Defining and Mitigating Cyber Risks to Reap the Benefits of IIoT

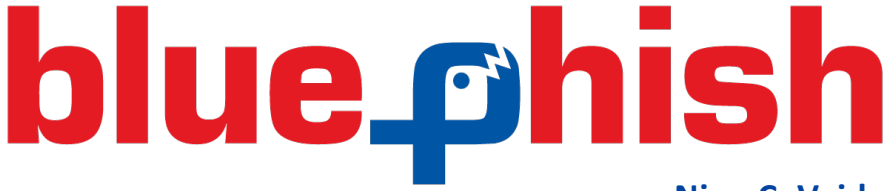
National Defense Industrial Association

Cybersecurity for Advanced Manufacturing Joint Working Group Forum

Lockheed Martin Global Vision Center

2121 Crystal Drive, Suite 100

Arlington, VA 22202-3706



Nina C. Vajda

November 15, 2016

Today's Topics:

- Terminology
- Stats & Facts
- OT / IT Roles and Responsibilities
- Benefits
- Challenges
- Attacker Motives – Industry Specific
- AaaS
- Act to Prevent the Attack

Terminology

- IIOT – Industrial Internet of Things – Network of physical objects that contains embedded technologies to sense, communicate and interact with an external environment for business operations
- IOT – Internet of Things – Same as IIOT, but specific to consumer and household products
- IOE – Internet of Everything – Used interchangeably with IIOT and IOT

Stats & Facts

- First IOT Device: ATMs (deployed for field testing mid-1970s)
- Social media estimates > 80% of population do not know what "IOT" means or references
- In 2008, the number of "connected" devices surpassed the number of people on Earth
- By 2020 it is estimated 50B devices will be I(I)OT connected

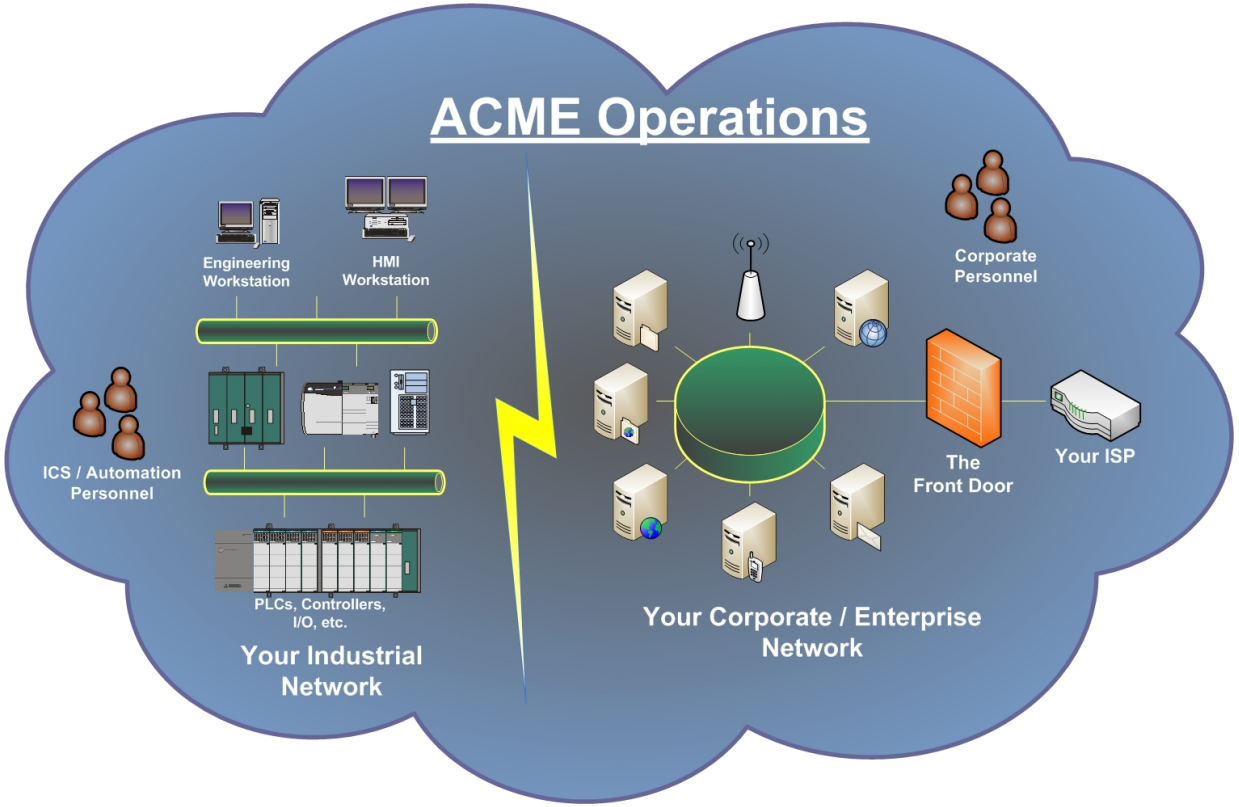
WHY? The ability to draw BIG Data from assets to establish decision support for innovation and technology enhancements

Stats & Facts

- By definition, an I(I)OT/E device must contain which seven(7) attributes?:
  1. Sensors
  2. Internet Connectivity
  3. Processors
  4. Energy Efficiency
  5. Cost Effectiveness
  6. Quality & Reliability
  7. Security

Source: Big Data, Big Ideas & Innovation, Technology, January 5, 2016

OT / IT – Who does what?



OT:

- Sensor & processor manufacturing

Corporate / IT:

- Internet connectivity

Joint:

- Define requirements and baselines for:
  - Energy Efficiency
  - Cost Effectiveness
  - Quality & Reliability
  - Security

Buckle Up!

Increased Connectivity equals
Additional Attack Surfaces which equals
> Risks

Benefits

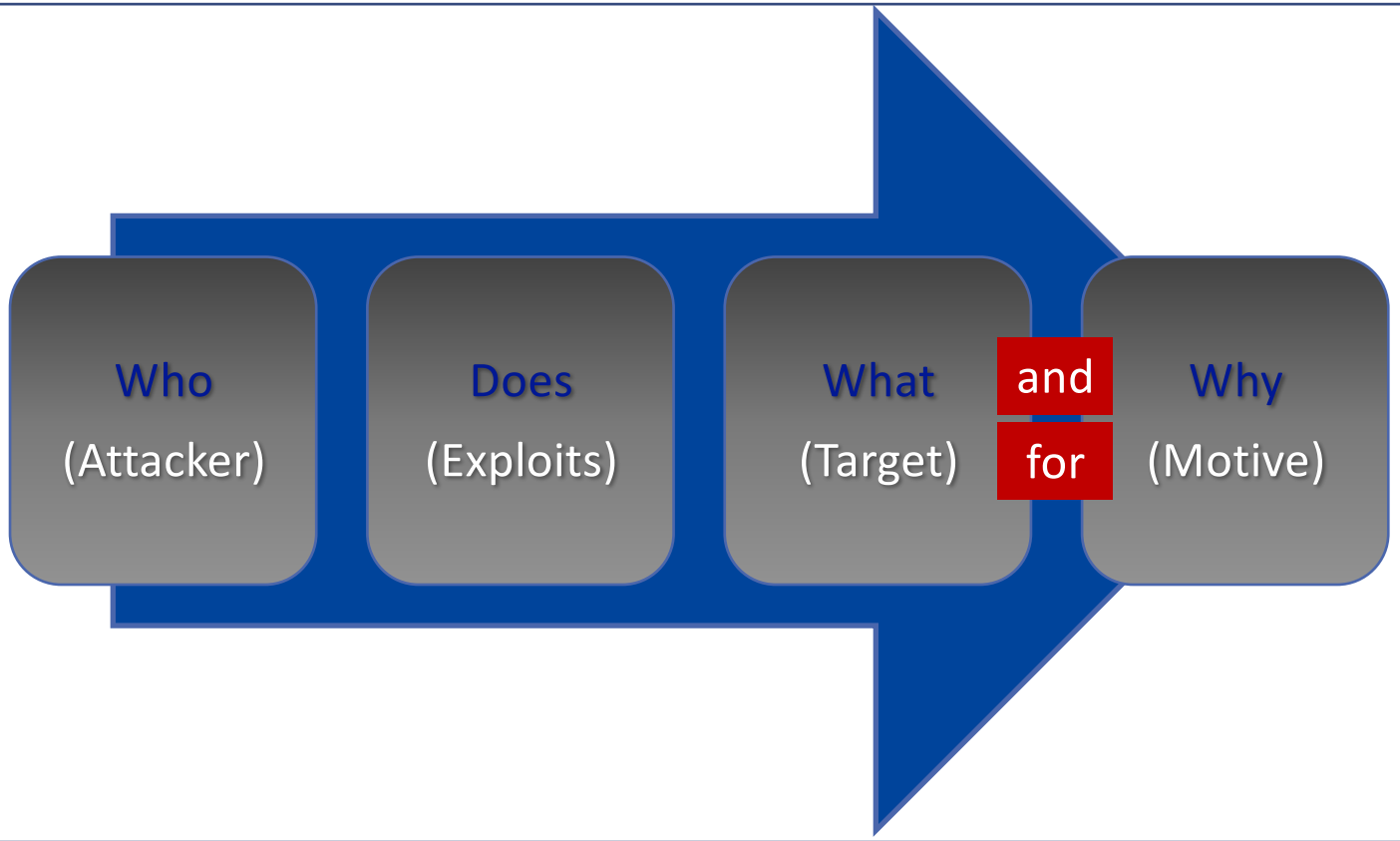
- Increased efficiencies for manufacturing uptime / downtime
- Streamline manufacturing processes
- Effective control production of field assets
- Increased efficiencies for monitoring impacts of production
- Increased production & quality
- Improved customer service response
- Increased network capabilities
- Lower risks attributable to improved troubleshooting and safety
- Streamlined maintenance
- Supply Chain optimization

Challenges

- It's a lot of data to store, move around, account for, analyze and SECURE.
- Must consider low bandwidth areas
- Performance and security issues associated with protocol translation and handoff (especially over Wi-Fi)
- Limited access to real-time updates

Estimated BIG data generation - 2.5B Gigabytes per day!

Attacker Motive

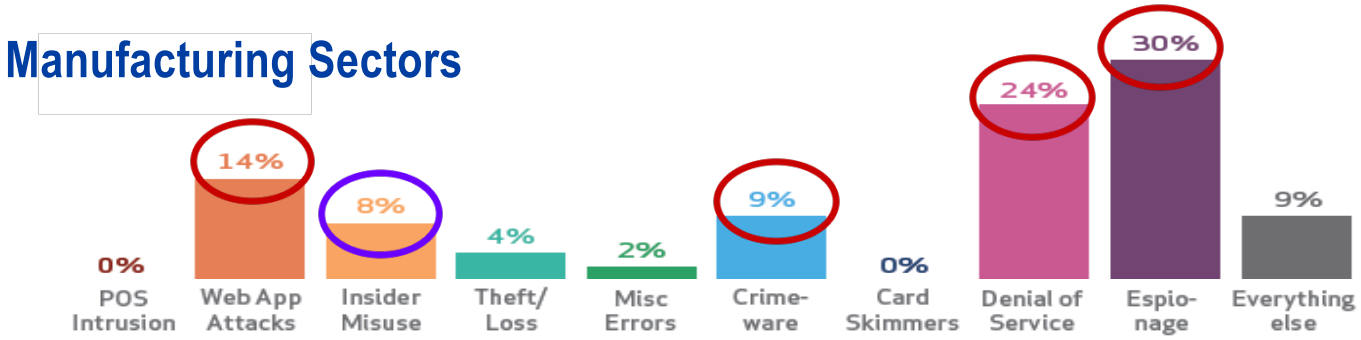


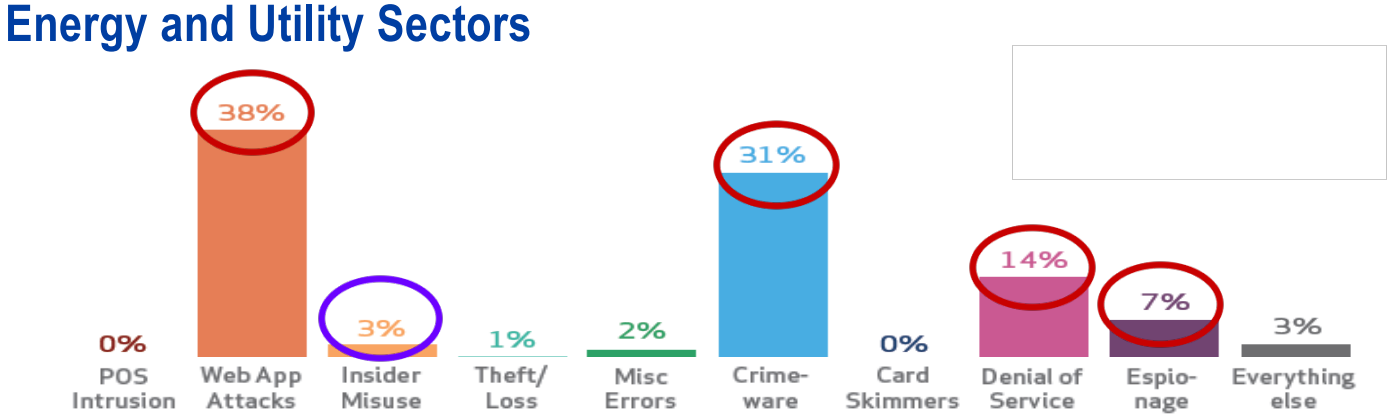
Cyber Attacks are Sector / Industry Specific

INDUSTRY	POS INTRUS-ION	WEB APP ATTACK	INSIDER MISUSE	THEFT/ LOSS	MISC. ERROR	CRIME-WARE	PAYMENT CARD SKIMMER	DENIAL OF SERVICE	CYBER ESPION-AGE	EVERY-THING ELSE
Accommodation [72]	75%	1%	8%	1%	1%	1%	<1%	10%		4%
Administrative [56]		8%	27%	12%	43%	1%		1%	1%	7%
Construction [23]	7%		13%	13%	7%	33%			13%	13%
Education [61]	<1%	19%	8%	15%	20%	6%	<1%	6%	2%	22%
Entertainment [71]	7%	22%	10%	7%	12%	2%	2%	32%		5%
Finance [52]	<1%	27%	7%	3%	5%	4%	22%	26%	<1%	6%
Healthcare [62]	9%	3%	15%	46%	12%	3%	<1%	2%	<1%	10%
Information [51]	<1%	41%	1%	1%	1%	31%	<1%	9%	1%	16%
Management [55]		11%	6%	6%	6%		11%	44%	11%	6%
Manufacturing [31,32,33]		14%	8%	4%	2%	9%		24%	30%	9%
Mining [21]			25%	10%	5%	5%	5%	5%	40%	5%
Professional [54]	<1%	9%	6%	4%	3%	3%		37%	29%	8%
Public [92]		<1%	24%	19%	34%	21%		<1%	<1%	2%
Real Estate [53]		10%	37%	13%	20%	7%			3%	10%
Retail [44,45]	31%	10%	4%	2%	2%	2%	6%	33%	<1%	10%
Trade [42]	6%	30%	6%	6%	9%	9%	3%	3%		27%
Transportation [48,49]		15%	16%	7%	6%	15%	5%	3%	24%	8%
Utilities [22]		38%	3%	1%	2%	31%		14%	7%	3%
Other [81]	1%	29%	13%	13%	10%	3%		9%	6%	17%

Source DBIR 2014

Cyber Attacks are Sector / Industry Specific





Source DBIR 2014

Anonymity as a Service (AaaS)

TOR / The DarkNet

What is TOR / DarkNet?

Developed for military use in 1994

- US Navy holds initial patent (1996) – NRL and DARPA funded

Resistant to eavesdropping and traffic analysis

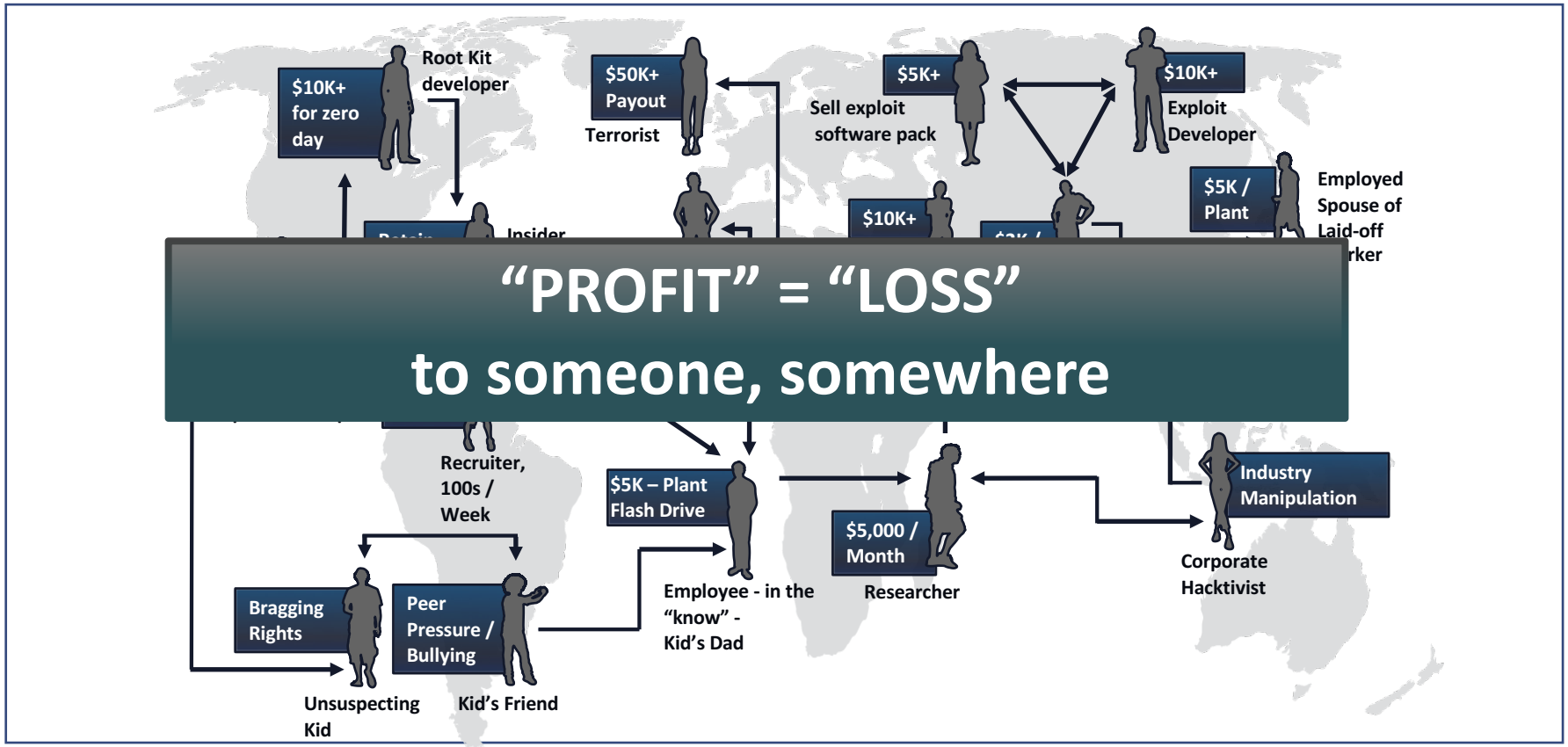
- Protects payl
- Hides count
- Prevents we
- Blocks ISP-d

Now a 501(c)(3) with

- Free softwa
- All platform
- Connections a
- 30 paid staff, 3K volunteers – GLOBALLY – that host the infrastructure assets
- 16 Gbps processed by 500K users daily
- 2012 Revenue $2.6M (up from $1.3M in 2011)

The de facto network for cyber espionage...

Anonymity as a Service (AaaS)

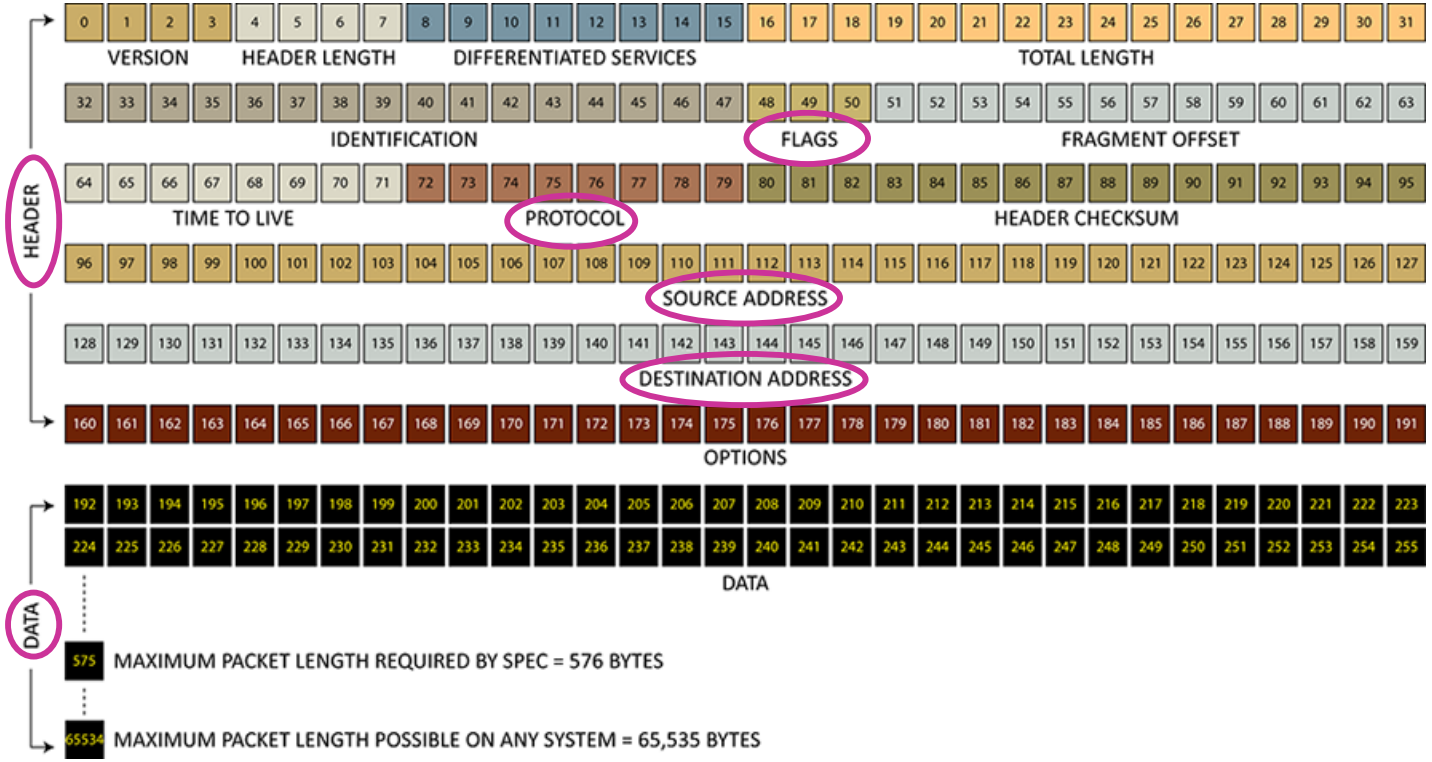


Conventional Networks

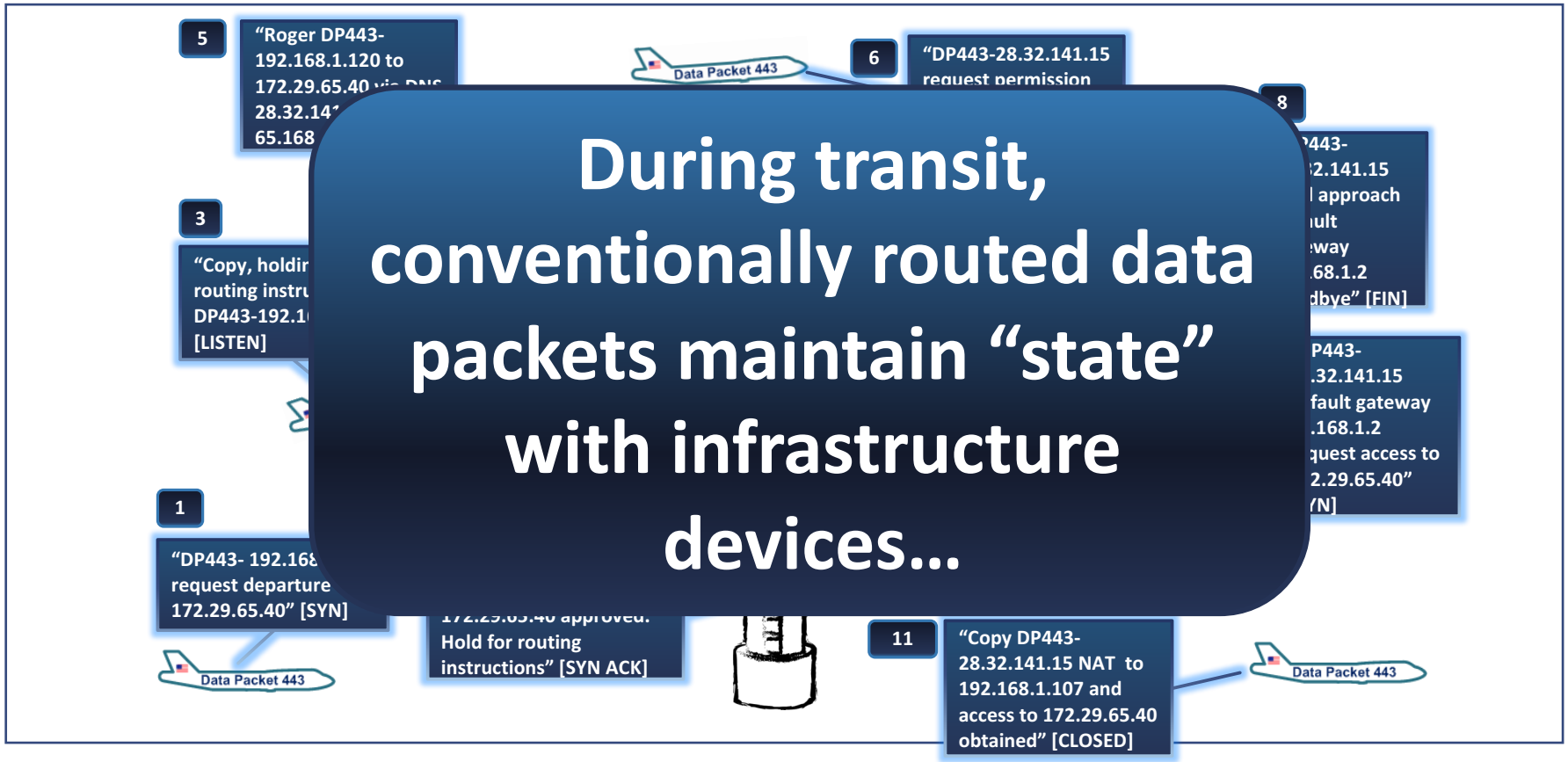
YOUR Network has "RULES":

- **Data packets have headers and a payload:**
  - **Headers have identifying information:**
    - ✓ **Who are you (IP Address, MAC, etc.)**
    - ✓ **Where did you start (Source Address)**
    - ✓ **Where are you going (Destination Address)**
    - ✓ **Where will you Pit-stop (Hops)**
  - **Payload is inspected / "protected" in transit and upon arrival:**
    - ✓ **Vulnerability identification**
    - ✓ **Encryption**
    - ✓ **Application Verifications & Validations**
    - ✓ **Intrusion Detection**

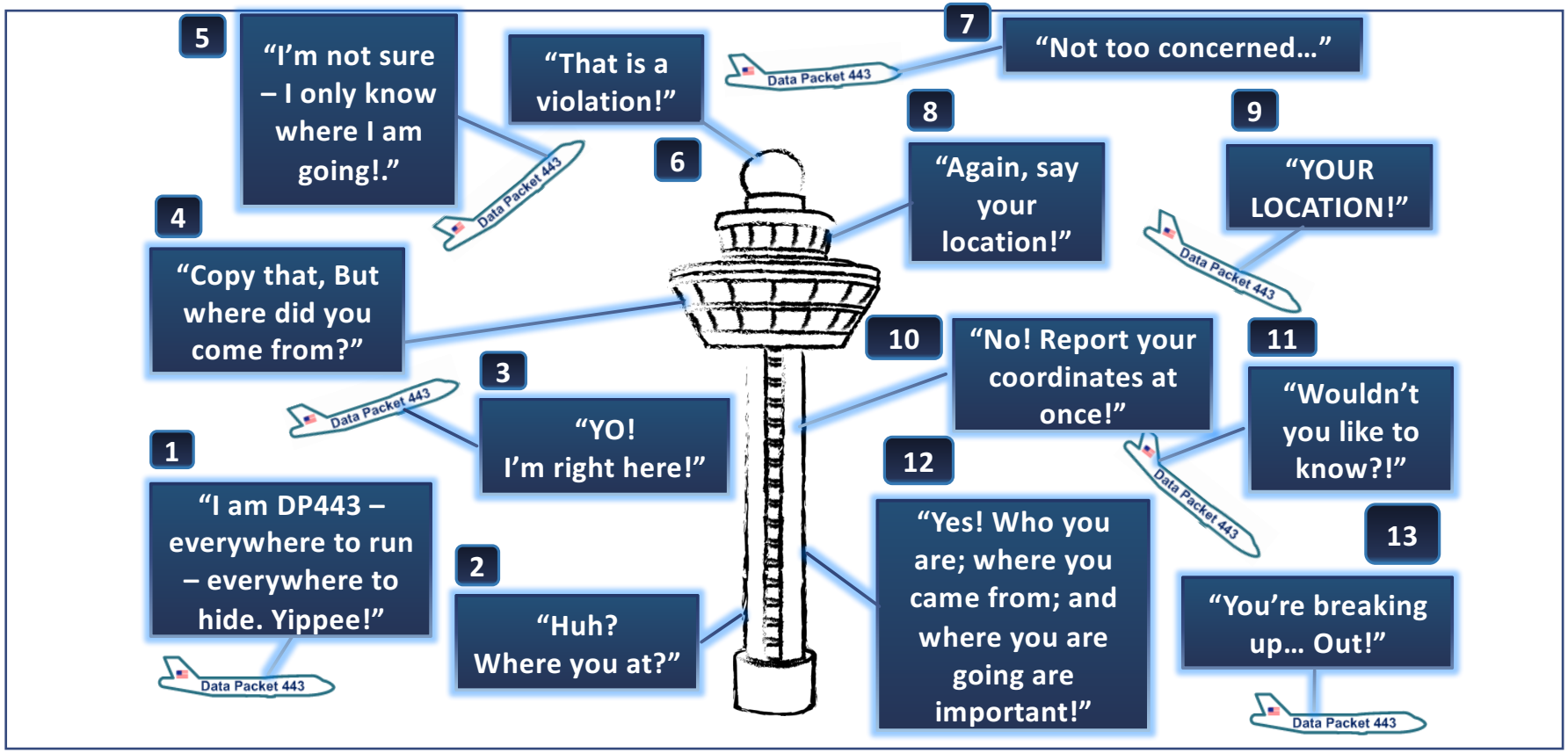
An IP Data Packet…



An IP Data Packet…

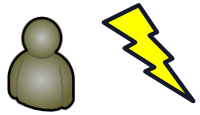


A TOR or AaaS Data Packet Transcript…



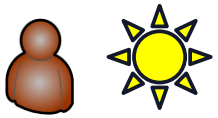
Profiles

Attacker:



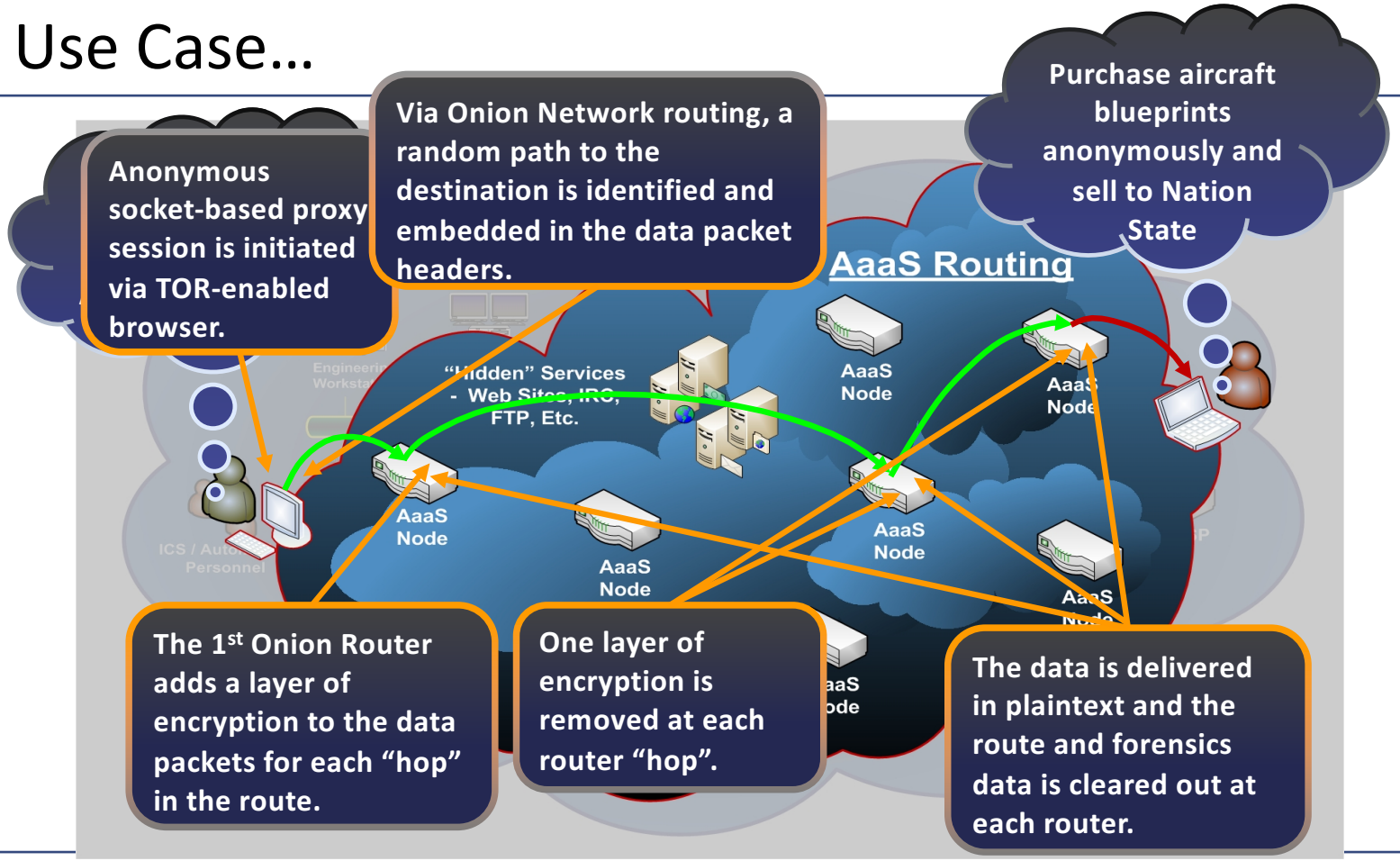
- Wants something
- Illegally Motivated
- Extensive Offensive Toolkit
- STEM Educational Immersion
- Nation State Employed
- Deliberate target selection:
  - ✓ High Value
  - ✓ High Impact
  - ✓ Exploit Driven

Victim:



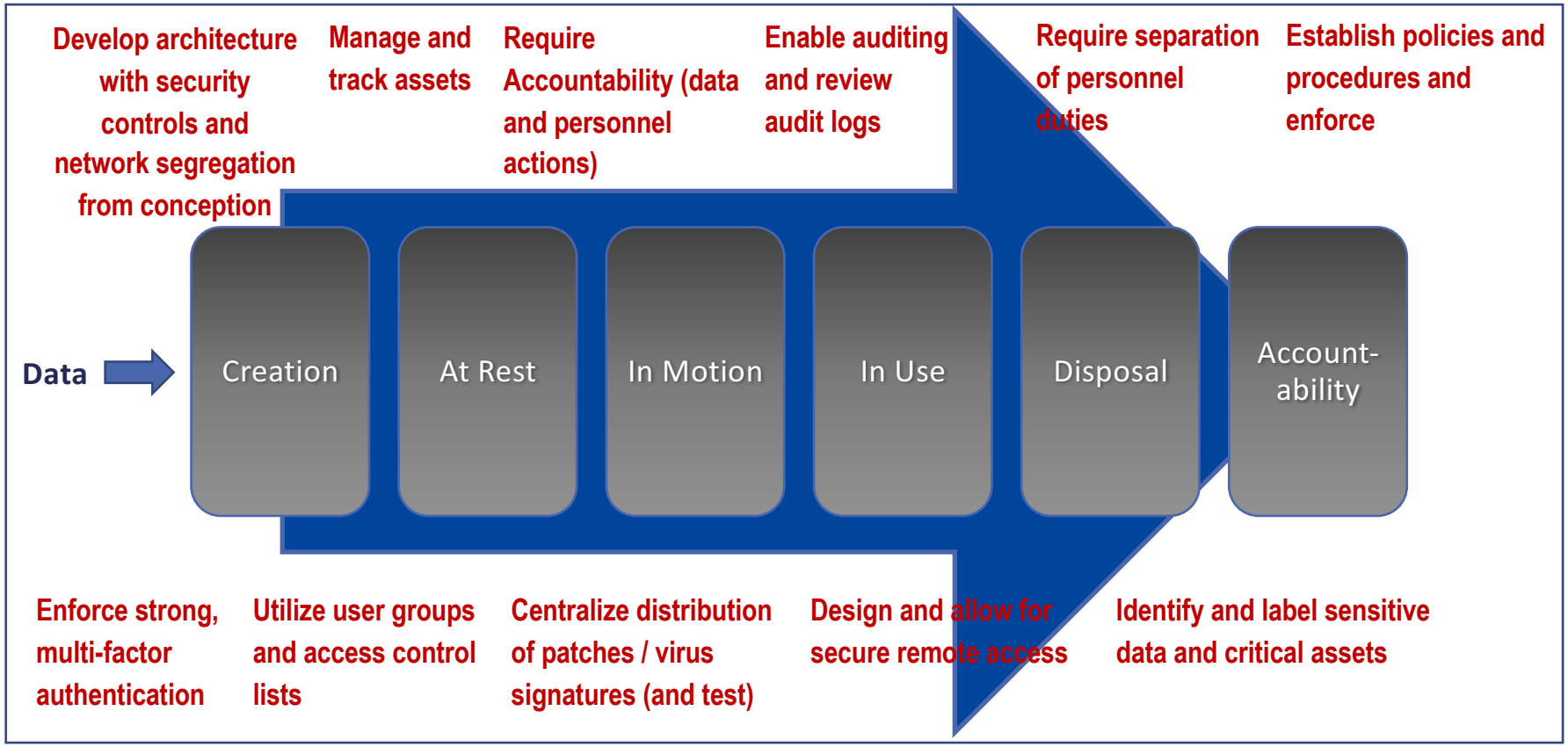
- Has something
- Responsible Corporation / Citizen
- Limited to Defensive Tools
- Broad / Diverse Knowledge
- Corporate Citizen
- Once a target, always a target:
  - ✓ Statistics Prove This!
  - ✓ Detection, Containment, Eradication is Challenging

A Use Case…


Anonymous socket-based proxy session is initiated via TOR-enabled browser.
Via Onion Network routing, a random path to the destination is identified and embedded in the data packet headers.
Purchase aircraft blueprints anonymously and sell to Nation State
AaaS Routing
"Hidden" Services
- Web Sites, IRC, FTP, Etc.
AaaS Node
AaaS Node
AaaS Node
AaaS Node
AaaS Node
The 1st Onion Router adds a layer of encryption to the data packets for each "hop" in the route.
One layer of encryption is removed at each router "hop".
The data is delivered in plaintext and the route and forensics data is cleared out at each router.

”Sphere Theory”…

Act to Prevent the Attack



Courses of Action

You must augment your compliance programs with additional activities aligned to address continuously evolving threats!

- Develop tailored activities based upon industry standards and lessons learned – it may be necessary to "think outside the proverbial box".
- Deploy a balance of technical and non-technical controls and consider that relying on "compensating / inherited" features may be your weakest link
- "Normal" operations do not indicate a threat-free environment
  - Assumptions can kill, literally
- Respond to threats with serious and deliberate intentions
- Evaluate your supply chain
- Assign knowledgeable, dedicated resources
- Ask for help…

COMPLIANCE does not necessarily = SECURE!

Thank you!

Nina C. Vajda, CISSP, CISM, CRISC
IIOT Industrial Automation & Cybersecurity Consultant

nina@blue-phish.com
+1 (701) 651-5514

blue phish