Data Security
- Beyond Compliance

Hughes Team:
Bill Rumancik
David Henning
KJ Lian
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
Presenters

Conexxus Host
- Allie Russell
  Conexxus
  arussell@conexxus.org

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

Speakers
- Bill Rumancik
  Sr. Director
  Enterprise Solutions Marketing
- David Henning
  Sr. Director
  Network Security
  N.A. Division
- KJ Lian
  Sr. Director
  Solution Consulting
  Comcl & Franchise
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 Webinar Schedule

<table>
<thead>
<tr>
<th>Month</th>
<th>Subject</th>
<th>Speaker(s)</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 15 2016</td>
<td>Protect Your Fuel Dispensers Against Skimming</td>
<td>Doug Spencer Tim Weston Luke Grant Gray Taylor</td>
<td>NACS Wayne Gilbarco Conexxus</td>
</tr>
<tr>
<td>January 2017</td>
<td>Visa Level 4 Merchant Requirements Eff 1/31/17: PCI DSS Validation &amp; QIR Technician Requirements</td>
<td>Stewart Fey</td>
<td>LBMC</td>
</tr>
<tr>
<td>February 2017</td>
<td>How Stores Comply with Updated PCI Version</td>
<td>Tabitha Greiner Kimberly Ford Branden Williams</td>
<td>Acumera Valero DBA, CISSP, CISM</td>
</tr>
<tr>
<td>March 2017</td>
<td>SIEM Presentation</td>
<td>Matt Bradley</td>
<td>EchoSat</td>
</tr>
<tr>
<td>April 2017</td>
<td>Internet of Things &amp; Impact of Bring Your Own Device to the Workplace</td>
<td>Bradford Lowey Jeff Gibson</td>
<td>Wayne Fueling EchoSat</td>
</tr>
<tr>
<td>May 2017</td>
<td>Customer Engagement Technologies to Enhance Sales and Profitability</td>
<td>Ed Collupy Gray Taylor Lesley Saitta</td>
<td>W. Capra Conexxus Impact 21</td>
</tr>
</tbody>
</table>
2017 Conexxus Annual Conference
Loews Annapolis Hotel
Annapolis, Maryland
April 23 – 27, 2017
KJ Lian  
Senior Director  
Solution Consulting, Commercial and Franchise  

- More than 20 years in the information technology industry  
- Leads Solution Consulting for retail petroleum, QSR/casual dining, oil, and gas  

https://www.linkedin.com/in/kj-lian-4a9a341

Bill Rumancik  
Senior Director  
Enterprise Solutions, Marketing  

- Over 20 years of experience in WAN and managed services  
- Focusing on technology trends impacting distributed branch industries  

https://www.linkedin.com/in/williamrumancik

David Henning  
Senior Director, CISSP  
Network Security, North America Division  

- 17+ years of experience in Network Security  
- Hughes PCI Internal Security Auditor and SOC Director  
- Ensures managed services are secure and compliant while assisting customers with security-related questions  

https://www.linkedin.com/in/david-henning-5413572
Hughes® Business Focus: To Connect

PCI DSS
Consumer
Level-1 Merchant

PCI DSS
Enterprise
Level-1 Service Provider

http://www.visa.com/splisting

<table>
<thead>
<tr>
<th>COMPANY</th>
<th>SERVICE PROVIDER TYPE</th>
<th>VALIDATION TYPE</th>
<th>SERVICES</th>
<th>VALID THROUGH DATE</th>
<th>ASSESSOR</th>
<th>REGION OF OPERATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hughes Network Systems</td>
<td>AGENT</td>
<td>PCI/DSS</td>
<td>PCI DSS Services</td>
<td>Sep 30, 2016</td>
<td>Internet Security Systems, a wholly owned IBM Company</td>
<td>U.S., CAN</td>
</tr>
</tbody>
</table>
Does being compliant mean you are secure?
Breached

- Third-party HVAC company opened virus-laden email attachment
  - ~40M card numbers stolen
  - Validated as “PCI-compliant” 2 months before the breach

Breached

- Stolen third-party vendor credentials then malware installed
  - ~56M card numbers stolen
  - Preventative MS Windows security update was available but had not been installed
Breached

- Malicious code entered through MICROS support/ticketing portal
- August 2016, 700+ infected systems in Retail Division at Oracle
- Impact yet to be determined

300K+ POS locations world-wide
Evolving Cybercrime Threat Landscape

FACTORS CONTRIBUTING TO COMPROMISE

- Remote Access: 17%
- SQL Injection: 13%
- Misconfiguration: 12%
- File Upload: 12%
- Phishing/Social Engineering: 12%
- Malicious Insider: 10%
- Code Injection: 8%
- OS App Server: 7%
- Weak Password: 7%
- Other: 7%

- More than $1B stolen in last few years

- Organized Criminals: Intelligent, Creative, Relentless

- Conexxus Protecting Retail ATMs

- Map of Carbanak targets

- – 2015, Trustwave on Cybercrime

- – 2016, C2 Data, KrebsonSecurity
Compliant

- Set of requirements were in place at a given point in time (typically only yearly)
- Does not mean you, the brand, or your customers are safe
- Is not a blueprint for overall security
- Simple “check box” resulting in a minimal baseline of protection

you must go beyond...
- Cost of fines and remediation
- Personal revenue and customer loyalty
- Brand reputation
- Fellow owner/operators
- Sensitive information (PII, CCN, etc.)

Biggest Financial Consequence Is Lost Business

Average Cost $221 per record

– 2016 Ponemon Report

IF A RETAILER EXPERIENCED A SECURITY BREACH; HOW LONG WOULD IT TAKE TO FEEL COMFORTABLE SHOPPING THERE AGAIN?

– 2014 Interactions Consumer Experience
PCI DSS Compliance

Applies to every company that
- Stores
- Processes
- Transmits
the cardholder’s information

<table>
<thead>
<tr>
<th>Merchant</th>
<th>Transactions and Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>&gt;6M/year, AoC, RoC by QSA, Quarterly ASV</td>
</tr>
<tr>
<td>Level 2</td>
<td>1M–6M/year, SAQ, Quarterly ASV, AoC</td>
</tr>
<tr>
<td>Level 3</td>
<td>20K–1M/year, SAQ, AoC, Quarterly ASV</td>
</tr>
<tr>
<td>Level 4</td>
<td>&lt;20K/year, SAQ, Annual Scans</td>
</tr>
</tbody>
</table>

Payment Card Industry Data Security Standard

Required but not sufficient security

PCI EMPHASIZES THE WRONG THING: COMPLIANCE. WE DON’T CARE ABOUT COMPLIANCE, WE’RE FOCUSING ON RISK MITIGATION.
PCI: Event or Process?

Because of costs, retailers see PCI as event, not process-intended

- 15% of IT budget is spent on data security with 56% of that on PCI
- 93.6% of all victims were PCI-compliant within 12 months prior
- Only 9% regularly test security systems and processes (vulnerability scans, scan for rogue networks, integrity monitoring)

– 2015 IHL Group Store Survey

Compliance with the Payment Card Industry Data Security Standard (PCI DSS) continues to improve, but four out of five companies still fail at interim assessment. This indicates that they’ve failed to sustain the security controls they put in place.

– 2015 Verizon PCI Report
Establish IT Cybersecurity Governance

- Focus on **managing risk**, not just compliance audits

- **IT security and business goals/risk alignment**
  - Minimize “shadow IT” and “workarounds”

- **Proactively** monitor, evaluate, train, and adapt
  - No “wait and react”

---

Invest in Training

• Educate your employees **routinely**
  – Cooperation, not compliance

Trained users are the frontline with technology being your last line of defense

• **IT security, business, and personal**
  – Phishing emails
  – Social engineering
    • *Rogers Communications breach* (March ’15)
  – Policies and expectations
  – Ransomware
  – Antivirus, antimalware, in and current
  – Passwords
Passwords

No default passwords……ANYWHERE

Websites dedicated to default password lists

- IP cameras
  - https://ipvm.com/reports/ip-cameras-default-passwords-directory
- Firewalls, switches, IP phones, Wi-Fi APs, etc.
  - https://cirt.net/passwords

Password age

5 years: 47%
>10 years: 21%

– 2015, TeleSign Survey

NEVER share and

CHANGE often
Does This Look Familiar?
Backoffice PC with two NICs

- What’s wrong with this picture?
- Why is it dangerous?
- How do you fix this?

Internet Access

- Credit/Debit/Loyalty Traffic
- Nonpayment Traffic

Backoffice PC (collecting sales receipt)

Router

POS

Firewall
Better Solution
Backoffice PC with two NICs

Backoffice PC (Collecting sales receipt)

Router

POS

Firewall

Internet Access

Credit/Debit/Loyalty Traffic

Nonpayment Traffic
Does This Look Familiar?
Allowing access to security cameras via public static IPs

- What’s wrong with this picture?
- Why is it dangerous?
- Access being logged?
Network Segmentation

- Minimize attack surface through isolation
  - Isolating wired from wireless and inter-VLAN traffic
  - Isolating wireless devices (IoT) with weak security
    - Loss prevention cameras
    - HVAC thermostat, lighting, inventory tracking, sensors
  - Firewall to Internet
    - Not second NIC on manager PC or POS
  - Barring remote site-to-site communications
Remote Access

- Principle of **least privilege access**
  - Limited Internet, fixed IPs, minimal systems, and configuration
  - Minimize who uses remote desktop and POS access
    - Disable split-tunneling on remote access machines
  - Two-factor authentication
  - Logging
    - Reviews of the logs

Conexxus Guide to Remote Access Management
Partnerships for Success

- Managed security services partner

<table>
<thead>
<tr>
<th>Two-factor Authentication</th>
<th>Endpoint Protection</th>
<th>UTM, IDS/IPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall management</td>
<td>SIEM</td>
<td>Log analysis</td>
</tr>
</tbody>
</table>

- Technical expertise
  - Tools and facilities
- Shared experiences
- Cost-effective ROI
- Frees customer to focus on business
Layered Security Approach Is Best

- Combining **multiple** mitigating security measures
  - Defense in depth

- Rapidly evolving threat landscape
  - SME fail to accept as target: **45%**
  - Targeting SME: **60%–70%** of attacks

- Nearly **80%** of attacks are stopped by “combining standard security measures”
Have a Breach Incident Response Plan

1. Assign responsible owner/executive
2. Develop easily accessible quick-response guides for likely scenarios
3. Maintain relationships and processes with external providers
4. Ensure staff understands roles and responsibilities in event of cyber incident
5. Identify primary and secondary incident response individuals
Security is in Your Hands
December 15, 2016 @ 12:00 Eastern:
Protecting Your Fuel Dispensers Against Skimming