Alberto Daniel Hill

Definitions for Clarification

- According to *Best College Reviews*, a PMP Certification, or a Project Management Professional Certification, is a designation given by the Project Management Institute (PMI) to professionals who meet certain education and experience criteria. There are a number of requirements that professionals must meet before they can apply for certification.The PMP credential applies to managing projects in any industry.
- A *Synopsys* article explains ethical hacking as involving an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers. Also known as "white hats," ethical hackers are security experts that perform these assessments.
- According to *ISACA*, a Cybersecurity Fundamentals Certificate (CSX) verifies that successful candidates have the knowledge and skills required to identify assets and remediate vulnerabilities; configure and implement protective technologies; and detect, respond and recover from incidents.

- Wikipedia explains ISO/IEC 27000-series as comprising information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).The series provides best practice recommendations on information security management—the management of information risks through information security controls—within the context of an overall Information security management system (ISMS), similar in design to management systems for quality assurance (the ISO 9000 series), environmental protection (the ISO 14000 series) and other management systems.
- Sourced from a PwC article: Blockchain is the technology that enables the existence of cryptocurrency (among other things). A cryptocurrency is a medium of exchange, such as the US dollar, but is digital and uses encryption techniques to control the creation of monetary units and to verify the transfer of funds.Blockchain isn't an optional technology for cryptocurrency, but a foundational feature of cryptocurrency. According to an article on *getsmarter*, ultimately, blockchain and cryptocurrencies are joined through common beginnings. However, they are by no means of a similar calibre; when it's one versus the other, blockchain transcends cryptocurrencies. Not restricted to the financial sector, blockchain offers multiple solutions that are likely to disrupt diverse markets in the years to come.
- A *Norton* article offered a succinct definition of a black hat hacker. Like all hackers, black hat hackers usually have extensive knowledge about breaking into computer networks and bypassing security protocols. They are also responsible for writing malware, which is a method used to gain access to these systems. Their primary motivation is usually for personal or financial gain, but they can also be involved in cyber espionage, protest or perhaps are just addicted to the thrill of cybercrime. Black hat hackers can range from amateurs getting their feet wet by spreading malware, to experienced hackers that aim to steal data, specifically financial information, personal information and login

credentials. Not only do black hat hackers seek to steal data, they also seek to modify or destroy data as well.

- White hat hackers choose to use their powers for good rather than evil. Also known as “ethical hackers,” white hat hackers can sometimes be paid employees or contractors working for companies as security specialists that attempt to find security holes via hacking. White hat hackers employ the same methods of hacking as black hats, with one exception- they do it with permission from the owner of the system first, which makes the process completely legal. White hat hackers perform penetration testing, test in-place security systems and perform vulnerability assessments for companies. There are even courses, training, conferences and certifications for ethical hacking.
- Grey hat hackers: As in life, there are grey areas that are neither black nor white. Grey hat hackers are a blend of both black hat and white hat activities. Often, grey hat hackers will look for vulnerabilities in a system without the owner’s permission or knowledge. If issues are found, they will report them to the owner, sometimes requesting a small fee to fix the issue. If the owner does not respond or comply, then sometimes the hackers will post the newly found exploit online for the world to see.These types of hackers are not inherently malicious with their intentions; they’re just looking to get something out of their discoveries for themselves. Usually, grey hat hackers will not exploit the found vulnerabilities. However, this type of hacking is still considered illegal because the hacker did not receive permission from the owner prior to attempting to attack the system. Although the word hacker tends to evoke negative connotations when referred to, it is important to remember that all hackers are not created equal. If we didn’t have white hat hackers diligently seeking out threats and vulnerabilities before the black hats can find them, then there would probably be a lot more activity

involving cybercriminals exploiting vulnerabilities and collecting sensitive data than there is now.

Hill’s Profile Moon Books Publishing Blurb

As featured on the Moon Books Publishing website: Alberto Daniel Hill is the first Information Security Professional (The media gave him the title of 'Hacker') that was sent to prison in Uruguay he is working hard to change how computer crimes are investigated in his country.

Alberto is a computer engineer with more than 20 years of experience linked to Information Security (Consulting, IT security, Computer Forensics, Ethical Hacking, Information Security). He worked in many large companies in Uruguay and provided services for companies in other countries. In 2011, he specialized in the norms ISO/IEC-27000, also on Ethical Hacking and approved several courses related to a wide range of IT Security fields such as computer forensics, as well as an ISO/IEC-20000 specialization.

He is PMP-certified and has led many Information Security projects since 2011. He has the Cybersecurity Fundamentals Certificate (CSX) from ISACA, organization that awarded him with a PLATINUM membership recognition. The CSX certification in Cybersecurity demonstrates knowledge aligned with the National Institute of Standards and Technology (NIST), National Initiative for Cybersecurity Education (NICE), which is compatible with global cybersecurity issues, activities and job roles. He has been part of the team of volunteers of the chapter OWASP Uruguay since 2012.

He is recognized worldwide for his knowledge about Blockchain and Cryptocurrencies as well as every aspect that involves security in them. He has been selected as a speaker about those topics in the most important information security events in the world.

From Hill's Reddit AMA: The Highlights

- My name is Alberto and I am the first hacker sent to prison in Uruguay and I would like to change how computer crimes are investigated in my Country as the situation I lived along with my experience in information security and computer forensics made me see and feel a complete lack of guarantees in many processes followed by the police in the case I was involved. I also want to get support from everybody to a petition in CHANGE.ORG to change the points mentioned above. I spent 8 months behind bars but I was release(d) after appealing and being release(d) paying a bail. The process is still going on. I want to tell people how (life is) for a hacker in a prison in South America. I am willing to answer any question people should have about the world of hacking, the dangers you are exposed to living in that world where there is a very fine line between white and black but it's easy and sometimes you just cannot avoid crossing it. The experience I live in changed me, I am not the same person I was before this situation. I am now somebody who sees the world in a different way understanding many things I didn't ever care to understand before, and I am also a person that can get anything in life despite the obstacles I might find.

- Hacker in english is mainly interpreted as somebody doing illegal activities, that's why they try to explain the differences using white hat, black hat, gray hack hacker, a white hat hacker is the opposite of a criminal, fights against crime.I consider myself as a gray hat hacker, if i had to define myself. you must be in front of that ambiguous and tiny line that separates both worlds in order to better understand your enemy.
- I performed the first computer forensics work in a criminal case in Uruguay in 2004, then worked in government offices as information security consultant and i ended up in charge of the ISMS of the place, aligned to the iso iec 27000 norms. Then I worked in

the largest company of the country, the petrol company of Uruguay as an information security professional with a nice salary but i was not happy so i quit.

- I would actually love to hear the story from those who investigated it, and those who executed the warrant order to find answers to many questions that I would love to know. but no, there is only one press release, that as somebody says, is just a first draft of a story, is not complete, lacks of key information, and includes wrong information such as the fact that they said i was also cloning credit cards, and i had stolen money from other peoples banks accounts, that is what the DIRECTOR of Interpol in Uruguay said to the press.

- In 2004, I was the first person in a computer forensics process during a criminal case related to child pornography. So I worked for the law enforcement, and I know more or less the way they work and the tools they have and mainly, the human resources working in computer related crimes. in 2017, i was the first hacker that served time in prison, first it was like i had been taken from heaven to hell, for me it was the end of the world, but then, I could cope with it and to answer your question, It might be sound arrogant, but, I cant believe what I will write, my EGO jumped to the moon as I quickly realized that the most important hackers in the world served time in prison at some point of their lives.

Side Note: Another Reddit AMA involving Dark New Diaries

Highlights of a 2020 Interview

Source

- Alberto had everything going for him. But then everything went against him, thanks to his own tools of the trade, some of which were suspicious and questionable, that became damning evidence. In 2014, Alberto responsibly alerted a medical provider in Uruguay that they had a severe problem with their security after poking into it when his girlfriend requested him for her medical information. He even alerted the Uruguayan CERT. However, years later another individual hacked into the same website, stole information and threatened to reveal sensitive medical records in exchange for bitcoin. The authorities had two suspects, an unknown and Alberto. Thanks to his equipment and some questionable items, plus an admission taken through intimidation, Alberto was put behind bars for 8 months charged not with cybercrime, but with attempted extortion. But Alberto had the honor of becoming Uruguay's first jailed hacker. Here's part of an interview conducted with Alberto.
- "What are you most proud of in your career?"
    - **Alberto**: "Well, I lived in an extreme situation that took me to prison for a computer related crime I did not commit, and that changed my life forever. After being released, my story was part of the podcast **Darknet Diaries** and reached about 200k people by now, and I got the support from so many people, many of them telling me that my story inspired them, so, I felt that all the pain and damage caused to me by the situation, if inspired one person, maybe was worth it. I am proud of being respected in the field and the community."
- "What do you think are the biggest cybersecurity threats we are facing right now?"

    - **Alberto**: “Organized crime that is structured as enterprises, with clear business models with highly skilled people making a lot of money from computer crimes are a real threat now. Another one is the governments financed hacking activities that are happening now, and the next war will not be with guns, it is happening now and it's all about zeros and ones, and virtually unlimited budgets to support that.”

- Alberto had a harrowing experience while he was in prison, similar to him having a Hank Pym/Scott Lang moment with some businessman who recognized his talents. The man, who allegedly owned several companies wanted Alberto to hack into a bank for a certain amount of money. Alberto said no but the fact that man was stalking him and the possibility that the crime will still be pinned on him whether he committed it or not put him under extreme anxiety that he overdosed on Xanax and almost died. Alberto’s whole prison ordeal was eventually cleared and because of Uruguay’s inept cybersecurity law enforcement, Alberto decided to share his story in Darknet Diaries, to write a book about his life and ordeal and help in crafting legislation to prevent the same thing to happen to someone else.

In-Depth Interview

From Responsible Disclosure to a Prison Cell

Excerpt: “firstly, it was professional curiosity. I am a certified cybersecurity professional after all. Once I discovered the first minor flaw I decided to dig deeper because I thought about the medical information of hundreds of thousands of people. Sensitive data like that should be properly protected.

It was “responsible disclosure”, which means that if you want to help to solve a cybersecurity vulnerability, act in a way that will not make the initial problem bigger or affect the system in a more negative way.

I reported the problem correctly and responsibly. I did not take advantage of the vulnerability.

But I must admit that talking about it now, I do regret reporting the whole thing.”

The Case Against Alberto

Excerpt:“The police had a court warrant for search and seizure of “electronic media”. They interpreted that definition very liberally and selectively.

I later realised that the search warrant was severely flawed.

It actually named the defendant as “Alvaro Daniel Hill”, instead of Alberto.

The court authorised date for the search was wrong, it was the 7th of September instead of the 10th.

Effectively, there were so many irregularities around this search that I don’t believe anything that was taken during could have been used as legally admissible evidence. It was based on completely flawed legal documentation.

And it was a joke, the way the search was conducted. Because the police guys arrived unprepared and were overwhelmed by the amount of computer equipment they found, they had a problem with packing it all and removing it from my place.

They had no means of storage, no evidence bags, nothing. I think they were just expecting to find a desktop PC in my apartment that one could carry away under their arm. So they started

taking bags, backpacks and cardboard boxes from my apartment to load all the seized equipment into."

The Aftermath of Operation Bitcoins

Excerpt: "The cell I was first in had 12 other inmates, there was no available bed for me so I had to sleep on the floor initially. It wasn't nice, and I knew I had to adapt myself to that place and those people. I did not belong there. This was their world, they were not going to change to suit me.

The prison was depressing, it was not dirty or anything, but I felt very uncomfortable. I did not feel much fear initially, but any fear I could have had of that place disappeared when I was released."

"Anyway, I was used to being active all day, performing various tasks all the time, mostly anything that involved technology. But being there felt empty; days were dragging on endlessly and I only wanted them to be over so I could sleep. It might sound stupid, but this is how I looked at things.

Nobody starved in prison. The food was okay and there was food for everybody. Also you were allowed to receive food from your family so most of us did get one package with food, clothes and other items every week. We shared and helped those who did not get anything just because they had nobody outside to help them or their family couldn't afford to send anything.

Cell phones without cameras were allowed, that really helped me a lot as I could spend hours on the phone with my mother. She was unable to visit me due to serious health problems she has.

We also had satellite TV and an old Playstation 2. After my first week where I had to sleep on the floor with inmates that were violent or volatile, I was transferred to a cell equipped with all the things I just mentioned. For me it was like transitioning from living on the street to moving to a 5-star hotel.

Summer was cruel, due to the heat. In the middle of the summer in 2018, to keep myself busy, I started to give basic computer classes to almost 50 inmates. It was a nice experience but not only that."

Official Press Release from Police

A rough google translation:
The denunciation was rooted by the representatives of a private medical assistance mutualist from another country, before the Section for Technological Crimes of the General Directorate of Lucha Contra el Crimen Organizado and INTERPOL (D.G.L.C.C.O. and I.).

In the misma, I explained that the computer system of the misma received a cyber attack against its data base, since it was a sensitive information robot for the company. Subsequently, this entity received a request for money in exchange for releasing this information through an electronic mail.

According to the information (DGLCCO and I.), "the author asked for 15 bitcoins (virtual currency that amounts to a $ 4,000 unit, on the market) and from the request, every 24 hours spent, it would be increased by 5 bitcoins" .

The Investigation:

Personal de la Sección Technological Crimes (SDT), together with the Presidency of the Republic through the Security Agency of the Government (AGESIC) followed the tracks of the IP directions that were used to send the mails, in an operation that took several months.
I was in charge of Juzgado Criminal Literature of 11er. 20o shift and inspection. Shift, which I dispose of the immediate actions.

In the past few days, researchers have identified the source of this cyber attack, as well as the identity of who carried it out. This is the determination of an allanamiento in the capital of the country from where the Uruguayan of 41 years old, of naive computer profession a large number of computer material and other effects have been discovered.

From the author's home, the Police was unsure of 6 notebook computers, 5 cell phones; a card reader / recorder (device used to clone magnetic cards); a hard disk lector / recorder; a router; 13 computer hard drives; 125 original magnetic stripe plastics, 1 magnetic stripe post; 16 pendrives; 2 printers in color and a guillotine.

Other Offenses:

The Police located in this person's apartment an important corner of money, of dubious origin, which by mandate of Justice was sent to his analysis by the National Directorate of Political Science, to determine whether it is a false money. In this case, they were paid $ 1,460 dollars, $ 8,320 euros, $ 157 reals and $ 3,180 Uruguayan pesos.

Since the SDT, UNICOM has indicated that "this is the first case registered in Uruguay of a person who commits this type of crime and who has a thorough knowledge of transactions with bitcoins".

The Justicia I dispose of the process with the imprisonment of A.D.H.A. as responsible author of a crime of fraudulent knowledge of secret documents, in competition, it was a real reiteration, with a crime of extortion as a result of attempt.

Likewise, I would like that professionals from this University to carry out the pertinent expertise to the unsuspecting computer teams to determine other possible attacks by the author.

On the other hand, this operation continues on course "in order to determine whether he is responsible for committing other similar crimes that have not yet been reported" indicated from the SDT.