



Building Security Strategies for Commercial Contract Relationships

Robin J. Lee

Technology Transactions Group – Palo Alto
Prepared for the SF Bay Area InfraGard IMA

November 17, 2011

attorney advertisement

© 2011 Cooley LLP, Five Palo Alto Square, 3000 El Camino Real, Palo Alto, CA 94306
The content of this packet is an introduction to Cooley LLP's capabilities and is not intended, by itself, to provide legal advice or create an attorney-client relationship. Prior results do not guarantee future outcome.

What we'll cover today...

- ▶ Framing the problem: What do contracts have to do with my security posture?
- ▶ What are the problems with contracts today?
- ▶ How to critically read security-related contract clauses
 - ▶ Prevention clauses
 - ▶ Detection clauses
 - ▶ Reaction clauses
- ▶ Fun with risk allocation
- ▶ SPEARCAP
- ▶ Questions



What we won't cover...

- ▶ For this session, we'll focus on:
 - ▶ Security gaps in supply chain/commercial relationships
 - ▶ Common ways that legal contracts deal (or don't deal) with them
 - ▶ How we can improve things
- ▶ As a result, we won't be talking about:
 - ▶ Legal compliance issues: legislation or regulations (pending or otherwise)
 - ▶ Privacy questions
 - ▶ Litigation or e-discovery issues
 - ▶ Criminal issues

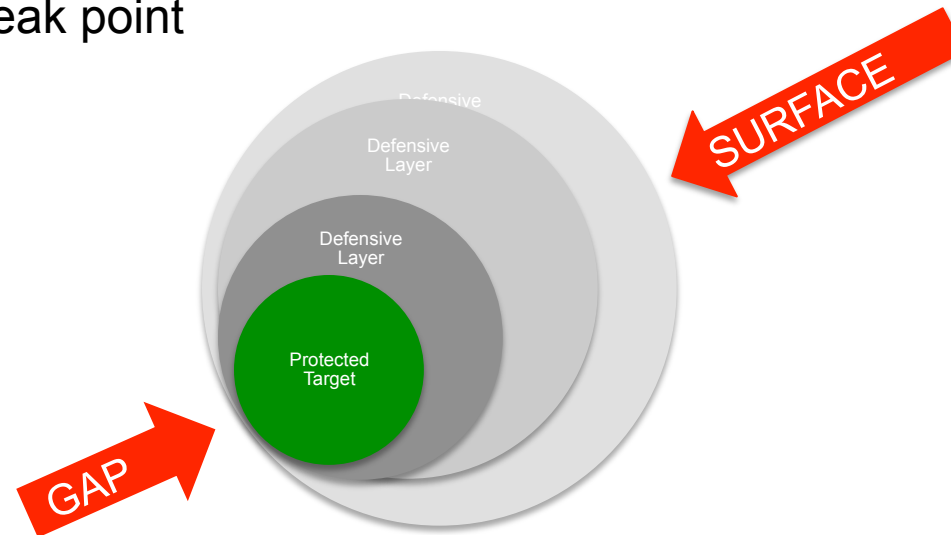


Framing the problem

- ▶ In today's threat environment, every organization with something of value is subject to attack
- ▶ Realizing this, most organizations have made various investments in security
- ▶ But some avenues of attack are defended better than others
 - ▶ Limited resources
 - ▶ Limited control over certain parts of the ecosystem
 - ▶ Operating compromises
- ▶ This will not change: **making intelligent choices about scarce resources is essential**
 - ▶ “He who defends everything, defends nothing.” -- Frederick the Great

Framing the problem

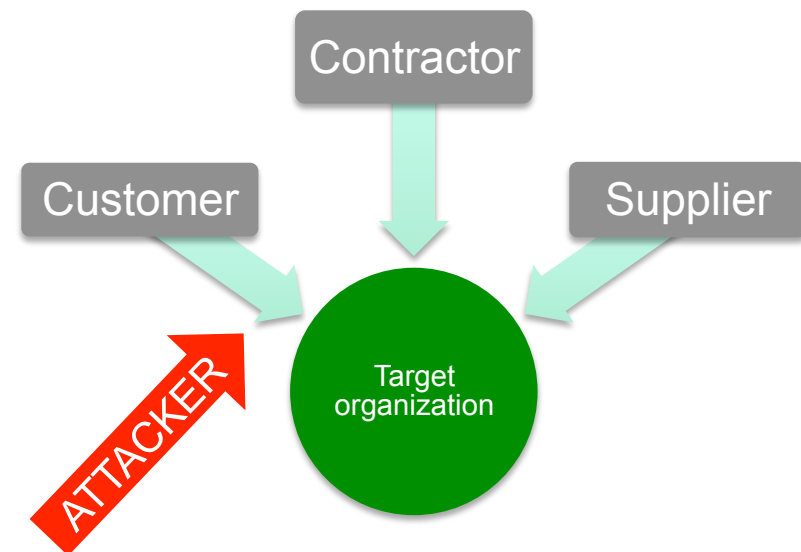
- ▶ Because of this unevenness, the organization's defensive architecture is comprised of **surfaces** and **gaps**
 - ▶ A surface is a "hard spot" in the defense
 - ▶ A gap is a weak point



- ▶ Attackers seek the path of least resistance: **avoid surfaces** and **exploit gaps**

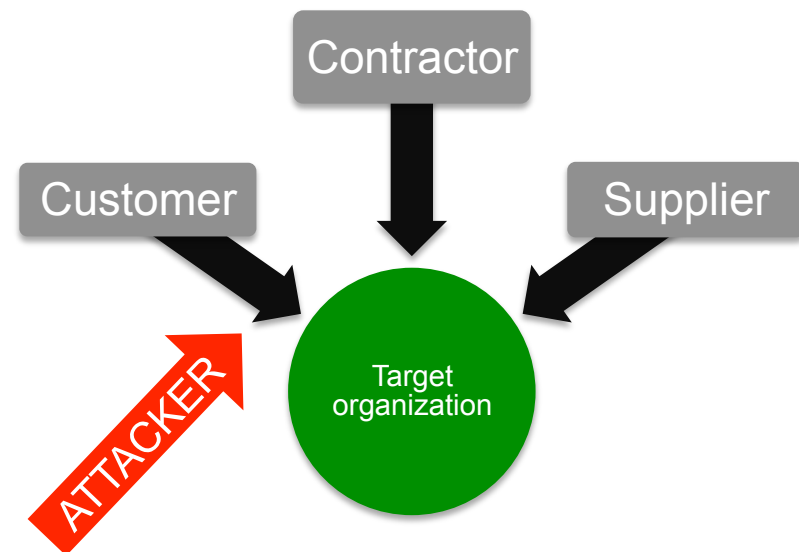
Framing the problem

- ▶ Third-party relationships create junctions in your operational chain
- ▶ These junctions are potential gaps
 - ▶ Varying trust relationships
 - ▶ Incompatible security processes
 - ▶ Limited visibility beyond the organizational boundary
 - ▶ Limited control beyond the organizational boundary
- ▶ Classic point of entry for social engineering
- ▶ Increase in cloud-based services, other outsourced functions make this a growing issue



Great, but what do contracts have to do with it?

- ▶ Contracts (and their associated legal processes) cover these third-party junctions
 - ▶ Regulate their creation
 - ▶ Establish “hardening” processes
 - ▶ Create visibility into the partner’s activities
 - ▶ Implement reaction drills
- ▶ By themselves, contracts will not prevent attack, but they can mitigate the factors that make third-party junctions an attractive target for attackers



So what's the problem with today's contracts?

- ▶ Lawyers and legal administrators are not security experts
- ▶ Most commercial contracts are not particularly well-suited for the contemporary security threat
 - ▶ Many of the relevant concepts were traditionally designed to protect intellectual property
 - ▶ Generally have not changed in many years
 - ▶ Tends to exist at a very high level of generality: “reasonable security measures (whatever that means)”



Stovepipes...

Legal function

Liability

Security is a
technical issue.

Technical function

Technical issues

We can build some
security
mechanisms, but
true security is a
management issue.

Management function

P&L

Security is a
specialized
technical/legal
issue.

Three classic dimensions of security

Dimension	Function
Prevention	Forestalling a successful attack
Detection	Detecting an attempted attack
Reaction	Containing/recovering from an attack

Mapping contract clauses to security strategy

Security Function	Contract Mechanism
Prevention: forestalling a successful attack	Basic confidentiality/NDA provisions, data handling and storage provisions
Detection: detecting an attempted attack	Intrusion reporting, audit provisions
Reaction: containing/recovering from an attack	Backup/recovery plans, containment and breach response protocols

Let's take a critical look at some contract language in each of these areas...

Prevention: Basic confidentiality obligation

“Contractor shall treat as confidential all Company Confidential Information, shall not use such Confidential Information for any purpose except as expressly set forth in this Agreement, and shall not disclose such Confidential Information to any third party. Without limiting the foregoing, Contractor shall use at least the same degree of care that it uses to prevent the disclosure of its own information of like importance, **but in no event shall Contractor exercise less than the degree of care that a reasonably prudent business would exercise under similar circumstances.**”

- Extremely common formulation in many NDAs
- Vague; not very prescriptive
- Could be problematic when dealing with business partners in different circumstances



Prevention: Logical access controls

- ▶ **“When used, system logon passwords will be randomly selected and will be at least six (6) characters in length.** Passwords must be validated by the system each time the user accesses the system. System logon passwords must not be displayed at any terminal or printed on any printer. Under no circumstances will passwords be shared. Passwords must be changed no less frequently than once every six (6) months. Master data files containing user population system logon passwords will be encrypted when stored or transmitted.”
- ▶ “Successive logon attempts shall be controlled by **denying access after five (5) consecutive unsuccessful attempts** on the same user ID, by limiting the number of access attempts in a specified time period, or other such methods.”

- Specific and prescriptive
- Becomes dated very rapidly?



Prevention: Logical access controls

- ▶ “Contractor shall maintain **reasonable data security controls** on its servers and workstations including, without limitation, user logon identification and authentication, mandatory access controls restricting access to sensitive files based on positive user permissions, accountability tracking, and restricted download-to-disk capability.”
 - ▶ “Contractor shall ensure that all workstations from which Company Confidential Information may be accessed are (a) equipped with appropriate session controls, including **automatic session timeouts after ten (10) minutes or less of user inactivity** and forced logoff procedures at the end of the day; and (b) located in such a manner that their displays are not readily visible to observers in common or open areas of the facility.”
- Combination of general “reasonable” standard plus prescriptive examples



Prevention: Logical access controls

- ▶ “Contractor will maintain an adequate account purging process, under which user accounts are **disabled after thirty (30) consecutive days of logon inactivity** and deleted after sixty (60) consecutive days of logon inactivity.”
 - ▶ “Contractor will display the date and time of the last successful logon to the user of the account, and will train all users to report unusual or suspicious logon records.”
 - ▶ “Upon the (a) termination of any employee or (b) transfer of an employee that removes the need for system access by such employee, Contractor shall ensure that the **associated security profiles are immediately updated** to reflect the new status of the user.”
- Also very prescriptive, but addresses revocation of access—something rarely addressed in commercial contracts



Prevention: Physical access controls

- ▶ “Contractor shall maintain reasonable physical security controls at the facility, including, without limitation, human-monitored alarm systems, facility access controls (including off-hours controls), visitor access procedures, human-monitored video surveillance systems, and personnel egress searches.”
 - ▶ “Contractor will ensure that its Secure Rooms (a) have full-height walls and fireproof ceilings; (b) have no more than two doors leading to unsecured areas, each of which is fireproof, lockable, and observable by security staff; and (c) have no window openings large enough for a person to enter.”
- Derived from industrial security practices for defense contractors
 - Who bears the cost to implement these kinds of controls?



Prevention: Physical access controls

“Contractor shall (a) limit and monitor access to equipment areas; (b) maintain an up-to-date list of personnel authorized to access sensitive areas; (c) enact on-site service policies that **forbid the servicing or removal of equipment unless the task is preauthorized and service personnel can produce an authentic work order and acceptable identification**; and (d) ensure that all (i) employees or independent contractors whose responsibilities do not ordinarily require their presence in the equipment areas, and (ii) third parties be accompanied at all times by an escort while in such equipment areas.”

- Addresses common social engineering “walk-in” technique
- Not just for third-party contracts—a good in-house practice



Detection: Intrusion reporting obligations

- ▶ “In the event that Contractor learns, or suspects facts that would lead a reasonable person to believe, that a compromise or other breach of security has taken place, Contractor will (a) immediately notify the Company; and (b) take all measures necessary to isolate and contain the actual or suspected breach.”

- Simple
- “Knowledge-qualified”: is vague on the specific measures a Contractor should take to be aware of possible compromises



Detection: General audit clauses

- ▶ “During the Term and for a period of three (3) years thereafter, Contractor will keep and maintain accurate records pertaining to use, maintenance, and operation of the System. Company shall have the right, during normal business hours and with twenty-four (24) hours’ notice to the Contractor, to visit the Contractor’s premises; audit Contractor’s records, files, and data (including access logs); and inspect Contractor’s facilities for the purpose of **ensuring compliance with the security protocols** set forth in this Agreement. Such audits shall be conducted no more than once every four (4) months. Notwithstanding the foregoing, if Company has reasonable grounds to believe that a breach of security has actually occurred, Company may conduct an audit unannounced during normal business hours.”

- Generic, and fairly common
- Not tailored to security audits



Detection: Security audits/red-teaming

- ▶ “From time to time during the Term, the parties will cooperate to (a) conduct ongoing security audits to identify emerging vulnerabilities within the system; and (b) address any such vulnerabilities.”
- ▶ “From time to time during the Term and at Company’s expense, **Company may conduct controlled penetration tests to test the implementation of security measures**. Such tests (a) will be agreed upon in advance by Contractor and Company; (b) may include the use of “password crackers,” planned network sniffing, social engineering exercises, and other intrusion checks; and (c) will not involve permanent damage to equipment or denial-of-service attacks. Contractor will use commercially reasonable efforts to correct any security deficiencies revealed by such testing.”

- Much more specific
- Much more intrusive—hard to negotiate



Reaction: Establishing a CSIRC capability

- ▶ “Within thirty (30) days after the Effective Date, Contractor shall implement a Computer Security Incident Response Capability that, without limitation, (a) facilitates centralized reporting of incidents throughout the system; (b) coordinates responses to incidents; (c) manages the cooperative technical interaction between Company and Contractor; (d) provides direct technical assistance as needed; and (e) serves as a liaison to legal and criminal investigation authorities.”
 - An attempt to establish compatible interfaces across organizational boundaries
 - But do the parties ever remember to do this?



Reaction: Disaster Recovery Plan

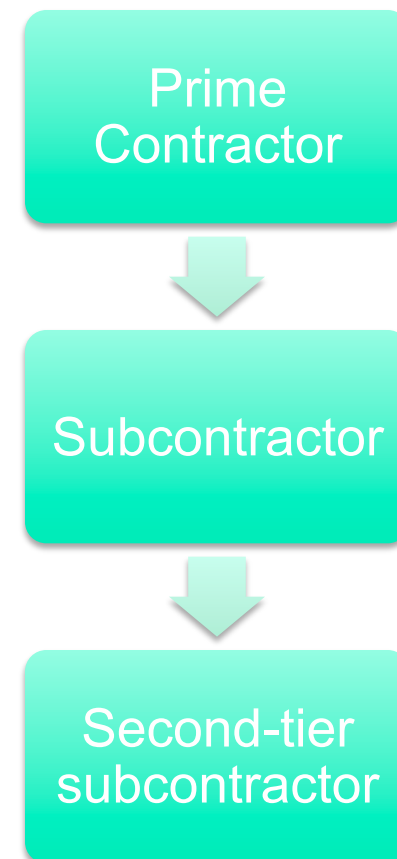
- ▶ “Within thirty (30) days after the Effective Date, Contractor will implement a disaster recovery plan with all of the characteristics set forth in **Exhibit A (“Disaster Recovery Plan”)**.”
 - ▶ System and database backups
 - ▶ Alternate power sources
 - ▶ Redundant servers (geographically separated)
 - ▶ Access shutdown and controlled reactivation

- Possibly too generic
- Probing function: Contractor’s reaction/pushback gives insight into their level of preparedness



Maintaining downstream integrity

- ▶ Contractors have subcontractors, who have subcontractors...
 - ▶ Approval rights
 - ▶ Mandatory pass-through obligations
 - ▶ Third-party beneficiary clauses
 - ▶ Reporting/audit flowdown



Risk allocation trends and issues

- ▶ “Risk allocation”: who shoulders the liability when things go wrong?
 - ▶ Commonly thought of as a “lawyer’s issue”
 - ▶ But it’s fundamentally a business call, so it’s important for security professionals to understand



Indemnification

- ▶ Obligates one party to defend and pay damages if the other party gets sued based on certain claims
 - ▶ Like insurance, in a way
- ▶ Central issue: for security-related problems, what should the scope of the indemnified claims be?
 - ▶ Breach of obligation to implement defined security procedure?
 - ▶ Strict liability: any security breach, period?
- ▶ Trend: for security-conscious businesses, we're seeing more asks for broad indemnification for security problems



Limitations of liability

- ▶ Common tool in commercial contracts to limit the downside
- ▶ They do two things:
 - ▶ Disclaim “consequential” or “indirect” damages
 - ▶ Cap direct damages at some amount
- ▶ Hot issue: what cap, if any, should apply to damages arising from a security breach?
- ▶ Trend: Starting to see some movement around privacy-related liabilities arising from data breaches



There are no quick fixes

- ▶ No “magic language”!
 - ▶ Sample contract clauses are just examples of possible legal approaches to dealing with current security problems—but tomorrow, the vulnerabilities and risks will be different
- ▶ Effective security strategy requires ongoing collaboration between all three functions within the organization:
 - ▶ Technical function: identify the nature of the current threat
 - ▶ Legal function: formulate possible legal mechanisms to mitigate threat
 - ▶ Management function: decide the right balance to strike between security and operating necessity



SPEARCAP program

- ▶ **Security Posture Enhancement and Review: Commercial Agreement Provisions**
- ▶ New initiative started earlier this year to:
 - ▶ Encourage a focused review of existing legal practices in light of the current security environment
 - ▶ Create a tailored set of options for varying levels of criticality – not everything requires the strictest security protocols
 - ▶ Promote the emergence of best practices
- ▶ Not just for lawyers – need the informed participation of security professionals
- ▶ Dialogue between the legal function and the technical/management function is essential

Questions?



Robin J. Lee
rjlee@cooley.com
(650) 849-7013