A CISO's Perspective: Friend or Foe? Effectively Managing Vendor Information Security Risks

Presented by Elliott Glazer
Chief Security Officer
Dun and Bradstreet

Interop New York 2014
October 1, 2014

Vision and Context

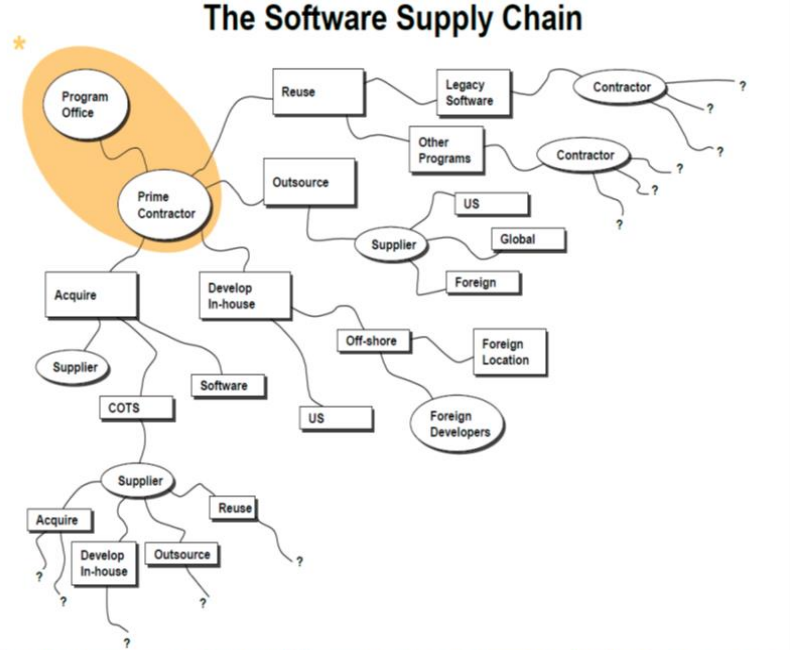
- Often speak about dwindling perimeter
  - Still act like one exists…
  - 70% of activities leverage vendors and third parties
  - With vendors, cloud the perimeter becomes even more vague
- Lots of time protecting technology;
  - Diverts focus on business process and data
  - Databases, servers, networks
- Costs and skills required of adversaries has lowered
  - Easier to attack and exploit data assets
  - Cost and frequency of data breaches are rising
- Users remain one of the biggest challenges
  - Most challenging vulnerability yet greatest asset
  - Most valuable target to attack
- Community is strengthening by working together
  - Information sharing and external governance key to success

Supply Chain Security

- Supply Chain includes customers, partners, vendors…
  - Understand their impact on your business and your impact on theirs
- Often ignored key attack vector
  - Traditional focus has been on what can be controlled not what can only be influenced
- Lowest paid or least perceived risks are often ignored and can be weakest link
  - Target, Inc. - HVAC vendor network access used as gateway to compromise environment
- Maintain consistent and comprehensive assessment of supply chain risks
  - Unstructured risk assessments lead to overlooked threats and vulnerabilities
  - Assumptions often misleading

Supply Chain Security: A Growing Concern

- Products and services are acquired creating complex supply chain
  - Vendors, open source repositories, and contractors
  - Identities, locations, and trustworthiness are often unclear or unknown
- Everything is connected in the modern world



Current Regulations and Supply Chain Security Drivers

- Regulations that specifically highlight supply chain security enhancements and requirements
  - OCC Bulletin - 2013-29
  - PCI - 3.0
  - NIST 800 - 161
  - Monetary Authority of Singapore
- Customer contracts and agreements
  - Expect supply chain to be as secure or better then we are
  - Evidence exists of business being stopped for lack of controls or capabilities
  - More questionnaires on the way…

Strategy for Supply Chain Security

- Vendors should be held accountable for having the same or equivalent security controls as applied internally
- Security requirements should be based on the risk of the target use of the product or service, business value, data classification, and access requirements
- Security requirements should target finding issues as early in the interaction process as possible
- Accountability reporting should be used to enable behavior change
- Artifacts on practices for building security into business processes should be used to demonstrate security

Risk Based Approach to Supply Chain Security

- Identify and classify assets that interact with supply chain
  - Physical, logical, personnel, and data assets
- Not all vendors are created equal
  - Identify and classify vendors
  - Scrutinize based on business value and material impact
- Look upstream as well as downstream
  - Identify if you are a key partner/vendor to someone else
  - Control requirements based on risk of vendor and their products and services
- Effectively manage disconnects
  - Audit and compliance, risk and security, business and revenue
  - Each has different interests and looks through a different lens
  - All views are appropriate but must ultimately service business expectations and goals

What to Release and Not Release

- Just because the auditor/examiner asks does not mean you have to give…
- Provide proof of controls existence and effectiveness without providing sensitive intelligence
  - A table of contents is sometimes as good as the content itself
  - Metrics and measures can often provide adequate proof of effectiveness
  - Responsibility to protect all customers not just the one asking questions
- Honest and forthcoming vs. waiting to be asked
  - Proactivity often results in better outcomes

Mutually Assured Destruction
Limit Liability of Third Parties

- Include reciprocal security language in contracts and agreements
  - I will be as good or better than you…
- Before you release sensitive information you must be assured of its safety
  - You show me yours, I will show you mine…
- The moment a third party comes into contact with sensitive information they may become personally and corporate liable
  - Ensure implications are understood by all parties
- Find a mutually agreeable third party reviewer as a middle ground
  - Independent examination that can be reused

Flow Down Attestation

- Starting point will establish expectations and requirements
  - Customer, regulatory, or industry
- Contractually ensure that vendors meet your requirements
- Vendors must attest that they have appropriately reviewed and actively monitor their vendors for compliance
- Binding multiple layers enforces good practice across multiple industries and touch points
  - Security will propagate throughout supply chain

Sample Contract Language

- Software maintenance and accountability
  - If the COMPANY is completely responsible for the software development and maintenance of existing systems/applications for more than two years; they are responsible for the full remediation of all the security vulnerabilities that are identified. The scope of these remediation include the sections that were previously developed by other parties
- Verification of compliance
  - COMPANY may request VENDOR provides COMPANY verification that the security requirements herein described are being performed in a manner COMPANY reasonably considers adequate to protect the confidentiality, integrity, and availability of COMPANY Data. VENDOR will provide such verification in writing no later than 30 days after COMPANY's request
- Right to audit
  - COMPANY shall have the right, upon reasonable notice, to examine and inspect the VENDOR's security processes, policies and records to determine compliance with the above requirements to the extent applicable to a specific statement of work. VENDOR agrees to cure all noted deficiencies within a reasonable time period given the nature of the deficiency.

Point in Time Assessments vs. Regular and Consistent Monitoring

- Everyone can look good for the day of the audit…
- Point in time assessments can be effective for low risk vendors
  - Ensures they are aware of expectations and requirements
- High risk vendors need regular monitoring
  - Metrics and measures agreed upon by all parties and reported consistently
- Engage in regular dialogue and collaboration with high risk vendors
  - Demonstrate willingness to work together to achieve goals

How to Manage the Onslaught of Vendor Questionnaires

- Shared Assessment SIG (Standardized Information Gathering), custom questionnaires, when will it end?
- Create a repository of common questions and answers
  - Ensure answers are reviewed periodically
- Identify artifacts that can be used as evidence
  - Develop processes to create artifacts on demand
- Fill out the SIG yourself for each product or solution
- Maintain records of what information you have sent to which requestors
  - Ensure you are consistent in responses

Finding Ways To Say “Yes”

- What happens when the business says “Yes” and you say “No” to a vendor?
  - Vendor fails review or assessment
- Not our job to say “No”
  - Provide information to decision makers to make informed decisions
- Only true failure is when supply chain unwilling to participate compliance program
- Develop and monitor a remediation roadmap with supply chain
  - Ensure it is acceptable to both parties

Cloud Providers
How Do You Assess the Inaccessible?

- Public cloud providers typically service all customers the same way
  - Key to their business model
- You may ask questions but may not like the answers (or get no answers)
  - Ultimately a business decision on their use
  - Limited ability to influence change in their operations
- Use competition amongst vendors to create leverage for visibility and driving your requirements
  - Maintain central control over vendor interactions

Using Supply Chain Security to Benefit the Business

- Ensure business understands the risks associated with partners and vendors
  - Before and during the business relationship
- Leverage risks insights to benefit pricing
- Provide business with information to assist management of relationships
  - Security only owns review and remediation governance

Final Thoughts

- Supply Chain Security May Be Key Component to Advancing Security Goals
  - Business are getting better because we are governing each other
- Risk based approach ensures proper focus of resources
  - Gets the right job done at the right time
- Collaborate with your supply chain
- Do not ask for something you do not really want
  - Mutually assured destruction

Thank You!

Elliott Glazer
Chief Security Officer
Dun and Bradstreet
E-mail: GlazerE@dnb.com