data is out of scope, instead start from the premise that all encrypted data is in scope until proven (verified) otherwise



Beware Silver Bullets

▶ Encrypted/tokenized data

- ✓ ...helps protect CHD
- ✓ ...is always in scope for someone
- ✓ ...does not replace all other PCI DSS requirements
- ✓ ...might be out of scope for a particular entity if VERIFIED that it:
 - is irreversible
 - is isolated from cryptographic/tokenization processes and CDE
 - truly has no value if environment compromised

▶ Payment applications validated to PA-DSS

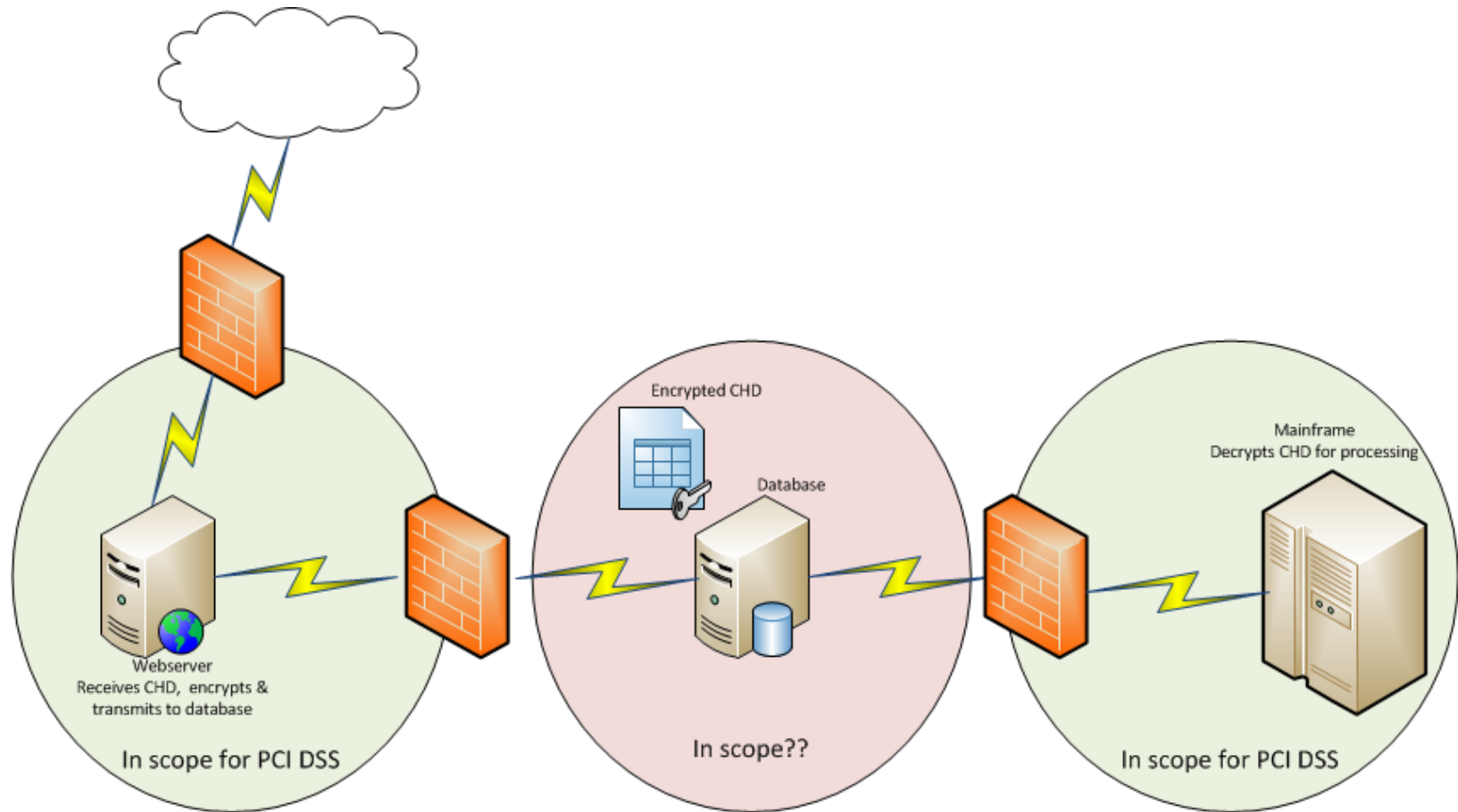
- ✓ ... are validated as being able to support PCI DSS compliance
- ✓ ... do not guarantee compliance with PCI DSS
- ✓ ... are configurable
- ✓ ... are in scope

Beware Silver Bullets

- ▶ EMV (chip-and-PIN)
 - ✓ ... is a great anti-fraud mechanism for F2F EMV environments
 - ✓ ... complements PCI DSS controls
 - ✓ ... provides authentication, does not provide confidentiality
 - ✓ ... does not protect card-not-present transactions
 - ✓ ... are in scope for PCI DSS

- ▶ “Scoping Method X” says my data is out of scope
 - ✓ ... can help identify scoping considerations
 - ✓ ... may not be applicable to your environment
 - ✓ ... is not endorsed by the SSC or the payment brands
 - ✓ ... cannot determine your scope for you
 - ✓ ... may result in incorrect scoping

What is Segmentation?



Is the database segmented from the CDE?

What is Segmentation?

- ▶ To be out of scope: segmentation = isolation = no access
- ▶ Controlled access \neq isolation
- ▶ Controlled access:
 - ▶ Is still access
 - ▶ Is a PCI DSS requirement
 - ▶ Does not isolate one system/network from another
 - ▶ Provides entry point into CDE
 - ▶ Is in scope for PCI DSS
 - Verify access controls are working
 - Verify the connection / point of entry is secure
- ▶ If it can impact the security of the CDE, it is in scope
- ▶ Remember non-CHD systems may be in scope too

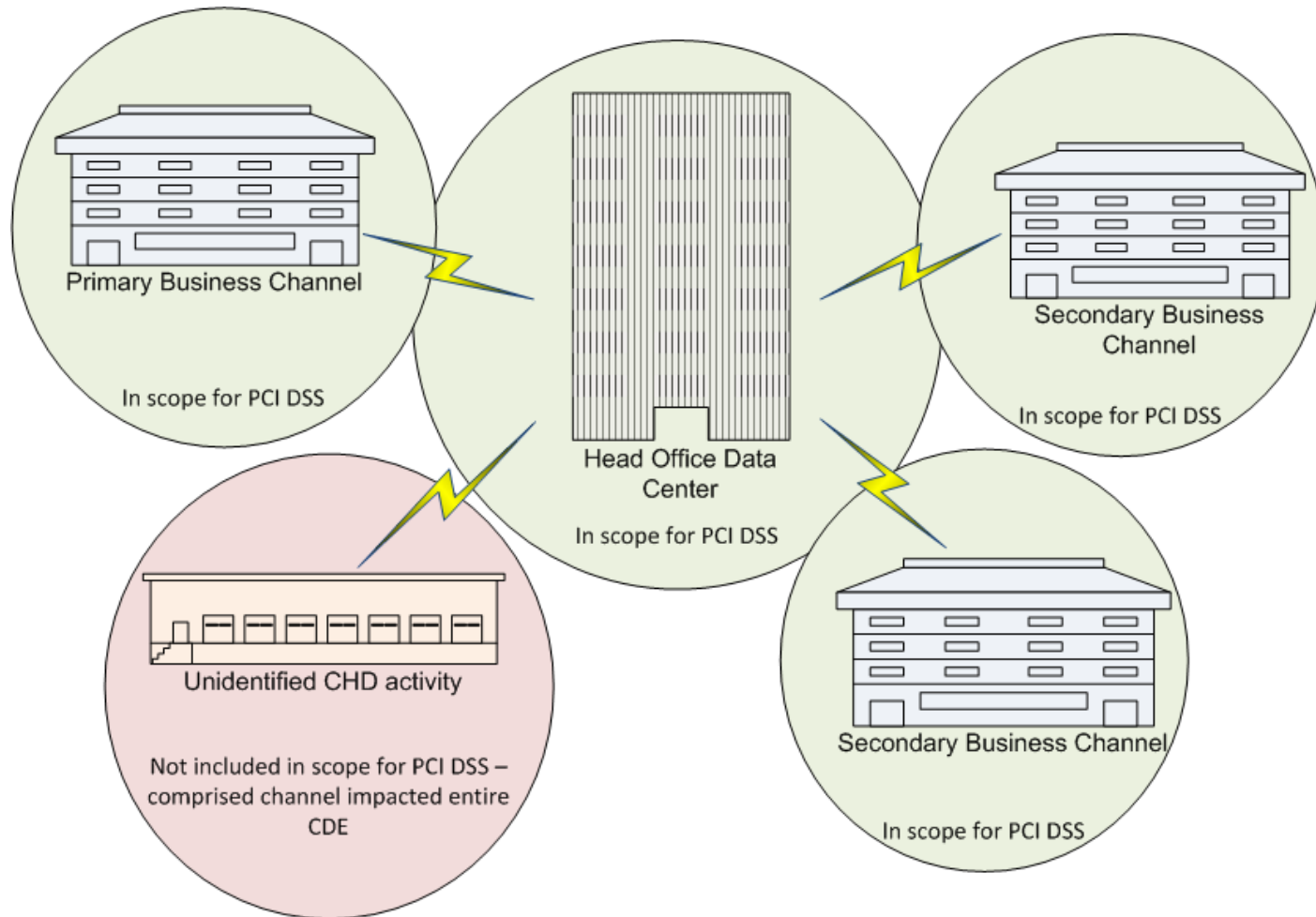
All my CHD is in my CDE. Isn't it?

2008: In 66% of data breaches, the organization didn't know the data was on the system that was compromised.

Verizon 2008 Data Breach Investigations Report

All my CHD is in my CDE. Isn't it?

- ▶ Breach example: PCI DSS compliant payment processor



All my CHD is in my CDE. Isn't it?

Data leaks!

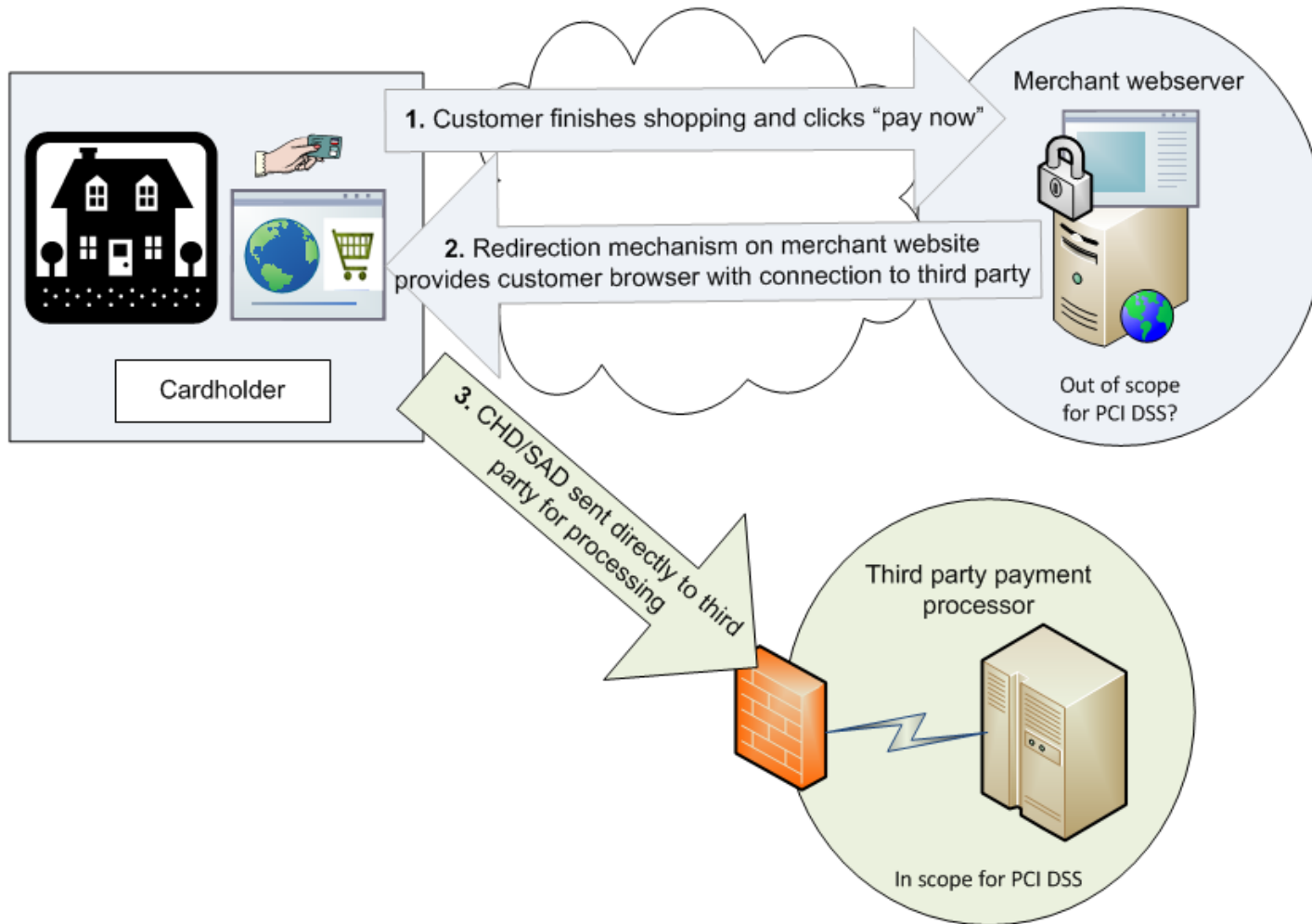
- ▶ Ongoing effort is required to ensure all cardholder data is located
 - ▶ Identify your unknowns
 - ▶ Don't forget about people!
 - ▶ Don't assume last year's scope is still accurate
- ▶ You can't protect what you don't know about

Scoping Confusion?

- ▶ What does “in scope” mean?
 - ▶ Every PCI DSS requirement may not apply to an in-scope system. Consider:
 - ▶ Requirements applicable for system function/use
 - ▶ Requirements applied at network level rather than on every system
 - ▶ Controls to reduce applicability of certain PCI DSS requirements (must be verified!)
- ▶ What does “out of scope” mean?
 - ▶ Consider as ‘untrusted’
 - ▶ No security evaluation or validation of the system/network
 - ▶ If an “out-of-scope” system could lead a CDE compromise, it should not have been considered out of scope

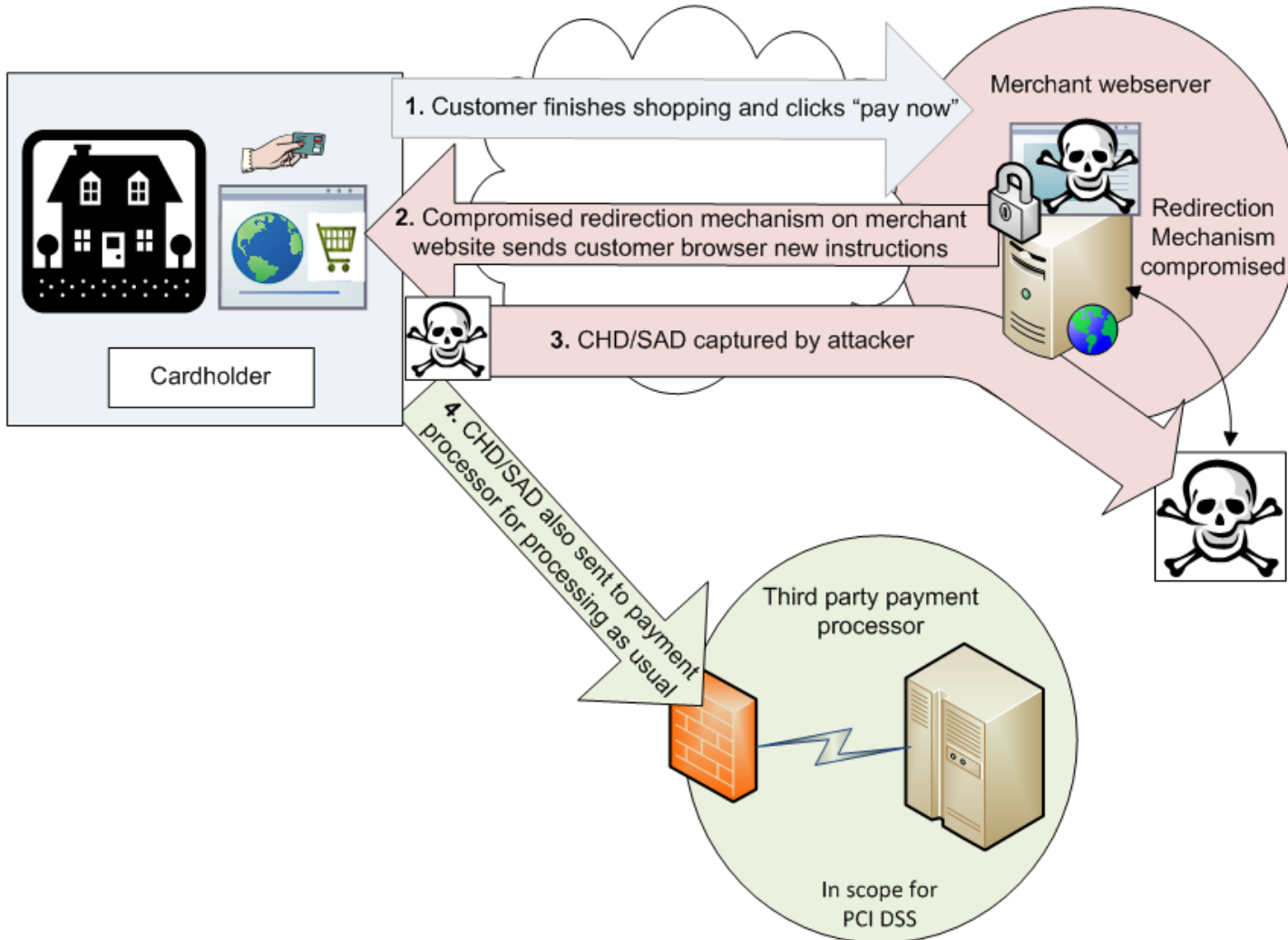
Doesn't my vendor do my compliance for me?

Example: Outsource payment processing to third-party e-commerce provider



Doesn't my vendor do my compliance for me?

Breach: Outsource payment processing to third-party e-commerce



Doesn't my vendor do my compliance for me?

- ▶ An entity cannot outsource their PCI DSS responsibility
 - ▶ May outsource operational responsibility for maintaining security controls
- ▶ Vendors aren't always secure
 - ▶ Vendors may need to be included in your PCI DSS assessment
 - ▶ Consider all relationships - vendor, integrator/reseller, IT delivery
 - ▶ Common weak points include insecure remote access and default/shared passwords



Top Tips for PCI DSS Scoping



Security in knowledge

TIP #1: Plan your Scoping

- ▶ Step 1. Identify CHD locations and evaluate the business need for all CHD
- ▶ Step 2. Identify in-scope components and networks
- ▶ Step 3. Define and implement CDE boundaries
- ▶ Step 4. Apply PCI DSS controls
- ▶ Step 5. Maintain and Monitor



TIP #2: Think Outside the Box

- ▶ Don't limit data discovery to existing CDE
- ▶ Think outside of IT
- ▶ Don't forget about people
- ▶ Consider 'what if' scenarios

TIP #3: Risk Assessments as a Scoping Aid

- ▶ Risk assessments include identifying sensitive data and determining who needs access to it
 - ▶ Once you know who needs access, remove (segment) all other access
- ▶ Risk assessments can help identify CHD that is not needed and can be removed
 - ▶ If you don't need it, don't store it (or collect it in the first place)
 - ▶ Securely delete what is not needed
 - ▶ Migrate what is needed into the CDE
- ▶ Risk assessments can help facilitate an effective scoping methodology

TIP #4: Keep your Scope Up-to-Date

- ▶ Environments change – ongoing processes needed to maintain security
- ▶ Security as part of BAU helps keep scope up-to-date and accurate
 - ▶ Change management
 - ▶ Periodic reviews
 - ▶ Ongoing monitoring

TIP #5 Trust but Verify

- ▶ Engage trusted providers
 - ▶ Due diligence
 - ▶ Risk assessments
- ▶ Don't fall into the *"I am secure because my service provider is compliant"* trap
 - ▶ Remember the "compliance vs. security" discussion?
 - ▶ Verify details of service provider compliance
 - ▶ Does it cover all aspects of the services you are using?
 - ▶ Does it include all PCI DSS requirements?
- ▶ Document roles and responsibilities in written agreements
- ▶ Verify through ongoing monitoring and reporting

TIP #6: Confirm your Segmentation

- ▶ Segmentation controls also need to be verified
 - ▶ Additional to verifying PCI DSS requirements
- ▶ Check segmentation controls as part of annual assessment AND periodically
- ▶ Your segmentation is not the same as my segmentation
- ▶ Segmentation is not a requirement
 - ▶ May not be necessary – for example, small merchant environments
 - ▶ PCI DSS controls applied to entire environment

TIP #7: Don't Rely on "Silver Bullets"

- ▶ There are no scoping "silver bullets"
- ▶ Start with the assumption that everything is in scope
- ▶ Technology/method can assist with PCI DSS
- ▶ Technology/method must still be validated for PCI DSS
- ▶ Any potential scope reduction must be verified

Wrap-up and Questions

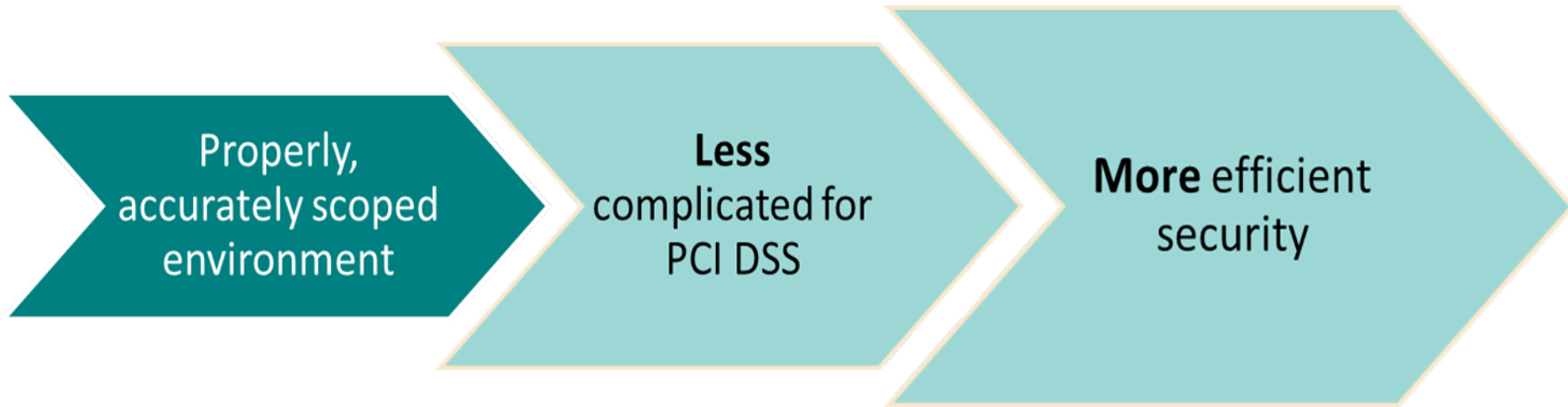


Security in knowledge

Remember...

- ▶ Improper scoping puts your business at risk
- ▶ Focus on security, not compliance
- ▶ Scoping is not a one-time activity
- ▶ Understanding segmentation is key

Less is More



Questions?



Visit our website at www.pcisecuritystandards.org

Lauren Holloway: lholloway@pcisecuritystandards.org

Emma Sutcliffe: esutcliffe@pcisecuritystandards.org

General queries: info@pcisecuritystandards.org

About the Council

Open, global forum

Founded 2006

Guiding open standards for payment card security

- Development
- Management
- Education
- Awareness



PCI Resources to Help You

PCI security is not a one-time event...these resources will help you maintain a secure environment

Web

Merchants,
Financial
Institutions,
HW / SW
Providers,
Services &
Professionals

Toolkit

Quick
Reference
Guide

Prioritized
Approach

Fact Sheets

Webinars

FAQ Tool

Training

ASV

ISA

PA-QSA

PCI
Awareness

QSA

Guidance

Mobile

P2PE

Virtualization

EMV

Tokenization

Standards

PCI DSS

PA-DSS

PTS

P2PE