SeedPod CYBER

How to fill out a cyber insurance application with confidence

Recently an electronic manufacturing services company, ICT Systems, was denied coverage for a ransomware incident by Travelers Insurance. The reason? An easy-to-avoid but very costly misstep, it would seem:

In federal court, Travelers said ICT "lied about the extent to which it used multi factor authentication to secure its systems."
Travelers said it would never have issued a $1 million cybersecurity policy if it had known what it claims was the actual scant use ICT made of multi factor authentication.

The sobering bottom line? Travelers asked the court to find that it owes ICT zero in coverage for a May 2022 ransomware attack that targeted ICS' servers.

That's huge. Although the two companies settled out of court, the expense and stress were significant – and we don't know the terms of the settlement. Either way, it seems a clear loss for ICT.
You might suppose this misstep was entirely avoidable – but the ease with which it's avoidable may be overestimated. Why weren't they just "honest" in their declarations of how they used MFA?

The truth is, it's not that simple. It seems possible, in the current changing environment, that ICT intended to be truthful, but failed at that by not understanding questions on the

insurance application, or by not understanding potential underlying complexity of even such a simple measure as MFA.

The question is: how can you avoid making the same misstep?

The new challenges of applying for cyber insurance

A challenge now for many businesses, including MSPs and clients of MSPs, is that cyber insurers are paying closer attention to security controls as part of their underwriting process, and as a result, many applicants are surprised by the number of questions asked. Moreover, confusion can easily result from the wording of the questions.

As one example, almost all carriers are now requiring multi factor authentication (MFA). That seems straightforward enough at first glance. But careful applicants can be rightly unsure what exactly that may mean in any specific situation: Where does the insurer want MFA? What constitutes an acceptable MFA? And that's just one of the security controls insurers are asking for on almost all cyber insurance applications.

These applications have become so detailed, and often so confusing, that many businesses are now turning to their MSP to help complete the application, which puts the MSP in the uncomfortable position of the arbiter of what the questions are asking, what level of detail is required for the answers. They

also in many cases need to figure out how best to inform their client that they can't in good conscience answer all the insurer's questions affirmatively.

Whether you're an MSP or IT manager trying to answer these questions, this article offers you solid guidelines that will help you appropriately respond to questions in the application in order to put the business into the best position of getting good coverage that will be there if or when claim time arises.

1. Answer the question truthfully.

Sometimes answering truthfully is as easy as checking yes or no. In other cases, you may want to add clarifying information in response to the question. For example, given the Travelers Insurance and ICT lawsuit, you may want to define specifically where MFA is deployed within the environment. Or, if the question is around endpoint detection and response (EDR), you may want to clarify at which category of end points EDR is deployed.

2. Ask the carrier for clarification

If you don't completely understand the question, or it is poorly written, or if the question doesn't fall into a neat yes or no response, ask the carrier in writing for clarification, and get their response in writing – an email will do. Then base your truthful answer on that response.

3. Ensure that the application is treated as a business application

That is to say, not just an IT application. A number of questions require business leadership to answer. It shouldn't be left to IT to determine whether certain policies and procedures are in place. A good example is HR background checks, or policies and procedures about wire transfers.

4. Before the application is sent to the carrier, conduct your own vulnerability scan

This means specifically an external vulnerability scan of your environment and to implement a plan to remediate as much of the vulnerability as you can before submitting the application. A vulnerability scan is done via systems tool that takes an automated look at the network environment, checking to see what ports are open, what's running on the ports, identifies software versions and whether specific things are patched or not, in order to give you a sense of where there may be potential holes in your defenses. Many carriers will run their own scans after you apply. In this way you can get ahead of their findings so you can be in a good position, both at the time they review your application and at the effective date of coverage, of having your appropriate controls in place.

5. Conduct a joint discussion between business and systems leaders

Business and systems leaders should review the application together. Does the business have question for IT? Does IT have questions or concerns that need further clarification vis a vis business practices that may affect IT measures. (An example might be HR or client-facing privacy concerns regarding IT security measures that could be chosen or disallowed.)

Conclusion

Every application is its own animal, and these guidelines come from a necessary first view at 40,000 feet. But by being truthful, meticulously clear (and getting clarification in turn from the carrier), testing your own environment before the carrier tests it, and by having good relationships and communication between business and IT, the cyber insurance application or renewal doesn't have to be a painful process. Instead it can put in place one cornerstone of security for MSPs.