Alexander Cannell

CSIA 6010

Webinar Attendance 2-Chaos Ex Machina: Security from Obscurity?

**Summarize the Webinar.**

My Webinar 2 was the presentation you did, Professor Christopher Pogue. Professor Pogue is the Chief Information Security Officer for NUIX and also the Adjunct Professor for this class at Southern Utah University. Your presentation was about and titled Chaos Ex Machina. I hope it is ok I talk to you about you, or you not in the third person. There was four subjects that you talked about Our Digital Footprint, A New Order of Things, The Mess We’re In, and Security 2.0. You quoted Jeff Goldblum or Dr. Ian Malcolm from the movie Jurassic Park (1997) which I thought was entertaining but he states in the movie about the ethics of cloning a dinosaur, “Your Scientists were so preoccupied with whether or not the could; That they didn’t stop to think if they should.” You tied it to the point that we are advancing in technology in such leaps and bounds, but along with technology advancing we are also seeing an increase in data breaches. You asked, “are we creating problems that we won't be able to solve?” I agree with you on this point, I believe we are creating a lot of problems that we can solve. Just look at the Stir Fry weekly that we do. Each week we see at least two new security Breaches. But I would like to ask you a question do you believe that this progress is something we can stop or are we just going to have to be putting out fires as we go in order to accommodate that change?

Our Digital Footprint - You start this section by pointing out that looking back to when we first started to have computers and where we are today that technology is becoming a part of our everyday. You went through your technology history. I personally started off with a Macintosh Classic, but the computer I remember most from my childhood was the Mac OS 8 machine. That thing was legit I can remember playing WarCraft and other games on that machine. We had a computer in my house my whole life, but I’m a Millennial. Looking at life now, each one of my family has at least their own Computer and Smartphone. The point you were making was that we as a people have a massive digital footprint. We will have about 101 Internet of Things Devices for every person by 2022, then we need to concentrate on the computing aspect of those devices and most of them are single functional devices. With a number of devices we are seeing, we are seeing an increase in techno trash. I have even seen it in my own life, my closet at my parent's house is full of old parts, and the part that is still functional but is so out of date I highly doubt that I will ever use them again.

*The Mess We’re In -* We have a crazy amount of devices, where security is an afterthought. Companies want to push out this crazy new thing before the competition but neglect to put security first. Just so we as the consumer will buy it. Just look at after product release updates. I just bought a recently released game and had to wait an hour for all the DLC, but mostly the updates. We live in a society of release now and fix the problems with the product later. I can still remember when we had products that were built to last the apocalypse, but now we are seeing products being released with faults and bugs that break after a year or two of use. You called this a go to market society instead of a focus on security and blamed it on Microsoft, which I think is so funny and true. We aren't securing our data, or these new devices. You summed up your point nicely by saying, “We are not any better at defending our data today then we were 20 years ago. Arguably we are worse at it.”

*A New Order of Things -* How do we address this problem will determine or implement “a new order of thing” or a new way of doing things. You quoted Niccolo Machiavelli saying, “There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success than to take the lead in the introduction of a new order of things.” In Order to get into this new order of things, we need to start to be able to make sense of all this data, no matter what form or what device it coming from. This is where you brought up my favorite part of your presentation which is where is the point when we start to see change? You point out that we are seeing change correlating with major change. You used the example of the post-breach litigation being introduced more in the board rooms after the Target Breach in 2013. We need to as security professionals are able to tell a compelling data-driven the story in order to initiate change. When you tell a POLE (People, Objects, Locations, and Events) Stories then you can start assigning patterns to that story and through telling that story you can detect unwanted behavior because the anomaly behavior steps out of the norm. You then talked how new legislation shows that we moved from the server room to the boardroom and now into the courtroom.

*Security 2.0-* We have all this data that we are not good at protecting nor investigating we need to be able to tell the story of what is going on. You stated that we have all this data, device, etc and it all is meaningless it is just stuff, but when we add perspective then that stuff has context. When we can apply this data centered storytelling we are able to find the meaning behind that data. When we can determine the meaning we can understand the data, so we know what we need to do with it. You state that we are at a crossroads where we choose to move along the same path or do we choose to change where we start looking at these events in a new way so we don't have another trigger event.

*How do we move from where we are now to where we need to be? -* You say you hope that it doesn't hit the tipping point of loss of life, where we are forced to think about security/data differently. But it might need to happen. If something isn't important to an organization they don't invest in that thing. Companies are going to follow legislation. If you aren't protecting data in a reasonable way you become a criminal and are exposed to those consequences.

**Was the presentation succinct?**

I believe that you did a really good job on your presentation. I totally understood and agree with you about the need of change. I think that it will take a critical event to change but I still feel there is a need.

**Was the presenter prepared and knowledgeable about the subject matter?**

I feel you are very knowledgeable about the subject matter, you stated yourself you have been in the industry for about 20 years. That is a lot of experience in my book. I feel you were well prepared, for this presentation. It brings an aspect of storytelling and philosophy to our field which is exciting to me.

**Did the presentation clearly present a defensible position or was it merely a sales pitch?**

You mentioned your company NUIX once, I wouldn't say it was pitchy at all.

**What was your opinion of the presentation?**

I really enjoyed your presentation. It opened me up to some ideas about problems that I had not even considered to be problems before. I did see the problems like the data breaches, but I didn’t recognize one of the causes to be the lack of interest or prioritization of security. This presentation sparks an interesting conversation with my CISO, he thinks that you are right. But he believes that in general, it will require major events to instill change from the normal. That being said security needs to change at the individual and the company levels before there is a major change globally.

**What could the presenter have done better?**

I thought you did an excellent job, I am glad you assigned us to review two webinars. I’m now watching them all the time now, they are my new Ted talks addiction. My question is how do we become better storytellers?