TRANSCRIPTION OF WEBINAR: PROTECTING CRITICAL INFRASTRUCTURE FROM CYBERATTACKS

1. ***Question #1: Would you draw any parallels between today's cyber threats and today's date (9/11)?***

ANSWER: These are interesting times. When 9/11 occurred, the threat was more "kinetic" in nature. This simply means that we were dealing with physical objects at the time, but today's threat is not well understood, given its Virtual nature. These times are very scary, for a wide number of reasons:

- When compared to the costs of planning to build a bomb or crash an airplane through a building, the costs to launch a Cyber attack are very low. This allows for nation states, Cyber attack groups, and criminal organizations, or even those individuals that are not happy with the world at the present time to cause both virtual and physical destruction, and even loss of life. Yes, Cyber-attacks are a nuisance, but there is a part of them which is not well understood - that is the loss of human life, and the ultimate level of chaos.

- The latter can happen when Critical Infrastructure has been impacted, such as gas lines, utilities, medical facilities, water lines, etc. In the past, our oceans protected us, but the Cyber threat is one that literally moves in nanoseconds. Either you are prepared or you are not. As a result, this makes hard for government leaders to grasp and understand, and because of this, it is very difficult for them to formulate policy to protect the United States that much more difficult.

2. ***Question #2: What are the biggest threats right now to critical infrastructure? How large are the risks to business and individuals?***

First, we will provide a strategic, or macro view first. The Cyber threat of course is a new one, and in the past, in order to take conquest of a Critical Infrastructure, one would have to send in an entire army to invade and gain control. The Cyber threats are coming from all over, for example from satellites, undersea network cables, etc. In Congress, there is no Critical Infrastructure group per se to help craft, formulate and implement policy to protect our Critical Infrastructures. A prime example of this is the national power grid. This is a Critical Infrastructure which of course spans many states, thus it is hard to get multiple states to come together as one unified group. Individual states may work on their own, but the probability of this happening is very low. The power grid is not resilient to handle a Cyber-attack, but it is getting better. Thus, having a large, private partnership for oversight is not something that "democracies relish", thus making a unified set of standards for Cyber-attacks against Critical Infrastructure. This is actually viewed as an increase in cost. But now there is a change in mindset that is occurring, but there are government officials that simply do not fully comprehend what a Cyber attack is, and even do not believe that a Cyber threat to a Critical Infrastructure is even real. There is now a fundamental shift towards having a public-private partnership with the Federal Government, in that companies can still remain as private entities, but still work on creating a strategic framework with the Federal Government, such as NIST type standards. Back to the example of the power grid, customers probably would be willing to pay a few extra cents in order to make sure that there power supply is safe from a Cyber-attack.

Unfortunately, this is a very slow process, and it may take a Cyber attack catastrophe in order to get things moving and the mindset of government officials to change.

In terms of risks to business and individuals, some of the largest Critical Infrastructures at risk are as follows:

- Electrical facilities;
- Gas pipelines (which include that of Propane and Natural Gas);
- Water.

So far, the least understood risk is that of how confidential information and data are moved across a network medium. This must be understood, as it will lay the fundamentals for the following:

- Intellectual Property;
- Sensors that are involved with the Internet of Things (IoT);
- Robotic Factories;
- Smart Cities.

This future Critical Infrastructure is at grave risk if a set of best standards is not created, and is not updated and/or upgraded in real time. There are a lot of strategies set in motion, but few are actually taking any grip or traction to fight off the Cyber attacker. It is imperative now to stop relying upon the conventional thinking of Perimeter Defenses, and to think more outside the box – such as how to reduce and take away the surface area of attack from the Cyber attacker.

The risks to businesses/individuals include the following:

- The loss of confidential information and data;
- The loss of Intellectual Property;
- The loss of the control of Shared Resources (a prime example of this is the Cloud Infrastructure);
- Water loss;
- Power loss.

Finally, the United States Critical Infrastructure cannot handle more than a few days of downtime, at most.

3. ***Is our perimeter mindset to security outdated?***
Can critical infrastructure still rely on air-gaps (the components that make it up are isolated from other components and/or the outside world)?

Answer to second question:

A lot of the Critical Infrastructure of the past did not need a lot of Security protection, because they were enclosed in a Closed Loop Network. But technically speaking, a Closed Loop Network is not really "Closed" to the outside world because they need to have connections to outside resources, for example. in order to install firmware upgrades, and other kinds and types of software patches and upgrades as well. The use of wireless technologies, which is actually part

of a Closed Loop Network is fast making it not so "Closed Loop" anymore, with the prime example of this being the use Radio Frequency (RF) Technologies to deploy various forms of Malware. This conventional thinking that Closed Loop Networks are isolated from the outside world needs to change in a drastic and quick way, if not, there could be grave Security risks.

Answer to first question:

No, simply relying upon the concepts of Perimeter Defense is clearly not enough, especially when you think Zero Day Attacks, Malware being formed from multiple sources, etc. Perimeter Defense is just a piece of the overall Security puzzle, but albeit, an expensive one. There is a "Nexus" now forming of the need for Security from a top down approach, such as addressing the needs of a democracy as a whole all the way down to the individual. Clearly, even Perimeter Defense will not be enough here either. It is important to note that there are not just Firewalls and Routers involved, but the human element as well.

4. ***How useful is attribution in defending against attacks?***

In other words, how useful is it to determine the origination point of the Cyber-attack and to actually confirm the identity of the Cyber attacker(s)? There are two sides of thinking here:

- Yes, it can be useful to do the above in order to bring them to justice;
- But it can be hurtful to you as well, because it can further expose you if you trying to conduct covert Cyber intelligence gathering activities.

But, if you are trying to build up a community of nations that the United States can rely upon, it is then useful to use the concepts of attribution to get the actual Cyber attacker, so that the country of origination can come forward and bring the Cyber attacker to justice. It is important to have a set of international norms with regards to attribution, if we are to get their cooperation in combating today's Cyber threat landscape. But this will be a slow and difficult process to achieve, in order to get to the actual "food source" of the Cyber-attack. But, there must be a crucial balance as well in terms of understanding the Cyber threat, defending against it, and apprehending the Cyber attacker. Thus, it is very important for more nations to get involved with this particular process from the standpoint of international law enforcement. Thus, if this were to actually transpire, it would be very "expensive" for the Cyber attacker to launch their specific threat.

5. ***What new hacking techniques concern you?***
What have we seen in recent high-profile attacks?

Answer to first question:

As opposed to the Security threats of the past ("Smash and Grab"), the Cyber attacker of today is taking their time (in fact as much as needed) in observing their victims, in order to figure out a plan of attack, and figuring out multiple backdoors. As a result, because of these efforts, once the Cyber attacker has penetrated your lines of defenses, it is then very difficult to spot them, and if you do, it is even that much more difficult to get them out of your impacted IT Infrastructure. The next hacking technique that is of grave concern is not the actual theft of data (albeit it still remains a Cyber threat), but the modification and changing of those datasets

will be very devastating, especially when it comes to the use of "Big Data", and the scrambling of information that resides in it. The financial sector is a huge victim here. Third, in terms of the traditional attacks, those lines of malicious code that assembles themselves together at run time still remains to be a huge Cyber threat. Or, take the example of the Linux Operating System. It has literally millions of lines of Source Code that resides in it. All a Cyber attacker has to do is take a few lines of code, and have the reassemble again, thus crippling the entire Operating System. Thus, it is very important not to just look at the Cyber threats that are coming to the software application in question, but also understand what its main purpose is and how it was created. In other words, it is very critical to examine if the system has been infected from within its internal structure. 97% of IT Systems here in the United States do not take the reassembling of Source Code into consideration.

Answer to second question:

Recent attacks are those that have occurred in the Middle East, where in one instance, some 30,000+ servers were knocked "out of commission". The governments in this part of the world are also changing how they interact with businesses and corporations, by shaming and embarrassing them if they are a victim of a Cyber-attack so that they lose their market share, and subsequently, their customer base. Another instance is that of Cyber-attack group based in Iran. They were literally able to open up a dam in New Jersey that was still under construction. The meddling into elections all over the world will be the next Cyber based threat. There was also the "Triton" Cyber-attack which had an impact upon the Security mechanisms of its target. Nothing was hijacked or stolen, but it did cost of millions of dollars in damages. This could be the next wave of Cyber-attacks as well – those that really don't steal anything, but cost a lot to the victim in financial terms.

6. ***How have fileless and memory-based threats changed the Kill Chain?***

The basic premise here is to break up the individual sequence of events (aka the "Kill Chain") that lead to the ultimate launch and execution of a Cyber-attack. But in response, the Cyber attacker will then say, Ok, if they are coming after me, all I have to do is just take out the sequencing of events, put in new ones, or even change the order of the existing ones so that I can still launch my Cyber-attack. With this kind of mindset, the traditional methods of Security will not stop the Cyber-attack, because the hacker is changing their every move in response to any risk mitigation strategy that is being deployed by a business or a corporation. Information Technology processes must still continue to operate even if there if Malware is still residing upon it – you can no longer afford to just completely shut down an entire system because of that. In other words, organizations must still continue to operate even thought there might be a "bad guy" present. How can this be done? This can be accomplished by running only the absolute necessary business processes, and isolating them. The use of Perimeter Defenses will not work under these circumstances. By destroying the Kill Chain, makes the Security solution we are trying to implement change drastically. Therefore, it is thus imperative to think "outside of the box" in this particular aspect.

7. ***What kind of accountability to we need – C-Suite and Government?***

In terms of examining this at the strategic level, the Federal Government is taking a very proactive stance on this. This is primarily due to the fact that C-Levels Execs simply cannot hold themselves accountable. There are two schools of thought here:

- The market forces can dictate what needs to be done;
- We need to have Federal Government intervention in order to hold the "C-Suite" responsible.

It is important to have a set of Best Standards that is both interoperable and to protect the individual consumer. There is a trend today for the Chief Information Officer (CIO) to report directly to the CEO, versus reporting to the Chief Financial Officer (CFO) or the Chief Operating Officer (COO). This is so because the CIO is now being held more accountable by the Board of Directors. Also, many businesses and corporations are now taking our Cyber Security insurance policies in order to protect themselves in the case that they become a victim of a Cyber-attack. Thus, it is very important for the "C-Suite" to do conduct their due diligence and to maintain the proper levels of "Cyber Hygiene". By doing this, a business entity will not only be entitled to a higher level of Cyber insurance favorability (especially when it is time for them to file a claim), but if they are also facing a lawsuit(s) in a Court of Law, they will also be treated differently. There is a "Cost Imperative" for the CIO to do their appropriate "homework". The market forces are now reacting towards this trend, but in a very slow process; not as fast as what people would like. There is also a movement in some states to hold all kinds of information and data private, under all circumstances. The emphasis here in the United States is more for implementing criminal penalties when compared to other countries around the world.

8. hat are your recommendations for the Public Sector, the Private Sector, and Individuals?

General Wheeler is a not a proponent of having "Big Government" getting involved in all facets of Cyber security. Rather, what is needed is to have a Cabinet Level Group within the United States Federal Government that is responsible for the oversight of domestic Cyber security. This involves having a set of Best Cyber security standards, Red Teams to conduct exhaustive Penetration Testing, and having a group come out to visit businesses and corporations after they have been hit by a major Cyber-attack (like what FEMA does in cases of natural disasters). Giving this potential entity autonomy and the ability to cut across all lines of the Federal Government (such as Congressional Committees, etc.) is an absolute must. It would also offer Cyber security assistance across all businesses and corporations in the United States, as well as implement some kind of warning system in the case that a large-scale Cyber-attack is imminent.

Other important takeaways:

*It is important to have Cyber security awareness training for your employees, but even more critical is to train them in the right way so that they have good levels of "Cyber Hygiene". Need to have so called "Threat Hunters"; it is important to implement Two Factor Authentication (2FA), End to End Security, specific Security Policies which are established to deal with the proper usage of Wireless Devices (especially "Bring Your Own Device" – aka "BYOD").

*You also need to hold employees accountable and responsible for any accidental leak of confidential information and data. This can also be referred to as the “negligent release of secure data”.

*Should we assume that the bad guys are already in our system? This is not an easy question to answer, you need to have all sorts of Cyber security layers implemented in order to avoid this from happening. But if there is a bad guy still present in your Network Infrastructure, this could mean that an Insider Attack could be in the works.