Security in requests for proposals in healthcare IT

By Andreas Ehrlund,
Senior Security Architect at Sectra

Buying new software systems for your healthcare enterprise is a precarious endeavor. On the one hand, replacing an old system that is holding you back or purchasing new functionality that will increase efficiency is a promising and positive thing. On the other, selecting the wrong vendor could cause delays, setbacks and even security incidents. In this article, I will offer my empirical experience of the current state of the request for proposal (RFP) process with a specific focus on cybersecurity. Lastly, I will give you seven concrete tips that will make your RFP more successful. But first, bear with me for a while. Or scroll down to the end if you are in a hurry.

At Sectra, we pride ourselves on knowing security. A large part of our company sells solutions for secure communications to the most selective of customers, such as NATO. The better-known part of Sectra has built software for hospitals for the last 30 years, so the complexity of systems such as PACS is well known to us. When you combine purchasing a complex system with high demands on cybersecurity, the proposal can quickly become daunting. Let's come back to this.

Responsibilities

What is security in this context? One way of looking at it is that security—or cybersecurity if you will—consists of three parts.

First, there is *Product Security*, which is our—the vendor's—responsibility. As a Security Architect, I make sure that the software we create is "Secure by Design". This is a fancy slogan to describe our ambition to ensure that all developers and testers are aware of and consider security in their daily work. If we can stick to that ambition as a vendor, we have a good chance of delivering secure products and keeping the trust that we have earned.

Second, there is *Deployment Security*. The most secure product in the world can be rendered useless from a security perspective if it is incorrectly installed and configured. Firewalls, proxies, hardening of servers, certificate management—the list goes on. This is a joint responsibility between us and the customer. We enable secure deployment through our products and documentation, and together with customers we create best practices for secure deployment. Our project engineers work closely with our customers to make sure the finished result is secure and adapted to the environment and infrastructure it will reside in.

Third, we have *Operational Security*. A system like PACS is a living thing, and any system in operation with users must be maintained and administrated. Passwords must exist, access and privileges must be given, and integration projects will be carried out. Security patching must be done on a regular basis. This is primarily the customer's responsibility. We—the vendors—are again the enablers but we do not run your operations.

For cloud or hybrid products, the last two areas are somewhat different since more responsibility is shifted to the vendor.

The RFP process

Now that we have established a context and language, we can talk about the RFP process. Lately, I have seen the number of questions in RFPs related to cybersecurity increase tenfold. It went from being a side note to a deal-breaker in just a couple of years. This is a good thing; it shows that the healthcare business is catching up with the rest of the world. The downside is that when scrambling for a better security focus in proposals, one might be tempted to think that more questions, broader questions or even more strict requirements are the answer. A cynical person might even believe that there are consultancy firms out there profiting from selling question packs with promises of compliance and all-encompassing coverage.

In fact, I would argue that fewer questions are better as long as those questions are the right ones. What are we actually purchasing here? A secure system yes, but in fact, if the product is good, are we not shopping for a long-term partnership and trust? Establishing that one of the vendors is the best one for you—the customer—should be our goal.

To establish that, one of the most important factors is that the customer understands all the questions and sees the need for each one. The customer should know what to look for in the answers, both good and bad responses. Because there will be red flags in those answers.

Questions should be constructed so that they, when seen as a whole, paint a picture of the vendor's security competence, capabilities and preferably also its stance on developing secure software. How transparent the vendor is willing to be could be a very important factor in your potential multi-year partnership.

Another drawback of overly strict or catch-all types of questions is that the vendors may be fatigued by the sheer number and scope of the questions. This might lead them to make assumptions as to what answers are expected or how others might answer the questions, rather than providing the most accurate depiction of the situation.

To summarize: fewer questions, targeting areas that really show the security capabilities of the vendors. Only use questions that you understand and see the need for. The RFP process is not an ISO certification audit; avoid noise.

Seven tips for a more successful RFP

Since you have read this far (or skipped to the last page), I will now reward you with some tailor-made questions and desired answers to look for. These are quite possibly already in your procurement templates. If so, good job!

I hope this advice can be of help to you. As vendors and customers, we are all in this together, and the goal is better security for our patients' data and for the critical healthcare services we provide to society.

Q: Are your applications, especially those facing public networks, penetration tested by an accredited external firm(s)? If yes, which one(s)?

A: Yes.
Comment: Using a third party for these types of assessments is not only a good idea, but might also be required depending on the legal environment and jurisdiction.

Q: Are you prepared to share the results of penetration tests conducted on your products? If so, how?

A: Yes (with elaboration on how).
Comment: A vendor with good security processes would not share penetration test reports in paper form, either physical or digital, without some sort of NDA. Look for replies like "we want to be transparent and are prepared to talk about penetration test results and mitigation in person or over voice conference".

Q: For application integrations such as URL launch integration, are your applications capable of PKI-based authentication?

A: Yes.
Comment: Moving away from legacy solutions like shared secrets (or worse, hard-coded passwords) for integration is a significant step up in operational security for application integration.

Q: Do you, as a vendor, regularly conduct your own internal security reviews, assessments and/or penetration tests of your products?

A: Yes (with details on methodology or even a documented process).
Comment: A security-aware software company should have at least some competence and capacity in this area.

Q: Do any of your software components contain hard-coded passwords or other credentials?

A: No.
Comment: In recent events, certain software vendors have been using these practices, and the resulting security vulnerabilities are always devastating.

Q: What is your stance on allowing customers to penetration test products, systems and/or services supplied by you?

A: Approves of these practices and is interested in taking part in either or both the results and the actual testing.
Comment: A security-minded vendor should always be keen to have its products tested.

Q: Do you conduct security patching of your products on a regular basis? If so, describe the method.

A: Yes. Look for signs of both reactive capabilities (acting on sudden vulnerabilities) and established processes (deploying remotely, code signing, etc.). Look for the use of modern operating systems, which greatly improves this area.

Comment: A good vendor makes it easy to stay up-to-date, and taking swift action on known vulnerabilities can avoid situations like the WannaCry incident in 2017.

This is a marketing material and may be changed at any time without prior notice.
Sectra will not be held liable for any errors or misconceptions herein.

SECTRA
Knowledge and passion