Determining when you may need a consultant

Michael D'Angelo, CPP, CSC, CHPA

The author and other experienced independent consultants explain when to consider a consultant and what to look for.

(Michael S. D'Angelo, CPP, CSC, CHPA, is the Principal and Lead Consultant for Secure Direction Consulting, LLC. He is a member of IAHSS and a frequent contributor to this journal. He and the other consultants quoted in this article can be reached via their respective websites, LinkedIn, or the IAHSS membership directory.)

The ecosystem of healthcare security has several functional components. These may include the hospital's security leadership; line-level officers; policies and procedures; validated security technologies; training applications; the adoption of IAHSS guidelines; and the ongoing program assessment. Another component can be the engagement of an outside security consultant.

I have been a practicing independent security consultant for about a decade. After spending a career in law enforcement and a second career in healthcare security management, I felt I could be helpful to healthcare organizations beyond the one I was employed by, so I became a consultant. Below, I will address the circumstances under which bringing in a security consultant can be helpful, but I want to stress that I do not intend for this article to be a marketing piece for consultants. I can think of no better way to provide truly useful information than to draw on input

from several highly respected and experienced independent security consultants in our industry. As this article progresses, six of these individuals will help me demonstrate the "when" and the "how" when it comes to engaging consultant.

A DEFINITION

In this article, I am focusing on *independent consultants*—that is, people who are not employed by an industry provider. There are, of course, fantastic, qualified professionals who work for industry providers and deliver consulting-like guidance. However, engaging a consultant who has no direct ties to a security technology, hardware, or guard service provider should mean that the healthcare facility will receive guidance derived from an objective assessment of its current security program, an outline of its present vulnerabilities, and realistic, cost-effective potential solutions to those vulnerabilities. And that guidance should be free from any brand promotion or specific vendor recommendation. What should be delivered is a report serving the healthcare organization's own best interests.

WHEN TO CONSIDER A CONSULTANT

When you engage an outside security consultant, you are not merely signing a contract, writing a check, and then sitting back and awaiting a report. The healthcare facility and its leadership team must be dedicated to getting the absolute most out of the project's deliverables by putting in the time and resources necessary to aid the consultant in completing the project. I say "project," as opposed to "assessment," for several reasons. As you will soon see, the scenarios in which a consultant may be of great assistance to a healthcare facility extend beyond the completion of a security vulnerability assessment, and it is wise to be clear on what to expect.

Drew Neckar, of Security Advisors Consulting Group, LLC, says the first question he is asked when introducing himself to a potential client is often, Why would a business spend thousand or tens of thousands of dollars to hire a consultant? "I typically respond," he says, "by explaining why I regularly utilized a consultant when I was a security director running a healthcare security program. Early in my career, the

chief administrative officer of the system I was working for asked that I bring in an outside consultant to validate the recommendations I had made for changes to our security program. In this case, an independent security consultant not only validated the proposed changes but suggested some structural changes that would make my recommendations even more effective."

Neckar adds, "The other benefit of utilizing a consultant has to do with the nature of their work: Many consultants specialize in a particular area of the security industry, and they quickly evolve into walking and talking libraries of industry best practices."

Michael Dunning, of The Healthcare Security Consulting Group, divides some reasons a facility might need a consultant into a few categories:

- **Lack of time.** "Doing your daily job keeps you busy, so when an extra project is laid at your feet, you have to determine how you will rearrange your schedule and what other tasks can be delayed," Dunning says. "By engaging a consultant, you gain the flexibility of passing the new project to the consultant or allowing them to assist with tasks you have put aside."
- **Lack of resources**. "The new project may entail more resources than you currently have at your disposal. For example, perhaps you want to create a new training program but do not have the software or equipment to do so. Hiring a consultant will allow you to avoid having to buy new equipment and the learning curve involved — because the consultant would already have the development resources.
- **A gap in expertise**. "If the new project requires experience or expertise that you do not possess, hiring a consultant can bring that needed experience, and you can pick up additional knowledge during the process. Knowing your personal limits is a admirable trait for a security leader."
- **A need for a third-party review**. "There will be times when bringing in a fresh set of eyes to a project can provide a new or different perspective and identify things you may have missed. A sen-

sitive project or issue may benefit from a review by a disinterested party."

Tom Smith, of Healthcare Security Consultants, Inc, agrees that a consultant can help with areas that pose challenges to in-house staff. "In-house staff sometimes have difficulty maintaining knowledge of regulatory changes," he notes. "There are numerous regulatory bodies (TJC, CMS, OSHA, local health departments, etc.) that bombard healthcare facilities with additions or modifications to regulations. An outside consultant stays on top of these changes along with legal updates impacting the industry."

A security consultant can be a great source for best practices in our industry, he notes. "They can provide a fresh set of eyes to an existing security program or problem. Consultants also work hard to stay current on the latest and greatest in security technology. If your facility is starting a specific new program such as standing up metal screening points, a consultant may save you time and energy by recommending proven technologies."

"Security consultants," Smith adds, are usually seasoned, experienced former healthcare security leaders. They can be resources for internal professional development and the mentoring of your security team leaders and subordinates."

William Marcisz, of Strategic Security Management Consulting, who is an attorney as well as a practicing security consultant, observes that many hospitals seek out a healthcare security consultant after a critical event at the hospital or a care site. "In a 'near miss' situation, where something has occurred that exposes a suspected gap in security measures or processes, a consultant may be the source of how to properly address the issue."

Marcisz provides a sample scenario: "Say a psychiatric patient in the ER comes into possession of a firearm and fires a shot from the weapon into a wall without pointing it at anyone. Although this may be thought of as a 'no harm-no foul' event, there are repercussions in terms of process breakdown; most likely, staff will be justifiably upset that their lives were put in jeopardy and will begin asking questions about all kinds of issues that impact security and safety. Hospitals will do a root cause analysis

to find out what was missed and how to fix it. More often than not, this type of incident gets people thinking that maybe there are other issues they should be looking at in addition. In that case, bringing in an independent security consultant to look over the security program and safety processes is a good idea because they come with a fresh set of eyes and have the benefit of seeing how multiple different health systems address your issue."

It goes without saying that a consultant is not needed for the annual review of security vulnerability assessment if no major issues have arisen; keeping tabs on the overall security posture is well within the purview of the director of security or similar senior security leaders. It can make sense, however, to engage a consultant for a new security vulnerability assessment when significant architectural renovations have been done, a critical incident has occurred, or it has been a very long time since the last assessment was conducted.

WHAT TO LOOK FOR IN A CONSULTANT

Look for independence and direct experience in the healthcare setting. Although seasoned consultants may be qualified to provide security guidance in many industries, healthcare experience is a must. Healthcare has historically been one of the most highly regulated of all industries. In particular, standards and guidelines relating to the security function have grown more and more strict. There are now some aspects of CMS, TJC, NFPA, and several other professional and accreditations bodies that either directly or indirectly connect to a security function. A consultant with little to no healthcare experience would struggle to digest the environment and may find functioning in its highly regulated world difficult.

John White, of Protection Management, LLC, agrees about the importance of independence and experience in the healthcare environment. "The value of bringing in an unbiased healthcare security expert is immeasurable, provided that the 'expert' has the experience of running a healthcare security department. There are literally hundreds of so-called healthcare security experts advertising their services who do not understand the complexities of the healthcare field."

Second to direct experience is training and education, which should include formal education, specific industry training, and professional certifications. Related to this category would be memberships in applicable professional associations. For the readers of this journal, I need not spend any time explaining the importance of membership in the IAHSS.

Karim Vellani of Threat Analysis Group, LLC, highlights the importance of certifications: "There are many reputable security industry certifications a consultant may possess. These certifications demonstrate competency in knowledge of different aspects of security management. Some of the more commonly recognized industry certifications are the Certified Protection Professional (CPP), Physical Security Professional (PSP), Certified Healthcare Protection Administrator (CHPA), and the Certified Security Consultant (CSC). Along with industry certifications, consultants should be active in the many relevant professional associations. Consultants who attend associations' conferences and training seminars are typically more knowledgeable than those that do not."

QUESTIONS TO ASK

As is true of all groups of service professionals, security consultants are a diverse group. Vellani says. "Many have years of experience," Vellani notes, "while others have just entered the field. Some are specialized in specific industries, while others are generalists. Many consultant rely on their prior experience in law enforcement, the military, or as security managers and directors until they have developed the acumen for specific facilities and industries through their work in those areas." He suggests asking the following questions before hiring a healthcare security consultant:

- Is the consultant independent?
- Does the consultant have the requisite experience in healthcare?
- Does the consultant have any relevant certifications or credentials?
- Does the consultant have a track record of research and publication?
- Does the consultant have the business acumen to provide solid, defensible recommendations?

Dunning additionally suggests interviewing a potential contractor as you would interview a new employee. "They may have the knowledge you need," he notes, "but if personalities clash or they don't understand the environment you work in or the culture of your industry, the results will be less than you expected." He also recommends asking for references. "I can tell you how great I am," he comments, "but I am a little biased. Call the references and talk to them about what their project was, how the consultant performed, what they would have liked to have seen differently, and if they would hire them again."

CLOSING THOUGHTS

A recurring theme in the comments above is the value of a "fresh set of eyes." Healthcare security leaders are accustomed to working in a silo with restrictive budgets and staffing limitations. Yet, they work in an industry that is constantly changing—full of evolving regulations and the development of new best practices. Whether an organization is being proactive and using a consultant to assess and improve its program or being reactive in the aftermath of a critical incident, it may find that having an outside security consultant is an efficient way to meet its goals.

White has some advice for security managers whose organizations bring in an outside consultant: "A security manager has to be open to the assessment and exploring new ways of doing things. If the organization is going through the expense and due diligence of bringing in an expert, get to know that person and learn everything you can from them. Rest assured that whatever issues you may be facing at your organization, the expert has likely dealt with it in the past before they became a consultant, and they have helped others just like you to find a way to resolve the issue."