Internet of Things and Bring Your Own Device in your Business

Presenter:
Jeff Gibson, ControlScan
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

Speakers
Jeff Gibson
Dir Product Strategy, ControlScan
Jgibson@controlscan.com

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
## 2017 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 27, 2017</td>
<td>Third Party Risk Management: How to Identify and Manage Data Security Risks from your Vendors</td>
<td>Sam Pfanstiel</td>
<td>Coalfire Systems</td>
</tr>
<tr>
<td>August 31, 2017</td>
<td>Using the NIST Cybersecurity Framework to Guide your Security Program</td>
<td>Chris Lietz</td>
<td>Coalfire Systems</td>
</tr>
<tr>
<td>October 12, 2017</td>
<td>Things &amp; Impact of Bring Your Own Device to the Workplace</td>
<td>Jeff Gibson</td>
<td>ControlScan</td>
</tr>
<tr>
<td>December 2017</td>
<td>Conexxus: EB2B White Paper Presentation</td>
<td>TBD</td>
<td>EB2B WG</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>January 2018</td>
<td>Securing and Penn Testing your Mobile Payment App</td>
<td>Denis Sheridan</td>
<td>Citigal</td>
</tr>
<tr>
<td>February 2018</td>
<td>Unified threat management: What is it and why is it important?</td>
<td>Thomas Duncan</td>
<td>Omega</td>
</tr>
<tr>
<td>March 2018</td>
<td>Penetration Testing: How to Test What Matters Most</td>
<td>Sam Pfanstiel &amp; Coalfire Lab Personnel</td>
<td>Coalfire</td>
</tr>
<tr>
<td>May 2018</td>
<td>QIR Program Update</td>
<td>Chris Bucolo</td>
<td>ControlScan</td>
</tr>
</tbody>
</table>
At the NACS Show
October 17-20, 2017
Chicago, IL
Booth 4384
IoT – Internet of Things

IoT is the network of physical objects – devices and embedded sensor systems that enables these objects to collect and exchange data over the internet.
Gartner, Inc. forecasts that 8.4 billion connected things will be in use worldwide in 2017, up 31 percent from 2016, and will reach 20.4 billion by 2020. Total spending on endpoints and services will reach almost $2 trillion in 2017.

"IoT services are central to the rise in IoT devices,"

Source: Gartner News Room
IoT in Retail

• Customer Experience
  – Customer engagement
  – Buying habits
  – Loyalty programs
  – Automated checkout

• Operations
  – Energy management
  – Equipment management
  – Inventory Management
  – Security
Source: LinkedIn Redefining Smart Retail
Business Relevance

Detect
Data about every visitor

Connect
Optimized for branding

Engage
Real-time location based apps
Consumer Analytics = Interesting Data
Internet of Things - Infrastructure

Source: RTC Magazine
Integrating the Internet of Things (IoT) into your business requires robust security measures. Here are some key considerations:

- **Endpoints**
  - Protect data at rest and in transit
  - Security policies
  - Patch management
  - Restrict access

- **Network**
  - Segment endpoints
  - Restrict access to known destinations
  - Monitor network traffic
  - Intrusion prevention and detection systems

- **Cloud Providers**
  - Security policies
  - Authentication
  - Data Rights

- **End-user applications**
  - Security policies
  - Scalability
  - Authentication

By implementing these strategies, you can enhance the security of your IoT ecosystem and protect your business assets effectively.
What are we wanting to accomplish?
Who needs to be involved?
What are the risks?
When does it need to be completed?

✓ Evaluate multiple vendors
✓ Involve other departments early on
✓ Clearly define the scope of the project
✓ Develop an implementation plan
Resources

IoT Analytics: https://iot-analytics.com
IoT Newsletter: https://iotnewsletter.org/
IoT Central: https://www.iotcentral.io/
IoT Security Foundation: https://www.iotsecurityfoundation.org
Gartner: http://www.gartner.com
BYOD – Bring Your Own Device

Traditional Definition: The policy of permitting employees to bring personally owned devices to their workplace, and to use those devices to access privileged company information and applications.
BYOD Drivers

- Improved employee mobility: 61%
- Greater employee satisfaction: 56%
- Increased employee productivity: 55%
- Reduced cost: 47%
- Reduced security risk: 21%
- Employee privacy: 16%
- Other: 5%

BYOD Adoption Today

- 40% BYOD is available to all employees
- 32% BYOD is available to select employees
- 13% We have no plans to support BYOD
- 9% We do not support BYOD, but plan to start in the next 12 months
- 3% BYOD was tried but abandoned
- 3% Other

BYOD - Risks

- Employees are their own Administrators
- May not always be used by the employee
- May not have endpoint protection
- Updates may not always be maintained
- Wireless Access Point connection
- Application features enabled may pose security risks
- External Cloud based storage solutions
- Increase in Malware
- Lost / Stolen device
BYOD Planning

• Eligibility
• Devices
• Accessibility
• Employee Communication
• Costs
• Security and Compliance
• Support and Maintenance
EMM – Enterprise Mobility Management

An all-encompassing approach to securing and enabling employee use of smartphones and tablets. Typically involves some combination of mobile device management (MDM), mobile application management (MAM) and mobile information management (MIM).
BYOD – Beyond Employees

- Vendors
- Contractors
- Mobile payments
- IoT Devices
- Inventory
What are the supported devices?
What access is needed?
Who are the vendors?
How easy is it to deploy?

✓ Evaluate multiple vendors
✓ Clearly define the scope of the project
✓ Evaluate all costs
✓ Develop an implementation plan
• Website: www.conexxus.org
• Email: info@conexxus.org
• LinkedIn Group: Conexxus Online
• Follow us on Twitter: @Conexxusonline