# Cybersecurity Situation In Fiji

Shelveen Pandey, Nadeem Shah, Amit Sharma, Mohammed Farik

**Abstract**: We buy, work, play and essentially live online. As our lives progressively depend on information technology services, the necessity to protect our information from being maliciously disrupted is critical. Anything that is networked can be hacked, and with the increasing dependence on the Internet everything is being networked, therefore everything is vulnerable. This paper discusses common computer crimes threats, reflects on challenges & weaknesses of computer crime & cybercrime laws in Fiji, and provides novel recommendations for the way forward in fight against cybercrime.

**Index Terms**: Computer Crime, Cyber Security, Cybercrime, Cybercrime Law

## 1 Introduction

Cyberspace today is part of the daily life of people, industry, educational institutions and governments all over the world. Online shopping, online banking and social media are becoming ever more popular resulting in a powerful economy by enabling borderless exchange of information. This borderless ecosystem facilitates effortless and swift communication amongst citizens, businesses, educational institutions and governments. Nevertheless these benefits provided by the borderless environment come with immeasurable threats and costs. Dependency on networked systems generates novel vulnerabilities which lead to the increasing growth in cybercrimes. While computer crimes may not involve damage to physical property but rather include exploitation of critical information and confidential data. Computer crimes are costing billions of dollars worldwide. It is simply threatening the future of communication. Despite Fiji being a small country, there are Computer Laws which punishes criminals and these laws will be discussed herein highlighting the strengths and weakness of such laws. We are in 21st century and new types of crimes are evolving frequently and there needs to be a process of documenting and amending it in the law system so that these crimes can be challenged in the court of law. Some of the computer crimes are hacking, money-laundering, phishing, computer viruses and cyber-stalking to name a few. In Fiji, according to The Fiji Times newspaper (Fijitimes.com, 2016) more than 45 cybercrimes were received over the past five years of which 15 cases were related to internet banking fraud where the amount was totaling more than $120,000 from local banks accounts. An additional 16 cases related to email spoofing were also reported between 2013 and 2015. According to ABC news recently, Finance Intelligence Unit stated (ABC News, 2016) that cybercriminals stole more than $US 330,000.00 from locals over past 3 years According to ("Cybercrime Rose Significantly In 2015: Dell Security Annual Threat Report") cybercrime around the world increased radically in 2015 despite organizations deploying end-to-end security solutions flawlessly. Numerous security breaches were triumphant because cybercriminals found and exploited a fragile link in victims' security systems owing to obsolete solutions that could not catch these anomalies in their system environment.


- *Shelveen Pandey, Nadeem Shah, and Amit Sharma are postgraduate students in Information Technology in the School of Science and Technology at The University of Fiji.*
- *Mohammed Farik is a Lecturer in Information Technology in the School of Science and Technology at The University of Fiji, Email: mohammedf@unifiji.ac.fj*


## 2 Types of Computer Crimes

According to ("Cyber Crime – Types & Preventive Measures") crimes committed over the Internet are referred to as Cyber Crimes. The most universal types of cyber crimes are elucidated as follows:

### 2.1 Identity Theft

One of the most common types of cybercrime is Identity theft and fraud. When a person declares to be someone else with the intention of creating a fraud for financial gains, it is referred as Identity theft and impersonating to be someone else online is referred to as Online Identity Theft. Common reasons associated with assuming a false identity Online are obtaining credit card information, physical address, electronic mail identity, usernames and passwords to secure accounts such as banking and other financial institutions etc.

### 2.2 Ransomware

One of the most revolting malware based attacks are Ransomware which enters your computer network and encrypts your files using public-key encryption. Unlike traditional file encryption, with Ransomware the encryption key remains on the hackers server and the victim is ransomed usually with a monetary value to obtain this private key (Khanse, 2014).

### 2.3 DDoS Attacks

Bringing down an online service and making it unavailable by overwhelming it with traffic from multiple sources and locations is a form of a Distributed Denial of Service (DDoS) attack. Botnets which are large networks of infected computers are developed by planting malware on the victim's computers. This is usually done to draw attention to the DDoS attack which enables the hacker to hack into a system with the ultimate motivation of blackmail or extortion.

### 2.4 Botnets

Networks which consist of compromised computers remotely controlled by hackers to perform illicit tasks such as sending spam are called Botnets. Malicious tasks can be carried out by the use of Computer Bots which performs like malware to assemble a network of compromised computers.

### 2.5 Spamming and Phishing

Two very common forms of cybercrime are Spamming and Phishing. Unwanted electronic mails are categorized as spam. Phishing is when cyber criminals offer you bait in the form of a lucrative business proposal or a lottery which you never subscribe to and request for personal information prior to being able to claim this lottery. This usually involves divulging of credit card information or banking details which the cybercriminal claims will be used to deposit the lottery amount. Doing business with such claim ensures suffering both financially and mentally. Spamming and phishing attempts are mostly in the form of emails send by random people with offers that are too good to resist. These offers are usually also too good to be true with the ultimate goal of obtaining information to make fraudulent financial gains at the victim's expense.

### 2.6 Social Engineering

According to ("Cyber Crime – Types & Preventive Measures") a technique where cyber criminals make a direct contact with prospective victims using emails and phones are termed as social engineering. Criminals gain the victims confidence and once successful, they are able to extract the information such as banking details, employment details or anything that the criminal may be interested in which will assist them in committing the intended cybercrime. Using social media and social networking sites, basic information about people can be extracted quite easily. This basic information in then utilized as the base to befriend someone and extract additional information. Once required information is extracted, the criminals will vanish leaving the victim with financial injuries or the likes. Information obtained through social engineering can also be sold online, or utilized to defame someone of the public status.

### 2.7 Malvertising

A technique whereby users download malicious code by basically clicking on certain advertisements on infected websites is known as malvertising. In majority of the cases, the websites involved are not guilty. It is the cyber criminals who insert malicious advertisements on the websites without the knowledge of the latter. Usually cyber criminals demonstrate spotless advertisements for a short phase and thereafter substitute it with malverts so that the websites and advertisements do not suspect their malicious behavior. These malverts are removed from the various sites after the cybercriminals have met their targets. This happens so fast that the website does not even realize that they were used as an instrument for cybercrime. Malvertising is one of the fastest, increasing types of cybercrime.

### 2.8 PUPs

Potentially Unwanted Programs (PUPs) are less destructive however more exasperating than malware. PUPs install superfluous software in your system inclusive of search agents and toolbars. PUPs include spyware, adware and dialers. One of the most commonly noticed PUPs in 2013 was the Bitcoin miner ("Cyber Crime – Types & Preventive Measures").

### 2.9 Remote Administration Tools (RATS)

Remote Administration Tools are utilized to facilitate unlawful activities. Remote Administration Tools can be utilized to control remote computer using shell commands, embezzle data, and transmit locations of the affected computer to a remote controlling mechanism.

### 2.10 Exploit Kits

Vulnerabilities are problems in the coding of software that permits cyber criminals to obtain control a computer system. Exploit kits are ready made tools available in the online bazaar which can be purchased and used against individuals and organizations. Furthermore these exploit kits are upgraded like ordinary software however unlike legitimate software these are illegal and mostly available in hacking forums and on the Darknet.

### 2.12 Scams

Some noteworthy Internet scams are scams which have exploited the Microsoft name and other big technical support names by phoning computer users randomly and offering to fix their computer for a certain fee. Innocent citizens are ensnared by scam artists into Online Tech Support Scams and are strained to fork out money for non-existent computer and fabricated problems.

## 3 Computer Crime Laws in Fiji

The Crimes Decree 2009 (Decree No. 44 of 2009) covers Computer Offences in Division 6 from Section 336 to Section 351. According to (Cybersecurity in the Republic of Fiji, Tamanikaiwaimaro) the Crimes Decree is the primary legal instrument that criminalizes computer offences and this Crimes Decree is not equipped to capture the convolutions and the varied collection of cyber security breaches that occur in Fiji which influence the cyber security ecosystem and infrastructure in Fiji. The cybercrimes unit and the law enforcement authorities of Fiji are challenged when attempting to criminalize computer offences when complaints against computer offences are investigated. The primary contributor to this challenge is the lack of articulate legislative provisions criminalizing computer offences which would enable criminal charges to bring against suspected lawbreakers. Due to this, the crimes committed do not to represent a criminal act under the current legislations. This makes Fiji incredibly susceptible in terms of the ability to criminalize cyber offences under the current Crimes Decree, especially considering the complex types of cybercrimes committed in more developed countries and their associated and existing cybercrime laws.

## 4 Some Recent Cyber Crime Cases in Fiji

### 4.1 Cases in 2013

- In 2013, a Suva based company lost US$65,000 to cybercrime in a single remittance transaction for acquisition of soft goods from Taiwan whereby payment was diverted to UAE and then to India.
- In 2013 a Suva based company lost US$44,000 to cybercrime in 3 transactions for acquisition of raw materials from China & Belgium whereby payments were diverted to UK; ("Fijian Firms Lose Thousands Of Dollars Through Cyber Crime | Fiji Sun")

### 4.2 Cases in 2014

- In 2014 a company in Savusavu lost NZ$58,000 to cybercrime in a single transaction for purchase of an excavator from NZ whereby payment was diverted to Scotland.
- In 2014 a Suva based agency lost US$101,000 to cybercrime for the acquisition of clothing from Israel whereby payment was diverted to UK.

- In 2014 a Suva based company lost US$10,000 to cybercriminals a single transactions for the acquisition of industrial spare parts from China whereby payment was diverted to another company in China; ("Fijian Firms Lose Thousands Of Dollars Through Cyber Crime | Fiji Sun")

### 4.3 Cases in 2015

- In 2015 a Nausori based company lost US$13,000 to cybercrime for the acquisition of food and supermarket products from Pakistan whereby payment was diverted to UK.
- In 2015 a Suva based company lost US$14,000 to cybercrime for the acquisition of motor vehicle spare parts and tyres from China whereby payment diverted to another company in China. ("Fijian Firms Lose Thousands Of Dollars Through Cyber Crime | Fiji Sun")

### 4.4 Summary of Cases

In total 18 cases of Cyber laundering through email spoofing were investigated by the FIU (Finance Intelligence Unit) between 2013 to 2015, ("Fijian Firms Lose Thousands Of Dollars Through Cyber Crime | Fiji Sun"). Summary of offences were as follows:

- 4 attempted cases amounting to F$300,000.
- 1 case of recovery of stolen funds: amounting to F$60,000.
- 13 cases of stolen funds amounting to F$724,000.

## 5 Weaknesses in Fiji Cybercrime Laws

An Online boutique which had operated before as "Pink Window Creation" in 2013 (Swamy, 2014) never delivered the items which the customers purchased through Online Social Networks. Later in the report it understood that the charges will be dropped if refund is made before the first hearing date. Due to not having specific cyber crime laws in Fiji regarding Online Buying in Fiji, the absence of law allowed the same owner to create another Online boutique account (Desi Fashion House) and again after (Newswire, 2016) items were purchased, delivery of these items was only done initially to build a customer base. Once customers were satisfied and trusted the Online Store, a request of large orders was made by payment of large sums of money, and these items were never delivered. A case according to (Paclii.org, 2016), where the accused used false information in the social media sites and took $240 which later has been charged as "used computer to gain financial advantage" under "Serious Computer Offence" and "Obtaining Financial Advantage by Deception" contrary to sections 318 and 341 according to Crimes Decree No 44 of 2009 at a sentence of 1 year imprisonment and a suspended sentence of 3 years. Due to no presence of specific and stringent cyber crime laws in Fiji, this sentence could have had a harsher penalty which would act as a deterrent for future cybercriminals.

## 6 Fiji's Participation in Cybercrime Awareness And Prevention

According to (Anon, 2014), Fiji is a member of ITU-IMPACT initiative which has access to appropriate cybersecurity services. Fiji is also partakes in Asia Pacific CIRT (Computer Incidents Response Team) cyber security forums. According to (ITU, 2016) Fiji is also a recipient country of EU/ITU co-funded project “Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Counties". Fiji is also a member of the Pacific Regional PacCERT (Pacific Computer Emergency Incidents Response Team) and the International Telecommunications Union conducted a CIRT assessment for Fiji in 2014, however Fiji is yet to have a legitimately acknowledged national CIRT. Explicit legislations and directives related to cyber security are yet to be established in Fiji. Fiji also does not have any formally documented comprehensive National Cybersecurity Frameworks for implementing cybersecurity principles. Countries like Germany, UK and USA recognize the need to address the challenges associated with cybersecurity and have developed and implemented robust cybersecurity strategies. The United States of America has acknowledged cybersecurity as one of the most serious economic and national security challenge and have subsequently ordered a thorough analysis of federal efforts to defend the US information and communications infrastructure and the development of a complete approach towards protecting the US information infrastructure (Cybersecurity in the Republic of Fiji, Tamanikaiwaimaro). Fiji is yet to establish and an authoritatively accepted agency responsible for employing a National cybersecurity strategy, guidelines and roadmap

## 6 Effects of Cyber Crime

### 6.1 Identity Theft

According to (Kazmeyer, "Effects Of Cyber Crime") the victimization through cyber crime can have long-lasting effects on a person's life. Scammers employ a technique known as phishing by sending false emails pretending to come from a bank or other financial institution requesting private information. If this information is released, it can allow the criminal to access your bank and credit accounts, as well as open new accounts and destroy your credit rating. Damages similar to this can take months or even years to fix, hence protecting your personal information online is imperative.

### 6.2 Security Costs

Cyber criminals also focus their attacks on both large and small business. Hackers could attempt to take over business servers to embezzle information or use the machines for their own intentions. This creates the need for businesses to recruit security staffs that have the necessary qualifications and skills to keep intruders out of their systems. A survey of large companies found an average spending of $8.9 million yearly on cyber security, with 100 percent of businesses surveyed reporting at least one malware incident in the foregoing 1 year and 71 percent reporting the hijacking of company computers by intruders (Kazmeyer, "Effects of Cyber Crime").

### 6.3 Monetary Losses

Monetary losses through cybercrime can be massive and according to a 2012 report by Symantec, more than 1.5 million people become victim to some sort of cyber crime daily, ranging from simple password theft to extensive monetary defraud. Average losses of $197 per victim are estimated, which amounts to over $110 billion dollars lost to cyber crime worldwide yearly. As consumers become aware of traditional methods of attack, cyber criminals develop new methods involving mobile devices and social networks to keep their illegal gains flowing (Kazmeyer, "Effects of Cyber Crime").

### 6.4 Piracy

Piracy has had foremost effects on the entertainment, music and software industries. Damage claims are difficult to estimate and even more difficult to verify, with estimates ranging widely from hundreds of millions to hundreds of billions of dollars yearly. Copyright holders have requested for more stringent laws against intellectual property theft, which has resulted in laws like the Digital Millennium Copyright Act. Severe laws permits copyright holders to target people sharing intellectual property illegally and sue them for large sums of money to neutralize the financial damages done through the illegal sharing of intellectual property (Kazmeyer, "Effects of Cyber Crime").

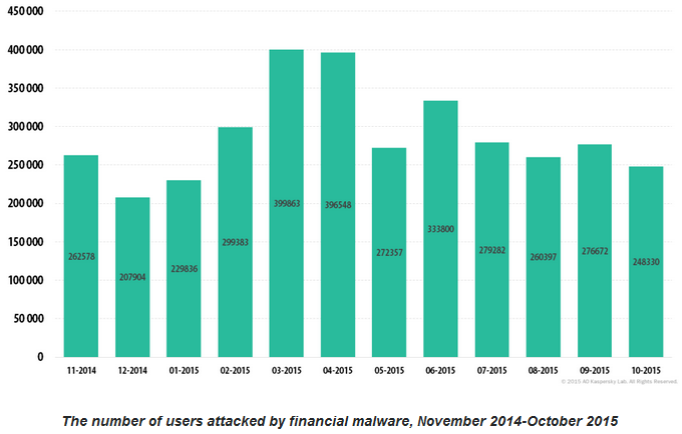


***FIG. 1** THE NUMBER OF USERS ATTACKED BY FINANCIAL MALWARE, NOVEMBER 2014-OCTOBER 2015 ("KASPERSKY SECURITY BULLETIN 2015. OVERALL STATISTICS FOR 2015 - SECURELIST")*

## 7 COMBATING CYBER CRIME IN FIJI

According to (The Cyber Index, UNIDIR 2013) Fiji instituted a cybercrime unit within the police force. Furthermore in 2010, Fiji founded the Cybersecurity Working Group led by the Cybercrimes Unit of the national police force and the Ministry of Defense. The Cyber Security Working Group is based on a public–private partnership, which includes government information technology departments, licensed operators, network services providers, and banks. The Financial Intelligence Unit scrutinizes illegal activities, for instance money laundering. With the establishment of the Fiji Inland Revenue and Customs Excise Authority, Fiji has addressed online financial fortification as well as online customs and tax avoidance issues.

## 8 GROWING TRENDS OF CYBERSECURITY

According to the Australian Cybersecurity Strategy report, Internet of Things, it is anticipated that by year 2020, 50 billion devices will be connected to the internet globally. There is a high risk of malicious actors as the problem is Online security has not been considered in the design of many of the devices connected to the (Legislation.gov.au, 2012) internet and it will make it easier for malicious actors to disrupt and damage the network. In 2015 as reported by wired.com that security researches had hacked into the electronics of a US car through the online entertainment system and had changes made in the speed and braking capability before the car was shut down remotely. This led to the manufacturer providing software updates for 1.4 million US cars and trucks fitted with the entertainment system.

## 9 RECOMMENDATION FOR THE FUTURE

### 9.1 Strategize For The Future

The Australian Government has come up with a cyber security strategy for the next 4 years. The report discusses the Australian Cyber Security Center (ACSC) which partners with:

- Australian Crime Commission
- Australian Federal Police
- Australian security Intelligence Organization
- Australian Signals Directorate
- Computer Emergency Response Team (CERT) Australia
- Defense Intelligence Organization

According to the report, Australian Government is investing more than $230 million over the next four years to enhance and deliver new initiatives. This report also discusses the action plan which the Australian Government is taking and Fiji should also invest in Cyber Security Law in order to punish the law breakers. Australia has (Legislation.gov.au, 2012) Cybercrime Legislation Amendment Act 2012 which outlines all the computer offences amendments and Fiji needs to have similar laws. Fiji should also come up with a strategy similar to Australia which is taking serious steps to combat cybercrime.

### 9.2 Europe Convention

Fiji should sign up Europe Convention on Cybercrime. It is an international (Computerworld, 2016) treaty on crimes committed through the internet. Countries like Australia have already joined Europe Convention on Cybercrime in 2013. A total of 39 countries have joined this treaty.

### 9.3 Cyber Security Laws for Cloud Computing

Since there is a high demand in Cloud Computing, Fiji should also ensure that there is a law for cloud computing as more and more business are adopting to cloud.

### 9.4 Research, Training, and Development

Nationally recognized research and development projects for establishing cybersecurity principles should be implemented in Fiji and these principles should be applied across the country. Professionally recognized training programs should be implemented in Fiji to promote awareness on cybersecurity, and ensure that the people leading these training programs are internationally recognized and certified in cybersecurity programs. Educational institutions should also seriously consider implementing cyber security courses in their course offerings. With the increasing growth rate of internet users in Fiji and the abundance of internet aware devices, cybercrime is likely to increase rather than decrease. Therefore having cybersecurity courses offered within the education system ensures that the future generation will be better aware of the effects of cybercrime and how to mitigate the risks associated with cybersecurity.

### 9.5 Legislations - Child Online Protection

Specific legislations should be developed by Fiji on Child Online protection and children are innocent and can easily become victims of cybercrimes. A good example would be (Legislation.gov.au, 2016) the Australian Criminal Code Act 1995, Subdivision D whereby offences relating to use of

carriage service for child pornography material or child abuse material is punishable with up to 15 years of imprisonment. Legislation such as this, acts as a strong deterrent against offences involving children. If legislations similar to the Australian Criminal Code Act are developed in Fiji cyber offenses against children will be mitigated due to the harsh penalties associated with the crime.

## 10 Conclusion

We can conclude from the research carried out that we should not only depend on cyber security laws to protect citizens and business against cybercrimes. Cybercriminals are very innovative and with the changing nature of information and communications technology cybercriminals will find novel ways of committing cybercrimes to bypass existing laws. Laws are developed or amended as required after a new type of crime has been committed. Therefore one should be extremely vigilant when dealing with strangers online or on the phone, and never disclose personal or corporate confidential information until you are absolutely certain that you are dealing with a legitimate or trusted entity. Laws also act as a deterrent to cybercrime therefore the presence of stringent laws are required and Fiji should incorporate more specific and stringent laws against computer offences to better cater for the novel and innovative types of cybercrimes. Extensive campaign should be carried out about the new laws and people must be educated through the media about the impacts of violating the law and punishments that await violators. From a device security perspective, it must be ensured that all networked devices and systems are protected with the most current security technologies. These should include but should not be limited to Intrusion Prevention and Detection Systems, current and regularly updated antivirus, anti-malware and anti-spam devices and programs. Server and Client operating systems also be regularly updated and patched to protect against vulnerabilities.

## References

[1] Khanse, A. (2014). Types of Cybercrime, Fraud, Acts and Preventive Measures. [online] The Windows Club. Available at: http://www.thewindowsclub.com/types-cybercrime [Accessed 15 Jun. 2016].

[2] Republic of Fiji Islands Government Gazette, Vol. 10, Thursday, 5th November 2009, No. 95, Crimes Decree No. 44 of 2009

[3] Computerworld. (2016). Australia signs up to Europe Convention on Cybercrime. [online] Available at: http://www.computerworld.com.au/article/455433/australia_signs_up_europe_convention_cybercrime_/ [Accessed 10 Jun. 2016].

[4] Legislation.gov.au. (2012). Cybercrime Legislation Amendment Act 2012. [online] Available at: https://www.legislation.gov.au/Details/C2012A00120/Download [Accessed 10 Jun. 2016].

[5] Swamy, N. (2014). Online boutique refunds most of its customers. [online] Cybercrime rate on the rise as hackers cash in. Available at: http://www.fbc.com.fj/fiji/25642/online-boutique-refunds-most-of-its-customers [Accessed 15 Apr. 2016].

[6] Anon, (2014). [online] Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/.../Fiji.pdf [Accessed 15 Jun. 2016].

[7] ITU. (2016). ICB4PAC PROJECT. [online] Available at: http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/ICB4PAC/Pages/default.aspx [Accessed 15 Jun. 2016].

[8] Legislation.gov.au. (2016). Criminal Code Act 1995. [online] Available at: https://www.legislation.gov.au/Details/C2012C00776 [Accessed 15 Jun. 2016].

[9] "Introduction To Cyber Security - The Open University". FutureLearn. N.p., 2016. Web. 17 June 2016.

[10] "Cyber Crime – Types & Preventive Measures". Crossdomainsolutions.com. N.p., 2016. Web. 17 June 2016.

[11] The Cyber Index, International Security Trends and Realities, UNIDIR/2013/3, Copyright © United Nations, 2013

[12] "Cybercrime Rose Significantly In 2015: Dell Security Annual Threat Report". NDTV Gadgets360.com. N.p., 2016. Web. 17 June 2016.

[13] "Fijian Firms Lose Thousands Of Dollars Through Cyber Crime | Fiji Sun". Fijisun.com.fj. N.p., 2015. Web. 17 June 2016.

[14] Tamanikaiwaimaro, Salanieta. "Cybersecurity In The Republic Of Fiji". Diplomacy.edu. N.p., 2016. Web. 17 June 2016.

[15] Kazmeyer, Milton. "Effects Of Cyber Crime". Science.opposingviews.com. N.p., 2016. Web. 20 June 2016.

[16] "Kaspersky Security Bulletin 2015. Overall Statistics For 2015 - Securelist". Securelist.com. N.p., 2016. Web. 20 June 2016.