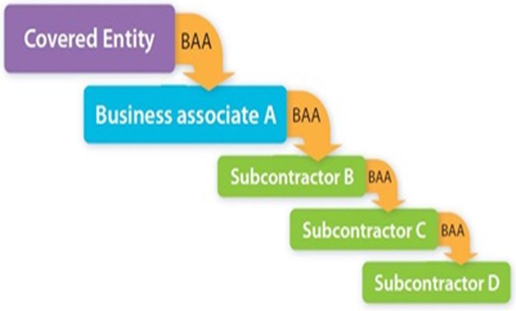
The IT Supply Chain Trojan Horse - What have you brought in the door?

By Daniel P Marcellus, President/CEO of SkyPort IT, Inc.

How do you trust that what's out there is truly helping your business? Recently, we helped a customer implement a new Ambulatory Surgery Center (ASC) management system that they had purchased. As a managed security services provider (MSSP), we provide services and systems that protects clients' data and provide reliable access to that data. Once the ASC system was implemented, we got a complaint from the client that one of their screens had a lag or pause of about 7-10 seconds, which was greatly affecting the data entry productivity. The software publisher could not reproduce this issue on their systems and had no other customer having the same issue. They came to the conclusion that it was our problem, so we started to investigate. There was no problem with the server or network infrastructure. So we reviewed the firewall from the internal side and found that systems were trying to access a server on the internet. As part of our security setup, we block access to the internet and then allow sites as needed, as well as provide a limited bypass via login to those who need greater access.

As it turns out, a programmer at the software publisher was using an unsecure Java applet server for some unknown "code." The delay was caused by the program trying to connect to the server but failing, and it would timeout after 7-10 seconds. From our perspective, the code in question could have been maliciously or inadvertently sending out patient information on the screen around each time of delay. Since the publisher claimed this wasn't happening with other clients, this also highlights a concern that security and coding may not be properly monitored by the publisher and their associated client networks. There really would be no way for our client to have known this was happening unless we implemented the internet access as we recommend doing.

HIPAA/HITECH regulations depend on trust but due diligence is lacking in the relationship between covered entities, their business associates and subcontractors they use. All of whom are supposed to follow the requirements of the regulations. In our course of doing HIPAA audits we find that many do not even realize they are business associates. Even without a formal agreement with a covered entity, a business is still liable if found to be complacent in a breach situation, other HIPAA compliant or violation.



Trust relationships are key in the era of shared data; patient-doctor, doctor-doctor, doctor-institution, institution-vendor. All require a level of trust, but who is really verifying it? How can IT help minimize risk and lack of due diligence by others in these situations?

The concept reported by Bloomberg on China inserting hacking chips into computer hardware for Amazon and Apple is real— and doable. Cars have been hacked into by criminals, and medical equipment has been hacked into by North Korea using leaked NSA tools. Could pacemakers be next?

Anywhere in the supply chain there can be an infiltration of any level of hardware or software. Each level in the supply chain should be doing due diligence of the level below, and each level needs to minimize the risks that can play a role in a possible breach. There can be covert chips, hardware, firmware, software providing backdoors, covert monitoring, covert control and other security holes. Of course there is also the plain negligence, poor practices, and lack of training causing similar issues. For instance, this is how the whole "meltdown and Spectre" attacks came about. CPU manufactures knew about this flaw but choose to ignore it over more than a decade once it was discovered. There is now the ability to cause great harm both logically through data and physically to patients through medical devices.

The only way to really protect yourself is to implement a layered approach based on denial and providing access as needed. Controls and monitoring are essential to this process. It can be a challenge at first to implement, but like anything else, the good things in life are never easy. Dealing with “security over convenience” balance can be frustrating for all parties.

Medical equipment should be on its own separate physical network without access or limited access to the internet and monitored. This equipment should not be on your general private network with other computers, and if communications is required there would ideally be a firewall in between to control access.

Our team has seen unwitting users charging their cell phones on equipment that just happens to have a USB port. This should not be allowed on user PCs and should be in the usage policy along with other restrictions. There have been breaches that have occured via cell phone connection to USB, allowing access to the internal network.

This could happen in any business, not just medical. It was only due to the fact that we took the time to fully secure the client’s network that we prevented and blocked a possible breach. Our implementation policies and procedures that were accepted by the client—and then followed—made all the difference in this situation. Bottom line: if your infrastructure has not been designed to help minimize the risk of other’s lack of due diligence or training, you are at great risk and may never know... until it’s too late. Trust but verify, verify and oh yes, verify.