City Attorney's Guide to Navigating Cybersecurity and Lessons Learned

Thursday, May 8, 2025

Jason Alcala, City Attorney, Livermore
Mitesh Bhakta, Senior Assistant City Attorney, Mountain View
Derek Cole, City Attorney, Oakley and Sutter Creek, Partner, Cole Huber, LLP
Donald Hester, Cybersecurity Advisor, Cybersecurity and Infrastructure Security

Smart Cities Need Smart Procurement

The city attorney role in protecting your city from cybersecurity risks

Mitesh Bhakta
Senior Assistant City Attorney
Mountain View

Introduction

You might not realize it, but you are in the cybersecurity business as a city attorney. Almost every public service your city provides has a backend that is made possible by substantial internet-connected resources, and your city's long term vision likely includes many more "internet of things" (IOT) devices compared to five years ago. In 2025 your residents probably interact more frequently with the virtual form of your city than they do the brick and mortar of city hall. Even your city's employees spend most of their time working in a primarily digital-first environment. On a daily basis, residents and employees alike move large troves of sensitive data through your city's critical infrastructure. It should come as no surprise then that the modern city has become an attractive target for cyber threat actors, and the home front for a new form of global conflict that most closely resembles a "warm war".[1] [2]

Cyber threat actors generally fall into two major categories: those who are financially motivated, and nation state actors who are motivated by the winds of global politics. Both types of actors increasingly employ more sophisticated methods, including "hack now, ransom later" style attacks, or even turning their operations into an up-market business by selling successful methods of cyberattack as a kit.[3] Nation state actors have similarly become more sophisticated, finding new ways to silently enter, quietly gather data, and leverage common hardware en masse, or a "botnet" to devastating effect.[4]

---

[1] *China-Linked Hackers Breach U.S. Internet Providers in New "Salt Typhoon" Cyberattack* https://archive.today/20241007181947/https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835

[2] *Volt Typhoon Targets US Critical Infrastructure With Living-off-the-Land Techniques* *https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/*

[3] https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

[4] https://www.cybersecuritydive.com/news/86000-iot-compromised-eleven11-botnet/741507/

Unfortunately, local public agencies, and especially cities, attract both types of attackers. A financially motivated attacker might want to breach your city's utility billing system to acquire personally identifiable information (PII) for resale, while a state-sponsored actor may want to breach your city's utility system to understand how to manipulate the chemical composition of the water supply.[5]

While it can be tempting to assume that managing all of these issues can be outsourced to your security vendor or chief information security officer (CISO), in reality there are many practical steps you can take as a city attorney to improve your organization's defensive posture to both reduce the odds of a cyber attack, and mitigate harm when one does occur. This paper will provide practical guidance to help your office better understand your city's needs, properly frame risks for operational departments, and negotiate better vendor contracts.

Part I: Knowing Your Client

As is true with any other client, the first step in protecting your client is getting to know their strengths and weaknesses. A large city that has the resources to staff a fulltime IT department with a CISO and experienced software buyers is going to have some advantages, but also a larger attack surface compared to a medium or small city.[6] A large city is also likely to have far more legacy systems and bespoke solutions. A small city might have a small attack surface, but the unenviable task of delivering more robust security with the same budget as last year. A medium-sized city might be the luckiest of all: a fairly large attack surface, but with a limited budget.

This is where having a strong working relationship with your IT department is key. Your IT director probably has the best understanding of where the low-hanging fruit is for your city's cybersecurity defenses, what departments ask for the most, and what challenges they face when attempting to procure. You can use that information to help you effectively triage your city's procurement process into 3 groupings:

1) 90%-contracts that are on your paper, or cooperatively purchased/piggybacked.
2) 9%-contracts that are predominantly your terms, with minor redlines due to market conditions and extreme need.

---

[5] https://www.cybersecuritydive.com/news/federal-probe-vulnerabilities-us-water-systems/733331/

[6] The attack surface is the number of all possible points, or attack vectors, where an unauthorized user can access a system and extract data. The smaller the attack surface, the easier it is to protect. https://www.fortinet.com/resources/cyberglossary/attack-surface

3) 1%-contracts that are exceptionally high profile or high risk, negotiated with extensive participation by all stakeholders

If you can effectively triage your technology contracts into these three categories, you can maximize your effectiveness by limiting time allotted to 90% of contracts and maximizing your impact on the 1% of contracts that might truly make or break your city.

Of course, that sounds simple in theory, but in practice, it can be difficult, if not impossible, to determine which contracts are 1% contracts in advance. The key to solving that problem is helping your operational departments understand their risk profile and needs *before* the procurement process begins.

Part II: Framing and Articulating Risk

Understanding What's at Stake

The first step in helping your operating departments frame risk is clarifying what is potentially at stake with the contract. Suppose, for example, that your parks department wants to purchase a web-based application that will allow residents to book recreational facilities such as tennis and pickleball courts. The vendor is offering a hosted system, so your IT department doesn't need to acquire new hardware.[7] Your initial assessment might be that this presents no serious risk. After all, if the system is attacked and becomes unavailable for a period of time, idle tennis courts won't endanger your residents. Your parks department also doesn't want any of the application's payment features so no credit cards or banking information will be entered.

So far, you're optimistic. And then, you learn that your parks team plans to require names, dates of birth, home address, email, and contact phone number in order for residents to book; this is to prevent duplicate bookings, prevent bot-driven bookings, and ensure a legal adult is responsible for any minors planning to use recreational facilities. An anodyne booking system has now become a PII collection point, and you now have to help assess a risk for your client.

Your thought process probably immediately jumped to how you will contract for PII protections to shift liability away from your city and to the vendor, while also looking

[7] Hosted services are applications, IT infrastructure components or functions that organizations access from external service providers, typically through an internet connection. https://www.techtarget.com/searchitchannel/definition/hosted-services

out for insurance provisions that speak to the vendor's credibility in the market. That is certainly what you should do as an attorney, but your client needs a more digestible prompt in order to help bring actionable information to you in a timely manner. A simple ask is often the most effective:

> ***"Briefly describe the worst thing that will happen if the product stops functioning without warning".***

This appears deceptively simple, however, it can be very effective at encouraging your operational departments to look into the future beyond procurement. Departments are eager to solve a problem by purchasing a solution, but they often don't consider that a solution can sometimes fail and leave them in a worse position. By asking this simple question, you should receive a succinct answer that provides you with all of the following actionable information: 1) will health or safety be at risk?; 2) will critical infrastructure be at risk?; 3) will the city be exposed to a large financial liability?; 4) will the city face other material disruptions?

The next step is understanding how your operational department plans to actually use the product. Vendors can offer significant configurability, even for "out of the box" solutions and the exact configuration your city selects will greatly impact overall risk. For scheduling tennis courts, for example, the vendor might offer a solution that doesn't require PII entry but your parks department might still request that configuration for their needs. This leads to your next ask of the department:

> ***"Will any personally identifiable information, such as names, dates of birth, social security numbers, home address, emails, or phone numbers, be entered into this system?"***
>
> ***"If yes, which types of personally identifiable information will be entered?"***
>
> ***"How will your department use this information, and if it is not collected, can you successfully operate this system?"***

Note the prompt to consider avoiding PII collection altogether. Often operational departments continue past practices without considering their ongoing utility. This can be a very effective nudge that not only reduces your city's legal risks, but can also improve efficiency for operating departments.

Here again it can be important to pause and remember the value of your agency partners. Your city's risk manager and IT director probably have direct experience with the daily habits of your operational departments. If Post-It notes with passwords are

strewn on every monitor and those passwords are "1234", your IT director and risk manager may want to calibrate risk management differently and offer their own thoughts; even veterans and professional vendors can sometimes fall prey to these oversights, as Silicon Valley cities recently learned through some hacked crosswalk signals.[8] [9]

Understanding Your Vendor

So far, you've taken steps to understand your city's risk profile, but you haven't yet factored in the risk profile of your vendor. Technology vendors come in many flavors, and unlike with other public contracts, you can't lean on a surety or always find a peer city who has worked with the vendor. Nonetheless, you can build in some quality control measures to help round out the risk profile for your contract. Your risk manager will be able to offer standard cyber insurance clauses for the proposed scope of technology being purchased and intended uses. This is often the most efficient way to distinguish between good and bad actors.[10] Cyber insurance carriers act as signals in the market for a vendor's security readiness. They assess vendors before issuing any policy or increasing the limits on any policy, and conduct regular audits. While they can be notoriously difficult to collect from, their services as an auditor of best practices should not be overlooked. A vendor might offer many plausible reasons why they do not need insurance for your contract, but they will all distill into a simple fact: the vendor is unwilling or unable to meet the security demands of a qualified expert.

You can gather all of your city's risk factors and the vendor's factors into a simplified questionnaire shared by your office, IT, purchasing, and risk. By creating a one-stop-shop, you can reduce information silos and avoid creating resistance by operating departments. A sample has been incorporated at the end of this paper for your reference.

Finally, consider whether the vendor has appealed to your city using a lot of marketing jargon as opposed to concrete examples of performance. Many vendors, for example,

---

[8] Crosswalks in Redwood City, Palo Alto, and Menlo Park were hacked to imitate Elon Musk and Mark Zuckerberg. https://www.paloaltoonline.com/technology/2025/04/12/silicon-valley-crosswalk-buttons-apparently-hacked-to-imitate-musk-zuckerberg-voices/#:~:text=Crosswalk%20buttons%20along%20the%20mid%2DPeninsula%20were%20hacked,Mark%20Zuckerberg%20or%20Elon%20Musk%20began%20speaking.&text=Menlo%20Park%20spokesperson%20Kendra%20Calvert%20told%20this,and%20that%20city%2Dcontrolled%20crosswalks%20were%20not%20hacked.

[9] Subsequent investigation revealed that the vendor had not updated its default password, and had kept "1234" in place for the affected systems.
https://www.theregister.com/2025/04/19/us_crosswalk_button_hacking/

[10] https://www.fortinet.com/resources/cyberglossary/cyber-insurance

are eager to advertise that their product "leverages artificial intelligence" without explaining how that confers a benefit to your city. This might be an indication that the vendor is more likely to seek opportunities to use your city as a test subject for new features or new pricing models. A vendor who is carefully trying to incorporate new technology will be transparent about how they plan to manage this process, and typically provide assurances that they will use government-grade products, usually Microsoft Azure.[11]

Keep these factors in mind and work with your IT director and risk manager to assess the complete risk profile for the vendor. Low risk vendors working on low risk projects should easily fit into the 90% of contracts that can proceed along with minimal review time from your office. Contracts that have some mixed factors of vendor or project risk but can be easily contained should be part of the 9% that require some moderate effort.

Implementing this procurement approach will help you maximize your available time for the most challenging aspect of the procurement process: negotiation of the 1% contracts that are highest risk.

Part III: Negotiate Better Contracts

Negotiating new technology purchases has become increasingly difficult for cities of all sizes. The market is increasingly concentrated and vendors have become more brazen in suggesting they are replacing a professional service without offering the guarantees a typical professional would. Nonetheless you can still play a vital role at the negotiating table as part of your city's team by keeping a few things in mind. If you were able to help your client frame risks and complete a questionnaire as described in **Part II**, they have probably selected a good faith vendor who will be easier to collaborate with on critical areas of law.

First, distinguish what is a legal question from what is not a legal question. Your city charter, state procurement laws, and federal law will all come into play when working with a new vendor. Your city and the vendor will be concerned with different compliance requirements; you might not appreciate their limitations regarding incident

[11] Microsoft's Azure has become the gold standard for government technology vendors, including those offering artificial intelligence products. Its market position has become so robust it is now drawing anticompetitive concerns. https://www.techradar.com/pro/microsoft-accused-of-creating-a-monopoly-on-us-government-systems-through-free-upgrades

reporting, and they might not appreciate the scope of the California Public Records Act.[12]

Negotiating each party's ordinary compliance requirements is usually not fraught with difficulties. Most vendors will understand and accept that as local government agencies, we must seek certain common clauses such as requesting venue and jurisdiction in a city's home county, compliance with the California Consumer Privacy Act if a vendor interfaces directly with residents, and similar requests that are common across all California local agency customers. You will begin to encounter more challenges as you work with your operational department on the specifics of the work being delivered. For example, if your city is purchasing drones, your vendor is unlikely to be aware of AB 481 and the potential delays it might induce before the contract can be effectuated.

Your vendor might also commonly provide an uptime commitment and a series of credits if uptime doesn't meet contract minimums. Your operational departments will have to work with you to determine if this can create an unintended violation of state law. Similarly, there might be many aspects to the scope of work or performance of the technical delivery where an operating department or IT can verify a factual condition and address a legal requirement (think of this as a punch list). You can help your teams by flagging clauses that make it easy for them to know with certainty what they will be receiving and when.

Finally, go back to your questionnaire and review your operational department's assessment of what could go wrong if this vendor's product were to suddenly fail. Is life at risk? Is the city's ability to operate core functions at risk? Will the city be able to pivot away quickly in a crisis and terminate the contract? Consider these factors as you negotiate the most common pain points with technology vendors: 1) bankruptcy protections; 2) arbitration; and 3) damages caps.

Unlike many other vendors, technology vendors who file for bankruptcy protection can be especially disruptive for your city. Technology vendors provide specialized services for which a bankruptcy trustee may not be able to readily identify temporary talent to act as a manager of the firm or its assets as the company is reorganized or portions of its business sold off. From a security standpoint, much of the value a vendor offers at the time you enter into a contract is their reputation, much of which can be lost as a result of Chapter 11 reorganization.

---

[12] https://www.sec.gov/newsroom/press-releases/2023-139

A bankruptcy stay also prohibits your city from taking any adverse action against the vendor until the stay is lifted. This can put your operational department in a bind. To the greatest extent possible, attempt to characterize all or as many components of your contract as possible as 11 U.S.C. 365(n) contracts for the license of intellectual property.[13] Also keep in mind that any part of your contract not deemed to be a 365(n) contract will receive liquidated damages, and you may want to carve out a distinct liquidated damages formula for bankruptcy, up to the limit of California law.[14]

Vendors will commonly request arbitration or other alternative dispute resolution. Vendors prize this clause because it allows them to contain costs and avoid jury verdicts. If your contract is not the type that is likely to be controversial or lead to substantial damages, and if your city is able to retain highly qualified arbitration counsel, this can be an attractive incentive to offer a vendor in exchange for more valuable clauses elsewhere.

You should also be prepared for a vendor request to aggressively limit contract damages. Most technology vendors will seek to limit their maximum exposure to the trailing twelve months of contract payments, and obtain waivers for all special and consequential damages. Your bargaining position might allow you to obtain some more favorable terms at the margins, however, be prepared for an uphill climb on this issue. Keep in mind that if your goal is to keep your city secure and able to function during a crisis, you may have to make tradeoffs in order to achieve an optimal outcome.

<u>If All Else Fails, Observe the Business Judgment Rule</u>

There are many technology contract negotiations that become difficult not because of the law, but because of the attorney's perceived wisdom of the purchase. It can be tempting to blend legal judgment with business judgment and quickly become "The Office of No" in your city. This often results in operating departments avoiding legal review or worse, forum shopping. City attorneys often do have to be "The Office of No", however, unlike traditional procurement, technology purchases that avoid the city

---

[13] *See Mission Product Holdings Inc. v. Tempnology LLC 587 U.S.*__(2019). Please note that while this emerged as best practice after the US Supreme Court decided *Mission Product*, in practical terms its impact has been gradually blunted by economic reality. If your vendor is in serious enough financial straits and your contract or product is not profitable to the surviving entity, even transfer to a bankruptcy-remote entity may not solve the real-world problems of planned obsolesce or end of support for the product. Nonetheless, it can give your city precious time to find alternatives without a disruption in service that might otherwise occur.

[14] Civil Code Section 1671 quantifiability and reasonableness limits are not likely to be reached in most technology contracts that enter bankruptcy because your operational departments should be able to document the cost of onboarding a substitute vendor.

attorney's office can create more risk than an imperfect, but legally guard railed, agreement that you were able to negotiate.
When in doubt, borrow from the business judgment rule and ask yourself:

> ***"Is this contract so one-sided in favor of the vendor that no government official of ordinary sound judgment would conclude that consideration is adequate?"***

If the answer is "no", do your best to help your client with the agreement in front of you, and set them up for success for the next agreement. This will demonstrate that you intend to be a partner in their success, as opposed to an obstacle in their plan.

Conclusion

This brief summary to improve your city's technology procurement process should not neglect other preventative measures your office can take to help your city be prepared for a cyberattack. Work with your IT director to develop and regularly update your Cybersecurity Playbook. If you need help developing your playbook, or understanding vendor options for managing your security options, do not hesitate to contact me directly.