

Job 1: Finding Important Problems

Karan Thukral (20460691)

October 19 2016

1 Cyber Security

1.1 Problem Area

In order to understand the importance of cyber security, one must understand the implications of a compromised system and the effect hackers can have. In 2009-2010, suspicions arose that a sophisticated government-created computer worm called Stuxnet was loosed in order to disable Iranian nuclear plant centrifuges that could be used for making weapons-grade enriched uranium . It was found that a programming error allowed it to be propagated around the world on the internet ?? . The Ponemon Institute reported in September that 43% of firms in the United States had experienced a data breach in 2013 ?? . In July 2014, JPMorgan Chase & Co. was hacked, where information from 76 million households and 7 million small businesses was compromised ?? . Recently hackers extorted \$20,000 from the University of Calgary ?? . This happened due to the lack of proper security measures by the university in setting up their IT in-

frastructure ???. According to the FBI, ransomware attacks costed US business \$18 million between 2014-2015 ??. Access to the internet has made it extremely easy to transfer information and communicate but at the same time has made individuals more exposed. The internet allows individuals to organize protests against an oppressive government [egypt riots] but lack of security can make it easy for the government to track and capture these individuals. These attacks along with the recent Yahoo hack ?? which led to exposure of more than 500 million accounts are examples to show that security is not only a concern for individual or large corporations. The issue of cyber security is a concern for all users, corporations and even governments. Due to the large number of security breaches Eric Montague, president of Executech estimated that a company of approximately 50 people needs to spend \$57,600 a year ??. This cost rises the with the size of the companies and for companies like Yahoo this cost can be in the millions. The examples above show the importance and cost associated with user data and in turn the importance for individuals and corporations to invest in making sure this data is kept securely.

1.2 Existing Solution: Leapfrog

Canadian businesses can take up to two months to detect data breaches due to the lack of tools and resources while 75% of Canadian IT businesses don't have enough staff to run a security teams ??. In order to reduce this impact, Rogers Communications partnered with Trustwave in December 2015 to release a service for Canadian businesses called Leapfrog ??. As part of Leapfrog,

customers would receive real time monitoring around the clock by experienced security analysts. Customers would also get access to diagnostic tools to scan and run penetration tests against their network infrastructure to detect weaknesses. Besides tools, Leapfrog also gives customers access to dedicated support to help them meeting compliance laws and maintain their infrastructure ??.

As explained by the press release ?? Rogers attempted to solve the problem by using a combination of security tools and human interaction and expertise. Leapfrog relies both on software tools to run security tests as well as humans to monitor the network security along with providing support to the customers.

1.3 Existing Solution Mistakes

As mentioned above Rogers decided to use a combination of computer tools and human expertise in order to solve the problem. The first mistake here is relying on human expertise. According to Rogers 75% of Canadian IT companies cannot afford to hire enough security staff to run their infrastructure ??. Having Leapfrog rely on humans to monitor customer's network traffic adds a burden on Rogers to employ enough security professionals in order to support their customer base. This is a huge financial burden as most security professionals are paid between \$100,000 to \$150,000 a year ??. Besides monetary costs this is a huge undertaking due to the lack of security professionals available. The financial sector in Singapore is facing issues finding security professionals due to lack of skills and lack of awareness among companies ??. There is a similar trend in the US where a typical security person is paid the same salary as a

typical IT person despite the demand being higher. This slow increase in salary is not attracting enough people into the field leading to a lack of skills in the area ??.

The second mistake made by Rogers was only relying on exiting security tools which rely on IP and Domain blacklists amongst other things in order to detect malicious traffic ??. Blacklists are lists of domains and IPs that have been identified as malicious sites. Such tools rely on reactively preventing attacks instead of focusing on detecting them proactively. Blacklists are constantly updated when more malware hosts are detected ?? and these blacklists are used by other systems to prevent malware attacks. Google blacklists approximately 6,000 malware-infected sites everyday ?? but these are done either on detection of malware or discovery. The issue behind such an approach this that someone needs to get attacked or infected in order for these security companies to detect these malware infected sites reactively. Blocking such an IP does not guarantee security since the attacker can simply change the domain name or IP and continue the attack. The new domain or IP will only be blocked after its been detected and added to a blacklist. The simplest form of changing one's IP is using a VPN (virtual private network) ??. Thus relying simply on central blacklists is not enough to detect malicious traffic.

2 Heat Exhaustion

2.1 Problem Area

Heat exposure and heat illnesses are extremely serious and can also be life threatening ???. Toronto recently went through the worst heat wave of the summer ?? which according to research could lead to increased aggression, violence, increased rates of suicides and health concerns ??. Heat exhaustion is extremely prevalent in high school and college athletes in the United States claiming over 120 deaths between 1960 and 2009 ??. As per research approximately 1.5 for every 1,000 NCAA football players has a higher risk of heat illness due to exertion ??. As mentioned before heat exhaustion can be serious and lead to heat stroke and can also lead to death ??. Despite the high risk and casualty count, heat exhaustion is entirely preventable if its recognized and treated in time and before it leads to heat stroke which can have permanent effects. Pre-existing conditions like anaemia, asthma and heart conditions can increase risk of heat exhaustion ??. Extreme heat is especially dangerous for seniors and young children ??. As per a research published in the journal Environmental Research [4], there are significant negative effects on emotional well-being when the temperature was above 21° C. Aside from emotional effects, an estimated 120 people per year in Toronto die from extreme heat exposure [5]. The concern related to excessive heat exposure and exhaustion are extremely serious but at the same time easily preventable. Due to this, it's extremely important to solve this problem.