TABLE OF CONTENTS

INTRODUCTION

Cybercrime is the greatest threat to every company in the world, and one of the biggest problems with mankind. The impact on society is reflected in the numbers. Our entire society, the Planet Earth, is connecting up to the Internet – people, places, and Things. The rate of Internet connection is outpacing our ability to properly secure it.

Cybercrime include damage and destruction of data, stolen money, lost productivity, and theft of intellectual property, theft of personal and financial data, embezzlement, fraud, and post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

There are numerous types of cyber-attacks that criminals are using to achieve their goals. These types of attacks range include everything from hacking and phishing to distributed denial of service, SIM-swapping, and ransom ware attacks.

Regardless of their chosen method of attack, though, it’s essential for your business to implement cyber security awareness training as part of your prevention and risk mitigation methods. So, what are some of the top cybercrime statistics relating to attack methods.

85% of organizations reported experiencing phishing and social engineering attacks. The Cost of Cybercrime” annual report indicates that the number of organizations that reported experiencing phishing and social engineering attacks increased 16% year over year.

Malware ranks as the most costly type of attack for organizations Accenture Security’s 2019 report indicated that malware cost organizations an average of $2,613,952 in 2018.The next most costly type of attacks were web-based attacks, which cost an average of $2,275,024 per year in 2018.

96% of internet users report email phishing scams as the top security risk, email phishing scams as the greatest security threat to businesses. And considering that nearly

WORLDWIDE EFFECT OF CIBER CRIME

We all know that cybercrime is one of the fastest growing areas of crime around the globe. It can be committed residing in any part of world against individual/institution situated in other part. Advancing technologies have made people easier to commit these crimes. You can sit at your home and hack your neighbor’s WiFi easily with just a click. More and more criminals are exploiting the speed, convenience of the modern technology to commit more diverse types of crimes.

Nepal is not an exception when it comes to threat of cybercrime. Increasing internet and computer users, and the growth of technology has resulted the use of computers for cybercrime. Most Nepalese use computers and internet for entertainment purpose and are not aware of the risk they are involved in. They probably do not have the knowledge of cyber security.

Regarding the international system as a whole, cyber-attacks cause a major stumbling block for global economic growth due to its detrimental effects on innovation and the theft of ideas. Many small businesses without adequate protection are hacked without any knowledge of the act until their sales greatly suffer years later due to competitors gaining knowledge of the company's logistics, target markets, or personal information.

As even some of the largest companies involved in software development can still fall victim to these attacks, but fortunately international collaboration has begun to show signs of reducing the rate of cyber-crime. Therefore, as technological advances continue to spur on the efficiency in global commerce, firms must focus on protecting their personal and corporate information from information traders involved in the illicit markets of cybercrime.

The global cost of cybercrime has now reached as much as $600 billion about 0.8 percent of global GDP according to a new report. More worrying than that figure may be the massive growth from 2014, when the same analysis showed the cost was only as much as $445 billion.

CYBER FRAUD CASE AND HACKING

Nepal Police arrested Naresh Lamgade of Anarmani, Jhapa for allegedly hacking into the accounts of Nabil Bank’s customers by creating a fake website of the bank.The perpetrator first sent email messages to Nabil’s e-banking customers asking them to change their security codes and providing links to do so. Whoever clicked on the link was taken to the fake e-banking website of Bank. When its account holders entered their identity and password, they unsuspectingly revealed their private login details to Lamgade. Similar cases were reported to Police as crime committed for e-banking of Nepal Investment Bank.

Nepal Police have caught a 27 -year-old man, who allegedly impersonated a girl in a Facebook account. Acting on behalf of the girl, perpetrator posted vulgar comments and nude photographs to different men including her friends.

OFFENCIVE SMS AND IDENTITY THEPT

The Metropolitan Police Crime Division arrested Rahul Balmiki (23) of Nepalgunj, who had hacked Facebook accounts of more than 40 women and posted obscene images and sent lewd messages to blackmail the victims. Balmiki, 23, of Nepalgunj-12, Banke, who was arrested in his home district, was brought to Kathmandu for further investigation.

The Metropolitan Police Crime Division apprehended two persons for allegedly using fake social media accounts with female names to boyfriend, lure and blackmail businesspersons in Kathmandu.

HOW CYBER CRIME WORKS

There are numerous types of cyber-attacks that criminals are using to achieve their goals. These types of attacks range include everything from hacking and phishing to distributed denial of service, SIM-swapping, and ransom ware attacks.

Criminal communities share strategies and tools and can combine forces to launch coordinated attacks. They even have an underground marketplace where cyber criminals can buy and sell stolen information and identities.

It's very difficult to crack down on cyber criminals because the Internet makes it easier for people to do things anonymously and from any location on the globe. Many computers used in cyber-attacks have actually been hacked and are being controlled by someone far away. Crime laws are different in every country too, which can make things really complicated when a criminal launches an attack in another country.

Here are a few types of attacks cyber criminals use to commit crimes. You may recognize a few of them:

- **Botnet -** a network of software robots, or bots, that automatically spread malware
- Fast Flux - moving data quickly among the computers in a botnet to make it difficult to trace the source of malware or phishing websites
- **Zombie Computer -** a computer that has been hacked into and is used to launch malicious attacks or to become part of a botnet
- **Social Engineering -** using lies and manipulation to trick people into revealing their personal information. Phishing is a form of social engineering
- **Denial-of-Service attacks -** flooding a network or server with traffic in order to make it unavailable to its users
- **Skimmers -** Devices that steal credit card information when the card is swiped through them. This can happen in stores or restaurants when the card is out of the owner's view, and frequently the credit card information is then sold online through a criminal community.

Some identity thieves target organizations that store people's personal information, like schools or credit card companies. But most cyber criminals will target home computers rather than trying to break into a big institution's network because it's much easier.

RELATION OF CYBERCRIME WITH MONEY

It has become possible for people with comparatively low technical skills to steal thousands of pounds a day without leaving their homes. In fact, to make more money than can be made selling heroin (and with far less risk), the only time the criminal need leave his PC is to collect his cash. Sometimes they don't even need to do that.

In all industries, efficient business models depend upon horizontal separation of production processes, professional services, sales channels etc. (each requiring specialized skills and resources), as well as a good deal of trade at prices set by the market forces of supply and demand. Cybercrime is no different: it boasts a buoyant international market for skills, tools and finished product. It even has its own currency.

The rise of cybercrime is inextricably linked to the ubiquity of credit card transactions and online bank accounts. Get hold of this financial data and not only can you steal silently, but also – through a process of virus-driven automation – with ruthlessly efficient and hypothetically infinite frequency.

The question of how to obtain credit card/bank account data can be answered by a selection of methods each involving their own relative combinations of risk, expense and skill.

The most straightforward is to buy the ‘finished product’. In this case we’ll use the example of an online bank account. The product takes the form of information necessary to gain authorized control over a bank account with a six-figure balance. The cost to obtain this information is $400 (cybercriminals always deal in dollars). It seems like a small figure, but for the work involved and the risk incurred it’s very easy money for the criminal who can provide it. Also remember that this is an international trade; many cyber-criminals of this ilk are from poor countries in Eastern Europe, South America or South-East Asia.

The probable marketplace for this transaction will be a hidden IRC (Internet Relay Chat) chartroom. The $400 fee will most likely be exchanged in some form of virtual currency such as e-gold.

Not all cyber-criminals operate at the coalface, and certainly don’t work exclusively of one another; different protagonists in the crime community perform a range of important, specialized functions. These broadly encompass.