Module 5 - Lesson 1 (Export2)

Thu, 9/9 3:54PM 10:36

SUMMARY KEYWORDS

cybersecurity, talk, subculture, technical, speak, communication, communicate, language, playing, robot, game, warcraft, organisation, geek, conversation, communicating, hacker, katz, people, gap

---

About eight or nine years ago, I was invited to play World of Warcraft. This is a fantasy theme computer game. A bunch of my technical staff they were primarily programmers, a few engineers invited me to play this game I never played before. But the programmer that invited me insisted I would pick it up quickly. Word of Warcraft in case you haven't heard about it is a massively multiplayer online role playing game or MMO RPG, there'd be a lot of people playing the game. So I figured I could ask for help as I needed and figure it out. So I agreed. And when we started playing, I quickly realised that everybody was extremely advanced. You know, I was like the rookie playing this game. And I also realised that everyone is working in the game extremely well together. In the game, there's different characters like he could be a druid that has special qualities like magic, or someone's a warrior. But everyone worked together seamlessly in the game, these programmers, so they're able to solve problems or quest as they're called in the game very easily. And what's interesting is they were aware of their differences. But they knew in order to capitalise and win the game, or not win, but get the next quest accomplished, they had to embrace those differences, and leverage them to work together. And even though this was just a game, and the consequences weren't really that big of a deal. My technical colleagues, who had difficulty communicating in person seem to be communicating pretty seamlessly in this game. And when I, when I saw this behaviour, it was very eye opening to me, because throughout my entire career, I saw many technical staff struggle with communication, either with each other or with a non technical member. But in World of Warcraft, they didn't really struggle at all. In fact, they communicated very well in the game. And they achieved their objectives most of the time, the quest fairly easily. And the other thing is they seem to enjoy doing it, they enjoy this communication, and playing this game.

Lead speak.

There's a communication problem or gap between our technical people and our non technical people, such as our company leaders. And this communication gap is typically because of geek speak, robot talk and poor listening skills. Our desire, or the technical people's desire to be part of a geek subculture is human nature, what we want to be part of something unique and special. That's what makes us significant. And part of that being associated with something unique and special, often involves having our own language or vernacular, or how we communicate or how we behave. leet speak is an example of this. It's an internet language, where standard characters and numbers are replaced with symbols. It was developed in the 1980s. And it's not used so much anymore. But an example of what people do to come up with their special language and how they come up with these things to be a subculture of uniqueness. So that fulfils someone's need to be significant. After the internet started growing. Hackers used leet speak to throw search engines off their sense, it worked back then the hacker language is still used today. And even some companies like Google use it as a way to like show a sign of appreciation or respect for the hacking subculture, example of leet speak could be like if I were to write out hack the planet, if I wrote that out in leak speak, I might write H four c, capital K seven, H three, capital P L, four in three, seven. So replacing like an A with a four, a T with a seven. And I'm replacing some of the letters with numbers. So that's an example of leet speak. And it's very common if we create a subculture for us to come up with our own way of communicating. But what this does is it excludes

everyone else we're dealing with and with technical people, they tend to speak technical jargon, so only their own subculture can understand and even within an industry like cybersecurity, even within Nisha as a cyber security, the language is different and very specific as well. As example, penetration testers will speak very differently than auditors. So this leads to massive breakdowns in communication even amongst people that are technical in this Industry not too long ago, I had a conversation with the CTO of my former company Alpine security and the conversation went like this. We need to exploit the vulnerability, get a meterpreter shell and then run Mimi Katz, do we need to kill Avi before prodesk. So that conversation, anyone that heard that conversation, we would probably have no idea what we're talking about, you know, what is meterpreter? What is exploiting a vulnerability, what is Mimi Katz, what is progressed, but that's a how we communicate normally based normal basis. And we often forget other people we're speaking with may not understand that robot talk, or a specific way of communicating friend of mine used to call it robot talk, she would hear me on the phone talking to my teammates, to my engineers. And she would say she didn't have any idea what I just said. And it would be like a five or 10 minute conversation, she would say she might have caught like three words that were intelligible. The rest of it, she said, sounded like robot talk, kind of like Charlie Brown's teacher. And in the Charlie Brown cartoon, it was like that weird conversation that did wah wah, wah, you never really knew what they're saying. But there was somebody saying something. And the challenges are one of the problems is the robot talk is typically on purpose. We don't have to talk that way. But we almost talk that way. So others can't understand what we're talking about. And if others don't understand what we're talking about, then they're not going to offer any help or insight into what we're discussing

why we speak like robots. We often resist changing our communication patterns, because we're afraid everyone or most people will discover that our special language really isn't that special, after all, but some of the the terms we come up with are unnecessary. Just a couple months ago, I was getting interviewed on a news station. And the interviewer asked me what I thought of comb, see OMB and I've been in cybersecurity. I've been an engineer for you know, 27 years basically. And I had no idea what combs stood for, I had to ask the reporter, and it stood for compilation of many breaches. Again, we came up with another term. Just to kind of confuse the issue in either confused me who's been in cybersecurity basically my entire career, one of the things we need to realise is cybersecurity is not really a subculture anymore. It's actually quite mainstream, pretty much on the news every day, interacting with people every day, cybersecurity is a common topic of discussion. And it affects pretty much every organisation out there. So in order for us to get better at cybersecurity or other technical industries that have become mainstream, we need to communicate in a way where other people understand what we're talking about, not just people within our specific niche, and the challenges if business leaders don't understand what we're talking about, they're not going to care. We often complain in cybersecurity, that we don't get the budget we ask for poor often asking for the budget in a manner where it's not understood why we need that amount of money. So we need to alter how we communicate. And I'm a big fan that the meaning of communication is response you get. So if you want to get the budget, for example, and we don't get the budget, then we didn't communicate in the proper manner. in cybersecurity. This problem is compounded because of certifications. A lot of the cybersecurity certifications, have you memorise massive amounts of acronyms. So it's almost like they want you to be able to speak in this geek speak manner or robot talk manner, and they test you on it. So then, we're armed with this list of acronyms, and it makes it more difficult for us to talk to normal people outside the industry, which is who we interact with. Most of the time, actually, especially for someone that's helping protect a client's data, or someone that is interfacing with a business leader for the organisation. key takeaways. There's a communication gap between our technical people and our company leaders. It is caused by geek speak, or robot talk, and poor listening skills. technical people resist changing their communication patterns, because they're afraid. Other people might discover that this super special language isn't really that special. After all, the robot talk is on purpose. This primarily goes back to technical people's insecurities and fears. There's always a way to simplify the language in order to communicate more effectively. But most technical people don't want to take the initiative to make those changes or to simplify the language. What's next. In the next lesson, I'll talk about the seven 3855 formula or model for effective communication, and how you can apply this in your everyday life. We'll also analyse the gap in communication that exists between technical members and company leaders. And what this gap is really costing you will also explore the differences between left brain and right brain people and how it affects how they communicate is a super interesting lesson and I can't wait to share it with you. I'll see you in lesson two