TRANSCRIPTION OF: IS SECURITY THE ACHILLES' HEEL OF IOT?

BRIEF BIOGRAPHY ON PRITH BANARJEE (GUEST)

Prith Banarjee (originally from India) has been involved in both the academic and private worlds as a computer scientist. He holds many accolades, and has a Ph.D. in electrical engineering from the University of Illinois. His vast and exorbitant experience in cybersecurity includes being a senior VP of research at Hewlett Packard (HP) and being a director at HP labs. He was also employed by the ABB Group as the CTO and Executive VP.

Other roles have included being the Managing Director of the research and development arm of Global Technology at Accenture; and also, being the Executive VP and CTO at Schneider Electric.

At the present time, Prith is a Senior Client Partner at Korn Ferry, where he oversees all work that is related to the Internet of Things (IoT) and Digital Transformation Services at the Global Industrial Practice.

WEBNAR QUESTIONS AND ANSWERS

1) **How has your background influenced your thinking on the evolution of IT**?

   IoT is a very exciting field to be in. Companies like Schneider and ABB have products that deal with IoT. For example, they have come out with such items like switch gears, transformers, robots, etc. Once they are all connected amongst one another, other tools such as remote services, and predictive analytics will come into fruition. Also, the evolution of IoT will enable for brand new predictive based models to be built.

2) **Why is IoT is significant for industrial control companies like Schneider and ABB**?

   These companies are working on projects that relate to critical infrastructure, such as the oil and gas industry. They have been using traditional controls systems in order to run the process automation plants. The perimeters at these two companies has increased significantly, and as a result, they now have to deal with much larger security issues. This is why the implementation of IoT has become so important.

3) **As IT and OT converge, is there a gap in security understanding**?

   Let us take the example of an oil and gas customer, such as Exxon/Mobil or Chevron. Their IT infrastructure has been supported primarily by outside companies such as Oracle, SAP, Microsoft, etc. in the way of ERP and CRM systems. In terms of the IT side, people have always been present in order to operate the servers, switches, routers and other IT assets. But on the OT side, you are dealing with sensors, actuators, and other control systems. By nature, these systems have had to be located on premises in order to ensure strong levels of security for them. In the world of IoT, industrial companies are currently tying their control systems into the IT side. When this transfer occurs, this will lead to the generation of spare parts [NOTE: THIS PART DIFFICULT TO HEAR] that will become a component of the IT side. While the IT/OT convergence is good for the customer, security gaps evolve because the IT side is now being exposed and dependent upon the OT side. In other words, the perimeter of security has become widened.

4) **Is adequate security being baked into IoT or is it an afterthought**?

No, it is not an afterthought. With OT systems, traditional security methods (which have been physical in nature) have been deployed. These have been proprietary in nature, but they at least have some security baked into them. But, as the push for more open systems has evolved, and as the degree of connectivity has increased, people are realizing the greater needs for cybersecurity protocols to be implemented. The push for cybersecurity has been an active one, but approached cautiously.

5) **Is the perimeter security model out of date? Can critical infrastructure still rely on airgaps**?

Let us look at the oil and gas industry as example again. The plants here are very secure, from a perimeter standpoint, and thus are very difficult to break through. Also, the systems that reside in these plants are not connected, and as a result, they cannot be hacked into. Thus, this is the trade off with IoT. Along with the great value that it brings to the customer, there will also be greater levels of connectivity. There are much greater chances of being hacked into, and because of that, perimeter security is fading fast. An example of this are the metal detectors used at airports. The goal here has always been to detect people who are carrying a gun with them. But with the advent of technology (such as the 3-D printer), you can upload a 3-D design image of a gun. This can obviously get through a metal detector, and after passing through it, this plan can then be printed, and all sorts of bad things can happen. This illustrates the diffusion of perimeter security with the growth of IoT.

6) **What recent cyberattacks concern you? Has the game changed**?

Every day, there are new cyberthreats coming out. For example, who would have thought that a cyberattacker could hack into an IoT air conditioner through a backdoor? This is the reality of today. The surface in which a cyberattacker can penetrate into is now increasing at an alarming rate. Traditional attacks such as DDoS and database hacks are slowly starting to dissipate, because there are now mechanisms in place that can mitigate them. With the new world of IoT, there is a lot of damage that can done which people cannot even fathom yet. For example, if you have a very simple device like a panel or a breaker, with only an 8-bit processor in it, you obviously cannot use the software packages of McAfee or Symantec. This is so because the low level of memory cannot handle the processing power that is required by these applications. This is why cyberattacks are deemed to be very scary by the industrial companies.

Supplementary question:

What are the limitations you can do with signatures?

Yes, limitations do exist, because signatures have based upon the human interaction with computing systems. But in the world of IoT, there are many signatures that are being created, and because of that, a lot of data is required in order to interpret these kinds of attacks.

7) **Have fileless and memory-based attacks changed the cyber 'Kill Chain**?'

These kinds of attacks are very hard to detect. The weaponization by Lockheed Martin is now happening in the world of IoT as well as memory-based attacks. In these cases, perimeter defense is useless. Thus, there is a lot of interest in the products offered by Virsec, especially with companies like ABB and Schneider. The focus is on detecting subtle cyberattacks which try to mimic legitimate processes. As an example, in the oil and gas industries, the software automation processes have been in place for over 30 years. Thus, you simply cannot them out and replace them with new ones. As a result, whatever new security layers are being added on must be able to interact with this existing infrastructure. But, the industrial companies are reluctant to take this kind of approach. Instead, they are much more receptive to place a "little watchdog" in their legacy systems that can keep an eye out for fileless based attacks.

8) **Do we need greater C-level accountability for cybersecurity**?

At the board level, the topic of cybersecurity is brought up on a daily basis. The CEOs are constantly being grilled on how secure their systems are, and what the cyberthreat landscape looks like both at the present time and into the future. Cybersecurity has become a totally board related issue now. There needs to be a greater level of accountability for the C-Suite. The question that is now being asked is whether the CISO should report to the CIO or to the CFO. If the CISO reports to the CIO, conducting audits by the CISO often goes ignored. But if the CISO reports to the CFO, there are much greater chances for an audit to be conducted because the CFO is ultimately responsible for all of the assets of the company. This is a key governance issue that needs to be addressed.

9) **What are your recommendations for industry, businesses, and individuals**?

IoT comprises many market segments, which include the following:

- Industrial control companies;
- Automotive companies;
- Defense contractors;
- Aerospace companies.

It is the first group in the above list that is most interested in IoT. The questions that often get asked are as follows:

- How will the connectivity of IoT affect the bottom line of the business?
- What kinds of security be implemented?

The C-Suite is very concerned as to how security can be baked into the legacy systems. This is an issue that is getting a lot of attention, but there is no easy fix for it. This is due to the complex linkage that exists between the traditional systems and the new world of IoT.

<u>Other questions</u>:

1) **How important is security training**?

It is very important. The standard security procedures that are implemented must be taught to employees, including those that are involved in operations and research/development.

The cyberattacker is always changing their strategies, and thus, nothing can be considered as 100% cybersecure.

2) **How useful is attribution after a cyberattack is launched? Does it help you as a security professional to be engaged in this**?

There are three levels of cyberattacks:

- The threat of low level cyberattacks is now dissipating.
- The medium level involves many individuals trying to hack into larger organizations, such as banks, in order to capture assets and make money off it. This can be viewed as a "company attacking another company".
- The high-level attacks now involve nation state actors going against each other. An example of this is the US government cyber spying on China. For instance, it is possible to take down an entire electric grid of another country. Thus, nations need to make sure that their critical infrastructure is as cybersecure as possible.

3) **Should security be implemented at the controller level or the SCADA level**?

It should be implemented at both levels.