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
<table>
<thead>
<tr>
<th>Month/Date</th>
<th>Webinar Title</th>
<th>Speaker</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 24, 2019</td>
<td>Who’s Watching Your Network? What you should know about Managed Detection &amp; Response (MDR)</td>
<td>Mark Carl, Tom Callahan</td>
<td>ControlScan</td>
</tr>
<tr>
<td>March 21, 2019</td>
<td>Proactive Defense in Depth</td>
<td>Brett Stewart, DeWayne Mangan, Mark Palmer</td>
<td>Acumera</td>
</tr>
<tr>
<td>June 27, 2019</td>
<td>Web Payment Aspirations</td>
<td>Ian Jacobs</td>
<td>W3C</td>
</tr>
<tr>
<td>July 25, 2019</td>
<td>Skimming</td>
<td>Linda Toth, Paige Anderson, Caleb Burke</td>
<td>Conexxus, NACS, CITGO</td>
</tr>
<tr>
<td>August 8, 2019</td>
<td>Application Security 101</td>
<td>Denis Sheridan</td>
<td>Synopsys</td>
</tr>
<tr>
<td>Month/Date</td>
<td>Webinar Title</td>
<td>Speaker</td>
<td>Company</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>August 29, 2019</td>
<td>Don’t Get Phished!! Train Your Employees To Avoid Ransomware</td>
<td>Geoffrey Vaughan Ed Adams</td>
<td>Security Innovation</td>
</tr>
<tr>
<td>September 26, 2019</td>
<td>Using Data Science to Proactively Manage the Connected C-Store</td>
<td>Ashwin Swamy Thomas Duncan</td>
<td>Omega ATC Omega ATC</td>
</tr>
<tr>
<td>October 24, 2019</td>
<td>Easy PCI—How to Make PCI &amp; Attestation Easier</td>
<td>Ajith Edakandi</td>
<td>Hughes</td>
</tr>
<tr>
<td>November 21, 2019</td>
<td>Applicability of PCI DSS requirements for Merchants and MNSP’s</td>
<td>Sam Pfanstiel</td>
<td>ControlScan</td>
</tr>
<tr>
<td>December 5 and 12, 2019</td>
<td>EMV</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>January, 2020</td>
<td>TBD</td>
<td>TBD</td>
<td>Cybera</td>
</tr>
</tbody>
</table>
2020 Conexxus Annual Conference
April 26-30, 2020
Loews Ventana Canyon Resort
Tucson, AZ

Conexxus thanks our 2019 Annual Diamond Sponsors!
PCI Compliance: Made Simpler

Presenter:

Ajith Edakandi,
Director of Product Management & Marketing
Agenda

Why you need PCI Compliance?
Doing it yourself or getting help
How to make the process easier?
### Cost of a Data Breach 2019*

<table>
<thead>
<tr>
<th>Global Averages</th>
<th>United States Averages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Average total cost of a data breach</strong></td>
<td><strong>Average total cost of a data breach</strong></td>
</tr>
<tr>
<td>$3.92M</td>
<td>$8.19M</td>
</tr>
<tr>
<td><strong>Average size of a data breach</strong></td>
<td><strong>Average size of a data breach</strong></td>
</tr>
<tr>
<td>25,575 records</td>
<td>25,575 records</td>
</tr>
<tr>
<td><strong>Cost per lost record</strong></td>
<td><strong>Cost per lost record</strong></td>
</tr>
<tr>
<td>$150</td>
<td>$242</td>
</tr>
<tr>
<td><strong>Time to identify and contain a breach</strong></td>
<td><strong>Time to identify and contain a breach</strong></td>
</tr>
<tr>
<td>279 days</td>
<td>245 days</td>
</tr>
</tbody>
</table>

- **Highest country average cost of $8.19 million**
  - United States
- **Highest industry average cost of $6.45 million**
  - Healthcare
- **Country rank for total cost**
  - 1
- **Highest industry average for cost per record**
  - Healthcare

*Source: IBM Security/Ponemon
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.
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 achieve 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, lawsuits, and actions by state and federal governments that can result when you’re not truly PCI DSS compliant.
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.
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
### Roles & Responsibilities

<table>
<thead>
<tr>
<th>Level</th>
<th>Criteria</th>
<th>On-Site Security Audit</th>
<th>Self-Assessment Questionnaire (SAQ)</th>
<th>Network Scan (ASV)</th>
</tr>
</thead>
</table>
| 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 |
<p>| 2     | • Any merchant processing between <strong>150,000 to 6 million transactions</strong> per year | | Required Annually | Required Quarterly |
| 3     | • Any merchant processing between <strong>20,000 to 150,000 transactions</strong> per year | | Required Annually | Required Quarterly |
| 4     | • <strong>All other merchants</strong> not in Levels 1, 2, or 3, regardless of acceptance channel | | Required Annually | Required Quarterly |</p>
<table>
<thead>
<tr>
<th>SAQ Validation Type</th>
<th>Description</th>
<th># of Qs</th>
<th>ASV Scan Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Card-not-present merchants: all payment processing functions fully outsourced, no electronic cardholder data storage</td>
<td>14</td>
<td>No</td>
</tr>
<tr>
<td>A-EP</td>
<td>E-commerce merchants re-directing to a third-party, PCI compliant service provider for payment processing, no electronic cardholder data storage</td>
<td>139</td>
<td>Yes</td>
</tr>
<tr>
<td>B</td>
<td>Merchants with only imprint machines or only standalone dial-out payment terminals: No e-commerce or electronic cardholder data storage</td>
<td>41</td>
<td>No</td>
</tr>
<tr>
<td>B-IP</td>
<td>Merchants with standalone IP (Internet) connected payment terminals: No e-commerce or electronic cardholder data storage</td>
<td>83</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Self Assessment Questionnaire - SAQ

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

Without support from an outside partner, you can expect 3-4 weeks 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)
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)
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.
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
• Website: www.conexxus.org
• Email: info@conexxus.org
• LinkedIn Profile: Conexxus.org
• Follow us on Twitter: @Conexxusonline
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.