TRANSCRIPTION OF: CAN WE REIN IN THE GLOBAL CYBERSECURITY CRISIS?

GUEST BIOS

Troels Oerting

Troels is a highly experienced cybersecurity and law enforcement professional. He has established a new center for cybersecurity within the World Economic Forum (WEF). This entity is a global and, independent platform for addressing cybercrime and systemic risks.

He is also a former CISO/CSO for Barclays; the chair of the Europol EC3 Program Board; and a founding member of the Global Initiative against transnational organized crime. Troels has also been named as a 'Most Influential in Security' by Security Magazine in 2013.

He also has an M.Sc. from the University of Portsmouth, and is a graduate of the FBI Academy in Quantico, VA.

Usama Fayed

Usama is a well-known data scientist and co-founder of KDD conferences and ACM SIGKDD association for Knowledge Discovery and Data Mining. Recently, he served as the Chief Data Officer at Barclays Bank. He holds a Ph.D. in engineering from the University of Michigan.

Usama has also published over 100 technical articles on data mining and holds over 30 patents.

WEBINAR QUESTIONS

1) **The World Economic Forum ranks cyberattacks as a top global risk. What is the significance of this?**

   The cyberthreat landscape is 100% manmade. The cyberattacker wants to inflict as much damage as possible. We are going from bad to worse. One could hypothesize that things to a certain degree are getting better, but in reality, the trends are worsening. We are in the middle of a massive digital transformation. It is much bigger than the 4th industrial revolution. Really, this is more like a societal transformation because communications have widened and are happening at all levels, such as social media. Data storage is occurring in the cloud for cheap. Artificial Intelligence (AI) is now being used heavily, but this also creates huge vulnerabilities in terms of security, privacy, and integrity. The impacts are great, ranging from human lives to critical infrastructure to intellectual property. We have not been able to keep up with the cyberthreat landscape for the following reasons:

   - It is difficult to manage;
   - It is a different kind of climate;
   - Technology development is happening at a very fast pace, and because of that, we cannot keep up with the cyberattacker.

   There will be a very “bumpy road ahead” of us. The digital transformation is “ubiquitous”. The uncertainty of how to deal with the cyber risks is very real.

2) **How have cyberattacks evolved? What have been the consequences?**

There are two things to keep in mind with this evolution:

- We used to have a simple world where there were just a few cyberattackers. They could be easily tracked down via traces of evidence left behind, signature profiles, and temporary .EXE files.
- There has been a significant growth in the volume, variety, and tactics in terms of launching cyberattacks, especially with the increase of threats to fileless less memory systems. There are no traces of evidence left behind. It can take up to 40-60 weeks to detect a malicious file(s) in an IT infrastructure, and many more months after the fact to fully eradicate it. Difficult detection means that the patching process can be even slower as well.

Supplemental question:

Have the advanced threats now become "democratized? **In other words, you don't have to be a nation state in order to engage in cyberterrorism?**

The recent ransomware attacks have come out of the Eternal Blue, and weaponized by another entity. These are actually cyber spying tools, and it is the shadow broker that has brought them out to the "broader underworld". The focus needs to be placed upon the organized criminal groups that launch mainstream cyberattacks. We are now shifting from threat payloads that were launched from a malicious file attachment in an e-mail to file less memory attacks. The traditional security mechanisms cannot mitigate the latter. This is the real threat now. It is difficult to say with certainty if cyberattacks are democratized or not.

3) **Are concerned about cyber risks to critical infrastructure**?

This is a very strong concern. The next war will be in cyberspace. There will be a cascading chain of events that will follow, such as the electric and powerplants being knocked out, followed by a loss of communications and subsequently, control systems. The willingness to pay a ransom related to critical infrastructure will greatly increase. This is the "soft underbelly" – not enough attention is paid to it; thus, countries are scrambling to find fixes before a disaster happens. In terms of a digital perspective, the critical infrastructure is "fertile ground" here for the cyberattacker. Industrial companies still use very old IT systems, such as Windows 95 and Windows XP. Software patches and upgrades can take up to 24 hours push through, and even longer to deploy. Thus, there is a need to have technology added onto these legacy systems to detect advanced threats. Examples of this include machine learning, artificial intelligence, and deterministic analysis tools. The dilemma now is that older systems keep getting older, and newer systems are getting more complex and innovative, with no perimeter. Because of this, perimeter defense is eradicating quickly.

4) **What trends do you see in hacking techniques**?

Again, the volume and variety of this is very scary. For example, older cyberattacks (such as SQL injection attacks) are now appearing as newer variants. They now attack the APIs and other inputs of a software application. This kind of vulnerability can multiply very quickly. It is also important to examine what can happen at execution time. One needs to have the appropriate

tools to track if there are any differences that occur from the baseline profile. If they exist, then you know that an anomaly exists, which requires further investigation.

5) **Why aren't existing security layers adequate**?

There are lot of people out there that want to clean up the current levels of cyber hygiene, but doing it at a very basic level. There is a trend now to deploy malware directly into the memory itself, and not placing at the usual points of attack in a network or IT infrastructure. RDP is then used to deploy the malware to another point of attack. You can still have the traditional security layers in place, but the new ones need to be added on in order to keep up with the mainstream threats. Some 40% of file less attacks are now executed from memory. OT is often an overlooked area, and critical infrastructure is heavily dependent upon it. Cyberattacks are not aimed directly at the OT anymore, but rather at the supply chain provider. There are no tools at the present time to detect these kinds of attacks. Artificial intelligence is also being used for malicious purposes. The traditional methods of security are quickly getting outdated. Thus, it is important to look at the larger picture by examining what further steps can be taken beyond cleaning up the current levels of cyber hygiene. Air gapped security really does not exist anymore, because such systems are prone to insider attacks, social engineering, and inside leaks.

6) **How do attacks get Weaponized at Runtime**?

There is the known good and the known bad. In between these two, there is a small space. Security technology is being over done on the "non-bad"; and there is not enough being deployed for the "bad." The latter is a much larger space, and there are a lot of unknowns which exist here. A lot of threats are evolving at this level, such as going after the compiled code. Now, we are seeing the microcode vulnerable to cyberthreats and risks. In this unknown realm, anything can come through in bits and pieces, and get assembled. A few pieces may look "innocuous" at first, but after they get assembled, they become a weapon. It is important to figure out what to do here, as this is becoming an emerging threat where there is virtually no protection. There are a lot of security tools that are being duplicated, with very little value. The CISO is very concerned if the right protection is in place, and if there is too much being spent on too little. This will become a "game of clones". The new way of attacking is to make a profit, and scaling it up for further financial gain. There will never be fewer unknowns. It is up to the CISO to ensure that adequate levels of protection are in place, and that the right mix of security tools are being utilized to have maximum protection. This is not a "one-off", it is an ongoing process. This is done by constantly upgrading existing systems, but this could also lead to a sensor overload in the network. You should always assume that your system is compromised. If your data is not encrypted, and your key management approach is not tight enough, you will then have a data leakage problem. This issue is only going to get worse. You must also assume that your system is wide open to the public, and this will create a mindset that your "crown jewels" will need to be protected with the proper key management techniques.

7) **What are the top priorities for organizations to address these challenges**?

Cybersecurity is one of the top things to be worried about, focusing in on two key areas:

- Data protection;
- Critical infrastructure and system protection.

How can this be done? It can be done with the following:

- Having encryption in place, this should be the default functionality;
- Work on detecting the unknown threats, and try to exploit your knowledge of how systems should work normally. You should also be able to detect anomalies quickly.

In the end, it is not just about systems and software packages, but people are also a very important part of this process as well. It is not just the fusion of data, but the fusion of humans along with artificial intelligence tools. Cybersecurity is a combination of (in order of importance):

- Technology;
- People;
- Processes.

Risk assessment includes having the answers to the following questions:

- Who wants to attack me?
- What is their intent;
- What are their tools?

Once you know the above, then you need to critically examine the following:

- Your "crown jewels"
- The known vulnerabilities;
- Your controls that are in place – are they adequate enough?

It is very important to live in a protection mode, and always assume that you have been penetrated. With this in mind, there are two-time scales that are important to address:

- The protection time;
- The exposure times.

It is critical to encrypt both the data that is at rest and the data that is in motion.

Supplemental questions:

How do you document if protection is in place?

This sort of document needs to easily understood by an audience that is not tech savvy. You need to translate the cyber risks in such a way that they can be easily understood. This also needs to address not only the overall cyberthreat landscape, but also insider attacks. This document should also help your organization to formulate your "risk appetite".

How useful is attribution?

It is important to analyze the threat that you are being hit with. You need to understand the following:

- What is the cyberattacker after?
- What is their exploit motive?
- What are the tools that they are using?

Once you have the answers to these questions, you then need to extrapolate what future cyberthreats could look like. You need to have a balance of protecting both the knowns and the unknowns. This protection should have a mix of the following functionalities:

- Determining the time of execution;
- Detecting for anomalies;
- Establishing a low threshold for false alarm rates.

In the mind of the Cyber attacker there:

- Is no risk to launch a cyberthreat;
- There is not much investment needed to launch it;
- The profitability is high.

This trend will only lead to more levels of cybercrime. There is not much trust between nations to cooperate with each other in the cybersecurity world. Thus, you need attribution to create risk, in order for the cyberattacker to think twice before they launch their threat.