At Least We Can Agree on This: Working with Legal to Improve Cybersecurity in Standard Agreements
Disclaimer

I am giving a general explanation of some common provisions in legal agreements and their implications, and how tailored cybersecurity provisions can be added to agreements with relatively low risk.

I am not giving legal advice, and nothing here (or in the handouts) creates an attorney client relationship. Talk about everything with your attorney before doing anything.
What I hope you take away

Contractual methods to improve threat intelligence and defense, plus a couple pieces of low hanging fruit along the way.

Maybe some attorney jokes
Why does it matter?

Anyone’s vendors/customers have information they don’t want in the wild?

Would you like to know if that information is compromised?

How about if someone used a vendor’s VPN credentials to connect to your network, but they can’t validate who it was?
Why does it matter?

Why would they tell you?

Remember: The goals are: (1) more thorough defense of information, and (2) accurate, timely, and actionable information sharing.
The rest of our time

Two contract provisions related to confidentiality

Two contract provisions related to getting better intelligence

Getting the right team

“Do it yourself” and recap with ways to handle unfortunate language
Limited disclosure of Confidential Information

Where is it normally found?

◦ Nondisclosure/confidentiality agreements, any agreement involving disclosure or use of business processes, designs, and other Confidential Information.

What is it?

◦ All good agreements have “kick outs” where confidential information may be disclosed. A court order to hand over the information is very common.
Limited disclosure of Confidential Information

Why is this important to you?
- If you (or the third party you hired, or the subcontractor to the third party you hired) gets an order to hand over your Confidential Information, it still needs to be protected.
Limited disclosure of Confidential Information

Unfortunate language:
◦ “Confidential Information shall not include any information which:
  ... is required to be disclosed by a government agency, court order, or law; ...
  becomes publicly known through no violation of this Agreement;”

Example of what language will help you:
◦ This is more “what to avoid” than what to use. Your legal will have language they normally use.
Standard for protecting Confidential Information

Where is it normally found?
- Nondisclosure/confidentiality agreements, any agreement involving disclosure or use of business processes, designs, and other Confidential Information.

What is it?
- It defines due care to avoid talking about an ethereal “reasonable person”.

COPYRIGHT - BRENT FOSTER
Standard for protecting Confidential Information

Why is it important?

- Sensitive OT information is going to contractors, subcontractors, and others. Why compromise your (hopefully) monitored and segmented IT/OT network for recon when attackers can hit the lowest bidding subcontractor.

- Honestly even just bringing this up may help weed out some vendors...

- Realistically, this provision is critical path to get the intelligence provision.
Standard for protecting Confidential Information

Unfortunate language:
◦ “Receiving Party shall use efforts at least equal to those it uses for the protection of its own Confidential Information.”
◦ Language that's unworkable for one of the parties

Example of what language will help you:
◦ “Receiving Party must use efforts at least equal to those it uses for the protection of its own Confidential Information and, at a minimum, ensure it meets the standards proscribed by (insert regulation or standard for your industry here).”
Notice of unauthorized access to Confidential Information, and information sharing

Where is it normally found?
- Nondisclosure/confidentiality agreements, any agreement involving disclosure or use of business processes, designs, and other Confidential Information.

What is it?
- Defines when you will get notice of unintended access, and should also include language to support information sharing.
Notice of unauthorized access to Confidential Information, and information sharing

Why is this important to you?

◦ Your vendors (and hopefully also customers) really want to keep doing business with you. They may not let you know your information is out in the open, or if their access to your system was compromised.

◦ Intelligence - written appropriately, you can ingest information (as IOCs and for solid threat hunt hypothesis generation) that allows you to generate and prioritize alerts based on the tradecraft of adversaries who potentially completed ICS Kill Chain Stage 1 on someone else's network. Way better than a list of IP addresses to block.

Spoiler: This should be the hardest to get into agreements.
Notice of unauthorized access to Confidential Information, and information sharing

Unfortunate language:
- No Language
- Language that's unworkable for one or more parties

Basic Framework for what language will help you:
- In the event [insert Trigger – ex. the Receiving Party receives information from a credible source indicating unauthorized access to the Disclosing Party's CI], Receiving Party agrees to notify Disclosing Party [insert Time frame – ex. no less than 5 days after Receiving Party takes steps to remediate. Such notification must include [insert Information – ex. Yara rules identifying the attacker’s TTP, and access to relevant data so Disclosing Party may validate such rules and create additional rules].
Notice of unauthorized access to Confidential Information, and information sharing

**Trigger** - What triggers knowledge of unauthorized access?
- Examples: Random email from unknown sender, information from a credible source, opening an investigation, declaring an incident, root cause determined, incident response complete and report issued
- Maybe based on data access logs, but are they even logging access?

**Time frame** - How quickly information will be shared?
- Reasonable lawyers should agree you get (at least basic) information when they take action. (i.e. SOC resets the password of a user with access to your Confidential Information after a questionable login accessed your CI, if they remediate a box with access to your systems, etc.)
- Remember, their OpSec is important too.
Notice of unauthorized access to Confidential Information, and information sharing

**Information** – What information will be shared?

- Broad and cooperative in good faith... if possible...

- Meet and discuss annually – personally believe this is the preferred approach if there’s a chance for a solid relationship.

- Goal is for information sharing to be defined more or less by you and your counterpart on the other side without invoking a formal amendment process. That way it can be updated as collection and ingestion capabilities improve.
Duty to preserve data on triggering event

Where is it normally found?
• Nondisclosure/confidentiality agreements, any agreement involving disclosure or use of business processes, designs, and other Confidential Information.

What is it?
• Think of it as a litigation hold for OT data. If you or your contractors flash firmware or update config, you must keep a copy of the previous firmware or config.

Note: Contractors for either side may not be aware of this (or may have adverse interests if their product or service is implicated). This should be considered in maintenance contracts, warranties, etc.
Duty to preserve data on triggering event

Why is this important to you?

◦ If you get notice of unintended access, or they have an incident, it’s a good idea to prohibit wiping data and walking away.

◦ When an adversary does something novel in an OT environment, and it’s relevant to better safeguard the industry. Everyone benefits when the data is thoroughly analyzed and responsibly discussed.
Duty to preserve data on triggering event

Unfortunate language:
◦ No language

Example of what language will help you:
◦ [Append to previous section re: Notice] Finally, in the event unauthorized access to Confidential Information is suspected, Receiving Party will not destroy any data related to such unauthorized access. Further, Receiving Party will allow Disclosing Party to inspect such data so Disclosing Party can evaluate the extent its data was compromised.
Getting the right team

Getting the right lawyers

- My general rule for getting something done in attorney land can be graphed:
  - $X$ – number of attorneys
  - Slope – $Ix!$ where “I” is the Ignorance Factor
  - $Y$ axis – number of wasted hours you'll never get back
Getting the right team

Let’s focus on eliminating the Ignorance Factor!

◦ Get to know the lawyer(s) you’ll be working with, and make them comfortable with this disclosure. “We defined the standard of care and will live up to it, so disclosing unauthorized access isn't a liability.”

◦ Get to know their background and what they normally handle.

◦ Help by steering them toward definitions of terms in frameworks and regulations. Agreements can get bogged down over terminology.
Do It Yourself

Groups of 2-4 people

- 1-2 people per side
- Pick an industry
- What language would each side add or remove from the agreements?
- How would each side handle unauthorized access?

Agreement 1 – Confidentiality Agreement

Agreement 2 – Standard Terms and Conditions of Sale for Services
Recap – Confidentiality Agreement

I cherry picked sections from the past year or so to hit the high points.
Recap - Standard Terms and Conditions of Sale for Services

This is publicly available from a major manufacturer. Their Terms and Conditions for Products and Services was almost the same.