Agenda

- Housekeeping
- Presenters
- About Conexxus
- Presentation
- Q & A

Housekeeping

This webinar is being recorded and will be made available in approximately 15 days.

- YouTube (youtube.com/conexxusonline)
- Website Link (conexxus.org)

Slide Deck

- Survey Link – Presentation provided at end

Participants

- Ask questions via webinar interface
- Please, no vendor specific questions
- Our webinars may be used toward PCI continuing education credits. Please contact arussell@conexxus.org for questions regarding a certificate of webinar attendance.

Email: **info@conexxus.org**

Presenters

Conexxus Host

Allie Russell
Conexxus
arussell@conexxus.org

Moderator

Kara Gunderson
Chair, Data Security Committee
POS Manager, CITGO Petroleum
kgunder@citgo.com

Speakers

Ajith Edakandi: Product Director, HUGHES

About Conexxus

- We are an independent, non-profit, member driven technology organization
- We set standards…
  - Data exchange
  - Security
  - Mobile commerce
- We provide vision
  - Identify emerging tech/trends
- We advocate for our industry
  - Technology is policy

CONEXXUS solve forward

2019 Conexxus Webinar Schedule

Month/Date	Webinar Title	Speaker	Company
January 24, 2019	Who's Watching Your Network? What you should know about Managed Detection & Response (MDR)	Mark Carl Tom Callahan	ControlScan
February 28, 2019	Protect Your Business: PCI Resources for Securing Payment Data	Elizabeth Terry	PCI Security Standards Council
March 21, 2019	Proactive Defense in Depth	Brett Stewart DeWayne Mangan Mark Palmer	Acumera
May 30, 2019	Firewalls, LANS & WANS The Basics, The Benefits and The Security!	Simon Gamble	Mako Networks
June 27, 2019	Web Payment Asipirations	Ian Jacobs	W3C
July 25, 2019	Skimming	Linda Toth Paige Anderson Caleb Burke	Conexxus NACS CITGO
August 8, 2019	Application Security 101	Denis Sheridan	Synopsys

CONEXXUS solve forward

2019-2020 Conexxus Webinar Schedule

Month/Date	Webinar Title	Speaker	Company
August 29, 2019	Don't Get Phished!! Train Your Employees To Avoid Ransomware	Geoffrey Vaughan Ed Adams	Security Innovation
September 26, 2019	Using Data Science to Proactively Manage the Connected C-Store	Ashwin Swamy Thomas Duncan	Omega ATC Omega ATC
October 24, 2019	Easy PCI—How to Make PCI & Attestation Easier	Ajith Edakandi	Hughes
November 21, 2019	Applicability of PCI DSS requirements for Merchants and MNSP's	Sam Pfanstiel	ControlScan
December 5 and 12, 2019	EMV	TBD	TBD
January, 2020	TBD	TBD	Cybera

CONEXXUS
solve forward

2020 Conexxus Annual Conference
April 26-30, 2020
Loews Ventana Canyon Resort
Tucson, AZ

Conexxus thanks our 2019 Annual Diamond Sponsors!

mSHIFT. Relevant. Mobile. Solutions.

Stuzo

Diebold Nixdorf

wex

HUGHES An EchoStar Company

GILBARCO VEEDER-ROOT

Cybera

SECURITY INNOVATION

CONEXXUS solve forward

PCI Compliance: Made Simpler

Presenter:

Ajith Edakandi,
Director of Product Management & Marketing
HUGHES®
An EchoStar Company

CONEXXUS
solve forward

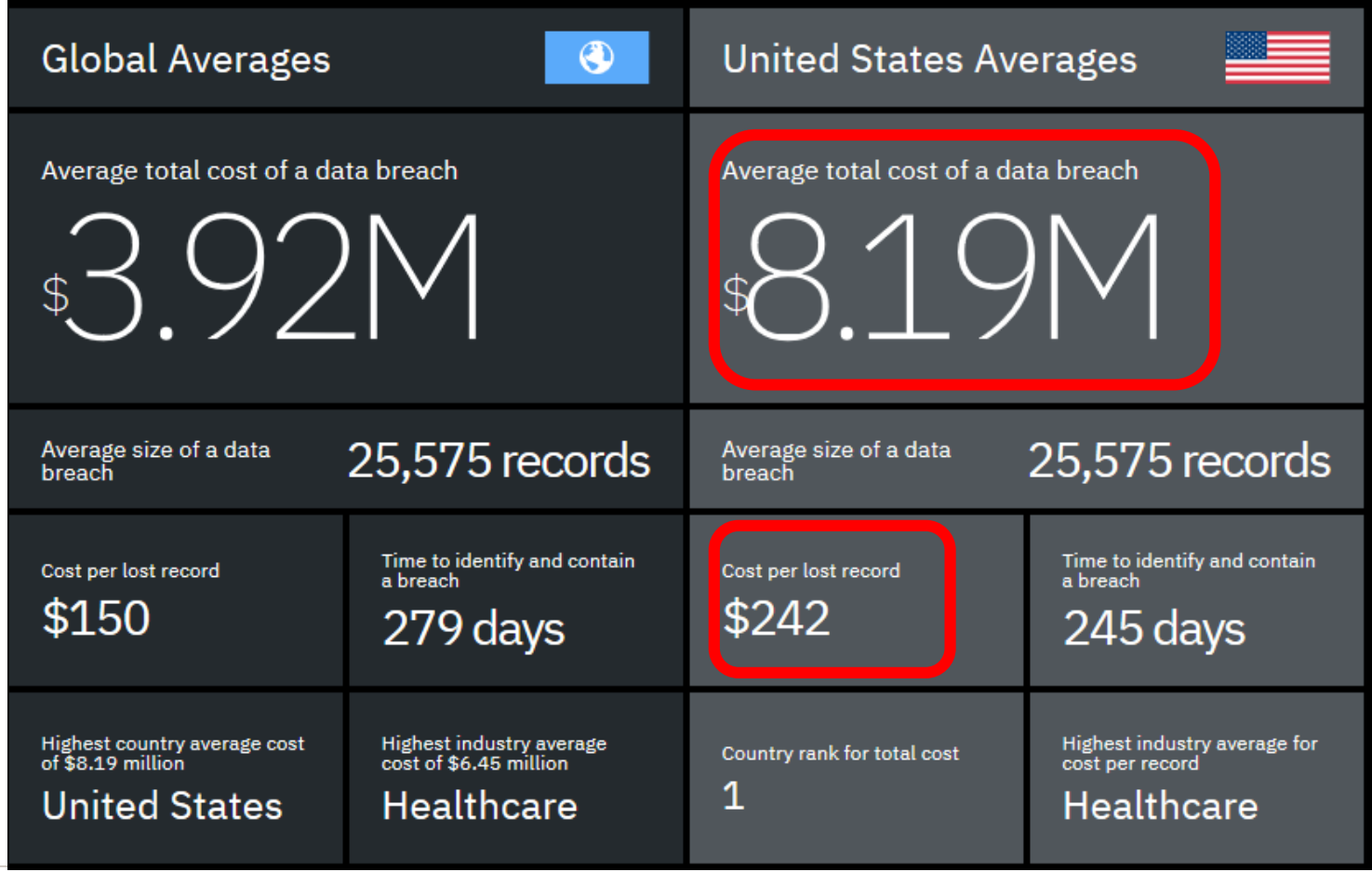
Agenda

Why you need PCI Compliance?

Doing it yourself or getting help

How to make the process easier?

Cost of a Data Breach 2019*



*Source:IBM Security/Ponemon

CONEXXUS
solve forward

Key Highlights from the Study

Lost business is the biggest contributor to data breach costs.

Data breach costs impact organization for years.

Small businesses face disproportionately larger costs relative to larger organizations

Even following a breach, organizations still don't get their overall security right and a breach is likely to happen within 2 years.

Suggested Security Practices

Companies with an incident response team and extensive testing of their response plans could save a lot of money.

Automation of security reduces costs.

Managed Service Providers (MSP's) can help an organization with customized solutions and thus ease the pain of maintaining a security solution

Security Hygiene

PCI Compliance

Guidelines defined by the Payment Card Industry Data Security Standards

Misconception

If your business process doesn't involve online transactions using credit cards, then you don't need to be PCI compliant.

I do very less transactions. So it doesn't apply

What happens if you are not PCI Compliant?

- Fines
- Ability to Accept Credit Cards maybe revoked
- Mandatory Forensic examination
- Reassessment for PCI Compliance

Penalties for Non-Compliance

According to the PCI Compliance Blog, fines are not published or reported, and usually end up passed to the merchants. Banks pass the fines along as increased transaction fees or termination of business relationships.

Fines vary from $5,000 to $100,000 per month until the merchants achieves compliance. That kind of fine is manageable for a big enterprise, but it could easily put a small business into bankruptcy.

But these fines issued by the PCI are small in comparison to credit monitoring fees, laws suits, and actions by state and federal governments that can result when you're not truly PCI DSS compliant.

CONEXXUS
solve forward

Safe Harbor

Safe Harbor is a term used to describe the protection of business entities from significant financial liability related to payment processing and data breaches. The law and specific Safe Harbor Protection rules are continually evolving.

What should Brands do?

You are impacted as well!

70%

Of companies believe that the cybersecurity shortage has had an impact on their organization

By 2020

78%

of enterprises will use MSP/MSSP's

CONEXXUS solve forward

Goals of
PCI DSS COMPLIANCE

Build and maintain a secure network and systems

Protect cardholder data

Maintain a vulnerability management program

Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

CONEXXUS
solve forward

Roles & Responsibilities

	Level	Criteria	On-Site Security Audit	Self-Assessment Questionnaire (SAQ)	Network Scan (ASV)
Merchant	1	• Any merchant, regardless of acceptance channel, processing **more than 6 million transactions** per year • Any merchant that suffered a security breach, resulting in an account compromise	Required Annually		Required Quarterly
	2	• Any merchant processing between **150,000 to 6 million transactions** per year		Required Annually	Required Quarterly
	3	• Any merchant processing between **20,000 to 150,000 transactions** per year		Required Annually	Required Quarterly
	4	• **All other merchants** not in Levels 1, 2, or 3, regardless of acceptance channel		Required Annually	Required Quarterly

Self Assessment Questionnaire - SAQ

SAQ Validation Type	Description	# of Qs	ASV Scan Required?
A	Card-not-present merchants: all payment processing functions fully outsourced, no electronic cardholder data storage	14	No
A-EP	E-commerce merchants re-directing to a third-party, PCI compliant service provider for payment processing, no electronic cardholder data storage	139	Yes
B	Merchants with only imprint machines or only standalone dial-out payment terminals: No e-commerce or electronic cardholder data storage	41	No
B-IP	Merchants with standalone IP (Internet) connected payment terminals: No e-commerce or electronic cardholder data storage	83	Yes

Self Assessment Questionnaire - SAQ

SAQ Validation Type	Description	# of Qs	ASV Scan Required?
C	Merchants with payment application systems connected to the Internet: No e-commerce or electronic cardholder data storage	139	Yes
C-VT	Merchants with web-based virtual payment terminals: No e-commerce or electronic cardholder data storage	73	No
D-Merchant	All other SAQ eligible Merchants, or those that electronically store cardholder data	326	Yes
D-Service Provider	SAQ eligible service providers	347	Yes
P2PE	Hardware payment terminals in a validated PCI P2PE solution only: No e-commerce or electronic cardholder data storage	35	No

CONEXXUS solve forward

Doing it Yourself or employing a Managed Service Provider?

Without support from an outside partner, you can expect 3-4 week on performing tasks like:

- Researching the PCI DSS standards
- Understanding which SAQ to use
- Creating and maintain portals for use by merchants
- Creating guides for merchants to help during the PCI onboard process
- Completing the PCI SAQ and Attestation of Compliance (AoC)

PCI Authorized Scan Vendor (ASV)

Run internal and external network vulnerability scans at least quarterly and after any significant change in the network

Requirement 11.2

The external scan must be done via an Approved Scanning Vendor (ASV)

CONEXXUS
solve forward

Cost of doing PCI Compliance

SAQ - $50 to $200

Vulnerability scanning (External & internal) - $100 to $200 per location

Training and policy development $50 to $100/employee

Insurance Premium (Breach protection)- based on coverage

What if the network differs from franchise to franchise?

Some of the most overlooked items after you achieve Compliance

- Vulnerability scanning (internal/external)
- Semi-annual review of firewall configuration and rules
- Consistent application of change management processes
- Quarterly reviews to verify security policies and procedures
- Continuous Training

You can make a plan or rely on a service provider to do it for you

With so many rules and stipulations , maintaining PCI compliance can be complicated. Companies can hire an Internal Security Assessor (ISA) who are certified through the council to help them through the process.

The distributed locations become a challenge for most brands and this is where the Managed service provider comes in.

CONEXXUS
solve forward

Critical Things to Consider

- This service provider who is also a Managed Network Provider
- Do they have a Security Operation Center (SOC)?
- Is their Approved Scan Vendor (ASV) in-house or do they use a 3rd party?
- How willing are they to make customizable solutions to help your individual merchants.

All Merchants

Need to be PCI Compliant.

It doesn’t need to be a daunting task… an MSP can help!

Critical features you are looking for, could help in your MSP selection.

THANK YOU

CONEXXUS
solve forward

CONEXXUS
solve forward

- Website: www.conexxus.org
- Email: info@conexxus.org
- LinkedIn Profile: Conexxus.org
- Follow us on Twitter: @Conexxusonline

CONEXXUS solve forward

DISCLAIMER: Conexxus does not endorse any products or services that may be described or mentioned in this presentation. The views and opinions expressed in this presentation are solely those of the speakers and not of Conexxus. By hosting this webinar, Conexxus is not providing any legal advice; if you have any questions about legal issues raised or discussed, you should seek the assistance of attorneys who are competent in that area.