CHECKLIST

# Top 5 Considerations for Deciding Whether to Outsource Incident Response or Create an In-house Team

**Every organization needs to have an incident response plan as a key component of their cybersecurity strategy. The first decision that needs to be made is whether to establish this function in-house or outsource it. The National Institute of Standards and Technology (NIST) published a great resource[1] to help security leaders make this critical decision. We've identified the following five questions to consider, based on NIST's guidance.**

## 1. Do you have/can you find the right cybersecurity staff for incident response (IR)?

Incident response team members need much broader knowledge than most IT staff members. They must also understand how to use the tools of incident response, such as digital forensics software. And they absolutely have to possess the right mentality (and passion) for the job. This is a specialty craft, within a specialized job function, making it more difficult to find professionals with appropriate knowledge and experience. And, at last count there were more than 4 million unfilled cybersecurity positions.[2]

## 2. Can I staff them 24/7?

Although you (hopefully) won't need incident response staff every day or even every week, as NIST notes, when you do need them, it has to be right away. This means they need to be available 24 hours a day, seven days a week. Real-time availability is required for incident response because the longer an incident lasts, the more potential there is for damage and loss.

## 3. Can I afford them?

Given the specialized skills, all-hours availability, and high-pressure environment, according to NIST, incident response staff should be fully dedicated to the function. While it may seem like a good idea to just make IR responsibility a side job, not only is it a critical capability, but NIST recommends segregating roles. For example, security administration and operations would be a separate position from incident response.

## 4. Can I afford the ongoing costs?

In addition to the compensation for specialized staff, NIST notes that organizations may fail to include incident response-specific costs in budgets. Examples include funding for training and maintaining skills and physical security for work areas.

## 5. 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.

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. Unless you answered yes to all of the questions above, you should consider outsourcing either all or part of the IR function to qualified experts.

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

[2] "Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study, 2019," (ISC)², 2019.

www.fortinet.com



August 12, 2020 9:08 PM

D:\Fortinet\Checklist\734783 - IR Services\cl-FA-ir-services-onepage-footer-812020

742454-0-0-EN