Contracting for Cybersecurity

(and what to do when you can't get everything you want)

Mark Francis

New York State Cyber Security Conference – June 4, 2019

Holland & Knight

Supply chain increasingly a focus of businesses and regulators

05 Target Hackers Broke in Via HVAC Company

FEB 14

Last week, **Target** told reporters at *The Wall Street Journal* and *Reuters* that the initial intrusion into its systems was traced back to network credentials that were stolen from a third party vendor. Sources now tell KrebsOnSecurity that the vendor in question was a refrigeration, heating and air conditioning subcontractor that has worked at a number of locations at Target and other top retailers.

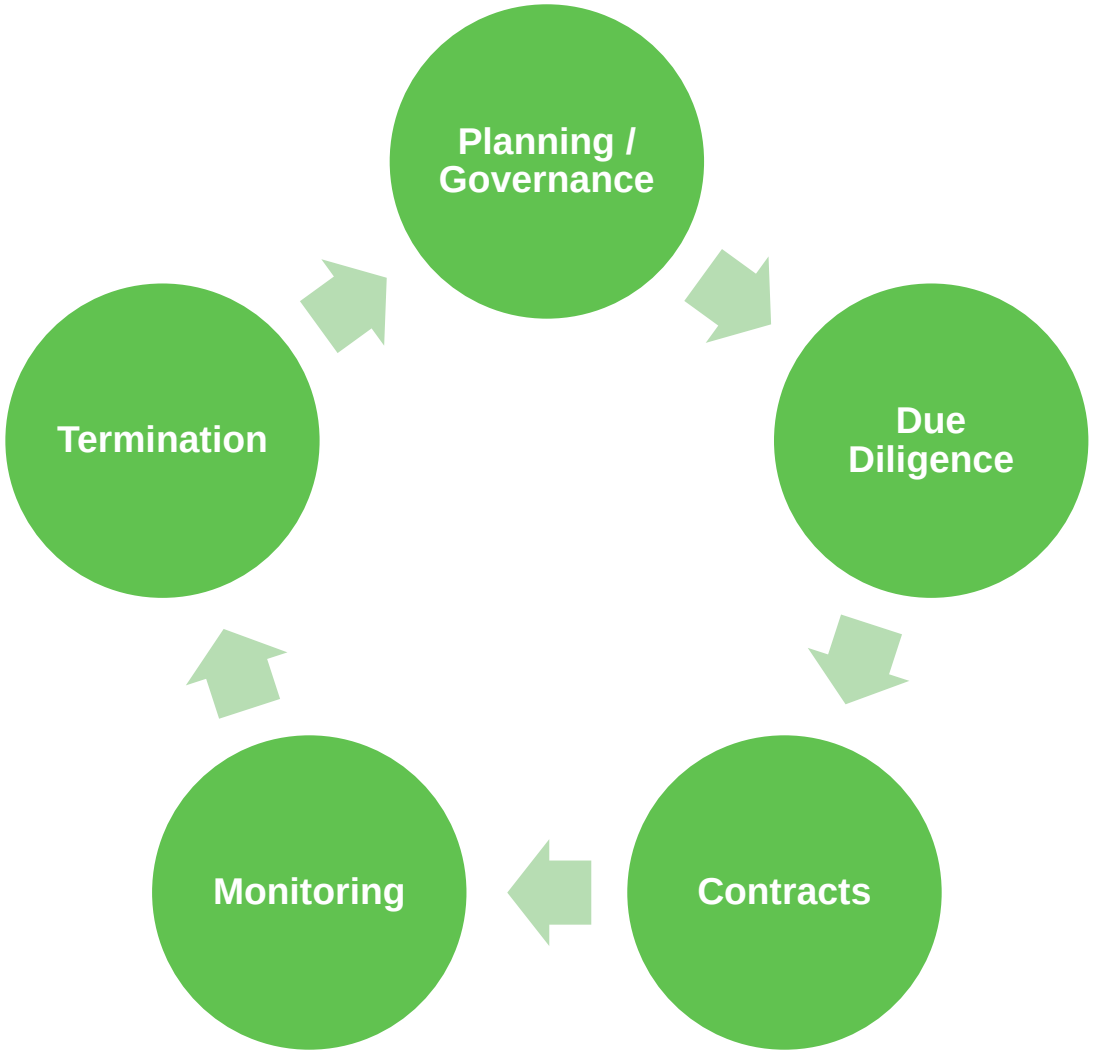
Sources close to the investigation said the attackers first broke into the retailer's network on Nov. 15, 2013 using network credentials stolen from Fazio Mechanical Services, a Sharpsburg, Penn.-based provider of refrigeration and HVAC systems.

Supply chain increasingly a focus of businesses and regulators

In 2017 roughly 90% of the motherboards used in the 13.9 million servers shipped worldwide were made in China. Last year that had dropped to less than 50% of motherboards used in the global total of 15.2 million"

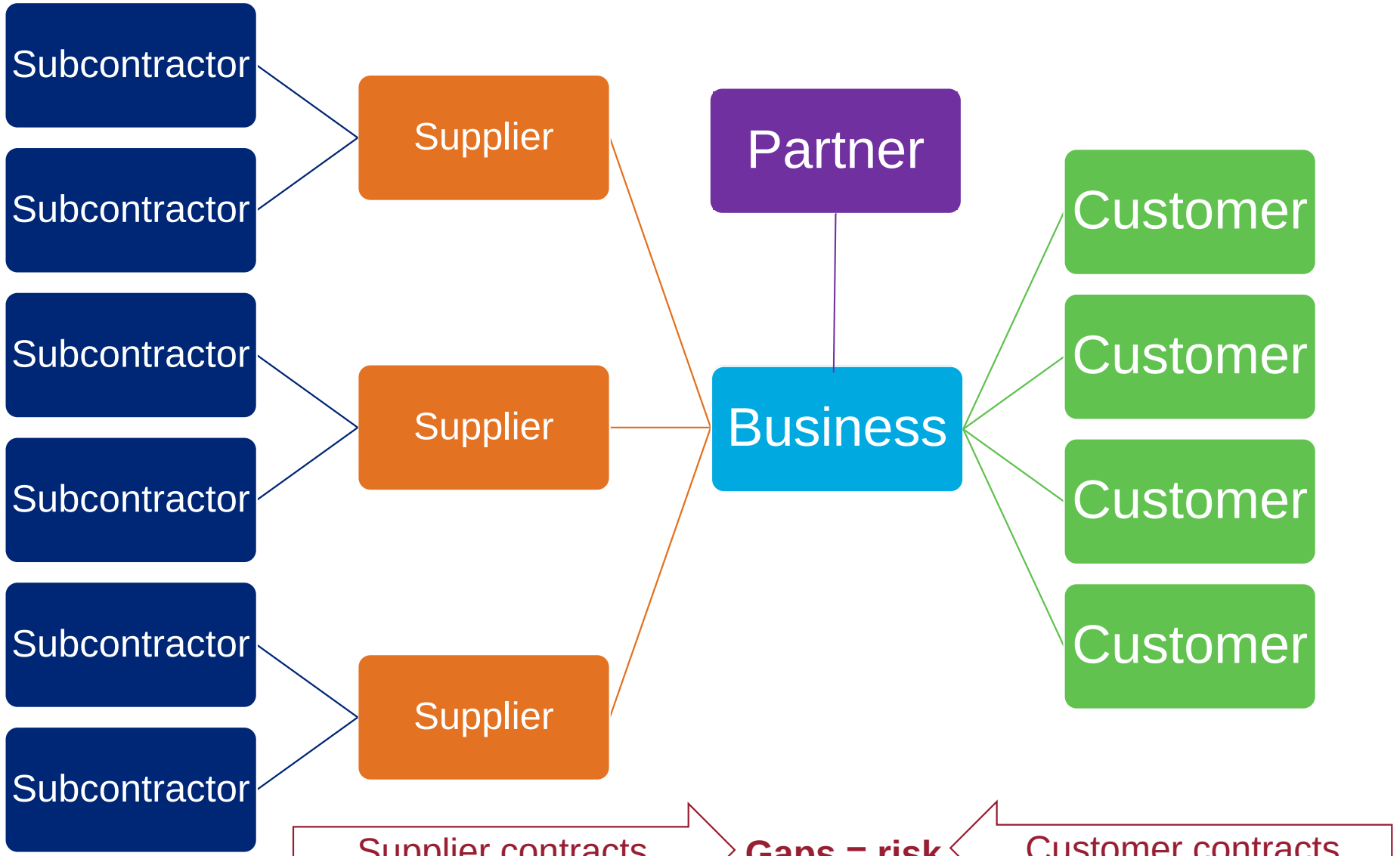
-Nikkei (Apr. 30, 2019)

Third Party Risk Management ("TPRM") Lifecycle



Holland & Knight

Businesses operate through contractual relationships



Cyber teams can experience compliance fatigue on many fronts

Laws

- Federal (GLBA, HIPAA)
- State laws (CCPA)
- Int'l (GDPR)
- Quasi-laws (PCI , IAB)

Industry Standards

- NIST CSF
- ISO 2700X
- OWASP

Contracts

- Customer
- Customer
- Customer
- Supplier
- Supplier
- Supplier
- Supplier
- Partner
- Partner

Key Contract Provisions: Cybersecurity

- Requirements for data security and privacy
  - *General language*
  - *Explicit requirements*
  - *Industry standards*
- Applicable laws (e.g., HIPAA, GLBA, EU DPD)
- Subcontractors (flow down provisions)
- Data breach and notice procedures
- Liability & Indemnity
- Cyber-insurance
- Audit rights
- Templates and exhibits

Key Contract Provisions: Data & Privacy

- Who owns the data and tech before/during/after the term?
  - *Personally-Identifiable Information (PII)*
  - *Aggregated/anonymized data*
  - *Intellectual Property*
- Data use restrictions
  - Strictly to perform services?
- Protecting PII
- Addressing evolving risks
- Compliance with legal requirements (which keep changing)
- Primary data processing function vs. incidental exposure (*e.g.,* temporary access)
- International concerns (Cross-border transfers, Privacy Shield, GDPR)

Common Conflicts

Customer → ← Supplier

Customer's view	Supplier's view
Vendor should assume all risk for security and privacy within its control	Vendor is not an insurance provider; fees are priced for the services provided and not sufficient to offset all customer risk
Vendor should provide detailed information about its security practices to satisfy regulator expectations and help customer assess risk	Cannot dedicate the personnel to respond to hundreds of different customer questionnaires and inquiries; not comfortable sharing detailed security practices
Vendor should provide pen test and risk assessment reports	Candid reporting for internal security purposes would be inhibited by forced disclosure to customers
Need immediate notice of incident due to potential risks and notification obligations	Need time to assess event and report accurately
Vendor should cooperate fully after an incident	Need to balance cooperation with personnel interests and potential legal action by customers
Use of subcontractors who will receive customer data is subject to written consent	Vendor can operate its business without requiring consents from all customers

Top 10 Stress Points

1. Liability (first party disputes)
2. Indemnity (third party disputes)
3. Legal compliance
4. Security – prescriptive requirements
5. Consent for subcontractors
6. Audit rights and questionnaires
7. Cyber insurance (scope and limits)
8. Notice obligations (incidents; vulnerabilities)
9. Changing requirements mid-contract (*e.g.,* supplier policies)
10. Penetration testing

Solutions & Strategies

- Above all else, it is about negotiation leverage
  - *Who needs who more?*
  - *Are you prepared to walk away?*
- Be pragmatic about your capabilities and compliance
  - *Do not overcommit*
  - *Buy time where needed for compliance (e.g., "within 6 months")*
- Evaluate the "cost" of concessions
  - *What is the added risk? Can it be offset other ways?*
  - *What are added obligations going to cost in compliance?*
  - *What are the lost opportunities?*
  - *How will this affect the business prospects (M&A, funding)*

Solutions & Strategies

- Be proactive, and leverage it
  - *Certifications (PCI; ISO; HITRUST)*
  - *Audit reports (SOC 2 Type II)*
  - *Standard exhibit templates, detailed requirements aligned with products/services*
- Understand and communicate your risk tolerance internally
  - *Are uncapped liability deals off the table?*
  - *Align deal value (actual and intangibly) to the risk tolerance*
- Understand your cyber insurance coverage
  - *Limits – will they cover all risk (multiple contracts) triggered by one incident?*
  - *Scope – what about ransomware, BEC and wire fraud*

Solutions & Strategies

- Be consistent (as much as possible)
  - *Resist the urge to agree to substantively different terms and conditions*
  - *Otherwise compliance becomes overwhelming*
- A signed contract is enforceable law, it is not just “best efforts”
  - *Be careful about representations and commitments*
  - *90% compliance is breach of contract*
  - *Questionnaire and audit responses can be incorporated into a contract*
- Opportunities available to small businesses may offset contractual demands
  - *Qualify for SMB programs*
  - *Qualify as a minority or women-owned business*

Q&A

Mark H. Francis

Partner, NY

212.513.3572

Mark.Francis@hklaw.com

The purpose of this presentation is to provide general information and context, not specific legal advice.