C-Stores as Critical Infrastructure: Cyber Resilience in a Multi-vendor Environment

Presenters:

Ashwin Swamy, Omega ATC

Greg DeClue, Omega ATC

Your Host:
Allie Russell

Standards Coordinator, Conexxus
arussell@conexxus.org

Your Moderator:
Kara Gunderson

Chair, Data Security Committee
Director of Payment Card Operations
CITGO Petroleum | kgunder@citgo.com

Agenda

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

Housekeeping

This webinar is being recorded and will be made available on Conexxus365.org

Participants

- Ask questions via webinar interface
- Please, no vendor specific questions
- Our webinars may be used toward PCI continuing education credits. Please contact 365@conexxus.org for questions regarding a certificate of webinar attendance.

Interested in speaking or sponsoring a Conexxus365 event?
Contact 365@conexxxus.org to discuss upcoming opportunities with our team.

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.

Thank you to our 2021 Diamond Sponsors!

Bulloch TECHNOLOGIES INC.
www.bullochtech.com

GILBARCO VEEDER-ROOT

HUGHES
An EchoStar Company

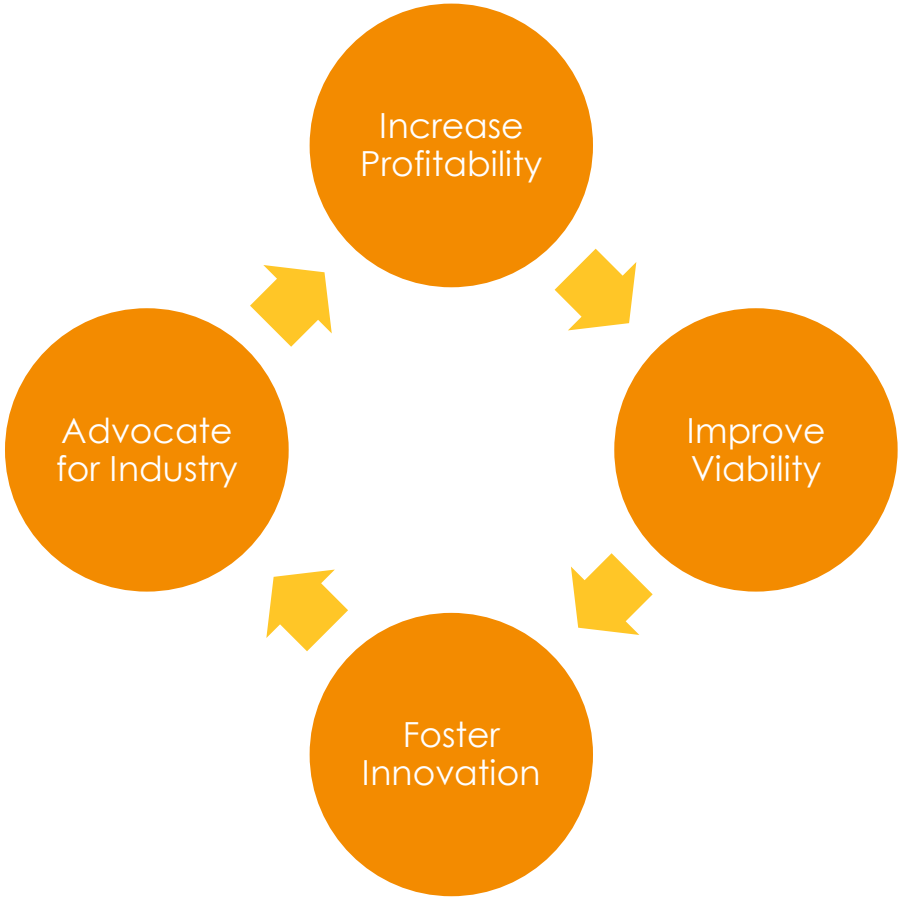
Mako NETWORKS

NACS

PDI

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 365

CONEXXUS solve forward

Upcoming Conexxus365 Schedule

Date	Topic	Event Type	Speaker	Sponsor
February 25, 2021	C-Stores as Critical Infrastructure – Cyber Resilience in a Multi-Vendor Environment	Free Webinar	Ashwin Swamy Greg DeClue	Omega ATC
March 4, 2021	TruAge™: The NACS Age Verification Initiative	Free Webinar	Gray Taylor	Conexxus
March 11, 2021	Autopsy of the SolarWinds Attack and Modern Malware Weaponization	Free Webinar	Danny Harris	Security Innovation
April 15, 2021	New Directions for Customer Loyalty	Content	Bill Hanifin Jeannie Amerson	Impact 21

Connect with Conexxus

www.conexxus365.org

365@conexxus.org

www.conexxus.org

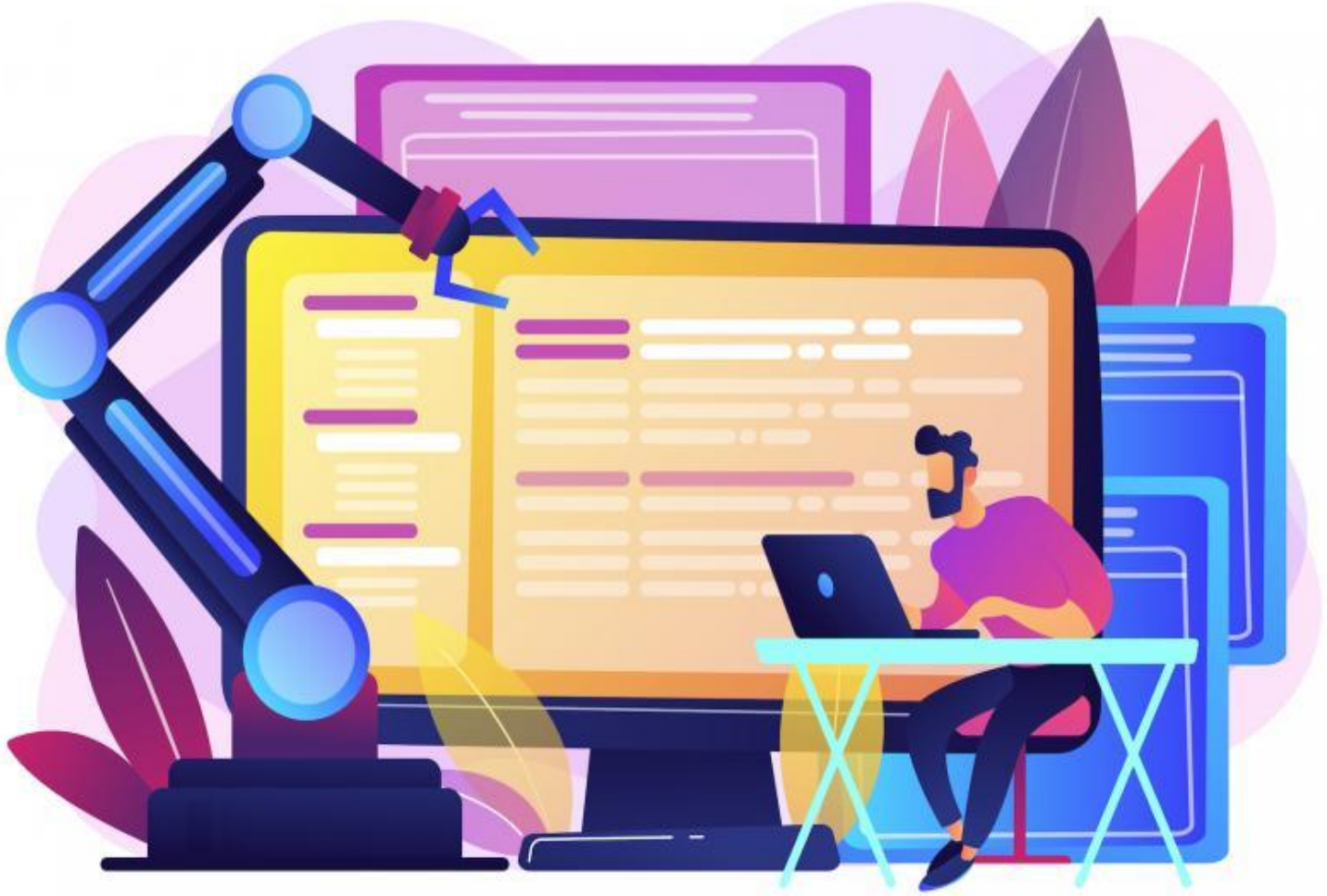
info@conexxus.org

Presenter:
Ashwin Swamy

Director of Cyber Resilience, Omega ATC
ashwin.swamy@omegaatc.com

Presenter:
Greg DeClue

Cyber Operations Manager, Omega ATC
greg.declue@omegaatc.com



C-Stores as Critical Infrastructure: Cyber Resilience in a Multi-vendor Environment

CONEXXUS 365

CONEXXUS solve forward

Critical infrastructure (including cyber-physical systems) are easy targets with severe impacts when compromised

- **December 2015 –** Ukrainian regional electricity grid was brought down by a cyberattack that leveraged BlackEnergy malware. Up to 230,000 customers lost power.
- **April 2020 –** Attempted cyberattack on Israeli water infrastructure – treatment plants, pumping stations, sewers
- **February 2021 –** Oldsmar, Florida water supply nearly contaminated; old Windows operating systems and poor password security were seen as a potential source of compromise. TeamViewer used for the remote access to the systems.

The SolarWinds breach carries several implications for convenience retail

Deeper coverage of the Solarwinds Orion breach in the Conexxus March 2020 presentation. However, there are some immediate takeaways as the breach pertains to convenience retail:

1. The Software Supply Chain (and overall supply chain) continues to pose a risk. Malicious behavior, unfortunately, can therefore come from trusted applications and networks which may not be detected by SIEMs and firewalls.

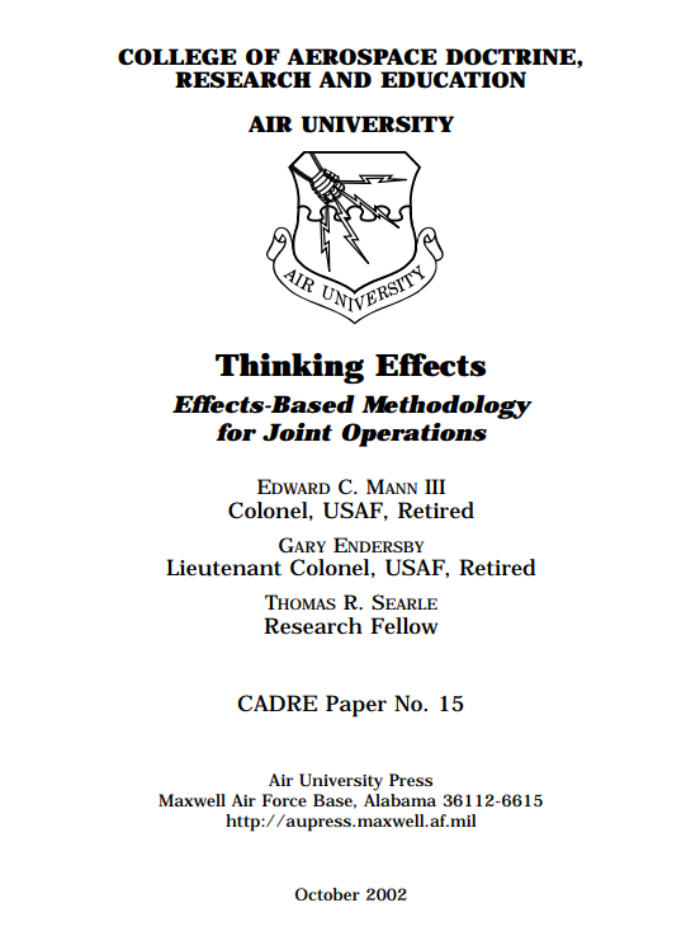
2. Breaches can and often do go unnoticed for extended periods of time, buying hackers time to compromise a wide range of networks and systems. There are always unknown unknowns.

3. We must be prepared to respond quickly, effectively, and at scale; multiple vendors, including FireEye, released monitors for detecting the presence of compromised tools to deploy on endpoints.

Attacks on critical infrastructure can cause multiple orders of effects on US systems

Advanced cyber attacks fit into a larger strategy of US adversaries. Effects are considered well ahead of time.

"For example, a bridge may be physically destroyed. As a result, the bridge is no longer functional, and its lack of functionality degrades the transportation system. Furthermore, the loss of the bridge may have a psychological impact on the adversary, especially if it was one of the primary avenues of escape or retreat in the face of advancing military forces. The important aspect is to develop a better understanding of the inherent interrelationship of effects and to incorporate this understanding into planning, execution, and assessment of operations."



COLLEGE OF AEROSPACE DOCTRINE, RESEARCH AND EDUCATION

AIR UNIVERSITY

Thinking Effects

Effects-Based Methodology for Joint Operations

EDWARD C. MANN III
Colonel, USAF, Retired

GARY ENDERSBY
Lieutenant Colonel, USAF, Retired

THOMAS R. SEARLE
Research Fellow

CADRE Paper No. 15

Air University Press
Maxwell Air Force Base, Alabama 36112-6615
http://aupress.maxwell.af.mil

October 2002

Are we ready to go toe-to-toe against today's threats?

What must change, industry-wide, for us to be as prepared as possible?

C-Stores as Critical Infrastructure: Cyber Resilience in a Multi-vendor Environment

C-stores as Critical Infrastructure

Challenges of Security Response in a Multi-vendor Environment

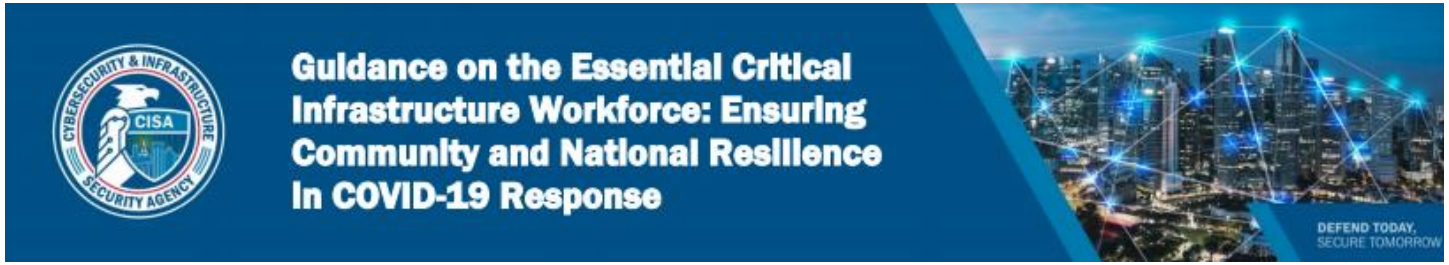
Strategies for Creating Alignment Between Third-Party Vendors

Preparing for ”Constant Response” with Third-party Vendors

C-Stores as Critical Infrastructure

1. C-stores are considered part of US critical infrastructure
2. PCI is not the goldmine for most advanced cyberattackers
3. The attack surface is increasing
4. Secondary effects of a targeted campaign against the industry could have severe consequences

We must think about convenience retail as U.S. critical infrastructure



In May 2020, Department of Homeland Security updated the Cybersecurity and Infrastructure Security Agency (CISA) guidance (v3.1) in identifying essential critical infrastructure workforce. Convenience stores were added to the list, and the following key businesses were recognized as essential:

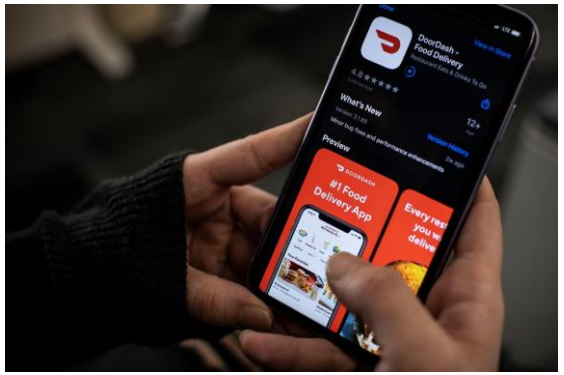
- Retail fuel centers, such as gas stations and truck stops, and the distribution systems that support them
- Retailers that sell food and beverage products
- Restaurant carry-out and quick-serve food operations
- Food manufacturer employees and their supplier employees
- Employees and firms supporting food, feed and beverage distribution, including warehouse workers, vendor-managed inventory controllers and blockchain managers”

https://www.cisa.gov/sites/default/files/publications/Version_3.1_CISA_Guidance_on_Essential_Critical_Infrastructure_Workers_0.pdf

The attack surface continues to increase in the c-store environment

In-store card data environment is no longer the only target. Today's environment goes beyond brick-and-mortar.

- Fuel Dispensers
- ATG's
- Back Office PC's
- IoT devices
- E-commerce



Targeted advanced attacks on c-stores could have first order, second order, and third order effects on US systems

FIRST ORDER | Supply Chain Interruption

- Refiner, Distributor, Hauler, Retailer - any interruption can cause fuel shortages

---

SECOND ORDER | Impacts on transportation, creation of chaos

- Traffic Bottlenecks

THIRD ORDER | Distraction, Loss of Trust, Hoarding

- Creating a sense of resource scarcity, which at an extreme, is capable of causing civil unrest

C-Stores as Critical Infrastructure: Cyber Resilience in a Multi-vendor Environment

C-stores as Critical Infrastructure

Challenges of Security Response in a Multi-vendor Environment

Strategies for Creating Alignment Between Third-Party Vendors

Preparing for ”Constant Response” with Third-party Vendors

Challenges of Security Response in a Multi-vendor Environment

1. Agility is a must; vendor gaps and bottlenecks prevent this
2. Lack of alignment in systems management can create security risks
3. Vendors are not typically aligned well-enough to conduct effective security response in-tandem
4. Business continuity measures are currently an afterthought and carried out in silos.

The multi-vendor retail environment presents a catch-22 that must be addressed

Operational necessity of a multi-vendor environment

- Different levels of control on different systems
- Completely different replacement rates (due to cost or vendor support/maintenance timelines)
- Necessity to reduce overhead and simplify operations
- Necessity to innovate and meet consumer demands, which requires the help of many parties

…creates unique security challenges

- Disparately managed Systems
- At times, misaligned incentives that reduces responsibility
- Slow or completely lacking coordination in security response
- Business continuity and disaster recovery strategies that fail on both accounts

Lack of alignment in systems management creates significant security challenges

Siloed maintenance and preparation

Data Siloing - many areas to go pull updates and patches from.

Expense - willing to replace out of date equipment that still works and time needed to correctly manage - Resource Intense

Performance - Minimizing outages to systems while upgrading and Collateral damage to other systems after upgrade

Assuming the risk and liability when maintenance is not done

…creates security challenges

System vulnerabilities

Network vulnerabilities

Poor user access management

Third-parties are not sufficiently aligned to coordinate effective security response and BCDR measures

- ✗ Minimal sharing of security data between vendors
- ✗ Near-zero ongoing communication between vendors
- ✗ Misaligned incentives
- ✗ No helpdesk alignment
- ✗ Disagreements about scope
- ✗ Minimal transparency into environment itself
- ✗ Not involved in overall planning and necessary internal exercises (e.g. business continuity planning)

Summary – key issues that must be addressed to ensure effective security response and overall resilience

CHALLENGES TO BE OVERCOME

SILOED SYSTEMS MANAGEMENT

Gap between vendors in systems management processes (updates, configurations, etc.)

MINIMAL PROCEDURES AND COMMUNICATION FLOWS NECESSARY FOR MULTI-VENDOR SECURITY RESPONSE

Third-parties do not have direct contacts, common data standards, or helpdesk integration

MISALIGNED INCENTIVES

Everyone wishes to reduce responsibility, but many merchants are ultimately depending on the vendor to handle security

BUSINESS CONTINUITY IS AN ATERTHOUGHT

BCDR planning is not coordinated between vendors and third-parties; this means it's not actionable whatsoever.

C-Stores as Critical Infrastructure: Cyber Resilience in a Multi-vendor Environment

C-stores as Critical Infrastructure

Challenges of Security Response in a Multi-vendor Environment

Strategies for Creating Alignment Between Third-Party Vendors

Preparing for ”Constant Response” with Third-party Vendors

Strategies for creating alignment between third-parties

1. Properly evaluate service providers ahead of time
2. User access management and zero-trust approaches are critical for reducing risks
3. Must actively form a cohesive unit which may consist of multiple organizations
4. Integrate data and systems to help coordinate response activities
5. Community-driven communication

Tip #1 – Select and evaluate third-party service providers thoroughly (see PCI 12.8 and 12.9)

Some questions to consider when vetting software vendors:

- ✓ Number of years in business?
- ✓ Do they background check employees?
- ✓ Incident response (IR) plan in place?
- ✓ What is included in the IR plan?
- ✓ BBB rating?
- ✓ PCI roles and responsibilities matrix?
- ✓ Have they previously been breached?

12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	**12.8.3** Verify that policies and procedures are documented and implemented including proper due diligence prior to engaging any service provider.	The process ensures that any engagement of a service provider is thoroughly vetted internally by an organization, which should include a risk analysis prior to establishing a formal relationship with the service provider. Specific due-diligence processes and goals will vary for each organization. Examples of considerations may include the provider's reporting practices, breach-notification and incident response procedures, details of how PCI DSS responsibilities are assigned between each party, how the provider validates their PCI DSS compliance and what evidence they will provide, etc.

PCI DSS Requirements	Testing Procedures	Guidance
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	**12.8.4** Verify that the entity maintains a program to monitor its service providers' PCI DSS compliance status at least annually.	Knowing your service providers' PCI DSS compliance status provides assurance and awareness about whether they comply with the same requirements that your organization is subject to. If the service provider offers a variety of services, this requirement should apply to those services delivered to the client, and those services in scope for the client's PCI DSS assessment. The specific information an entity maintains will depend on the particular agreement with their providers, the type of service, etc. The intent is for the assessed entity to understand which PCI DSS requirements their providers have agreed to meet.
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	**12.8.5** Verify the entity maintains information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	

CONEXXUS 365

CONEXXUS solve forward

Tip #2 – Implement robust user access management policies with an eye towards zero trust

Network Segmentation

Least privilege access

User Access Management (2FA, logging, password management)

Security Training for all employees

- Phishing, Vishing

Firewall rules setup with clear business justification

Tip #3 – Actively get everyone on the same page and working together

It mus be an expectation that all third parties, and the retailer, take part in a collaborative process

Shared Contact Lists and then communicate

- Share information throughout the lifecycle of the program
- Ask questions directly when necessary
- Work on key IT activities (updates, deployments) together

Coordinated Program Management

- Coordinated security program management
- Coordinated compliance program management
- Coordinated BCDR program management

Centralize Secure Data

- Helpdesk, logs, site asset data

Tip #4 – Integrate Helpdesks

1. What email can alerts or tickets add as a CC which will then show up on other helpdesks?
2. Leverage APIs. Common fields must be in place in order to be able to interchange information. Which fields map to which between two systems?
3. Shared chat threats (Teams, Slack, Skype, etc.)
4. A little bit of asset management hygiene goes a long way. Common access to site asset data makes all the difference.
    a. Primary devices in the environment
    b. Serial numbers
    c. Operating Systems/Versions
    d. Base functionality
    e. Network diagram and requirements

Tip #5 – Be able to share data whenever required (PCI Requirement 10)

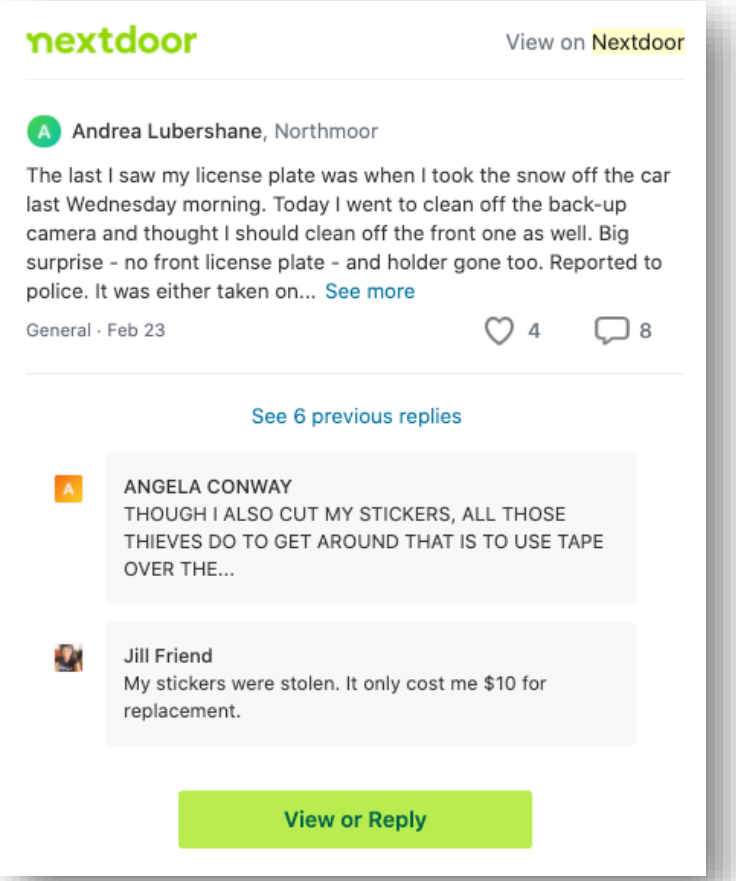
Use basic fields that can allow for clarity, for everyone:
Source System, Priority of the Log, Type of Log, Message, Time.

There's no time for data engineering when the "fit hits the shan."

1. It is critical to put log information into a common format so that all systems can read and ingest this information
2. Keep a "dictionary" or guide to know exactly which format you need log files in, in order to be able to ingest into your system. This allows you to be able to request precise information from multiple vendors that work in your environment.
3. You should be able to export to common format with basic fields (e.g. CSV) .

Date	Time	Facility	Level	Host Name	Message Text
2015-03-20	14:05:00	Cron	Warning	10.111.201.39	Logon failed
2015-03-20	14:05:00	Local1	Warning	10.111.201.39	Logoff Successful
2015-03-20	14:05:00	Local7	Critical	10.111.201.39	This is a test message generated by Kiwi SyslogGen
2015-03-20	14:05:00	Local1	Alert	10.111.201.39	Logon successful
2015-03-20	14:04:59	Cron	Error	10.111.201.39	Logon failed
2015-03-20	14:04:59	System1	Critical	10.111.201.39	Logoff Successful
2015-03-20	14:04:59	Syslog	Error	10.111.201.39	This is a test message generated by Kiwi SyslogGen
2015-03-20	14:04:59	System0	Critical	10.111.201.39	Logon successful
2015-03-20	14:04:58	Cron	Warning	10.111.201.39	Logon failed
2015-03-20	14:04:58	System2	Info	10.111.201.39	Logoff Successful
2015-03-20	14:04:58	User	Notice	10.111.201.39	This is a test message generated by Kiwi SyslogGen
2015-03-20	14:04:58	News	Debug	10.111.201.39	Logon successful
2015-03-20	14:04:57	Cron	Info	10.111.201.39	Logon failed

Tip #6 – Share new information about the threat landscape as often as possible. Community-driven intel is key.

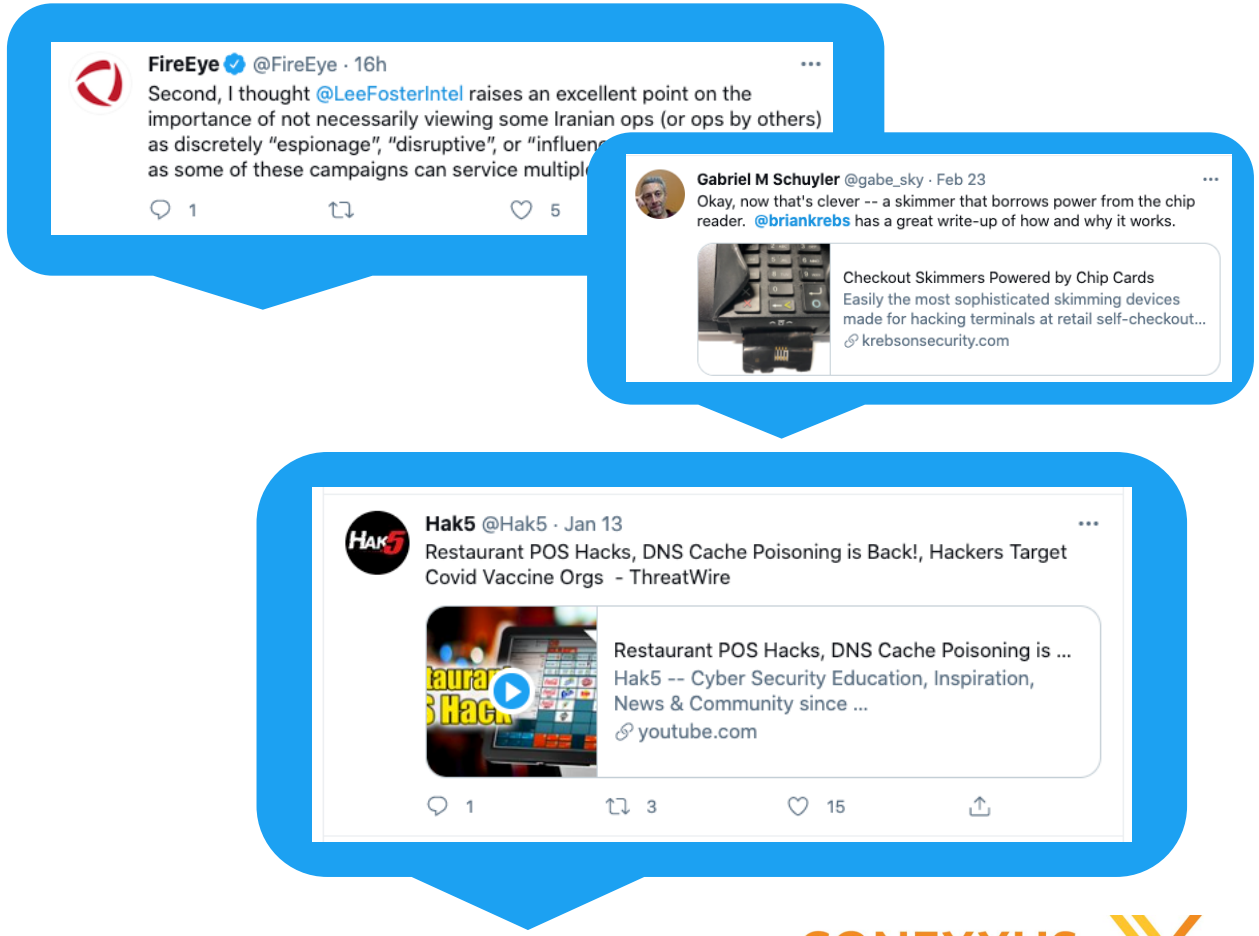


Threat intelligence feeds can help you stay on top of the latest threats

1. Retail and Hospitality Information Sharing Analysis Center | https://rhisac.org/
   Cybersecurity and Infrastructure Security Agency | https://www.cisa.gov/publication/ci-threat-info-sharing-framework
2. MITRE ATT&CK intrusion activity that are tracked by a common name | https://attack.mitre.org/groups/
3. Advanced Persistent Threat Groups | https://www.fireeye.com/current-threats/apt-groups.html -

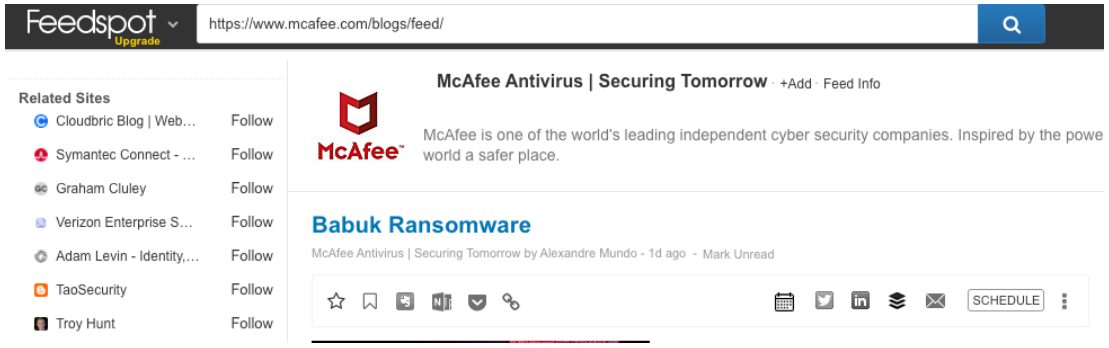
Twitter feeds are a great way to track major security events

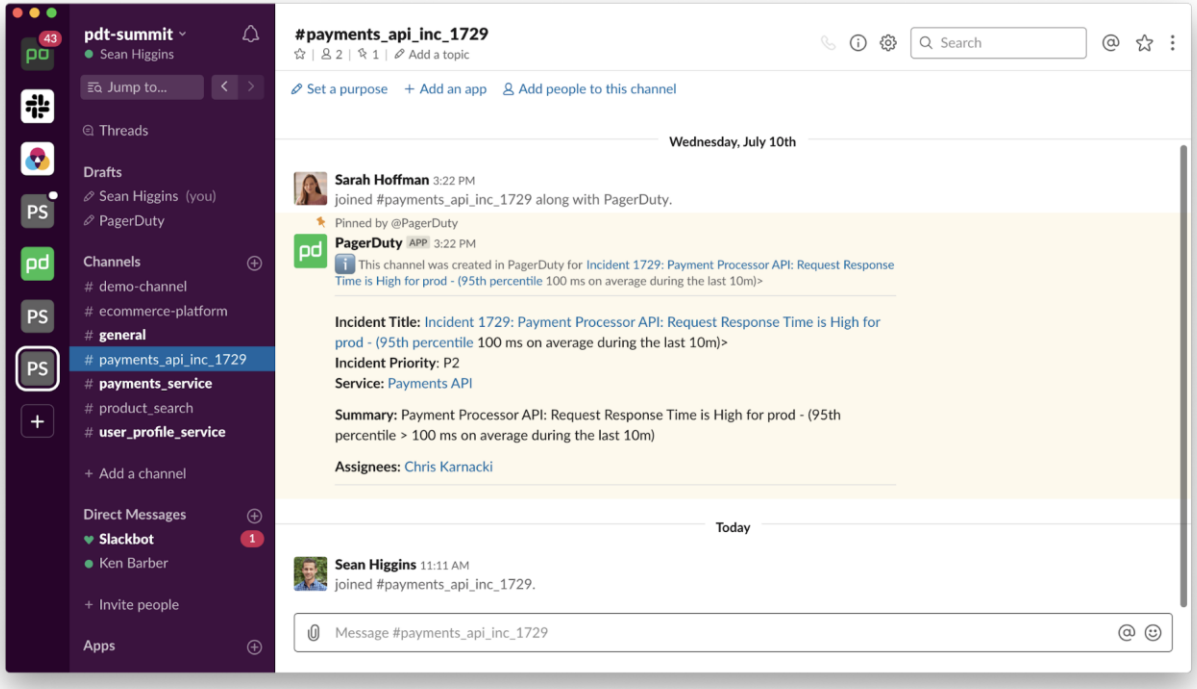
- Twitter is a fresh source of information around relevant compromises
- Pay attention to retweets, comments, and likes.
- If something is gaining traction, it is worth keeping an eye on.
- Simply follow security journalists, researchers, and select vendors for relevant reporting.



RSS feeds and chat channels can help you aggregate key security information

- Inter-organization group chat channels can be created for triage or sharing content.
- Blog content can be aggregated using RSS feeds, which can help curate what is most relevant





Summary - Strategies for Creating Alignment Between Third-Party Vendors

Vendor Management

Ensuring clearly defined responsibilities and a coordinated program with contact information shared, along with necessary buy-in, from all involved

Communication

Community-driven outlook on the threat landscape and security response keeps disparate teams ahead of the game and unified

Integration

Integrating data silos and helpdesks ensures that remediation and IR processes are efficient and transparent.

C-Stores as Critical Infrastructure: Cyber Resilience in a Multi-vendor Environment

C-stores as Critical Infrastructure

Challenges of Security Response in a Multi-vendor Environment

Strategies for Creating Alignment Between Third-Party Vendors

Preparing for ”Constant Response” with Third-party Vendors

Preparing for ”Constant Response” with Third-party Vendors

1. Must have the infrastructure for scalable detection and response on endpoints and networks
2. Must have a lab or test systems to ensure that deployments and updates can be carried out at speed
3. IR plans must continually evolve
4. Business continuity and disaster recovery must encompass the entire tech stack include necessary third-parties

Avoid Being the Ostrich!

- You can’t put your head in the sand and pretend you don’t see the problem.
- Any vulnerability or security issue in the environment impacts all other vendors; no more siloes.
- Stay vigilant, stay informed, stay resilient

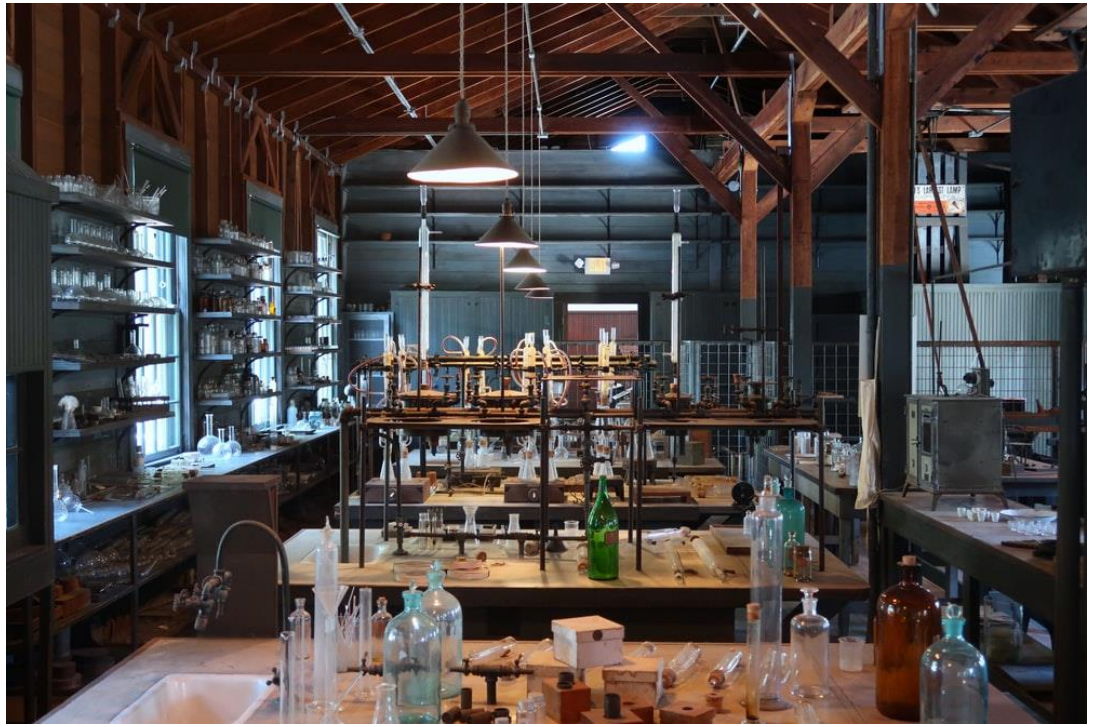
Get Your Necessary Detection and Response Mechanisms in Place

- Make sure to have extended detection and response (XDR) and SIEM tools in place that can aggregate data from the environment and detect on possible compromises.
- You must have the ability to run automations on the endpoint (kill scripts/vaccines, deployment of emergency monitors, scans, reboots, file quarantines, etc.)
- Central management of network infrastructure to run emergency firmware updates and firewall changes as needed.

Get Your Lab Ready!

Having access to production systems with updated configurations is critical for testing emergency updates, monitors, and scripts.

- Make sure the lab is as close to real-world as possible.
- Make sure the lab is as close to real-world as possible.
- If needed, have other vendors (including service contractors) take part in the testing process.



Continuously Improve and Update Your Incident Response and Disaster Recovery Plans

The biggest vulnerability in the IR process is laziness!

Update vendor contact list

- At the very minimum, IR plans should be updated annually; biannually is preferable.
- Establish SLAs with vendors that say, “every time X person is replaced/leaves, you MUST update us within 24 hours of who the new contact is.

Test IR plan with vendors annually

- Try calling/emailing and seeing what the response rate is. Be proactive.

Test disaster recovery LIVE

- Work through scenarios: if pump software goes down, what do you do? Payment processor?
- New systems need to be included in the IR/DR plan.
- You must test it out live; kick tires and break things.

Continuously Improve and Update Your Incident Response and Disaster Recovery Plans

The IR and BCDR process MUST consider the full the stack and all required vendors:

- Make sure clean ISO images can be provided to replacement equipment
- Service contractors should be ready to deploy hardware/software according to SLAs stated in BCDR plans
- Security operations vendors and networking vendors must ensure replacement devices are securely implemented and properly networked

Summary: Cyber Resilience in a Multi-vendor Environment

Avoid these scenarios

- **Ineffective or lacking security response in the face of modern threats**
- **Vulnerabilities in environment due to no alignment in systems management or responsibilities**
- **Business continuity plans that fail**

With the right strategy (and attitude!)

Program alignment: coordinated program management, open communication

Technical Alignment: integrations between helpdesks, data standards, lab environments

Comprehensive Policies: for incident response and business continuity/disaster recovery (BCDR) that accounts for the full tech stack and vendors

Presenter:
Ashwin Swamy

Director of Cyber Resilience, Omega ATC
ashwin.swamy@omegaatc.com

Presenter:
Greg DeClue

Cyber Operations Manager, Omega ATC
greg.declue@omegaatc.com

Stay Tuned for

Q&A

CONEXXUS 365

CONEXXUS
solve forward