RSA Conference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: CRWD-W01

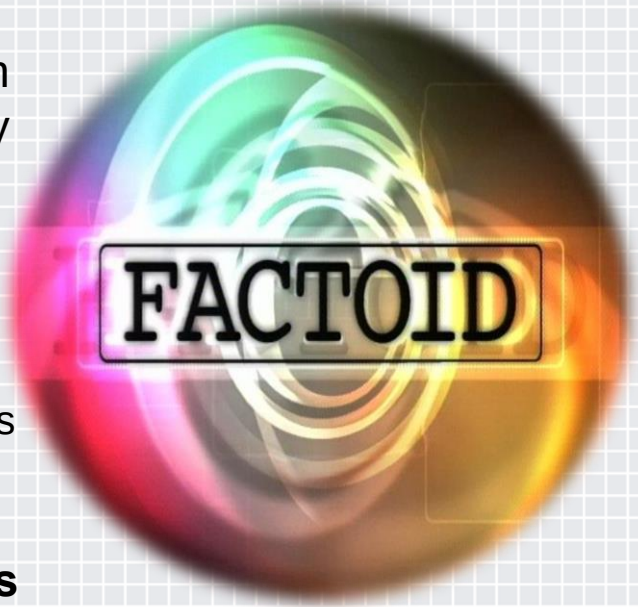
Combating Cyber Risk in the Supply Chain

Joshua C. Douglas

CTO
Raytheon Cyber Products
@RaytheonCyber

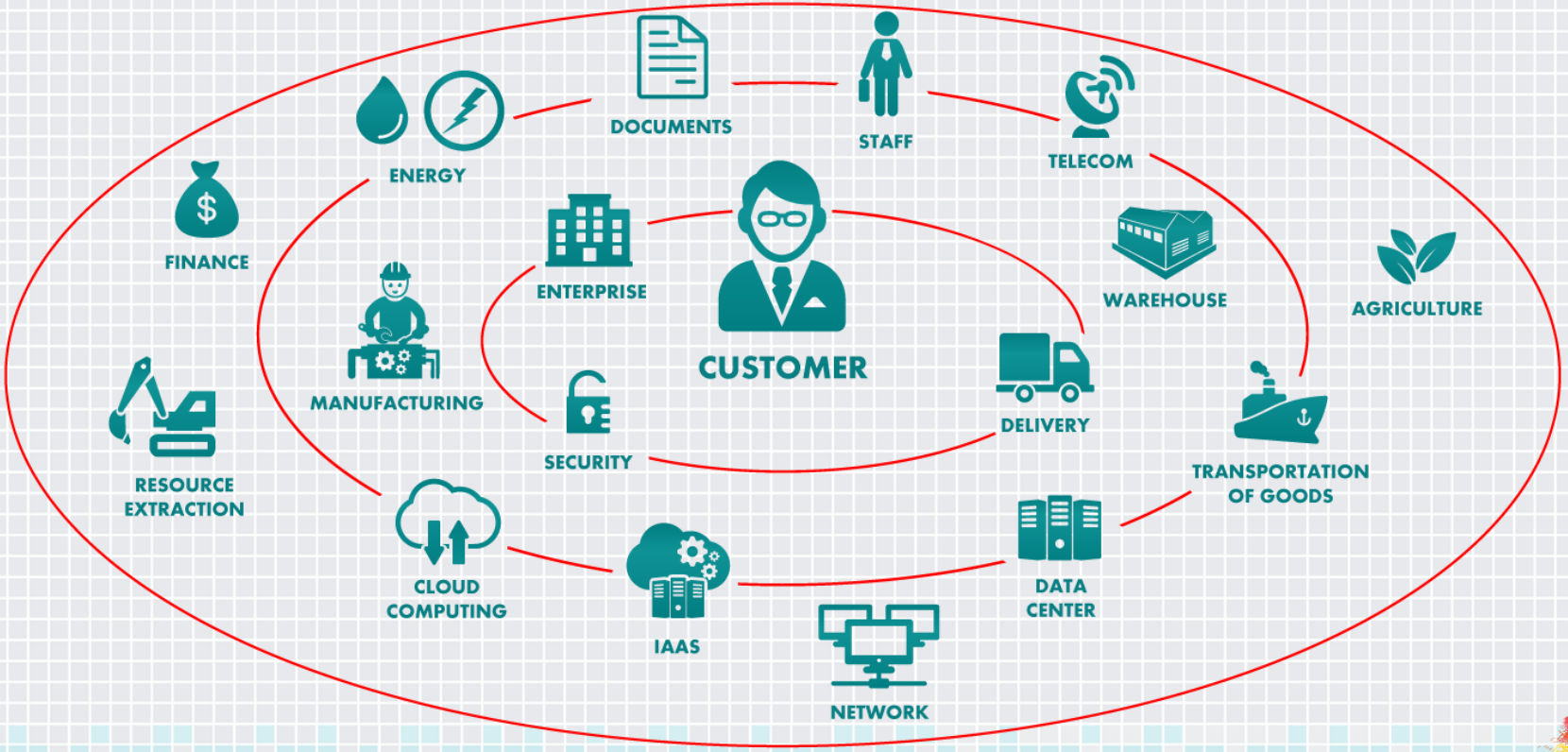
Did You Know?

- 76% of all data breaches result from a third-party which introduced the security deficiencies that were ultimately exploited[1]
- 44% of banks surveyed do not require warranty of the integrity of third-party data or products
  - One-third of them do not require notification by third-parties if breached[2]
- **"Compromised trusted partners expected to be less prevalent in the next three years by IT security leaders[3]…"** ***Really? Or is that a false sense of hope?***

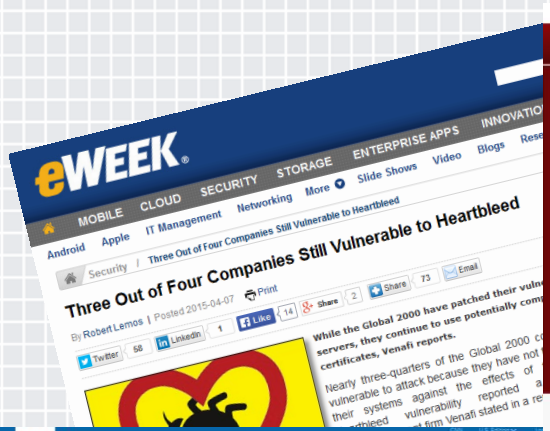


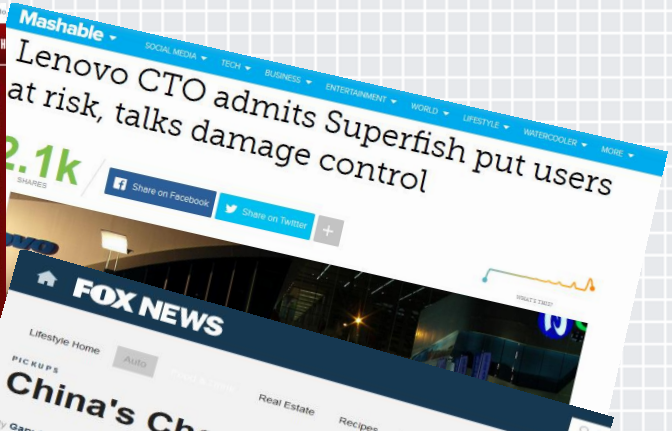
1 Trustwave 2012, Global Security Report
2 NYDFS – update on Cyber Security in the Banking Sector: Third Party Service Providers
3 Ponemon – Megatrends Cyber Security

What Do You Consider to be the Supply Chain?



Depends...Who is the consumer?





We All Are!

Modern Global Supply Chain Defined

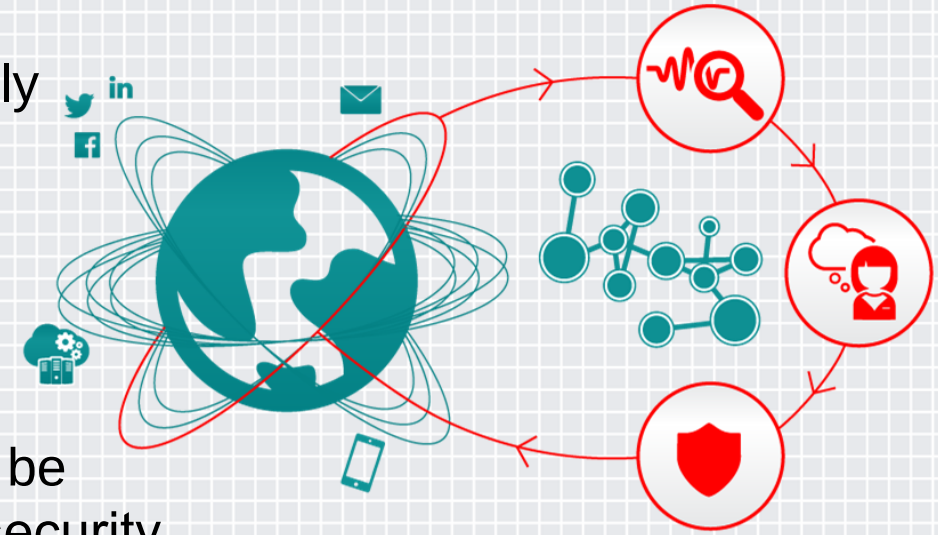
- A complex, global third-party network of suppliers, distributors, business partners, services providers, and customers that *share business processes, develop technology, as well as distribute products used in creating, sharing, and distributing information*

Vulnerabilities Introduced in the Supply Chain

- Supply chain vulnerabilities produce inherent risk and can be used to gain unauthorized access to data, alter data, or interrupt communications in the enterprise or mission
- ***You're only as strong as your weakest link in the chain!***

Deviation from the Norm – Malicious Behavior?

- *Today we are all connected* socially together in our personal life and / or work life
- *Reduce your dwell time* – no one is immune from compromise
- *Do not expect security vendors* to be the “end all be all” for your asset security
- Forward-thinking - focus on analytics, human behavior, and hardening of network systems, etc.

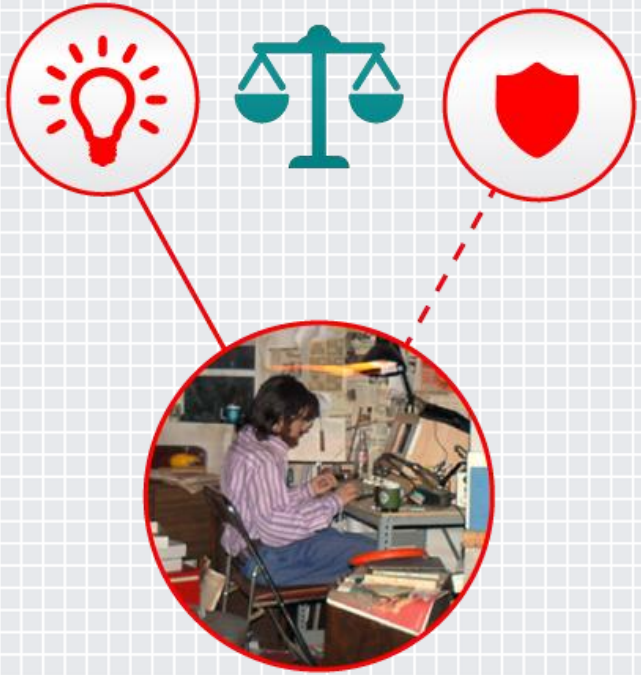


Cyber Security Regulations / Policies / Guidance

- Telecommunications Act 1996
  - 2007 CPNI Order
- DFARS
  - Sub part 204.73
- Comprehensive National Cybersecurity Initiative
  - #11 Develop a multi-pronged approach for global supply chain risk management
- NIST 800-161 (Second Draft)
- Other countries and adverse affects?
- ***If we do not do something about it, regulators will***

Balancing Act

- To protect our customers, we as providers, must protect our product, ourselves, and our global supply chain
- Do you help the supply chain or punish them over faults, breaches, etc.?
  - *Heavy hands often do not help anyone*
- ***A balance between innovation and cyber security***



Supply Chain Hardening

- Tiered Risk Management
  - Engage the ***supplier***
  - Secure the ***enterprise***
  - Protect the ***customer***
- **People, processes and technology**

ICT Supply Chain Risk…Effective?

Formula for Most Companies…

Engage the Supplier

- Create Contractual Obligations
  - Require breach notification (do not make this a negative…) with a timeline and parameters
  - Establish data handling requirements
  - Require product integrity
  - Ensure language mandates communication back to the supplier are only for updates (not data collection)
  - *Make your suppliers demand the same of their suppliers*
- Evaluation of technology and capabilities
  - Security Assessments
  - Source code and binary validation (quality, vulnerability, and FOSS)
- **Information Sharing**
  - **If you have threat information that can protect you both, *share it***

Secure the Enterprise

- Limit Vendor Access
  - Try to avoid direct access to your enterprise
  - Perform deep (content) application inspection on “trusted connections” – treat them like classified networks – inverse DLP
  - Do not directly share critical information - read only and encrypt
- Contain delivered goods and services
  - Zone software, products and services
  - Appliances should not have access to the internet unless for updates…
- Monitor installed products, endpoints and connections
  - Identity and human behavior monitoring are a must to combat today’s threats

Protect the Customer

- Follow the previous two slides
- Bake in security
  - Best practices…passwords, secure coding, etc.
  - Anti-tamper technology
- Assess your products and services
- ***Are you prepared to walk away from a supplier with poor security?***

Apply It…

- ***Next week, you should:***
  - Identify who handles all of the contracts for your company
    - Do they work with the IT Security/Cyber Operations teams?
    - Do they require your supply chain to provide software, hardware and services to be delivered with integrity?
    - Do they require to report to you when they have been breached?
  - Determine if your Intellectual Property has direct access by any third-party
  - Identify what you are doing to secure your products for your customers
- ***In the first three months following this presentation, you should:***
  - You should be able to clearly articulate how many suppliers you have and what they provide (or at least refer to a list)
  - Define appropriate security assessment questionnaire for critical supplier
  - Create plans to isolate critical IP from other data and standard access (treat it as if it were SOX or PCI data)
- ***Within six months, you should:***
  - Have clearly defined security requirements for your suppliers
  - Select cyber security products that go beyond prevention and look at human-based behaviors and malware-based ones
  - *Drive towards a risk-based security approach…understand that everyone gets breached…how do you reduce dwell time?*

Supply Chain Partnership

- Partnership with your traditional supply chain (how you make goods/services)
- Work in partnership with security vendors to harden our security
- Advanced analytics and behavior modeling

Recap

- As consumers and suppliers, we have to understand our supply chain
- We need to be partners to combat the evolving threats
- Malware detection is not solving the problem, nor can it combat the problem when it is human-based
- Security methodologies have to shift from a foundation of prevention to risk-based security

If you are APT, please send care packages to:

joshua_c_douglas@raytheon.com

@DouglasRTN