NOVEMBER 2021 VOLUME 05

The IISSM News

The International Institute of Security and Safety Management Newsletter

Change of Date : 31st IISSM Annual Global Conclave

The IISSM's Annual Global Conclave, the 31st, which was earlier scheduled to be held on 02-03 Dec 2021, has now been postponed to 16-17 Dec 21. The preparations are at the right direction and we will put up a good show. Just to remind the readers, the over arching theme for the conclave is "Modernisation of the Security, Safety and Loss Prevention Industry".There will be four Keynote addresses and four Panel discussions each, details of the speakers are given in the flier (added in this edition).

31ST IISSM ANNUAL
GLOBAL CONCLAVE 2021
Modernisation in the Security, Safety & Loss Prevention Industry
16-17 December 2021
PARTICIPATE
ADVERTISE
SPONSOR
सुरक्षाया वसति समृद्धिः
IISSM
(ISO 9001:2015 CERTIFIED)
"Professional Excellence through Continuing Education & Training"
Selflessly dedicated Service Since 1990 to the profession of Security and Loss Prevention

Content

01 Editorial **03**

02 Certified Security Practitoners' Course (VC) (18-19 & 25-26 September, 2021) : **A Report** **04-05**

03 Security in Digital World : Challenges and Solutions for Security Professionals **07-14**

Editorial

Dear Readers,

Greetings to you all!

We are at the end of major festivities of ‘Deewali and Chhath’, while we were busy in celebrations, the world leaders met at Glasgow for the safety of our environment at COP 26. This meeting was held for two weeks and finally ended in achieving nothing after hard negotiations between the developed and developing nations. The aim was to agree on measures to reduce the global temperature by 1.5 degrees by 2030. There were big talks but when it came to doing, the biggest polluters (Western countries) who have driven the world to this stage are now expecting India and China to do on their behalf. Well, India is committed to do its best and do the transition from fossil based energy to Clean Energy but cost is not being shared. India alone needs $1 Tn per year to do this transition but global leaders are failing to pay the committed amount of $100Bn per year since 2008. This lip service has brought us to brink of disaster and facing wrath of the nature collectively.

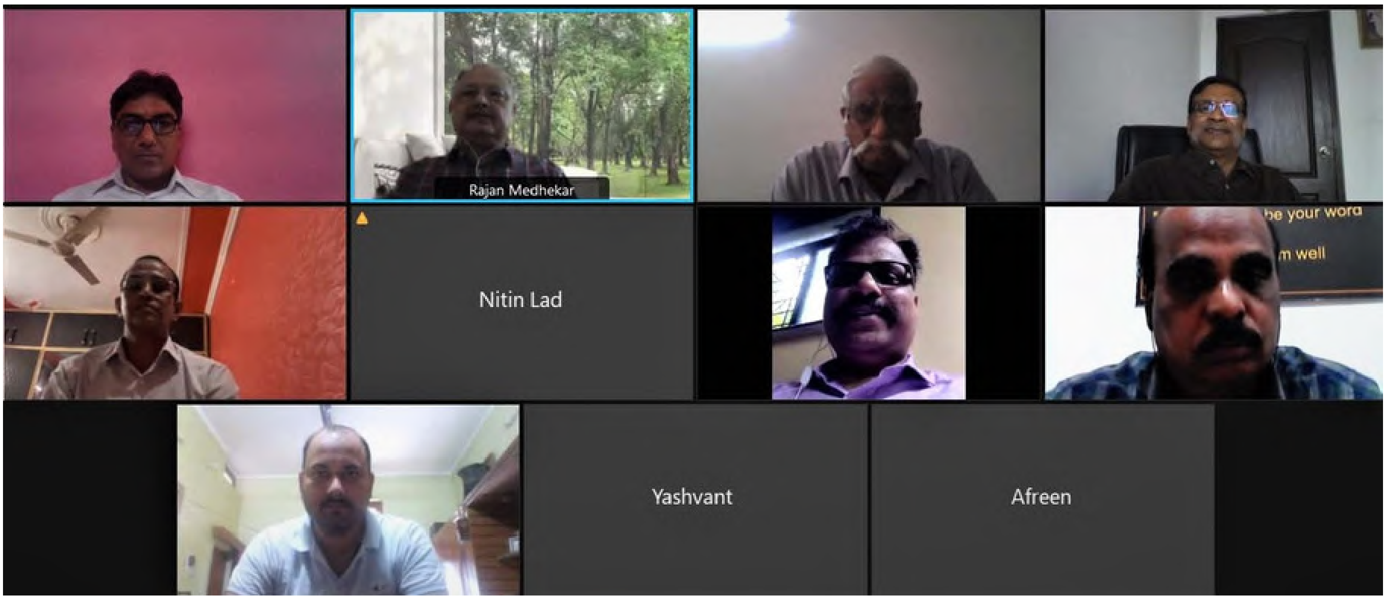
India is experiencing a downslide in Covid-19 but USA, Russia and Germany are grappling with high numbers since few months. It is matter of great concern. It leads me to the question, how and why these advanced nations are unable to control it? Is it the failure of the vaccines which is being hushed up? It was pretty clear that 1st world wanted NO competition from Indian vaccines which has proven its worth. Strangely the WHO was also playing the second fiddle. Well, that politics also has been put to rest now. The grand success in vaccination across India is paying rich dividends. however, present speed of vaccination is a matter of concern. The world is watching us with awe, disbelief and certainly with hope!
We are entering into the winters and experiencing smoggy conditions with very poor quality of air in Delhi and adjoining states primarily due to climatic conditions, stubble burning and pollution of industries and emissions from vehicles. While people are suffering from health issues, the state governments were busy doing politics than addressing it squarely. Finally the Hon’ble Supreme Court had to intervene and direct the governments to act. At our end, we need to maintain utmost caution and remain healthy. Let me end this with Vedic Prayer:

ॐ सर्वे भवन्तु सुखिनः
सर्वे सन्तु निरामयाः।
सर्वे भद्राणि पश्यन्तु मा कश्चिद्दुःखभाग्भवेत।
ॐ शान्तिः शान्तिः शान्तिः॥

May all sentient beings be at peace,
May no one suffer from illness,
May all see what is auspicious, may no one suffer.
Om peace, peace, peace.

Jai Hind!
Col (Dr.) MP Sen

Certified Security Practitioners' Course (VC) (18-19 & 25-26 Sep 2021) : A Report



Rajan K Medhekar, IPS (Retd), DG, IISSM interacting with the Students

The Certified Security Practitioner Course has been conducted by IISSM (18-19 & 25-26 Sep 2021, Weekend Course) on virtual platform. The participants were from Noida, Gurugram, Uttarakhand, Mumbai & Bangalore.

The sessions covered the topics like Fire safety Management, Risk Management, Disaster Risk Management, Fire Safety Management and Evacuation (National Building Code and NFPA Standards), IEDs and Bomb threat handling, Technological Application in Security Management, Bank, Hotel, Mall and Hospital Security, Incidence Response System & Crisis Management Framework, Corporate Vigilance - Overview & Preventive Aspects, Arms Act and Arms Licensing, , PSAR Act - 2005 - Need for review, Executive Protection and Role of PSOs, Cyber Security & Data Protection, and Business Continuity Planning.In addition, a Class Room Crisis Simulation Exercise, on Flood Situation Management was conducted which was highly appreciated.

The Classroom Exercise received an Excellent Response from the Participants.

The Faculty Members who conducted the Course were:
BrigAK Pathak (Retd) and Col (Dr.) M P Sen (Retd): IISSM Faculties
Brig (Dr.) VK Dutta (Retd) and Col Sumit Monga (Retd) : Guest Faculties

All Participants have also shown interest in our activities like Seminars, Conclaves and Membership in addition to future association.

Overall, the course was very well appreciated.

Few Quotes from Participants on Overall Assessment of the Course are mentioned below:-

Mr. Yashvant Singh, Manager Operations, G4S Security Solutions Pvt.Ltd, Uttarakhand
"...Overall sessions are very informative and were learning & memorable experience, techniques & the teaching illustrations to brief the topics were outstanding."

Mr Nitin Arjun Lad, Zonal Security & Safety Manager, ICICI Bank, Mumbai
"It should be mandatory for all security officers, Manager, Agency owner. Company must ask for CSP certification in India rather than going for other Intl. certification."

Mr. Dinesh Raj, Ex Serviceman, Indian Navy, Gurgaon
"Very Informative course and delivered by rich and experienced faculties."

Class is in progress

Security in Digital World: Challenges and Solutions for Security Professionals

Dr. Rajender Singh Chhillar
Professor & Head of the Department of Computer Science
Maharshi Dayanand University, Rohtak

1.OVERVIEW

During the COVID-19 pandemic, people are vulnerable to cybersecurity as E-learning, Work from Home (WFH), On-line shopping and others are increased. It is difficult for everyone to keep up to date on the latest knowledge on the equipment and on how to stay secure online in this developed digital environment. In order to meet the increasing requirements of business continuity, the classical model is insufficient and needs to be revised by emerging technologies/solutions such as Artificial Intelligence, Blockchain, cloud-based systems and employee/user awareness. This article describes how we have changed our way of living, learning, and communicating, both personally and professionally, leading to a more virtual life. Later cyber security attacks and their respective challenges were briefly addressed as well as some most popular Cyber resilience Solutions.

2.INTRODUCTION

Coronavirus disease 2019 (COVID-19) is the official name given by the World Health Organization (WHO) to the disease caused by SARS-CoV-2, the new coronavirus that surfaced in Wuhan, China in 2019 and spread around the globe. The WHO has characterized COVID-19 as a pandemic, a disease outbreak that covers a wide geographic area and affects an exceptionally high proportion of people. At the time of writing, the World Health Organization (WHO) Coronavirus Disease (COVID-19) Dashboard reported over 104.3 million confirmed cases and in excess of 2.27 million deaths globally [1] . Life may return in the same way after the vaccine program, but it will take some time. We must adjust to the condition before then.

During this COVID-19 pandemic the use and dependency on the Internet has increased exponentially. In just one month, the world became more digitally linked – and unsecure. An increasing number of people have done work online, including e-learning, remote work, shopping etc. The last report from the Coronavirus Multi Market Analysis in Global Web Index shows that people are continuing to increase their time spent on mobile by 70 percent and laptop by 47 percent, as illustrated in Figure 1 [2].

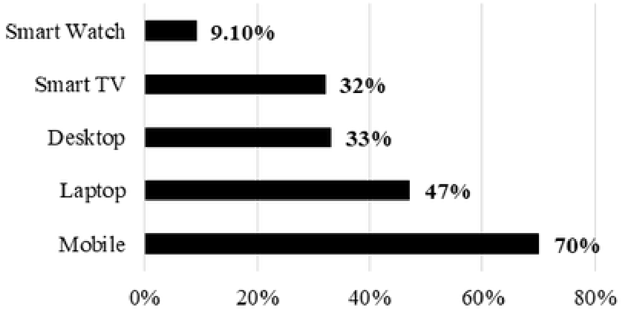


Figure 1: People Spending More time with Devices during COVID19 (July 2020)
(Source: https://datareportal.com/reports/digital-2020-july-global-statshot)

3.INFORMATION SECURITY

Information security refers to "the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption" [3].

Also in early phases, with these convincing 2020 cyber security figures, we see the effects of COVID-19 on individuals, companies and the whole globe. As per Tessian Research, almost half (47 percent) of respondents listed diversion as the main reason for a phishing scam. With 57 percent of staff admittedly distracted from their homework, a sudden step towards remote work could open up even more risks to employees and companies [4]. The new Cost of Data Breach Report 2020 report released by IBM Security shows a global rise in the cost of a data breach. The US had the highest data breach expense of $8,64 million on average in all 17 regions surveyed for the study with the hit hardest industry healthcare [5]. Remote work is considered a major security challenge and believes that the cost of data breach will surge by 70%. The study estimated the expense of each data breach because of remote work to be an abnormal of $137,000 additional.

4.TYPES OF INFORMATION SECURITY ATTACKS

At times when cyber dependence may be minimized because of the transfer of attention to the health crisis, cybercriminals target computer networks and systems of individuals, companies and even global organizations. Security threats on cyberspace have become a big concern. Phishing, malware, ransomware, social engineering, identity theft and denial of service, as described below, are all common forms of cyber security attacks.

A. Distributed Denial of Service (DDoS)

DDoS Attack is an attack in which many compromised computer systems attack the target for users of the targeted resource, for instance the server, the Website or another network resource as shown in Figure 2. The flux of incoming messages, connection requests or malformed packets into the target system causes it to slow down or even crash, thus denying legitimate users or systems services. DDoS attack can be carried out in many ways: SYN flood attack, teardrop attack, smurf attack, death ping and botnets.

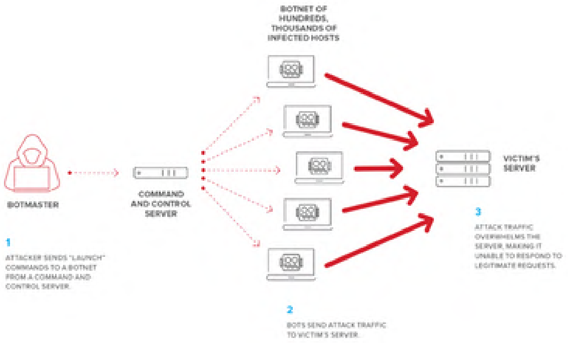

BOTNET OF HUNDREDS, THOUSANDS OF INFECTED HOSTS
BOTMASTER
COMMAND AND CONTROL SERVER
VICTIM'S SERVER
1
ATTACKER SENDS "LAUNCH" COMMANDS TO A BOTNET FROM A COMMAND-AND CONTROL SERVER.
2
BOTS SEND ATTACK TRAFFIC TO VICTIM'S SERVER.
3
ATTACK TRAFFIC OVERWHELMS THE SERVER, MAKING IT UNABLE TO RESPOND TO LEGITIMATE REQUESTS.

Figure 2:Attackers typically use a botnet to launch DDoS attacks
(Source: https://www.f5.com/labs/articles/education/what-is-a-distributed-denial-of-service-attack-)

Security researchers at Kaspersky claim that distributed denial of services attacks in the second quarter have risen dramatically, possibly because they switched to a WFH. According to a survey, 217 percent in the quarter, compared with the same time frame a year earlier, increased the number of attacks detected and blocked by DDoS. Attacks in the second quarter were 30 percent higher than in the first as shown in Figure 3. In the third quarter of this Kaspersky study, the rise in DDoS attacks will continue with many WFH employees. And they warns that during the holiday season, the fourth quarter usually see a rise in such attack [6].

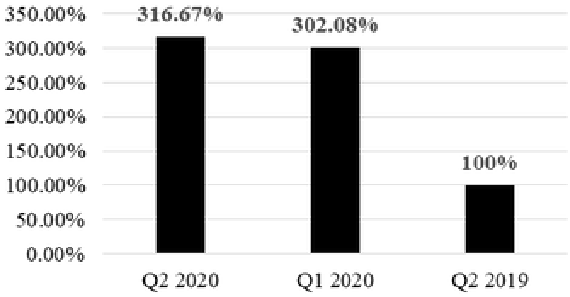


Figure 3: Comparative number of DDoS attacks from the first quarter and second quarter of 2020, and the second quarter of 2019
(Source: Kaspersky)

B.Man in the Middle (MitM) attacks

MitM Attack is a common term for the attack where attacker/perpetrator place himself between user and the web application for eavesdropping or to impersonate the user identity as shown in Figure 4. The purpose of an attack is to rob personal data including password, account and card numbers. This type of attack is especially a hazard for those from home without their companies' safety instructions [7]. The most common (and easy) way to do that is through a passive intrusion, which gives an attacker free malicious WiFi access for the general public. They are typically not secured in a way that suits their position by password names. When a target connects to this hotspot, any online data sharing makes the attacker fully accessible.

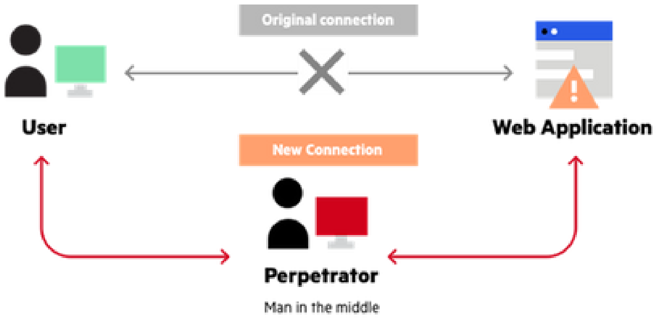


Figure 4: Man in the middle attack example
(Source: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/)

C.Phishing Websites

Phishing means attempted theft of personal details, typically in the form of a username, password, card numbers, bank account info, etc. as illustrated in Figure 5. When an attacker masks it as a credible source, he invites the victim to trick him, just as a fisherman uses bait to catch sharks [8].

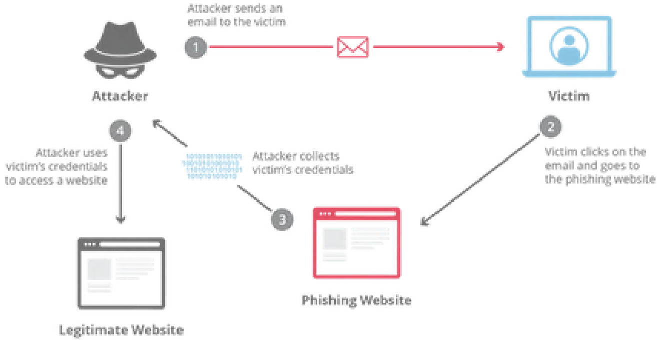

Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
Attacker collects victim's credentials
3
Phishing Website
Legitimate Website

Figure 5: Anatomy of Phishing Attack
(Source: https://www.cloudflare.com/learning/access-management/phishing-attack/)

According to Google's Transparency Report, the tech giant detected an average of 46,000 new phishing websites every week in 2020. The data also indicates that the problem was particularly acute in the first half of the year, with February, April, March and May witnessing weeks with over 50,000 new phishing site detections [9]. Google blocked 18 million Coronavirus-related malware and phishing emails in April [10].

According to cybersecurity expert Brian Krebs, GoDaddy staff were the victims of a social-technology and phishing scam, which was initiated to hit several crypto-current exchanges. This is not the first time that hackers attacked GoDaddy. A similar voice phishing attack allowed the attackers to take control of at least half a dozen domain names in March and GoDaddy disclosed that in May, the security incident in October 2019 resulted in a compromise to 28 000 web hosting accounts of customers [11].

D.Password Attacks

A third person attempting to gain entry to your systems by splitting the user's password is exactly what an assault by password sounds like. Usually, no malicious code or software of any kind is needed to run on the device. Software is used by an attacker to try to split your password, but it normally runs on your own device. Programs use several methods of accessing accounts, including brute force attacks for guessing passwords and matching different word combinations with a dictionary file [12]. Good passwords are the only way to secure your password from attacks. This means using a mixture of letters, symbols and numbers in the top and bottom divisions of at least eight or more characters. You can get passwords by sniffing, brute force, dictionary attack and phishing occasionally. Brute force approach includes the use of common combinations to formulate the password, which is particularly successful when the target uses a low password.
At least 530,000 Zoom accounts were sold at dark web hacker sites and sold at $0.0020 cents discovered by Computer security company Cyble. The company has checked that the accounts are valid and each has its username and password and registered e-mail address, host key and URL. It provides an attacker with malicious access not only to the account, it can also access the content of meetings that it may have conducted or held [13].

E.Malware

Another way of triggering attacks is to use malicious software, which is malware, which is any unauthorized software that is installed without the permission of the user on a target computer as shown in Figure 6. Malware may use the computer by replicating and hiding it in useful applications, to spread to other devices. Macro viruses, file infections, ransomwares, trojans, logical bombs etc., are all types of malware attacks. Ransomware is, by far, the most prevalent type of malware since it costs less and more to execute compared to other types of malware. In order to block entry, Ransomware encrypts valuable or confidential data of a target.

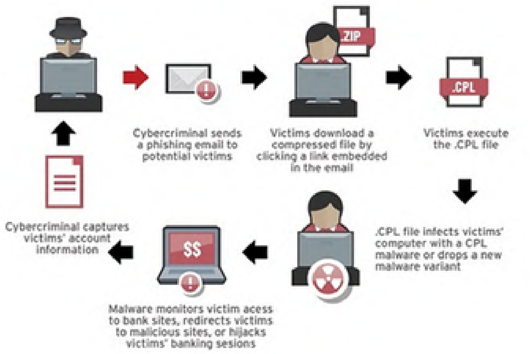

ZIP
.CPL
Cybercriminal sends a phishing email to potential victims
Victims download a compressed file by clicking a link embedded in the email
Victims execute the .CPL file
.CPL file infects victims' computer with a CPL malware or drops a new malware variant
$$
Malware monitors victim acess to bank sites, redirects victims to malicious sites, or hijacks victims' banking sesions
Cybercriminal captures victims' account information

Figure 6: CPL malware threat diagram
(Source: https://blog.trendmicro.com/trendlabs-security-intelligence/anatomy-of-a-control-panel-malware-attack-part-2/)

In order to legally submit organizations such as the WHO to spread phisher mails/websites and counteract false news and rob valuable information, cyber criminals have begun developing a large number of fake mobile applications on behalf of COVID-19. Malware supplied via Android applications to steal victims that provide a safety mask for Coronavirus after installation [14].

According to Fire Eye research, Hackers working on behalf of the Vietnamese Government targeting Chinese government agencies to handle the country's response to the coronavirus pandemic. Spear phishing e-mails with METALJACK malware were explicitly sent by the attackers to Chinese Ministry of Emergency Management and Wuhan, where it is suspected that the virus originated. The attackers Using phishing mails, the malware is finally loaded into your memory[15].

5.CURRENT CHALLENGES

The complexities of cyber security lie in keeping ahead with preventative measures to hack the infrastructure before attacks arise. It plays an important role in protecting our privacy in this digital age where hackers are rising every day intelligently. The following are the most popular challenges to be resolved.

1) Human Errors: People have to be up to date on all their software or devices such as computers, tablets or cell phones. However, most people don't feel the need of updating their system because they think the update process is a problem and requires a lot of data. This leaves your machine vulnerable to cyber protection because hackers can easily break into your system because they are not up to date. In addition, phishing attacks are also vulnerable to cyber security during COVID-19.Email as their key weapon is the most common form of phishing attack. The victims receive a spoofed email, and malware or ransomware can be installed on their computers by clicking on the malicious connection. More software applications such as Zoom, Cisco WebEx, and Microsoft Team can be downloaded during the COVID-19 Pandemic. Hackers can write code based on the software application's vulnerabilities. They can access something and rob the details of the victims. In this COVID-19 cyber security pandemic, malware is also vulnerable. Malware may be transmitted by the use of an email or website. There is a link on which users can click. Once you click on the link, the malware on your computer is installed. So, in order to defend against malware, people must be aware of this malware.

2) IoT Devices Vulnerability: The Internet of Things (IoT) and smart infrastructure are another field of emerging technology that is highly vulnerable to security attacks. It typically consists of low-power, loss network resource-controlled devices. Because of these features, these systems cannot use conventional security protocols. In addition, there is a lack of acceptable protocols and security resources that can be incorporated for safe deployment. Investigators work on solutions in this field; but, relative to the exponential unsafe implementation, it is still in its early stages. A lightweight and reliable authentication framework can be one of the many solutions. However, there are still several vulnerabilities in safe IoT system implementation, as a result of which protection and privacy attacks are a simple target.

3)Potential delays in cyber-attack detection and response: Owing to the COVID-19 pandemic, the functioning of several security teams is likely to be compromised, rendering malicious detection difficult and making it much more difficult to respond to these activities. A difficulty may also be installing updates on systems when security teams don't function. Organizations can assess security defenses and explore the use of co-sourcing in areas where significant human threats have been found with external consultants.

6.SOLUTIONS

Technology is advancing rapidly and with that there is an increase of cyber-attacks and elevated frequency of malicious attacks. Traditional Information Security Paradigm i.e. CIA (Confidently, Integrity, Availability) is unable to solve the problem with post COVID19 challenges. CIA Triad works properly in Identification, Protection and Detection of System but failed when it comes to Recovery i.e. Cyber resilience. We need to work on adapting of robust technologies like Artificial Intelligence (AI) based system, Serverless Technologies, Cloud based Systems and most importantly awareness among the employee/user. These are mentioned in detailed manner below.

1)AI based Security System: First novel way to identify and avoid threats with artificial intelligence before it starts rooting in your computer system. You may think of this as an advanced firewall or protector. His second role is also to search, review and raise warnings about the latest stored data on the computer system. The artificial intelligence implementation collects data from a server with which trends or popular attacks on the system are associated. The artificial intelligence system will utilize its machine learning capabilities as when a user rules out a potential threat as harmful, the program will learn of its pattern and send the data to a server where it will store the pattern. This programme, as if the program is confidently enough, can automatically perform the instructions, will delete the trouble of having to do a great deal of manual work for firewalls or security programs. When receiving e-mail information, the software will be able to detect scams and phishing efforts. It advises and warns users about possible scams and claims. The program also solves the issue of safety bugs and backdoors, as it steadily and automatically "patch."

2)Awareness: Awareness of the relevance of cyber security should be of the utmost importance. Cyber security, common cyber-threats and preventative measures are better informed. Prevention is easier than recovery, as they say. Employees can also attend workshops on the cyber security side with a view to making common strategies and approaches for scammers informed of them. This also helps IT workers spot hacking attempts or assaults on their workstations if this happens. The costs of sending staff to workshops in the future would be negligible relative to the amount saved from a corporate outlook for recovery from attacks and assaults. No silver bullet at all.

3)Blockchain Technologies: An originally blockchain block chain is an increasing list of records called cryptographically connected blocks. Each block includes a hash, a timestamp and transaction data of the previous block (generally represented as a Merkle tree). The validity of individual crypto currency buys is assured since the movement of the currency to its origin can be tracked. Encryption helps to monitor and stabilize the amount of crypto currencies generated. Hashed Health has been active in creating a safe digital blockchain network for patient information exchange and the internal contact networks for hundreds of healthcare organizations and hospitals. According to Accenture, 86% of defense, particularly in cyber security, intend to include blockchain into protocols in the following three years. Blockchain is considered to be the legitimate data security mechanism for military, defense and aerospace firms, which contain some of the most important data (mission coordinates, identifiable employees/persons, emerging technologies, etc.).[16].

7.CONCLUSION

In these times of great chaos, cybersecurity is undeniable. A significant number of entrepreneurs, companies and businesses have used digital technologies in this pandemic to ensure the sustainability of their businesses. However, with the advent of digital solutions, many companies ignore threats and obstacles associated with cyber attack. Research shows that most company owners only act first during cybersecurity attacks. In the future, emerging technologies will boost cyber security, including AI, Blockchain, and IoT etc. Traditional services can be expensive and risky but any transaction or business processes with Blockchain in asset management have proved very secure and efficient because Blockchain does not allow any errors. As far as the present situation is concerned, each user should begin child protection measures on his personal information before any unauthorized user breaks it.

REFERENCES

[1] "WHO Coronavirus Disease (COVID-19) Dashboard | WHO Coronavirus Disease (COVID-19) Dashboard." https://covid19.who.int/ (accessed Nov. 28, 2020).

[2] "Digital 2020: July Global Statshot — DataReportal – Global Digital Insights." https://datareportal.com/reports/digital-2020-july-global-statshot (accessed Nov. 29, 2020).

[3] "SANS Institute: Information Security Resources." https://www.sans.org/information-security/ (accessed Nov. 29, 2020).

[4] "Understand the mistakes that compromise your company ' s cybersecurity To err is human Why do these mistakes happen ? Why demographics."

[5]"Data Breach costs are increasing – what's the impact of COVID? - activereach Ltd." https://activereach.net/newsroom/blog/data-breach-costs-are-increasing-whats-the-impact-of-covid/ (accessed Nov. 29, 2020).

[6] "Kaspersky: DDoS Attacks Spike During COVID-19 Pandemic." https://www.inforisktoday.com/kaspersky-ddos-attacks-spike-during-covid-19-pandemic-a-14805 (accessed Nov. 28, 2020).

[7] "What is MITM (Man in the Middle) Attack | Imperva." https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/ (accessed Nov. 28, 2020).

[8] "What is a phishing attack? | Cloudflare." https://www.cloudflare.com/learning/access-management/phishing-attack/ (accessed Nov. 29, 2020).

[9]"Google Registers Record Two Million Phishing Websites In 2020." https://www.forbes.com/sites/simonchandler/2020/11/25/google-registers-record-two-million-phishing-websites-in-2020/?sh=6ab352301662 (accessed Nov. 29, 2020).

[10] "Protecting against cyber threats during COVID-19 and beyond | Google Cloud Blog." https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond (accessed Nov. 29, 2020).

[11] "GoDaddy employees fall prey to phishing attack, report says - The Hindu." https://www.thehindu.com/sci-tech/technology/godaddy-employees-fall-prey-to-phishing-attack-report-says/article33167499.ece (accessed Nov. 29, 2020).

[12] "Password Attack Information from the UK Cyber Security Association." https://cybersecurityassociation.co.uk/common-attacks/password-attack-advice/ (accessed Nov. 29, 2020).

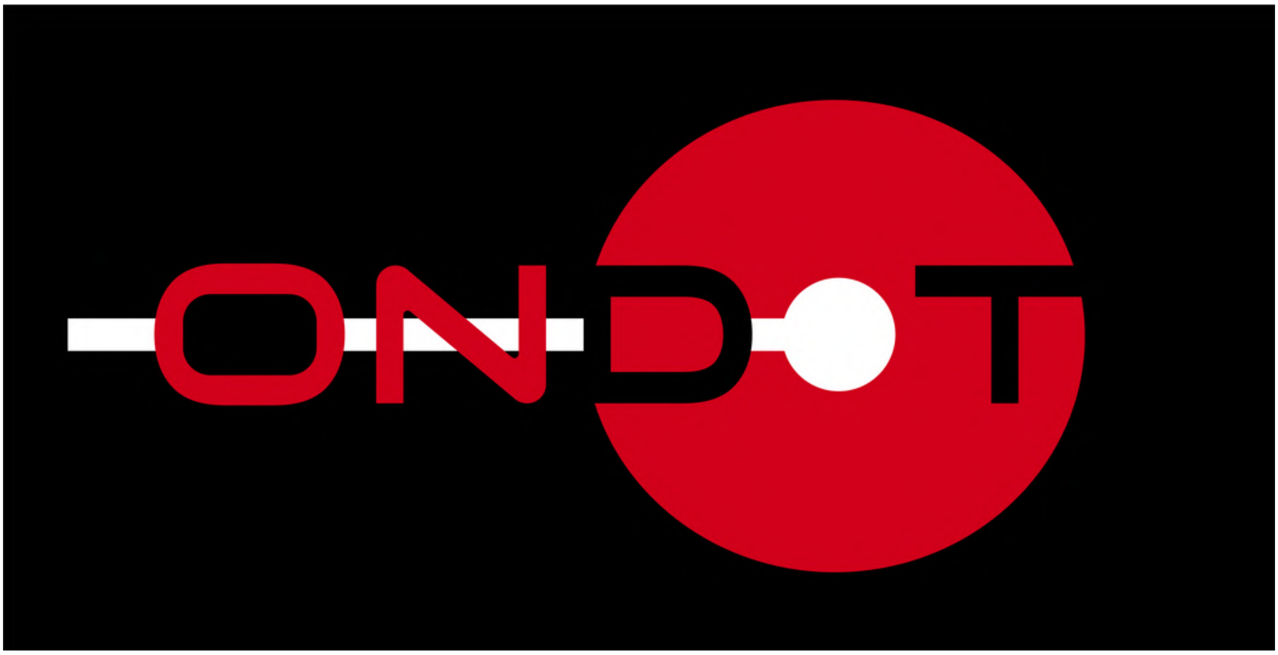
[13] "Half a Million Zoom Accounts Compromised by Credential Stuffing, Sold on Dark Web - CPO Magazine." https://www.cpomagazine.com/cyber-security/half-a-million-zoom-accounts-compromised-by-credential-stuffing-sold-on-dark-web/ (accessed Nov. 29, 2020).

[14] "Coronavirus Scam Alert: Rogue Android App Promises A Safety Mask But Spams All Your Friends." https://www.forbes.com/sites/thomasbrewster/2020/03/20/coronavirus-scam-alert-rogue-android-app-promises-a-safety-mask-but-spams-all-your-friends/?sh=31fefd832b34 (accessed Nov. 29, 2020).

[15] "Vietnamese cyber-espionage has pivoted to Beijing's coronavirus response." https://www.cyberscoop.com/vietnam-coronavirus-china-apt32-fireeye/ (accessed Nov. 29, 2020).

[16] "19 Cool Examples of Blockchain Cybersecurity | Built In." https://builtin.com/blockchain/blockchain-cybersecurity-uses (accessed Nov. 29, 2020).

Dr. Rajender Singh Chhillar is a professor and Head of the Department of Computer Science, Maharshi Dayanand University, Rohtak, India.He obtained his Ph.D. in Computer Science from Maharshi Dayanand University, Rohtak, India and master's degree from Kurukshetra University, Kurukshetra, India. He received his Master of Business Administration (MBA) degree from Sikkim Manipal University, Sikkim, India.His research interests include software engineering, software testing, software metrics, web metrics, bio metrics, data warehouse and data mining, computer networking, and software design. He has published more than 100 journal and 65 conference papers over the last several years and has also written two books in the fields of software engineering and information technology.



सुरक्षायां वसति समृद्धिः
IISSM
(ISO 9001:2015 CERTIFIED)
"Professional Excellence through Continuing Education & Training"
Selflessly dedicated Service Since 1990 to the profession of Security and Loss Prevention

31ST IISSM ANNUAL GLOBAL CONFERENCE 2021

Modernisation in the Security, Safety & Loss Prevention Industry

Keynote Speakers & Panellists

16-17 December 2021

Keynote Speakers

Jason L. Brown
National Security Director - Thales
Australia and New Zealand

Maj Gen P K Mallick, VSM (Retd)
Visiting Faculty
NDC, New Delhi

Lt Gen (Dr.) R S Panwar, VSM (Retd)
Think Tank on 'Future Warfare',
Former Commandant of MCTE MHOW

Panellists

Gurpawan Singh
IIRIS Consulting

Charlie Bennet
VP(Europe)
SAFR, Real Networks

Lt Cdr Farzana Tanni
(Ex Bangladesh Navy)

Alka Verma
Head of Security,
Indigo Airlines, India

Dr. MJ Shankar Raman
CEO IITM Pravartak
(Moderator)

Col Robin Sen (Retd)
Consulting Director
Speaking Mirror

Col(Dr.)Bipin C Pandey (Retd)
Visiting Faculty & Life Coach

Rajan Kotadi
Founder & CEO
Stezy.io
Blockchain Platform

Rukesh Patel
CTO & Technology
Evangelist

Suhash Mhaskar
Founder & CEO
Accent Technovation

Maj Sunny Meitei
Chief Functionery
Fortrop Asia

Geoffrey D Askew AM,
Principal and Founder
Askew & Associates, Australia

Dr. Arindam Basu
Healthcare Management
Consultant

Prof. Kamakoti
IIT Madras
(Moderator)

Ramkrishna V Bidri
Senior Agile Strategist,
Tata Consultancy Services

Col Inderjit Singh
CIO, Vara Technologies

Col Sumit Monga
Head - Government Affairs,
Lenovo Computers

Mahendra Singh Karakoti
Head Admin & Security
Schnider Electricals, India

Official Media Partners
SECURITY TODAY

Media Partners
SecurityLinkIndia

FOR MORE INFORMATION
+91 9999211650 | 9582026101
www.iissm.com

International Institute of Security and Safety Management
New Delhi

VIRTUAL PLATFORM