Securing the Technology Supply Chain

By Keith Turpin
CISO Universal Weather and Aviation
How Are Organizations Doing?

66% Lack a complete inventory of third parties

69% No centralized control over third-party relationships

18% Know if vendors are sharing their information

* 2018 Ponemon Institute Report: Data Risk in the Third-Party Ecosystem
When Supply Chains Fail

- Theft of intellectual property
- Data breaches
- Inability to conduct operations
- Direct financial loss
- Lawsuits
- Government fines
- Product recalls
In 2013 Target got hacked. They lost private data belonging to 70 Million Customers. Target paid settlements totaling $153.9 Million.
A Story about Ransomware targeting small municipal agencies

- 22 agencies from towns in Texas hit in August 2019 by a single attacker
- Most lost the ability to conduct important business operations
- Attacker demanded $2.5 million for the decryption key
A Story about Corruption in the Supply Chain

- Sinovel Wind Group stole source code for turbine software
- The theft cost American Superconductor more than $800 million

How did it happen?

American Superconductor
Makes wind turbine controller software

Sinovel
Builds Wind Turbines

Licensed Software

Disgruntled Programmer

Source Code

FBI

Sinovel
Found guilty of:
- Theft of trade secrets
- Wire fraud
Settled for $60 Million

$1.7 Million
Business Email Fraud

69,384 U.S. Victims

$26.2 Billion Fraud Reported in 6 Years

100% Increase in Losses

12 Months
The Basic Scam

Attacker poses as a legitimate business partner

Invoices your company

Says their company has changed banking providers

Bank where money should go

Fraudulent bank account
Reconnaissance

- Understand the business
- Identify suppliers, partners and customers
- Discover the identities of key people
- Collect document and email samples
- Understand financial processes
- Identify vulnerable email accounts and systems
Common Attack Characteristics

• Use branded email messages (*Logos, signature blocks, etc.*)

• May emphasize urgency, contain threats or state key people are unavailable

• May include phone calls to appear more legitimate

• Attacker may acquire an internet domain similar to that of the business
  • john.doe@singaporeair.com vs john.doe@singaporeair.com

➢ **Advanced attacks may include email account or email server compromise**
  • Forward email to gather information on current business transactions
  • Hide legitimate email correspondence
  • Step into the middle of the billing process
Defending Against Email Fraud

- Establish formal policies for handling banking account changes
- Verify change requests using a known good contact
- Use two-factor authentication on all email portals
- Train staff to identify suspicious email
- Use email security gateways to stop clearly malicious email
- Add an EXTERNAL label to email from outside the company
- Be prepared if your customer gets scammed by someone pretending to be you
Supply Chain Relationships

Organizations outside the core business have supply chains

- Technology services
- Software development
- Product engineering
- Transportation
- Enterprise resource planning
- Employee pay and benefits
- Sales and marketing
- Building operations and maintenance
- Cafeteria and food services
- Logistics and distribution
- Staffing
Contract Considerations

• Define security requirements as part of the RFP
• Create and use a baseline security addendum
• Include secure coding requirements for software
• Examine and document all assumptions
  ✓ Undocumented assumptions can lead to disputes and ambiguous liability
• Address sub-contracting limitations, visibility and approvals
• Specify how compliance will be measured
• Fully address vendor termination
Supply Chain Risks

- Supplier with access to your IT systems or sites
- Supplier managed code or IT systems running in your IT environment
- Supplier storing or processing sensitive data
- Regulatory requirements apply to your supply chain (Examples: PCI, GDPR, DFARs)
- Value of data or intellectual property exposed in the relationship
- Impact of supply chain disruption (Single sourcing)
- Contractual obligations
- Size of the supplier
Assessing Supplier Security

Conducting Your Own Evaluations

• Assessing security and privacy policies can reduce incidents by 20%

• Use a tiered assessment model based on levels of risk

• Security Standards like ISO 27001 or NIST 800 should be guidelines

• Tailor assessments to align with products and services

• Review the scope of assertion certifications like SSAE 16 SOC 2
Cybersecurity Rating Services

- **FICO Enterprise Security Score**
  - Ratings scale from 300 – 850

- **BitSight Third-Party Risk Management**
  - Rating scale from 250-900

- **SecurityScorecard**
  - Letter based rating scale from A to F

- **UpGuard**
  - Rating called CSTAR, that scores companies from 0-950

- **RiskRecon**
  - Rates cyber resilience from 0-10 in three categories
Questions