City Attorney's Guide to Navigating Cybersecurity and Lessons Learned

Thursday, May 8, 2025

Supplemental Resources

TECHNOLOGY PURCHASE QUESTIONNAIRE

VENDOR NAME: **Term:**

Description of Software, Service(s), and/or equipment:

Name: **Department:**

Req. #: **Req. Amount:** $

1. **General Questions**

a. What does the software/service(s) do? Please provide a short description. Paste link to all terms of service here as well

b. Who will use the software/service(s)?

c. How many user licenses will be purchased?

d. What is the worst thing that could happen by using the software/services being purchased? For example, if the software used to monitor industrial equipment temperature at a plant failed, the equipment could overheat and catch the plant on fire, causing employee injury or death and mass destruction of property.

e. How likely is it that something would go wrong? Include only actual vendor commitments to uptime, or external third party ratings of quality, no subjective assessments. Ex. Security Ratings.

2. **Commercial General Liability/Auto Insurance**

   a. Where is the work performed? Does the vendor ever come on-site?

   b. Does the vendor ever drive a car when performing tasks under the agreement?

3. **Workers' Compensation**

   a. Does the company have any employees?

4. **Cyber Liability**

   a. What types of information are included in the system, and what City information can the vendor access?

   b. Does the vendor access, store or process any personal information, such as personally identifiable information ("PII"), protected health information ("PHI"), or payment card information ("PCI")?

5. **Technical Professional Liability Insurance/Errors and Omissions Insurance**

   a. Will the vendor have access to City systems? Where City data/work product stored and what happens after the vendor no longer needs access?

   b. Where is the software located? Is the software on City systems, or does City staff log in through the internet to use the software?

c. If the software were to stop working or the software services were to no longer be available, how critical of an issue would this be?

6. AI Functionality:

Does the system utilize Artificial Intelligence?

If Yes:

a. AI Requirement:
Why is AI needed to address the issue?

b. Data Privacy:
What mechanisms are in place to protect people's data?

c. Transparency and Accountability:
If a problem occurs with the AI system, how would one know and who would be held responsible?

d. Reliability and Effectiveness:
How is the accuracy of this AI system ensured?

e. Fairness and Equity:
Could the use of this AI system result in discriminatory actions against certain demographic groups, or vulnerable populations, and how would one know?

f. AI Risk Management:
What processes are in place to manage AI risks?

7. Piggyback/Cooperative Contract? If Yes, California Agency? Contract#_____ (Attach)

8. Purchasing/IT: Similar product already in our portfolio?

CHECKLIST

Top Five Considerations for Deciding Whether to Insource or Outsource Incident Response

Today, every organization's cybersecurity strategy needs to include an incident response (IR) plan. Whether recovering from a ransomware attack or a compromised email, there are many aspects involved in responding to a cyber incident—such as containment, intra- and inter-department coordination, threat mitigation, business and data recovery, and after-action cleanup. There are several questions that can help you determine whether to manage this process internally or outsource this critical function.

The National Institute of Standards and Technology (NIST) Incident Handling Guide[1] is still a go-to resource today in helping security leaders make this critical decision. We've identified the following five questions to consider based on NIST's guidance.

Outsourcing remains as critical as ever for cybersecurity and response. Nearly 70% [of cybersecurity professionals] feel their organization does not have enough cybersecurity staff to be effective.[2]

☑ Do you have or can you find the right cybersecurity staff for IR?

IR team members need much broader security knowledge than most IT or security staff members. They must also understand how to use IR-specific tools, such as digital forensics software. And they absolutely must possess the right mentality (and passion) for the job. In a recent global survey of incident responders, it's no surprise that 67% noted daily anxiety in the role when dealing with an incident.[3] This is a specialty craft, within a specialized job function, making it more difficult to find professionals with appropriate knowledge and experience.

☑ Can I staff the function 24×7?

Although you hopefully won't need IR staff every day or even every week, as NIST notes, when you do need them, it must be right away. This means they need to be available 24 hours a day, seven days a week. Real-time availability is required for IR because the longer an incident lasts, the longer the adversary may be in the network moving laterally and invoking other processes like privilege escalation. The longer your data is at risk, the more potential there is for damage and loss.

☑ Can I afford the expertise?

Given the specialized skills, needed availability, and high-pressure environment, according to NIST, IR staff should be fully dedicated to the function. While it may seem like a good idea to make IR responsibilities a side job, it is a critical capability. Given this, NIST recommends separating this role from other security roles.[4] For example, IR would be a separate position from security administration and security operations.

☑ Can I afford the response-specific costs?

In addition to the compensation for specialized staff, NIST notes that organizations may fail to include IR-specific costs—such as the needed tools and up-to-date training on the latest adversary tactics, techniques, and procedures (TTPs)—in their budgets.

☑ Am I concerned about sharing access and information?

Keeping the IR function in-house keeps sensitive information, organization-specific systems knowledge, and privileged access in-house as well. But organizations must be realistic about all of the aforementioned realities and balance their risk accordingly. It can be a tall task to find the right specialized professionals, keep them segmented from the broader security team, and bear ongoing costs when they are often idle.

Conclusion

Unless you answered "yes" to all the questions above, you might seriously consider outsourcing either all or part of your IR function. When considering outsourcing, you can choose qualified cybersecurity companies that understand the landscape and hire qualified, trusted experts that have the necessary and evolving skills.

[1] Paul Cichonski, et al.,"Computer Security Incident Handling Guide, Special Publication 800-61 Revision 2," NIST, August 2012.

[2] 2022 Cybersecurity Workforce Study, (ISC)², October 2022.

[3] Security Incident Responder Study, IBM, July 2022.

[4] Paul Cichonski, et al.,"Computer Security Incident Handling Guide, Special Publication 800-61 Revision 2," NIST, August 2012.

FORTINET

www.fortinet.com

January 12, 2023 11:22 AM

1896566-0-0-EN