Protect Your Business: PCI Resources for Securing Payment Data

Presenter:
Elizabeth Terry
Community Engagement Manager
PCI Security Standards Council
Agenda

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

This webinar is being recorded and will be made available in approximately 30 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

Email: info@conexxus.org
Conexxus Host
Allie Russell
Conexxus
arussell@conexxus.org

Jenny Bullard
Conexxus
jbullard@conexxus.org

Speaker
Elizabeth Terry
PCI Security Standards Council
Community Engagement Manager

Moderator
Kara Gunderson
Chair, Data Security Committee
POS Manager, CITGO Petroleum
kgunder@citgo.com
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>Managed Detection and Response</td>
<td>Tom Callahan, Mark Carl</td>
<td>ControlScan</td>
</tr>
<tr>
<td>February 28, 2019</td>
<td>PCI DSS for Petro Merchants</td>
<td>Elizabeth Terry</td>
<td>PCI SSC</td>
</tr>
<tr>
<td>March 2019</td>
<td>Protecting Your Stores and Main Office from Data Security &amp; Ransomware Attacks</td>
<td>Dirk Heinen</td>
<td>Acumera</td>
</tr>
<tr>
<td>April 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>May 2019</td>
<td>Firewall compliance! The basics, the benefits, and the security</td>
<td>Simon Gamble</td>
<td>Mako Networks</td>
</tr>
<tr>
<td>June 2019</td>
<td>TBD</td>
<td>David Ezell, Ian Jacobs</td>
<td>Conexxus W3C</td>
</tr>
</tbody>
</table>
## 2019 Conexxus Webinar Schedule

<table>
<thead>
<tr>
<th>Month/Date</th>
<th>Webinar Title</th>
<th>Speaker</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2019</td>
<td>Skimming</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>August 2019</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>September 2019</td>
<td>Updated Data Science Presentation</td>
<td>Ashwin Swamy, Thomas Duncan</td>
<td>Omega ATC, Omega ATC</td>
</tr>
<tr>
<td>November 2019</td>
<td>Outdoor EMV</td>
<td>Brian Russell, Linda Toth</td>
<td>Verifone, Conexxus</td>
</tr>
<tr>
<td>December 2019</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
</tbody>
</table>
Conexxus thanks our 2018 Annual Diamond Sponsors!
Protect Your Business: PCI Resources for Securing Payment Data

Presenter: Elizabeth Terry
Community Engagement Manager
PCI SSC
PCI Security Standards Council

We Help
Secure
Payment
Data

Global, cross-industry effort to increase payment security
Industry-driven, flexible and effective standards and programs
Helping businesses detect, mitigate and prevent criminal attacks and breaches
PCI Security Standards and Programs

Standards, Training and Certification Programs, Educational Resources

Payment Equipment
Payment Software
Merchant & Payment Service Provider Environments

Certification – Equipment, Service Providers, Assessors, Investigators
Training – Assessors, Investigators
Small Merchant Resources
Organized Crime is a Business

The global impact of huge cyber security events such as the WannaCry ransomware epidemic has taken the threat from cybercrime to another level. Banks and other major businesses are now targeted on a scale not seen before.

- Europol
Leading Causes of Data Breaches

- Weak and default passwords
- Unpatched software
- Insecure Remote Access
Leading Causes of Data Breaches

- Weak and default passwords
- Unpatched software
- Insecure remote access

81% of hacking-related breaches succeeded through stolen passwords, default or weak passwords.

Verizon Data Breach Investigation Report (DBIR)
80% Of the majority of hacking attacks could be prevented by strengthening passwords and installing patches.

Verizon Data Breach Investigation Report (DBIR)
Insecure remote access is the number one point of entry for attacks against brick-and-mortar merchants.
POS Attacks Lead to Breaches

“At 40%, payment card data is the #1 type of data targeted in a breach.”

2018 Trustwave Global Security Report

“The chances of being struck by lightning this year are 1 in 960,000. When it comes to experiencing a data breach, the odds are as high as 1 in 4.”

2017 Ponemon Cost of Data Breach Study
90% of all accommodation breaches were POS breaches.

2018 Verizon Data Breach Investigations Report (DBIR)
Small Merchant Resources
PCISSC.org/Merchants

GUIDE TO SAFE PAYMENTS
Simple guidance for understanding the risk to small business, security basics to protect against payment data theft, and where to go for help.

COMMON PAYMENT SYSTEMS
Real-life visuals to help identify what type of payment system a small business uses, the kinds of risks associated with their system, and actions they can take to protect it.
How do you protect your business?

The good news is, you can start protecting your business today with these security basics:

<table>
<thead>
<tr>
<th>Business Activity</th>
<th>Cost</th>
<th>Ease</th>
<th>Risk Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use strong passwords and change default ones</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
</tr>
<tr>
<td>Protect your card data and only store what you need</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
</tr>
<tr>
<td>Inspect payment terminals for tampering</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
</tr>
<tr>
<td>Use trusted business partners and know how to contact them</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
</tr>
<tr>
<td>Install patches from your vendors</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
</tr>
<tr>
<td>Protect in-house access to your card data</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
</tr>
<tr>
<td>Don’t give hackers easy access to your systems</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
</tr>
<tr>
<td>Use anti-virus software</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
</tr>
<tr>
<td>Scan for vulnerabilities and fix issues</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
</tr>
<tr>
<td>Use secure payment terminals and solutions</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
</tr>
<tr>
<td>Protect your business from the Internet</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
</tr>
<tr>
<td>For the best protection, make your data useless to criminals</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
<td>🟢🟢</td>
</tr>
</tbody>
</table>

These security basics are organized from easiest and least costly to implement to those that are more complex and costly to implement. The amount of risk reduction that each provides to small merchants is also indicated in the “Risk Mitigation” column.
QUESTIONS TO ASK YOUR VENDORS
A list of the common vendors small business rely on and specific questions to ask them to make sure they are protecting customer payment data.

GLOSSARY OF PAYMENT AND INFORMATION SECURITY TERMS
Simplified glossary, based on PCI DSS Glossary and with extra definitions specific to small merchants.
What is a “Small Merchant”?

PCISSC.org/Merchants

- Typically an independently-owned and operated business
- With a single location or a few locations
- With limited or no IT budget
- Often with no IT personnel

Whether a small merchant is required to validate PCI compliance is determined by the payment brands or acquirer
Current Small Merchant Materials

**Small Merchant materials released in 2016 provided:**
- Education and awareness
- Simple security steps to address critical risks

**Small Merchant materials updated in 2018 to provide:**
- Clearer e-commerce guidance
- More types of payment diagrams for small merchants
- New, easy-to-understand DSE Evaluation Tool to help with validation
PCI Data Security Essentials Evaluation Tool
PCISSC.org/SmallMerchantTool

PCI DATA SECURITY ESSENTIALS EVALUATION TOOL FOR SMALL MERCHANTS

The PCI Data Security Essentials Resources for Small Merchants provides security basics to protect against payment data theft and to help small merchants simplify their security and reduce their risk. The Data Security Essentials Evaluation Tool provides an alternative for eligible small merchants to learn more about their security posture and perform a preliminary evaluation to understand how they are meeting these security basics for safe payments.

Each merchant’s acquirer (merchant bank), in coordination with the applicable payment brands, determines which merchants are eligible to use Data Security Evaluation forms. We encourage small merchants to review Data Security Essentials Resources for Small Merchants, talk to your acquirers for instructions on how to complete and submit a Data Security Essentials evaluation, and start your path to better security and simpler validation today.

CONEXXUS
solve forward
PCI Data Security Essentials Evaluation Tool
PCISSC.org/SmallMerchantTool

<table>
<thead>
<tr>
<th>Security Practice</th>
<th>How have you implemented this practice?</th>
<th>Additional Information as Needed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A. Use strong passwords and change default ones</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passwords are vital for security of your payment systems and card data. The confidentiality of all passwords should be protected and passwords should be changed if there is any suspicion of misuse. This includes all passwords you and your staff (including permanent full-time and part-time workers, contractors, consultants, etc.) use to log into or connect to your payment systems, computers, and other equipment. In addition, much equipment comes with default passwords “out of the box” (like “password” or “admin”). Hackers easily guess these out-of-the-box passwords since they are commonly known and often left unchanged. See “It’s time to change your password” at <a href="http://www.PCISecurityStandards.org">www.PCISecurityStandards.org</a>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. You and your staff change passwords for computer access regularly, at least every 90 days.</td>
<td>I do this consistently.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>I do this sometimes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This is N/A to my business environment (explain).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>I do not know / I do not understand.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>I do not do this (explain).</td>
<td></td>
</tr>
<tr>
<td>2. You and your staff make all passwords for computer access in your business unique and hard to guess: 7 or more characters and a combination of upper- and lower-case letters, numbers, and symbols. Consider using a passphrase as your password; you can make it personal and easy for you to remember.</td>
<td>I do this consistently.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>I do this sometimes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This is N/A to my business environment (explain).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>I do not know / I do not understand.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>I do not do this (explain).</td>
<td></td>
</tr>
<tr>
<td>3. Immediately, you change out-of-the-box default passwords from your equipment and/or software suppliers. If you do not know where these passwords are or how to change them, find out from your payment system vendor or supplier, the individual who set up your payment system, or your merchant bank.</td>
<td>I do this consistently.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>I do this sometimes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This is N/A to my business environment (explain).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>I do not know / I do not understand.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>I do not do this (explain).</td>
<td></td>
</tr>
</tbody>
</table>
Help Us Help Them

Share these resources with your small merchant customers

Let small merchants know the simple things they can do today

Help small merchants understand and address risks with remote access and default passwords

Use secure remote access into small merchant systems and help them manage it
Questions About Small Merchant Resources?

Co-branding?
Where are the documents?
Are paper versions available?

Find the documents at:
https://www.PCISSC.org/Merchants
PCI Resources for Securing Payment Data

**PEOPLE**
Hire qualified and trusted partners and train your staff to understand payment data security essentials.

**PROCESS**
Put the right policies and practices in place to make payment security a priority every day.

**TECHNOLOGY**
Make sure you are using the right technology and implementing it correctly to get the best security and business benefits.

Learn more about the PCI Data Security Standard (PCI DSS)
Learn more about secure technology
Learn more about training and qualified security professionals
People: Qualified Integrator and Reseller™
What Types of Organizations Employ QIRs?

- Certified POS Technicians
- Merchants
  - Retail
  - IT
  - Hospitality
  - Healthcare
  - Restaurant
- Financial Institutions
- Processors
- Service Providers
Who Becomes a QIR?

Technician
Integrator
Developer
Engineer
Implementer
Installer
Reseller
Software
What Do QIRs Actually Do?

• Ensure installation is implemented in a manner that addresses high-priority risks
• Protect confidential and sensitive information
• Support investigations by PCI Forensic Investigators
• Ongoing support/maintenance is in accordance with both application vendor guidance and PCI DSS
Key Security Controls for QIRs
QIR Value

- Recognition of criticality of security controls applied during installation
- Merchant trust in the quality, reliability and consistency of work
- Part of larger community of security professionals
QIR Value

- Industry recognized credential that follows the individual
- Public recognition of professional achievement
- Competitive career advantage
People: PCI Professionals
What Types of Organizations Employ PCIPs?

- Merchants
  - Retail
  - IT & Telecom
  - Hospitality
  - Finance
  - Food
- Financial Institutions
- Acquirers
- Service Providers
Who Becomes a PCIP?
What Do PCIPs Actually Do?

- Write/review PCI policies and procedures
- Owning and managing PCI DSS controls
- Work with ISA/QSA
- Advise internally on PCI projects
- Train staff on PCI DSS
- Input and maintenance of PCI processes
PCIP Value

• PCI DSS subject matter experts
• Confidence in interpreting requirements
• Ability to interact with other PCI entities
• PCI compliance often extends across many parts of an organization…
PCIP Value

• Become part of the PCIP Community
• Industry recognized credential that follows the individual
• Public recognition of professional achievement
• Competitive career advantage
Case Studies

Instructor-led PCIP training classes available

PCI PROFESSIONAL (PCIP)™ QUALIFICATION

The Payment Card Industry Professional is an individual, entry-level qualification in payment security information and provides you with the tools to build a secure payment environment and help your organization achieve PCI compliance. This renewable career qualification is not affected by changes in employment assignments and stays in effect as long as the individual continues to meet requirements. This three-year credential also provides a great foundation for other PCI qualifications.

- PCI SSC website under “Training and Qualification”
- Interested? Email us at PCIP@pcisecuritystandards.org
Other PCI Resources

https://www.pcisecuritystandards.org/document_library
PCI Guidance and Best Practices

- Building a security awareness program
- Protecting against malware
- Skimming prevention
- Defending against phishing attacks
- Working with third parties
- Maintaining PCI DSS compliance
- Accepting payments with a mobile phone
- PCI DSS compliance in the cloud
PCI Resource Center

Community Meeting
You are eligible to attend the annual PCI Community Meetings.

PCIP Newsletters
Get the quarterly PCIP Professional Update newsletter delivered to your inbox.

CPE Credits
Receive six (6) Continuing Education (CPE) credits for the 14-hour course, seven (7) for the instructor-led course.

Recognition
Get a PCI Professional certificate (suitable for printing and framing).

Exclusive PCIP Logo
You will be authorized to use the PCIP logo to create your own personal brand (use on resumes, email signatures and other professional communications).

Demonstrate Your Qualifications to the World
You will be included on a listing on the PCI website - searchable by name or certificate number.
Save the Date for 2019 Events

India
13 March
New Delhi, India

Latin America
15 August
São Paulo, Brazil

North America
17 – 19 September
Vancouver, BC, Canada

Europe
22 – 24 October
Dublin, Ireland

Asia-Pacific
20 – 21 November
Melbourne, Australia

events.pcisecuritystandards.org
Help Secure Payment Data
pcisecuritystandards.org
• Website: www.conexxus.org
• Email: info@conexxus.org
• LinkedIn Profile: Conexxus.org
• Follow us on Twitter: @Conexxusonline