RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: TECH-R04

Debunking “SOC Teams Vs. Vendors” in Cyber Firefights

Devon Bryan

Vice President, Global Technical Security Services (CISO)
ADP

Paul Davis

Director, Advanced Threats Security Solution Architects
Cisco
@Hypedupcat

#RSAC

Objective of Session

- Separate Fact From Fiction in Triaging Major Incidents
- Discuss The Role of Third Parties In Incident Handing
- Impart Lessons Learned From Cyber Firefights

Backgrounds

Devon Bryan

- Global CISO (Fortune 5)
- Federal Government (SES) Deputy Associate CIO Cybersecurity, IRS
- Capt USAF Comms Computer
- Strategist

cisco ADP

Paul Davis

- Director, Advanced Threats Security Solution Architects
- CISO (Fortune 5, critical infrastructure)
- Service Provider
- Solution Provider (software, hardware)
- IR
- SOC Builder and Strategist

When Ya Gonna Call?

- Visit From “3 Letter Agency”
- Somebody notices:
  - System Disruption
  - Suspicious Reboots
  - Strange Files
  - Unusual network traffic patterns
- A phone call from 3rd Party

Who Ya Gonna Call? No REALLY??

- What happens when something goes ‘bump’ in the ‘middle of the night’
  - Call Local Law Enforcement?
  - Call Federal Law Enforcement?
  - Call Ghost Busters? ☺

Teams

Customer
- Governance
- Business requirements
- Escalations
- Business expertise
- Compliance expertise

Process
Communications
Technology
Exchange

Service Provider
- Project/Program Management
- SLAs
- Escalations
- IT Security Expertise /authority
- SOC/IR Expertise

Vendor
- Communications
- Escalations
- Product Expertise

cisco ADP

Before The Breach….

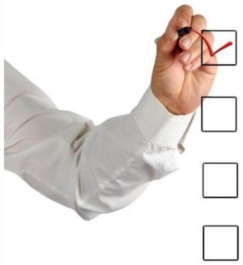
- The Plan….

- Contacts

- Agreements

- SLAs
- Skills Inventory

During The Breach…



Follow The Plan

“but adjust”

- Track Spend

Keep

Focused

- Call the right people in

Case Studies

- “Never get fired for hiring << company name>>”
- “This is Hollywood”

“Apply” Slide

- Today, write in your ToDo list for next week:
  - Schedule time to
    - Do an honest assessment of your security inventory (people, process, tech)
    - Review your service provider contracts
    - Reach out to your LE contacts, don’t be shy
- Within 3 months
  - Held a meeting that includes your IR team and the external IR team
  - Do a table top exercise
  - Build your Rolodex
  - Start building an outline of a plan

Q&A

Subhead if needed