Book Review – Fatal System Error, Joseph Menn

Fatal System Error is a nonfiction work written by Joseph Menn that tells a story of espionage that penetrates the network of international mobsters and hackers who use the Internet to extort money from businesses, steal from tens of millions of consumers, and attack government networks. The book covers significant milestones between 1995 and 2009 and discusses the emergence of organized hacker groups such as the Russian Business Network and Chinese Network Crack Program Hacker group. This book is a must-read for people who are trying to understand how cyber criminals works and the depths at which it functions. The author delivers the story using two early cyber security practitioners: Barrett Lyon and Andy Cocker. Barrett Lyon is a cyber security expert and built one of the first denial of service protection companies named Prolexic technologies. Andy Cocker was an agent for the UK’s National Hi-Tech Crime Unit. The book covers activities in Estonia, Georgia, and Kyrgyzstan, where cyber criminals proved that cyber warfare was possible. The book also documents some of the first uses of Distributed Denial of Service (DDoS) attacks as a tool for ransom against gambling companies in Costa Rica. Menn also explains the impotence of US law enforcement when tracking international cyber criminals during this period. Menn got a lot of help writing this book from various prominent cyber security researchers, journalists and important commercial cyber security intelligence organizations like iDefense, Team Cymru and SecureWorks.

From a global perspective, the book is divided into two parts which reflects upon:

1. Commercial cyber-security

In this part, the story revolves around the rise of off-shore gambling companies and pornographic content on the internet. Around the same time, hackers discovered the possibility of Denial of Service attacks. They discovered that they could take down websites and servers just by bombarding them with a bulk of random data streams from multiple computers. Cyber criminals used this technique to attack offshore gambling companies and then demanded ransom. Since the shutdown of their websites and servers caused major financial loss, they paid the ransom. However, during one such instance, Barrett was called to mitigate this issue to avoid further attacks. This was the beginning of the commercial cyber-security services industry. Through Barrett, Menn describes how companies started looking for cyber security experts to protect themselves. Experts like Barrett mitigated attacks as well as setup mechanisms to avoid further attacks by handling traffic much better. That was a difficult task since the attackers used zombies, which are computers which have been infected and compromised by botnets created by the attackers. The book also sheds light on how these shady businesses started investing in cyber security businesses in the United States and also used it for money laundering. The story goes on to tell how these businesses started suffering from the investors’ focus on laundering and compromising the security business.

This story sheds light on the early rise of the cyber security business. It also gives the reader an understanding the need for cyber security, the financial motivation and the impact it can cause to a business. Menn lets the reader know that attacks such as denial of service attacks can cause a huge impact on business leading to losses in millions. Additionally, he also emphasizes on the fact that since the traffic is received from so many different sources, identifying the culprit is very difficult. Through Barrett, the story tries to convey the difficulties involving prosecution of cyber criminals, issues faced by major companies and the financial loss that was faced by the companies due to the cyber criminals. Menn also hints on the problem of lack of international cooperation since most cases involving international hackers would go cold. To make readers understand this issue more clearly, the story of Andy Cocker proved useful.

2. Law Enforcement & International Policy

Andy Cocker was an old-school British police officer working as an agent for the National High-Tech Crime Unit. He was frustrated with the inability of law enforcement to break down jurisdictional lines across international borders to arrest known cyber criminals. When he was informed about the Russian hacker by Barrett through the FBI, he decided to travel to Russia to make sure that legal action would be taken and decided to not wait for Russian law enforcement. He went to Russia and developed relations with the local law enforcement officials who were eager to bring these cyber criminals to justice. As the story develops, Menn describes the difficulty Andy faced while successfully ensuring that these criminals were arrested and tried. While pursuing one of these criminals, Andy learned that the criminal was, in fact, the son of a police commissioner. The commissioner got rid of all the evidence that could be used against his son to prosecute him. This was one of the instances where law enforcement itself protected criminals. Andy, through his experiences, conveys the difficulties one faces to prosecute criminals in a foreign country. The court proceedings described in the book as show how political pressure is applied on the legal process to protect criminals. Andy describes how the legal procedures were different in Russia as compared to the UK. Overcoming all these difficulties, Andy was still able to ensure that a lot of criminals were prosecuted and sentenced.

In this part, through Andy Cocker, Menn tries to make the reader understand the global aspect of cybercrime and the legal challenges it faces. Through the book, the reader understands the need for international cooperation for cybercrime and organizations that help enable it. The story is told in such a fashion that the reader himself realizes how legal boundaries hinder prosecuting cyber criminals. Menn, through this story also shows how criminals started working in groups and functioned as a criminal organization making it more difficult for authorities to bring them down.

Menn, in his book, then goes on to describe how nations started recruiting hackers for espionage. The example he used was called the Chinese Network Crack Program Hacker (NCPH) group. He also explained the reason behind recruiting them, which was to gain information and create an impact on other countries. Nations saw it as an arms race. Moreover, China did not hide this information but publicized openly how it planned to develop their own hacker group. From Menn’s point of view, nations find it more profitable to recruit hacker to work for them rather than send them to prison, since their expertise and resources would go waste in prison.

This book is a must read for all people who do not have an idea of cybercrime or do not understand the extent of it. This book is especially good for people to understand all the aspects of cyber security and how it developed. The financial, legal and international aspect are excellently described in this book which makes it perfect for anyone to understand the depths of cyber security. It is natural that the US government included this book in their policy as a must read.