PON Live! Cyber Negotiations: The Case of Ransomware
December 7, 2023

Q&A responses from speaker Professor Lawrence Susskind, MIT

Hello I'm Brahim Khalloqi from Morocco my question: How to insure effective negotiation in this case where we don't have sufficient information about the other part to conduct an efficient discussion? There's very little room for efficient negotiation. No room for value creation. It is possible, though, to make a deal to get access to your data back for less money than the attackers originally requested. You've got to be ready to pay in bitcoin. You've got to know what you will counter-offer. Preparation is the key to being able to do this. Have you inventoried all your data assets? Do you know what it is going to cost to recreate them (do you have protected copies that can be transferred in seamlessly)? You have one shot at reducing the amount of ransom being requested. But no, it's anything but an efficient negotiating context. And, the hackers have every reason not to extend (or even engage ion) negotiation.
Do you know of any cyberattacker being caught by police? If so can you share the story? My focus is on ransomware attacks in the public sector in the United States. I do not know of any instances in which the police have been able to identify, arrest and prosecute the hackers. There are a number of instances in the UK where teenage hackers have been arrested, but these cases have not involved attacks on infrastructure systems. There are some who think that national governments ought to offer substantial rewards to get people to turn in cyber hackers. For the most part, there is very little information released on the detailed attacks that have happened and efforts to catch the hackers.
xCan we recognise some signs that a cyber attack is comming soon?
xAre there any good resources for doing internal phishing vulnerability testing (or any other testing)?
There is a trend amongst the hippie community, some people call themselves "bio hackers". What do you think of that ? I'm not familiar with the bio hacking phenomena. Sorry.
In a hostage situation, how is value created for both parties? The agency that is hacked gets control of its data back (and avoids the cost of having to re-create the data or deal with its publication) while the hacker gets their ransom. Ransomware attacks in the US are probably occurring at over 1,000 a day. There are tens if not hundreds of millions of dollars being paid in ransom each year.
xGood evening, since you mentioned that the amounts of ransom asked are increasing exponentially, don't you think that there is bigger room for negotiation there?? Isn't a negotiation training becoming more necessary?
xDo the dynamics change if the cyberattack spills over into the physical world, such disrupting as water treatment or gas distribution?

Are there any ways to tell the differences between a state sponsored attack and a private attack? Not really. Several years ago, the US intelligence community lost control of hacking tools it had created in case the US might want to use these against its enemies. Subsequently, these tools were released (i.e. sold on the dark web to hackers). They were pretty expensive. The assumption was that state-sponsored cyber attackers bought and used these. Now, both individual hackers and the equivalent of secret (state-sponsored) hacking companies have access to all the tools they need. I don't think there's any way going forward to know who the cyber hackers are in any specific situation.
xThank you Larry! (BTW thanks for the kind words, but to be fair, I have zero experience in the area of cyber :))
How will individual differentiate government cyber scam and individual cyber scam. Again, I don't know how government-sponsored cyberattacks can be differentiated from individual attacks.
How would you deal with the confidentiality of the information of the clientele of the public agencies? Don't they have a legal obligation of protecting the information i.e. letting people know that there. has been an attack? So far, public agencies have not been held "liable" for lost data about members of the public because government agencies have what is called "sovereign immunity." On the other hand, we may be reaching a point where the courts will decide what a minimum "standard of care" is that cities or states have to reach to be protected from liability if they lose control of individual private data (i.e. bank account info, etc.). There is no legislation establishing a standard of care that applies to public agencies at present.
xWill the attendees receive your presentation slides
does your program also include helping the city with establishing a 3rd party risk program? How well thas that been recieved? Yes. Third-party or vendor cybersecurity is a big concern for cities or public agencies. In the past year or two, cities have been to put much more emphasis on requiring any vendor doing business with the city to at least attest in writing that they meet the same basic requirements that the city itself is trying to meet. There are also new products being added to the market that allows agencies to scan the information management systems that third part vendors are using. Sometimes vulnerabilities can be identified. So, every city should have a policy regarding how they will check and monitor the cybersecurity practices and vulnerabilities of any and all vendors and partners to whom they are connected on line. These need to be reviewed at least once a year.
In a cyber nagotions be used for peace building eg conflict between US and Russia. I doubt it. Russia claims that it has no control over the cyber attacking groups/organizations in Russia. That they are not creatures of the state. The US doesn't believe that. It is possible that the issue of cyber attacks on national security systems could become the subject of something like the arms control treaties of decades ago. It is also possible there could be a global treaty-making effort to press countries to promise not to use cyber attacks (in the same way we want them to eliminate or promise not to use nuclear weapons). This hasn't begun.
If we are talking about ransomware will there be a time when we will be analysing the psychological aspects of the perpetrator and also of the victim and how it impacts the business that has been attacked? What kind of Legal and economic perimeters can be thought about if

the international law is followed by all the jurisdictions similarly? Kindly shed some light on the role of governments during the negotiation period of a cyber attack. Thanks in advance. National governments have agencies that have responsibility for protecting their national security systems (or vulnerable infrastructure) from cyber attacks. Some of these same agencies in different countries are also trying to create cyber warfare tools "in case they need to use them" There is no global treaty governing the use of these tools for either offensive or defensive reasons. Israel has clearly used cyber attacks to slow the rate at which Iran is developing nuclear weapons. When businesses are attacked by cyber hackers and lose control of their clients' personal data, they can be held liable in court. Each case is considered on its own. There are private corporations that have paid very substantial fines or compensation. But this is because a court has determined that the company didn't adequately meet a basic standard of care and failed to fulfill its contractual obligations to its clients.
Are international bad actors being monitored or is this ransomware too evasive to detect? It could be being monitored in very sophisticated ways. That's not something that I know about.
does the ignorance a tactic to influence the hacker? Not sure what you mean. Some companies have tried to add easily vulnerable pathways to certain controlled on their web site (i.e. honeypots). The hope is that hackers will think the company is too lazy to maintain its cybersecurity and take the easy way in and end up taking what is basically non-valuable data. I've not heard of this working, but I'm not sure anyone would report it if it were.
w¿What is the most common way to interact with hackers?, just email? As I said in my talk: message on the dark web at the location that the ransom taker gave the agency being attacked to deposit the Bitcode ransom. It is not email on the "regular" internet.
if Crypto disappears, then does the blood for ransomware disappear? Great question. If crypto disappears (which I don't think it will), ransom takers would have not a secure and untraceable way of collecting their ransoms. This would probably eliminate ransomware.
Another question: Do you have one template for Incident response plan that fits all critical infrastructures or do you use an already available playbook for response? Each public agency needs its own playbook as part of its incident response plan. There are ways that public agencies could share basic playbooks, but there isn't one template that I know about.
xCan we have a link to the videos on the list of attacks?