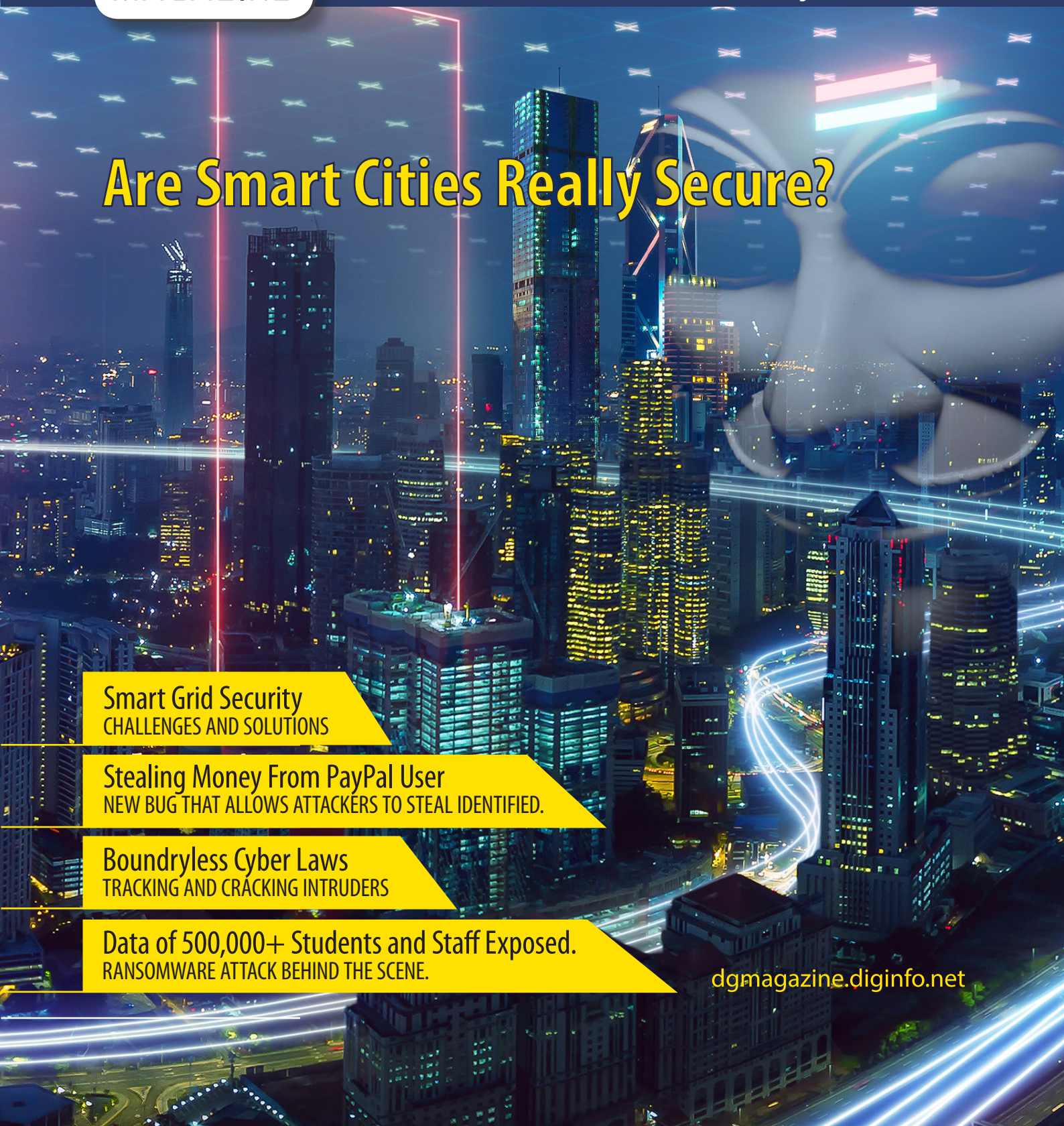
A Product of DIGINFO®

CYBER MAGAZINE

Volume 5 I 2022

DG MAGAZINE

The Ultimate Source of Cyber World



Are Smart Cities Really Secure?

Smart Grid Security
CHALLENGES AND SOLUTIONS

Stealing Money From PayPal User
NEW BUG THAT ALLOWS ATTACKERS TO STEAL IDENTIFIED.

Boundryless Cyber Laws
TRACKING AND CRACKING INTRUDERS

Data of 500,000+ Students and Staff Exposed.
RANSOMWARE ATTACK BEHIND THE SCENE.

dgmagazine.diginfo.net

CONTENTS

FROM THE EDITOR

Muhammad Saeed
Chief Editor

Here is the fifth volume marking completion of a set. In the next volume, things will be different. From layout to content. But the level of articles and selection of news will remain as pleasant as ever. And the layouts, though different, would remain as lovable and eye-catching as you have been accustomed to.

In months to come, you will get a diet of riveting, research-based articles on topical issues. And there will also be a stream of news reports gathered from all across the globe. Just like you have read in the five previous volumes.

For now, you will read articles on subjects like 'Smart Grids' and 'Smart Cities.' And there are thought provoking discussions on 'Leadership Crisis' in the profession and on 'Boundaryless Laws.' Every article is painstakingly produced backed by research, careful studies and analyses. You will come to realize that the content can easily be judged as reference material.

As always, the news items are picked from a vast repository of content available to everyone on the internet but hardly of any use because not everyone has the skill or time to search for stories that interest and inspire. In contrast to the usual prosaic and mundane stuff that you often come across elsewhere, you will settle with incisive and investigative reports that will entertain and provide substance.

Add to these, our regular features including interviews and first person accounts and you have a magazine that does not cease to amaze you with its content and presentation.

So, watch out for our next feed. You will get more of the entertaining, educative and enduring material right at your desktop—or your phone. The magazine you have come to like will always be available online.

EDITORIAL BOARD

Muhammad Saeed
Head of Editorial Board

Muhammad Saeed packs a lot more energy in his frame than anyone can guess. His biographical data reads like some stuff of dreams. Apparently he imagines something and goes out to get it without fail.

His academic record, to say the least, is impressive. A bachelor's from University of Karachi, a master's from LUMS and a doctorate from University of Karachi. As if that was not enough, he has also done some technical courses from prestigious institutions.

Now, as assistant professor at the same university he earned his doctoral degree from, he has carved a life steeped in erudition and academic pursuits. Already, he has authored or co-authored several research papers on subjects related to Computer Science or Information Technology. It is not surprising that quite a few of his students have demonstrated their creative talent under his tutelage.

Saeed is a restless soul. He is not the conventional 'sit back, relax and enjoy' type of person. He prefers to go out and discover what is there that can interest him. Inquisitiveness and enquiry mark his professional ethics. As a routine, therefore, he ventures out to participate in workshops, conferences and research studies, often on esoteric subjects.

Our country needs people of his type. Go-getters who define their goals and the path that takes them right there. In no time.

Dr. Ashfaq Malik
Member Editorial Board

He spent a lifetime in the strictures of the military environment. So, it was natural of him to become a disciplinarian that he is. The fact is evident from a list of educational accomplishments and work experiences that goes beyond the ordinary.

His first taste of victory within the military culture came in the early 90s when he graduated from Pakistan Naval Academy, which earned him a commission in Pakistan Navy as Naval Officer. That marked the beginning of his professional career. During his duty, he took up studies to graduate as an Electrical Engineer and then penned a doctoral thesis related to Electrical Engineering with specialization in Networks and Information Security.

He has a rich work experience that spans at least 25 years. During this time, he performed a variety of teaching and managerial duties at Pakistan Navy, National University of Sciences and Technology (NUST) and affiliated institutes of Sindh Board of Technical Education (SBTE). He has taken early retirement from the Navy to concentrate full time on research and teaching. At the time of leaving the services, he was working as a commander.

His knowledge and deep understanding of cyber security issues makes him an asset for DIGINFO, a company that has set top standards for itself.

In recognition of his illustrious career, both as an educationist as well as an administrator of top order, Dr Ashfaq was twice recommended for the prestigious Tamgha-e-Imtiaz. This alone speaks a lot about the singular dedication and extraordinary passion personified by him.

We desperately need such people. That he is in our midst is a privilege and an honour for all.

Shahzad Saleem
Member Editorial Board

He is an Assistant Professor at College of Computer Science and Engineering, University of Jeddah, KSA.

He also serves as head of the Department of Information Security, KTH-AIS Lab, School of Electrical Engineering and Computer Science, NUST, the top university of Pakistan.

He has over fourteen years of teaching, research and industry experience in various executive positions. He has been involved in more than twenty research publications indexed by Scopus, ISI and HEC. Right now, he is co-authoring a research proposal of US$400,000 under Pak-China Reseach Grant. The areas of research that interest him include Digital Forensics, Authentication and Access Controls.

His teaching experience touches on subjects like Digital Forensics, Computer Forensics, Network Security, Cryptography, Computer Security, Introduction to Algorithms and Data Structures. And there is a variety of other areas he is actively involved in which makes his portfolio rich and versatile. In his capasity as an Editorial Board member and with his valuable counsel, he is bound to make his presence felt at DG Magazine.

Adnan Masood
Member Editorial Board

He is an Artificial Intelligence and Machine Learning researcher, software architect and Microsoft MVP (Most Valuable Professional) for Artificial Intelligence. As Chief Architect of AI and Machine Learning, at UST Global, he collaborates with Stanford Artificial Intelligence Lab, and MIT AI Lab for building enterprise solutions. He has authored "Functional Programming with F#" which rose to become an Amazon bestseller in programming languages.

Dr. Masood teaches Data Science at Park University and Windows Communication Foundation (WCF) courses at the University of California, San Diego. He is a regular speaker to various academic and technology conferences, local code camps, and user groups. He also volunteers as STEM (Science Technology, Engineering and Math) robotics coach for elementary and middle school students.

Dr. Masood is a strong believer in community service. He co-founded and presides Pasadena .NET Developers group. He also organizes Tampa Bay Data Science Group, and Irvine Programmer meet-up. His recent talk at Women in Technology Conference (WICT) Denver highlighted the importance of diversity in STEM and technology areas, and was featured in press and on news channels.

His presence on the editorial board of DG Magazine means an assurance of quality content and up-to-date information.

Irfan Nabi
Member Editorial Board

He is a researcher, teacher and administrator all rolled into one healthy mind. In pursuit of his interests, he has gone to places far and wide and worked hard to reach milestones that others only dream about.

Dr. Irfan's ascension to a position of esteem and enlightenment began with a basic degree in Electrical Engineering from NWFP University of Engineering & Technology, Peshawar, Pakistan. Later on he earned a doctorate in Management Information Systems from Institute of Business Administration, Karachi. This institute is also the place where he works as Academic Director, Project Management Program. The position offers him a slew of opportunities to conduct research and provide guidance to the students. Dr. Irfan has contributed his research articles to various publications, journals and conferences. He also finds time to play an active community service role in and around his neighborhood.

It is easy to surmise that his knowledge and experience would go far in raising the standards of our magazine. More important, his counsel would be a great help in maintaining those standards.

CREDENTIALS

EDITORIAL

PRINCIPAL & FEATURE WRITER
Hamed Mohiuddin

ARTICLES RESEARCHER
Salman Khan

SENIOR RESEARCHER & NEWS WRITER
Okasha Mussa Sujela

CYBER RESEARCHER & COORDINATOR
Omer Imran

MANAGEMENT

DIRECTOR OF CYBER TECHNOLOGY
Muhammad Saleem

CONCEPT DIRECTION & STRATEGY PLANNING
Furqan Mirza

MARKETING & BUSINESS DEVELOPMENT
Akmal Khan

ART DIRECTION & DESIGN
Imran J

DG MAGAZINE is an initiative of DIGINFO Group aimed at creating awareness about cybersecurity. The publication is distributed in a variety of ways: electronically via mail, HTML, pdf, mobile message and online flipbook.

PRESIDENT
Muhammad Saleem

V.P. INTERNATIONAL
Muhammad Saeed

COO & STRATEGY
Furqan Mirza

Lead Graphic Designer / Creative Strategy
Quratul Ain Khalid

MEDIA & PUBLISHING
Entity of **DIGINFO Group**
info@diginfo.net

CYBER AWARENESS

In our country, people woke up to the dangers of cyber attacks when most others were at war and devising strategies to fight the scourge. Only recently, several hacking attacks on large businesses culminated in huge ransom demands. These attacks caught everyone unawares and caused tremendous financial losses together with bruised reputation.

Such incidents have highlighted the importance of cybersecurity and the issues surrounding it.

The pressure from the hackers is mounting and they have the power to put lives in turmoil. Anyone who is not aware of the fact is living dangerously.

The best strategy is to be aware and take proper safety measures.

Are Smart Cities Really Secure?

There was a time when the word 'SMART' was used solely for humans—only exception were blondes. But things have taken a dramatic turn. Now everything—mostly inanimate objects—from mobile phones and electronic gadgets to home appliances and personal cards can be described as smart. The latest addition to this list is 'Cities.'

A broader concept of a 'Smart City' is that it makes better use of Information and Communications Technology. A more comprehensive concept is that a 'Smart City' aims to improve city operations and quality of life for the citizens by employing an integrated approach. Giving a boost to the economy by creating new opportunities and expanding the facilities also constitute 'Smart City' features. These two concepts together define the true sense of a smart city. Andrea Caragliu, a google researcher affiliated with Polytechnic University of Milan has this to add to give a clear picture of a smart city: "Investments in human and social capital and traditional and modern ICT infrastructures fuel sustainable economic development and a high quality of life, with a wise management of natural resources, through participatory action and engagement" (Caragliu et al. 2009)

Smart cities are characterized by extensive use of information and communication technology—commonly referred to as 'digital technologies'. They are meant to improve the quality of life by enhancing civic services and making them available more easily at lower costs. The technologies are also geared towards engaging the people to work together with the urban administration for improving the facilities. Various sectors such as transport, power, healthcare, water, sewerage management and government services, are involved in developing a smart city.

THE THREE PILLARS

In recent times, every city is vying to become a 'smart city.' Most people relate it with technology. Although technology is at the heart of such a scheme and an indispensable component, that alone does not fully describe the picture. In a smart city, digital technology is embedded in the city systems and drives everything—from communication networks to city services. The ultimate aim is to improve quality of life for city dwellers through optimizing energy usage, traffic management and efficient city services.

Erroneous beliefs might pervade among the masses, but researchers on the subject seem to agree that three pillars are at the base of 'smart cities.' Human capital, infrastructure and information. First, human capital is all about involving the stakeholders in decision making processes. Second, infrastructure needs technology to carry out activities and provide services to the citizens. Third, the flow of information should ensure that it is open, transparent and reachable so that all the stakeholders have a sense of participation which is imperative in making a city smart.

EXPERTS SPEAK

Former mayor of Eindhoven, Rob van Gijzel, is extremely passionate about cities and city development. His work focuses on cooperation between various government entities, businesses and knowledge institutions. From an early stage of his career, he was interested in 'cooperation within cities.' When he was elected as mayor of Eindhoven and, later, acted as city renewal coordinator of Amsterdam, he got the opportunity to apply his knowledge and theories to bring about a positive change.

Gijzel believes that a smart city is all about intelligent communities. He likes to define the concept in terms of the whole texture of society rather than the cities themselves. It is all about cooperation between various city stakeholders who come together for new urban developments. Gijzel is convinced that while working across all sections of society, it is imperative to include everyone.

Gijzel also recognizes that technology offers a slew of benefits where other methods miserably fail. It gives us an opportunity to create and ensure solutions pertaining to advanced mobility, healthcare, communications and a lot more. But there seems to be a perennial discord between technology people and government functionaries. Techies allege that governments lack the will and speed to implement things required to bring about rapid and perceptible change in society. In fact, there is a lack of understanding about technology in and around government circles. Many of the technology entrepreneurs still insist that a society without governments would deliver a better lifestyle and a more satisfied population. Gijzel, however, thinks that such an arrangement would not endow power to the people. Instead, the world would be dependent on google to make all the decisions that matter. And that is not a comfortable proposition.

ANOTHER VIEW

The ideas and concepts put forth by Boyd Cohen, an urban and climate strategist, have earned wide acclaim and acceptance among researchers and management thinkers around the globe, He is primarily interested in studies revolving around sustainability and smart cities. Boyd Cohen is most recognized for co-authoring a book: Climate Capitalism: Capitalism in the Age of Climate Change. He is also well known for his work on smart cities where he devised a framework that measures the performance of cities on the basis of Smart Cities Wheel. The wheel is a listing of six axes, each with a set of indicators. Cohen proposes that smart cities can be identified with these axes:

- Smart economy
- Smart mobility
- Smart environment
- Smart government
- Smart government
- Smart people
- Smart living

These axes measure the worthiness of a smart city on the basis of information and communication technology implementation, human capital, quality of life, regional competitiveness and participation of stakeholders in city governance. This framework does not attempt to discard traditional theories; on the contrary, it accommodates and connects with older concepts of city governance while introducing radical new ideas.

Boyd's prophecies about future are remarkable and generate an interest to go there without much ado. He sees block-chain and AI as key players in smart cities of future. Furthermore, he visualizes a greater role of citizens in the decisions for cities' welfare. In matters of policy, projects, budgeting, education, welfare and healthcare, he sees innovation on a massive scale. The changes would be so radical and overbearing that the name 'smart cities' would lose its charm. Instead, names like 'livable cities', 'happy cities' or 'human centric cities' might be adopted. Technology will have a place in the scheme of things but it will only function as an enabler of something more valuable like citizens' well-being.

CITY CENTRIC ADMINISTRATION

Political theorist Benjamin Barber served as an advisor during Bill Clinton's presidency. He is known for advocating bold solutions for 'dysfunctional systems and political paralysis.' For a long time he advocated for decentralized local governments rather than federally administered ones. He observed that federal-level politicians often created obstacles and were not very enthusiastic in solving problems. They were prone to wasting time and engaging themselves in

useless debates. In contrast, city governments, led by the mayor, are keen to provide solution by taking bold steps. That's why, Barber suggested that the world should make a transition from nation states to city governments.

His book 'If Mayors Ruled the World' is replete with exciting new ideas about global administration and how mayors can provide solutions

to problems. Only mayors can feel the needs and empathize with the citizens' aspirations to improve lives. The sequel to this book 'Cool Cities: Urban Sovereignty and the Fix for Global Warming' puts forth the argument that cities, not nations, should take the lead in solving pressing global problems like climate change, poverty and disease. In each of the ideas, technology has a central role to play. It is not an end in itself but a means to achieve a far more valuable objective.

CYBER CHALLENGES OF SMART CITIES

We have seen that technology enhancements bring value to the quality of life but they do carry numerous inherent risks. In case of a smart city, a huge network of interconnected systems is in operation. And this huge network is deployed in novel and untested situations. Without security checks and tests malfunctions and glitches are bound to happen. Most of the systems that function in and around cities rely on wireless technology which entails encryption and security protocols. A seemingly minor glitch can swell into a huge problem. One such example is that of a system installed at a county courthouse in California. The system

erroneously sent out summons to 1200 people for jury duty on one morning. This event could have passed without much notice but the uncontrollable traffic jam it caused as a result made everyone sit up and take notice. Experts noticed that this glitch was unintentional but things like these can be introduced intentionally by hostile elements. A number of smart cities are in a nascent stage of development. They are still without a proper action plan to respond to possible cyber attacks. Hackers and hostile groups are always on the look out to make a breach wherever they can find a weak spot. In a smart city a vast surface exists to launch an attack. If the hackers succeed, it means the city's services, information communication technology and infrastructure will be affected. Evidently, cyber attacks cannot be cast aside as insignificant. A number of measures can be employed to minimize the risk although the threats cannot be eliminated completely.

1. Deployment of security check lists for encryption, authentication, authorization, and software updates while implementing new systems.

2. Strict implementation of foolproof and manual options on all city systems.

3. A set of actionable plans and procedures to combat cyber attacks when they occur.

Not far back in time, great hype and fear was generated against the supposed 'Weapons of Mass Destruction' (WMD). On a similar pattern, researchers at Hoover Institutions coined a similar term, eWMD, to refer to cyber attacks of great magnitude. The researchers believed that a cyber attack on chemical facilities, biological research institutes, nuclear plants and nuclear command centers can be no less than conventional WMDs in destructive power. While it is true that eWMDs may not necessarily cause damage to human lives, nevertheless they can deprive people of their livelihoods and can severely affect their economies.

FINAL WORDS

To make smart cities secure and free from risks and threats, the best time to act is now. The hard fact is if cities choose to employ technology, they should anticipate cyber attacks. Attacks increase in direct proportion to how wide the application of technology is. This is the reality. And a smart city requires continuous advancement in technology, organization and well defined action plan to make the place secure. If the cities are safe and secure, trust increases and people will be attracted to make the city their permanent home.

Condition of Greenland's Health Services Critical

Attack Launched On May 9. Patient Records Remain Inaccessible.

The country's government, Naalakkersuisut, has said that Greenland's healthcare system is 'severely limited' because of a cyber attack. Even after two weeks, the effects of the attack have not subsided despite government's efforts to revive the system.

The immediate response to the attack was to restart all IT systems but this action led to severing of access to all patient records. A government statement issued recently reads, "Health services are severely limited and increased waiting times are to be expected while some might miss their appointments."

The government has further confirmed that the attack has also induced malfunctioning in the healthcare service's email system. They have, therefore, asked the citizens to call up the hospitals for any urgent requests.

So far, authorities have not revealed about the nature of attack. Neither have they responded to requests for comment. The Information Security Media Group requested for details about the nature of cyber attack but the government officials chose to remain silent. Initial investigations have only established the fact that the patients' data was neither stolen nor damaged.

Doktor.gl is an online portal used by the healthcare authorities and patients. Often, the citizens use the portal for clinical appointments. The patients also use the communication platform to renew prescriptions. Until this condition persists, the government has requested the citizens to refresh their prescriptions at Queen Ingrid's

Health Center in Nuuk, the capital of Greenland. According to the latest government notification, "the health service continues to have some IT challenges after the cyber attack." Because of the system crash, doctor.gl went offline and will remain that way until the cyber security response team finds a solution. The officials have asked the citizens to use phone lines to contact the healthcare facilities to fulfill their needs.

It is a common observation that threat actors often target healthcare organizations for ransomware attacks, knowing fully well that governments cannot afford to wait for a long time. They are inclined to pay the ransom and get back to the routine. But the trouble is hackers are not bound by any ethical standard. Usually, they do not restore the systems after the payment of ransom. They demand more.

Attackers are also after personal information of patients. Such data can later be sold for lucrative profits. The Hive, a ransomware group recently stole nearly a million personal details and information records from Partnership Health Plan (PHP) of California.

Hackers do this routinely and with ease because healthcare facilities are not well equipped to face an attack. Obviously, the system design was aimed at providing facility to patients. Fighting off hackers and organized criminals was never their intended purpose.

It is now the job of system analysts and coders to design software that does not easily succumb to attacks. The systems have to be foolproof to ensure smooth operations at healthcare facilities.

SMART GRID SECURITY

CHALLENGES AND SOLUTIONS

Few people have a clear idea about what a grid really is although they hear the word frequently whenever news about power and power generation beams on channels and reports. The number of people who know about 'smart grid' might be infinitesimally small. In the wake of this lack of awareness, the discourse should begin with the basics. Electric power systems evolved during last seventy or eighty years. The systems provide electrical power collected from generators to a high voltage network, commonly referred to as a transmission grid. The generators are usually large having a capacity of 1000MW energy and they are powered by fossil fuel, hydro-power or nuclear plants.

To facilitate coordination between the generators and transmission circuits, the entire system consists of communication links. A fair amount of automatic controls are installed in this part of the system to ensure predictable actions during power disturbances.

On the other side, the distribution system is an extensive operation which is almost devoid of any communication except for some local controls.

SMART CHOICE. While the electrical grid is an engineering marvel in itself, the increasing complexity and urgent needs of this century has placed new demands. To move ahead, a new kind of electric grid, complete with computerized equipment and latest technology, is essential. Such an arrangement would be able to automate and manage complex networks of electricity distribution.

The current revolution in communication, triggered by the arrival of internet, presents a host of opportunities to monitor and control processes more effectively—offering flexibility and cost-efficiency. This realization gave rise to the concept of 'smart grids,' almost a decade ago. Smart grids allow the use of ICTs (Information and Communication Technologies) to radically transform electrical power systems. Essentially, smart grids are electricity networks that enable two-way flow of electricity and data. Smart metering is a vital component of this grid system, as it provides information about the loads and the power running throughout the network. When monitoring of entire system in a grid is done, it is possible to observe the current status of the system offering possibilities to control.

SMART REASONS. Sustainability and climate change have become the buzz words today. Scientists are aligned to the concept that man-made greenhouse gases have gravely affected the balance of nature. The climate change is drastic and it is causing unexpected changes around the world. Carbon emissions owing to industrial activity are at an all-time high. Scientists, therefore, have a consensus that new ways must be devised for effective use of energy and for electrical power generation without producing large amounts of carbon emissions including CO2.

Smart grids have generated great interest since at least 2005. Central to this wave of interest is the realization that information and communication technology offers significant possibilities to modernize network of operations. At the deeper level, there is an understanding that decarbonizing of the operations at reasonable cost can only be ensured with effective monitoring and control. So many variables are involved in regulating a network grid that such systems cannot operate cost -effectively without the technology of a Smart Grid which ensures proper monitoring and control.

Besides the above realization, there are various other reasons that have necessitated a shift to smart

grids for power generation and transmission:

AGEING ASSETS. The evolution of power systems dates back to the 1950s. The transmission lines, together with the equipment that were installed at that time, have served well beyond their lifespan. The ageing setup is now in urgent need of replacement. According to estimates, 80% of population of the world will be living in urban areas in the near future. The increasing complexity of systems because of this concentration of people

requires modernization and active participation of ICT. The old setup must go but this is easier said than done. The installations and assets are huge and they cannot just be replaced in a matter of days or even months. This will take a lot of painstaking work and intelligent working to gradually phase out the old system while bringing in the new systems and equipment.

HEATED ISSUES. When power cables carry current beyond their capacity, the wires get over-heated resulting in rapid deterioration of insulation. This leads to reduced life span of the equipment and increased incidences of power failures and disruptions. The increase in current passing through the transmission line together with the ensuing over-heating results in lengthening of the conductor. This in turn results in increased sagging of the cables suspended on steel supports. The sag again gives rise to more frequent faults. This phenomenon is a huge hazard to people dwelling near and underneath the power lines.

OPERATIONAL PROBLEMS. Power systems operate within defined limits of voltage and frequency. When the voltage goes beyond the upper limit, the insulation of components and consumer equipment may get damaged leading to short-circuit faults. In contrast, when the voltage is too low, flaws and malfunctions in customer equipment may develop easily.

Such problems revived interest among technologists to look for alternatives such as connecting power generation system to distribution network. But the distributed generation too can occasionally cause heightened voltages, requiring various corrective measures to regulate voltage in distribution circuits.

In case of renewable energy, like solar power and wind power, power generation varies and it is difficult to predict with accuracy about the expected output, say, a few hours later. Maintaining a balance in the supply-demand ratio becomes a task of considerable difficulty. In the face of these difficulties, power system operators are increasingly showing interest in frequency response and reserve services. It is surmised that future holds a promise: the new modes of transmission and generation relying on automated controls should help maintain network stability and reduce the need for network reinforcement.

CONTINUOUS SUPPLY. The current times place a premium on reliable and uninterrupted supply of electricity. The older method to increase reliability and ensuring continuous supply was to install additional circuits and disconnecting the faulty ones. But such methods cost heavily on the power supplier. A smart grid, in

contrast, uses intelligent post-fault configuration to address faults immediately and restore power supply to the customers. What's more, the smart grid efficiently uses the installations and does not require additional or redundant circuits. Better and efficient utilization of resources is the key

feature of delivering service and economizing at the same time.

GOVERNMENT PREFERENCES. Several governments across the world are putting their stakes on Smart Grid initiatives deeming them to be cost-effective methods to upgrade and modernize infrastructure. The grid also enables integration of low-carbon energy resources. Countries like China, Japan, UK, US and many more of the European Union are linking Smart Grid systems with development of nations. The State Grid Corporation of China (SGCC) has released a comprehensive plan for the development of Smart Grid:

"A strong and robust electric power system which is backboned with ultra high voltage networks; based on the coordinated development of power grids at different voltage levels; supported by information and communication infrastructure; characterized as an automated, and interoperable power system and the integration of electricity, information and business flows." The European Union has also emphasized the importance of Smart Grid technology platforms. The union has released a statement outlining vision and strategy for electricity networks operating in Europe:

"It is vital that networks are able to integrate all low carbon generation technologies as well as to encourage the demand side to play an active part in the supply chain. This must be done by upgrading and evolving networks efficiently and economically."

CHALLENGES
Since smart grids would be running huge power supplies, it is fair to assume that they should be riddled with risks and threats. Such risks have the potential to affect the performance of the organization and also the loyalty of customers. Another risk revolves around the privacy of data which can mean an attack on personal information which can harm the trust between customers and the organization.

Phishing. This could be the first attempt in putting the business or operation of an organization at risk. The hackers can gain access to customers very easily and from there they can get to sensitive information of the power supplier which can be exploited to the hilt.

Denial of Service Attack. This is a strategic move by hackers to strike where it hurts most. DoS or DDoS is a kind of attack that severs the link between the customer and the service provider. After the attack, the services are taken off from the communications channel—usually a website—and the hackers demand huge amounts of money as ransom to restore website to the previous state.

Malware Spreading. The hackers can acquire the ability to spread malware by infecting servers of the organization. A power supplier has a colossal infrastructure offering a good number of entry points to the hackers. This kind of attack can be very potent and can turn out to be a major risk to the organization. The fact is, hackers can manipulate the functions of devices and gain control of the infrastructure and equipment by using malware. Once this is done, hackers would assume the role of masters and will dictate their terms.

Traffic Analysis. Spoofing attacks have become weapons of choice for hackers. Of particular significance are eavesdropping and traffic analyses. Smart grids operate on a huge scale with larger networks and a variety of network nodes. The network operates under an ever-present threat of getting its data stolen.

SECURITY BREACHES
Although smart grids offer great benefits to the power sector, their size and huge infrasttructure is their biggest vulnerability. The world has seen numerous breaches aimed at power suppliers.

TrojanHorse Malware. Back in 2015, a cyber incident occurred in the electrical power station of Ukraine's Ivano-Frankivsk city. More than 1.4 m people were affected by this attack. Nearly 80,000 directly suffered by going without power for days. The cyber attack was perpetrated after launching a spear-phishing email campaign. With the help of this campaign, the attackers were able to infect the systems with a Trojan horse malware known as BlackEnergy. This virus not only deleted data and destroyed hard drives, it took control of infected computer to ultimately launch a coordinated denial of service attack to tarnish the image of the giant power supplier.

STUXNET MALWARE. This malware was specially developed by coordinated efforts of US and Israeli intelligence agencies to target Iran's nuclear power plant. It was meant for targeting SCADA networks by manipulating Programmable Logic Controllers. The Stuxnet worm ultimately gains control of electromechanical processes of

automated machine. This dangerous worm stealthily infiltrated computer systems of the nuclear facility and it could have wreaked havoc by destabilizing the nuclear fuel. But proper safety measures were adopted to avert the threat.

WANNACRY RANSOMWARE. A hugely devastating programme, it was responsible for attacks on well known companies worldwide including FedEx and Renault. It also crashed more than two hundred thousand computers belonging to individuals residing all over the world. For restoring the system ransom in crypto currency was demanded. The most notable exploit consisted of an attack on a healthcare facility, NHS, which led to cancellation of 19,000 appointments. The damages including restoration and upgrades to systems, and heavy fines added up to £100 million. Damages aside, the WannaCry Ransomware actually jeopardized the lives of nearly 19,000 patients, some of them seriously ill patients who could not afford to miss an appointment.

SOLUTIONS

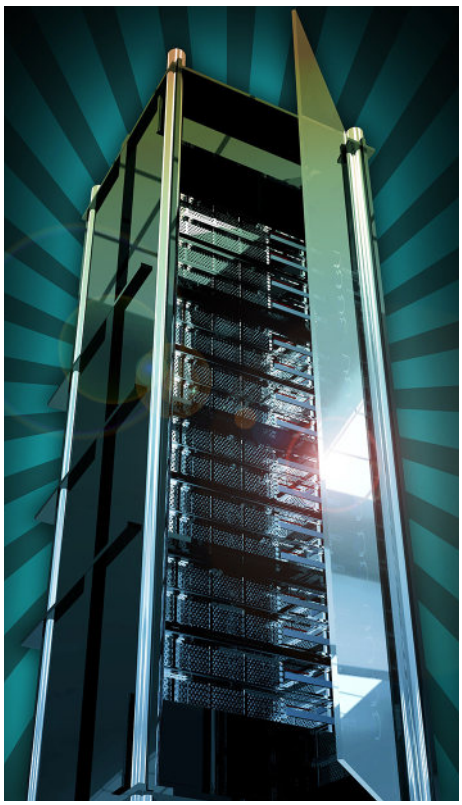
Although some level of security is required for systems at the lowest levels, elaborate setups that manage company data. Smart Grids are particularly large offering huge surface area of attack. Their vulnerability far surpasses those of smaller systems. Cybersecurity experts suggest a number of precautionary measures to avert any attempts of attack. Following are well known methods that are adopted to mitigate possibilities of attack.

Encryption
Authentication
Malware Protection
Nework Security
Remote Access VPN
Intrusion Detection System
Intrusion Prevention System

In terms of operational efficiency, smart grids conveniently outpace traditional power grids. Smart grids are environment friendly and support clean energy initiatives. But at the same time they are fraught with risks. The levels of vulnerability are extremely pronounced and experts suggest strict adherence to above measures. The greatest challenge of smart grids is that devices that are the components of this network are spread over a vast geographical area. With an exposure as vast as that, attackers can come from anywhere. Round the clock vigilance and an eye on suspicious activity is the order of the day.

Cybersecurity specialists also advise maintaining data backups on various alternative storage options so that in an event of attack, prompt retrievals can be made.

Even if the defense mechanism is seemingly impregnable, smart grids are sensitive systems that require cybersecurity of highest standard. A relaxed and casual approach to security issues, would only result in a breach. And that could mean a disaster on an unimaginable scale.



DIGINFO®

TRUSTED LEADER IN CYBER SECURITY

DGCLOUD

SECURE CLOUD PLATFORM

WITH CLOUD TECHNOLOGY, YOUR PERFORMANCE— AND BUSINESS—CAN REACH THE SKIES.

DG CLOUD helps customers to define, manage, operate, maintain and have full visibility on their cloud environment.

DG CLOUD is a unique platform that orchestrates the deployment of computer and virtual infrastructure resources and of complex multi-tier application architectures.

It integrates and leverages the strengths of a hybrid cloud environment, providing the ability to design and deploy enterprise-ready services tailored to the business needs of your organization.

DG CLOUD PRODUCTS

DG CLOUD Workplace

DG CLOUD Workplace is a fully automated virtual office with all necessary virtual servers: configured and ready to use.

DG CLOUD DevOps

DG CLOUD DevOps provides full, ready-to-use infrastructure for Cloud Based Collaborative Software Development.

DG CLOUD Sparks

DG CLOUD Sparks provides high end servers for dedicated tasks with dedicated computing resources for customers.

DG CLOUD Hosting

DG CLOUD provides robust, reliable and secure infrastructure for ERP, In-House Software, SAAS Applications.

Reconnaissance Operations Against Austria & Estonia.

Russian Hacker Group 'Turla' Behind The Attacks.

According to a cybersecurity company, Sekoia, Russian state-sponsored hacking group, Turla, is running a new reconnaissance campaign against Austrian Economic Chamber, a NATO platform and the Baltic Defense College.

This revelation is based on prior findings by Google's Threat Analysis Group (TAG) which is keeping a close eye on Russian hackers—either independent or state-sponsored. During a routine surveillance mission, Sekoia security specialists observed that Turla operatives were targeting an Austrian federal organization and a military institution in the Baltic region.

Google had already warned of renewed activity in the region by Russia-based threat actors. They had noticed that two of Turla domains were being employed in ongoing efforts.

Turla has remained in the news since at least 2014 and the group is known to have close ties with Russian Federation's FSB service. Turla's exploits are closely monitored and well-documented. The group was recently detected while deploying backdoors and Remote Access Trojans (RATs) against various EU governments, embassies and research institutes. The IP address, believed to be one used by the group, links it to targeted systems.

One of the targets is a military college in Estonia, jointly operated by Latvia, Lithuania and Estonia. The seat of learning also functions as the nerve-center for strategic and operational research in the Baltic region. The next target is Austrian Federal Economic Chamber, known as WKO, that advises governments on legislation and economic sanctions around the world. Finally, the last one is an e-learning portal of the NATO Joint Advanced Distributed Learning Platform.

The detective work performed by Sekoia is worth mentioning. It was observed that the domains were hosting a malicious Word document with the name 'War Bulletin19.00 CET 27.04.docx.' The document was infiltrated in various directories of the website. The word file contained an embedded PNG which is the key of reconnaissance operations. The word file itself had no malicious macros. With that discovery, Sekoia deduced that Turla was aiming its operations against Austrian federal organization and a military institution of the Baltic region.

Turla also focuses on getting hold of IP addresses belonging to their victims, which becomes a helpful tool in subsequent stages of operations.

For the aid of cyber defenders, Sekoia has provided a Yara rule which can be very helpful in combatting and neutralizing the attacks.

CRISIS OF LEADERSHIP
IN CYBERSECURITY

Nowadays, organizations are grouped in two ways: those that have experienced a serious breach and those living under the fear of experiencing one. The pandemic has only exacerbated the situation: the ranks of the first group have increased while the vulnerability of the latter has grown. The primary reason for this state of affairs is that the leaders of organizations give scant respect to cybersecurity matters.

DISSECTING THE PROBLEM.

As stated above, most CEOs today, do not give the support their organizations need. That is why a majority of companies still struggle to make cybersecurity a significant part of organizational structure which includes strategy, planning and operations. Two reasons are cited for this scenario:

a) cybersecurity is relegated to a dark corner of the organization with no significant role to perform.
b) most cyber leaders are clueless as to how to perform tasks of strategic importance.

In a study seeking to identify the key causes of this dismal performance, it was revealed that CEOs and CISOs of a large number of organizations barely interacted with one another to discuss matters of strategic importance. This turned out to be the single most important reason that cybersecurity ranks as an afterthought. About 21% of CISOs who were interviewed said that CEO of their company was among the three positions they had least contact with. By region the ballpark figures were no different. In Europe, nearly 28% CISOs counted CEO among the three positions they had least contact with. The figures for Asia-Pacific and North America were 21% and 19% respectively.

In the early days when information technology was still in the developing stage, companies and CEOs did not expect more from CISOs apart from routine technical tasks. At that time, cyber security was considered as a function of no significance.

This might have worked out back then when threats were fewer and breaches even more so. Times have changed. Now cyber leaders have a number of responsibilities including the primary task to embed security all across the organization. And they have added tasks to perform like regulating company's operations with regard to cybersecurity, responding to risks and threats and creating awareness about best practices throughout the

organization. To sum up, their task is to lead and that requires close cooperation with board members, particularly the CEO.

THE PURSUIT OF SOLUTIONS.

A breach is no ordinary event. First, it causes colossal damage in terms of assets. And then there are other losses that are not easily quantifiable like the reputational damage and loss of trust. Nowadays, all the stakeholders including the customers, shareholders and even employees consider a security breach as synonymous to breach of trust. Without trust of these stakeholders, businesses can neither thrive nor survive. The greatest responsibility of building and maintaining trust rests with the CEO who should play a proactive role in engaging fellow leaders like the CISO (Chief Information Security Officer), CIO (Chief Information Officer) and CTO (Chief Technology Officer) to put in place a framework for board members and C-suite executives when formulating a security strategy. And that also means the CEO and the company board members should be willing to hunt and hire security leaders who have what it takes to be a true leader.

SETTING THINGS STRAIGHT.

Now is the time for boards and C-suite executives to redefine and reposition the function of cybersecurity leaders. A framework drawn from research, extensive surveys and consulting engagements has emerged which suggests a number of steps to bring about a qualitative change.

Redefining Cybersecurity Strategy.

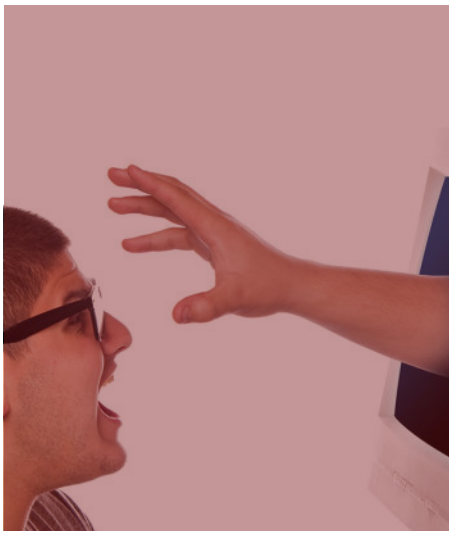
Businesses today vary in size, shape and type. The threat profiles of each company vary according to its type. Therefore, a single, ready-to-use cybersecurity framework cannot be as effective as one that incorporates few specifics along with the usual features. The context of business will drive the choices cyber leaders will make while framing the security policy. The leaders may consider formulating the strategy around regulatory needs, risk profiles, and customer demands after choosing the regular and usual options that are basic to security framework. The leaders will have to analyze the security needs of their company and then make informed choices. Only then will the effects translate into favorable business outcomes. Being generic or aimless might be as lethal to the business as a breach itself might be.

Repositioning Cybersecurity Function.

Historically, cybersecurity was conveniently consigned to an inferior position under the larger IT function. But now, it is no longer a wise step to put cybersecurity under the same management and within the same budget. A true cyber leader exercises authority and he must be independent to take decisions to bring about change across all departments of the company. The leader takes stock of the situation and determines about the types of influences cybersecurity must have in and around the business operations. The leader also ensures provision of incentives to stakeholders so that they work closely with the cybersecurity function. A global organization, for instance, offers bonuses to executives whose departments partner the cybersecurity function by observing strict compliance with the rules laid down by the security leader. Such incentives, which are initiatives in repositioning of the security function, ultimately result in success of the organization because such steps exclude obstacle that come from threats, risks and cyber attacks.

Hiring Right Leaders.

The CEO and the board members should be careful in choosing the right person to lead the cybersecurity initiative for the company. Skills set might be the basic requirement but the quality to look for in a prospective candidate is leadership. Some of the attributes the hiring squad may look for include a mindset inclined toward leadership, an empathizing attitude toward subjugates, bringing out the



best in others, a voracious appetite for learning new things and penchant to seek a global view of things to develop an understanding. While the CEO and board members may require some basic skills in a prospective cyber leader, such as network security rudiments, threat intelligence, and rapid response techniques in an event of attack, but these should not be the only parameters for selection. The mindset should stand out as the key characteristic in a cyber leader. This should take precedence over all others. A leader is different from others for he is out there to enforce his ideas to make things work the way he wants.

SOME ADVICES FOR CEOs.

Price Waterhouse Cooper conducted a 2022 Global Digital Insights Survey asking some 700 CEOs and 2900 C-suite executive about the extent of CEOs' involvement in cybersecurity matters. The CEOs' responses were in stark contrast with those of other executives. The CEOs considered themselves as engaged and strategic. They thought that their role was participatory in discussions on cybersecurity and privacy matters. In contrast, executives other than CEOs considered that their CEOs were reactive rather than proactive. They got themselves involved in security matters only when it was required as in an event of breach or when regulators wanted them to respond. Almost 63% of non-CEO executives claimed that their company did not get the support that it needed from the CEO.

In spite of this dismal picture, there are CEOs who have turned the tables in their favour. By adopting exemplary practices, almost 10% of organizations, led by their CEOs' created a work environment that is worth emulating. The analysis of data based on the survey has revealed that there were certain key elements were common to these CEOs and their companies. Their approach to cybersecurity was marked by four Ps: principle people, priority and perception. CEOs who have succeeded in turning the liabilities into advantages are actually those who have stuck to the four Ps. And they have embedded cyber leadership as a basic feature of strategy and goal.

Principle: Successful CEOs consciously believe that their first duty is to link the organization's mission to security of data and assets. They make sure of this by sticking to the principle of considering security and privacy as fundamental parts of operational goals and business essentials.

People: Having a goal to establish their organization as a cybersecurity leader, CEOs are always keen on attracting capable professionals. After hiring them, they invest time and money, and leave no stone unturned to retain them. The CEOs command a view of the entire operations and they can gauge the cyber needs of the company which helps them in attracting talent and developing their skills. This ultimately enables the new employees to focus their energies toward building and transforming their company into a much bigger and much better entity.

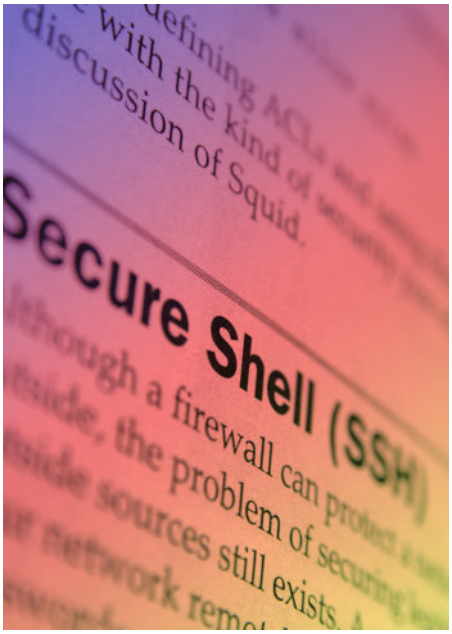
Nicola O'Connor, Chief Information Security and IT Risk Officer has highlighted the importance of hiring the right candidate to be a cyber leader. She said, "To be a successful CISO, you need to understand the business you're operating in and get behind what the business wants to do."

Priority: Successful CEOs have been known to prioritize cybersecurity in the decision making process. For instance, such CEOs and their companies would walk away from a deal—even if it is to their advantage—if the deal would introduce a risk. Likewise they would delay the launch of a product until key cyber vulnerabilities are checked and removed. CEOs, therefore, are charged with enthusiasm and they use their authority to set priorities that ultimately deliver advantage to the business.

Perception: The leading companies and their CEOs are fully aware of the cyber perception gap that might exist. Only 40% of the surveyed companies understood about the risks that were introduced as a result of interaction with third parties.

CEO of Special EU Programmes Body, Gina McIntyre insists that companies should pay attention to the human element of cyber defence. She said in a recent PwC webinar, "Your biggest vulnerability is going to be that one human being clicking on something that he should not."

The four P's might not be the last word but they provide a ground for initiation. Cyber threats are everywhere. And the best one can do is to bring dynamism to fight threats. That can only be done by testing new ways and adhering to old ones that have proved to be effective.



Sensitive Government Websites in Italy Hacked

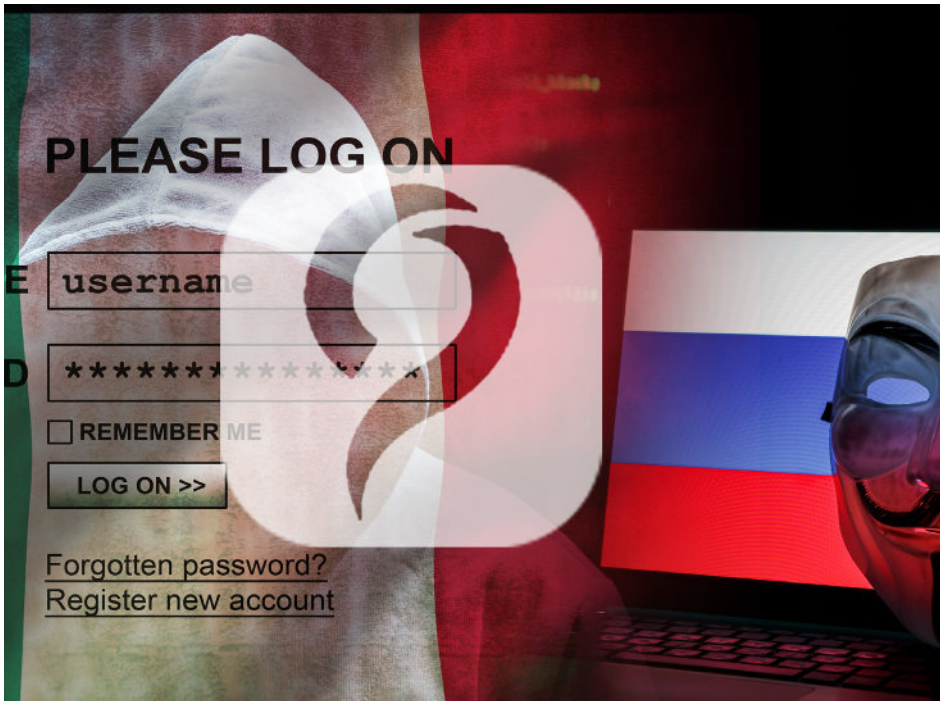
Investigators Believe Pro-Russian Groups Are Behind The Attack.

Among those hit by the malware are websites operated by Italian parliament, military, Defense Ministry, Senate and National Health Institute.

A pro-Russian group of hackers, Killnet, has claimed responsibility for the attack. The same group has also claimed responisibility for attacks on German government portals. Maximilian Kall, a spokesman for Interior Ministry, has confirmed the attacks but he also said that the attacks were repelled with full force and no data leak was reported. Der Spiegel, the news magazine, first broke the news saying that the attacks were aimed at Defense Ministry, the Bundestag, several police departments and federal police.

The conflict in Ukraine has contributed toward increased attacks on both sides. Anti-Russian hackers have taken it upon themselves to launch intermittent attacks on Russian government organizations, including the Kremlin, banks and financial institutions. Western governments are on high alert anticipating retaliatory attacks by state-sponsored groups and individuals sympathetic to Russian regime.

Intelligence agents of Romania disclosed last month that Killnet targeted Romanian government websites in retaliation to Bucharest's support to Ukranian causes. The same group has launched attacks on official websites of the US, Czech Republic, Poland, and Estonia besides some other NATO member states. The apparent reason is to put across a message that any ill intent toward Russia will be dealt with a harsh response.



The attack on Italy's key organizations and businesses was massive in scale. It affected various government bodies besides the Automobile Club d'Italia and many more institutions. Yet the attack was far less in intensity and destructive power than the one launched on Romania. The Killnet hacking group claimed responsibility for all the attacks and warned that more such attacks will follow soon.

National Cybersecurity Agency, responsible for providing security related solutions to Italy's IT installations, avoided all attempts my media sources to elicit a response, but the president of Italian senate, Maria Elisabetta Alberti Casellati, informed her countrymen that the attack did not cause any substantial damage to the parliament's website nor was any sensitive data stored on the systems stolen or copied. In her tweet, she stated, "No damage from the attack which involved the external network of the Senate. Thanks to the technicians for the immediate intervention. These are serious episodes which should not be underestimated. We will continue to keep our guard up."

Killnet's specialty is in Distributed Denial of Service (DDoS) attacks. The hackers try to paralyze servers with a flood of data which increases the traffic and slows down the servers. As a result, users are often unable to access the website or perform the intended tasks.

Vicious Cyber Attack on Washington Local Schools

The Attack Impaired Performance Of District's Digital Services

The Washington Local Schools district covers 17 square miles in Toledo, Ohio. Nearly 7000 students are enrolled at eight elementary schools, two single-grade junior highs and one comprehensive high school campus. Recently, the district administration admitted that a cyber attack hit the chain of schools leaving the phone-lines, email accounts, internet, WiFi and Google Classroom in disarray.

The facebook page of the schools carried this statement on May 19 at 2:59 a.m. soon after the incident.
"We are working with cyber forensic professionals to assist with the investigation and recovery. Please understand that teachers and staff do not have access to outgoing or incoming calls or email at this time.
"Tomorrow morning we will communicate an emergency phone number dedicated to each school. You will receive this information on our Swift K12 Alert System and in a printed letter that will go home with students.
"At this time, we are just beginning to learn some of the details of the attack. As the investigators learn more, we will provide updates.
"If you have a senior, we are working to ensure a smooth exam process and make their final two days memorable.
"Thank you for your patience and understanding as we work with cyber professionals to restore our system."

Luckily, the incident occurred when the academic year was coming to a close at the schools. In the last week before the close, the students were introduced to lessons in the 1990-way which essentially meant there was no internet.

Superintendent Kadee Anstadt said that the phone-lines have been restored and email can also be accessed as long as Washington Local's server is not being used for the purpose.

Several bodies came forward to provide assistance to the schools in this hour of test and tribulations. The Huntington Centre offered their space to hold the graduation ceremony while the Toledo Lucas County Public Library offered WiFi hotspots and meeting space for students and administrators who were taking online courses. The library's printer was also there for liberal use.
Jason Kucsma, the executive director at the library acknowledged that the entire district assisted the library when it was hit by a ransomware attack that encrypted data and demanded huge ransom for unlocking the files. At that time, WLS offered its facilities for the library staff enabling them to continue working for the community. When the WLS was suffered a similar attack some time later, it was automatic for the County Public Library to return the favours.

Ms Anstadt expressed her gratitude for this gesture and said, "Huge shout-out to the Toledo Lucas County Public Library who made a ton of hotspots available to us and helped us during all this. A lot of our teachers went to the library over the weekend and borrowed them so they could make use of them in the classroom this week."

The whole episode exemplifies how welfare communities respond and assist each other whenever an untoward incident takes place. The world should take the example of Washington Local Schools and take a lesson from them.

Dr. Masroor Ahmed Shaikh

Chairman, Sindh Board of Technical Education (S.B.T.E)

ENHANCING SKILLS

TO ACCELERATE THE EDUCATIONAL ACTIVITIES IN PAKISTAN

Dr. Masroor Ahmed has an enviable portfolio studded with educational accomplishments and work experience spanning over 31 years. His professional career started with a civil engineering degree, followed by master's degree in Transport Planning and Engineering. His educational pursuits culminated with a doctorate in Geotechnical Engineering from UK.

His work experience is just as impressive, taking him to far and wide places on projects and assignments that enriched his portfolio. Along the way, he has won several awards and accolades, wrote a number of research papers besides authoring a good many publications. Since 2016, he is heading the Sind Board of Technical Education. Under his leadership, the board has brought about radical improvements in the system and increased the value of its certifications and degrees which has meant tremendous benefits to the job-seekers who have earned their education from SBTE.

Q&A QUESTIONS & ANSWERS

As you are aware that cyber threats are everywhere in the world and no body or organization is safe, what do you think about this situation?

Yes, the escalation of cyber security breaches has alarmed every organization everywhere. Human negligence is the biggest threat to information security. Bad hats are using social engineering tactics to gain control in enterprise infrastructure. The human factor needs serious attention. And thoughtless migrations to cloud also have serious implications because cloud-based assets are compromised more than on-premises assets. Large parts of daily lives are shaped with computers, smart phones, the internet and number of unnoticed ICT dependent services we take for granted such as electricity, healthcare, etc. The fact that cyber dependency has become so widespread it resulted in emergence of new cyber threats. So,it is time to look deeper into the recent security incidents that can help information security leaders in both public and private organizations to allocate information security budgets to prevent, detect, and respond to attack.

Who can be involved in a cyber-attack, if we would like to know your enemies & why is it necessary to protect from cyber threats?

Cyber attacks hit businesses everyday in more ways than most people knows. Interestingly, there are two types of companies: those that have been compromised and those that don't yet know they have been compromised. The motives of cyber attacks are many and attacks are now more sophisticated than ever. The individuals are victims too as they save their personal information on their gadgets and use insecure public network.

In fact, companies are still not immune to evolving cyber attacks. Phishing, ransomware, cyber scams are some of the common yet highly serious cyber attacks that are designed with the aim to access and exploit the user's sensitive data. Moreover, cyber-attacks could also cause electrical blackouts and paralyze computer systems. The introduction of IoT technology i.e. Internet of Things, has not only simplified and sped up our tasks, it has also created a whole array of new vulnerabilities for bad actors to exploit. No matter how advanced security measures we take, cyber criminals will always stay one step ahead to attempt cyber crimes. If these internet-connected devices are not managed properly then they can provide a doorway to business to cyber criminals. Information Security professionals need to work to improve their knowledge related to modus operandi of attackers and threat intelligence

What cyber security measures have you introduced and implemented in your organization?

Well, the only thing that is crucial for your organization is a strong cyber security system along with the best cyber defense practices to reduce the cyber threat posture of your organization. Recently, we have established Information Security Policies and procedures, Disaster recovery site, implemented

NGFWs, multifactor authentication solution and micro-segmentation. These measures will work other information security tools like EPP, WAF, EDR, SIEM, VAPT etc. On fast track we are working on key area i-e cyber security awareness which is the essential measure to bridge gap of cyber security skills and to create a cyber-resilient working culture in the organization because mere technical controls will not stop cyber criminals from accessing your computer systems.

Most importantly, as a game changer, PIA is establishing its SOC (Security Operation Centre) that will help to improve information security posture of the company by monitoring, detecting and responding the cyber threats. The SOC will work 24/7/365 and be equipped with threat intelligence. In this year, PIA will be striving for ISO-27001: Information Security Management System (ISMS) standard.

How would we tackle with non-state actors--black hat hackers?

The dark part in tackling non-state actors is that international cyber laws are less effective and do little in preventing such cyber-attacks. This legal ambiguity makes an attractive domain for non-state actors in cyber conflict. Sadly, nations are currently pursuing cyber warfare capabilities and employing such non-state actors as hacktivists and patriot hackers. Tools used by these non-state actors include website defamation, internet resource redirect, denial-of-service attack, information-theft, website parodies and various form of cyber-sabotage. Again, I would say that organizations must efficiently shield all its cyber-resources by putting both technical and administrative controls.

How do black hat hackers damage the system?

The black-hat hackers are the malevolent type of hackers; they are people who exploit computer systems and networks for their own benefits. Black-hat hackers are commonly viewed as most destructive actors. They have scant respect for the law. They may also release malware that destroys files, holds computers hostage, or steal passwords, credit card numbers, and other personal information.

The security measures to survive are

1. Fine-tuned Firewalls.
2. Well organized Incident response.
3. Security awareness sessions.
4. Strong threat intelligence.
5. Formation of RED and BLACK Teams.
6. Well defined information Security Policies.
7. Rightfully placing administrative. and technical controls.

Do you have all the information that needs to oversee cyber risk?

Overseeing cyber risk is challenging and needs active engagement from management. First we need to incorporate cyber risk in strategic decisions as cyber risk management is no longer just about preventing breaches, it is also about mitigating financial and reputational damage when breach occurs. Stockholders also demand that companies do everything in power to prevent breaches.

We should at least know and do the following to oversee cyber risks:

- Organization of key cyber risks.
- Threat actors and their motives.
- Threat actor targets and business impact.
- Understand the regularity requirements.
- Quantifying the risk.
- Prioritize the risk.
- Aligning capital allocation with identified risk .
- Draft risk appetite statement.
- Integration of cyber risks into organization's risk management program.
- Monitoring cyber-resilience.

How effective is your cyber security strategy at addressing business risks?

For addressing business risks, cyber security strategy is critical.

Steps to Assess and Mitigate Cyber Security Risks:

Step #1: Target internal threats
Step # 2: Prioritize risk
Step # 3 : establish effective communication channels
Step # 4: Enable continuous monitoring
Step # 5 : Stick to an established cyber security framework
Step # 6. Develop incident response

plan.
Step # 7. Ensure business continuity
Step # 8. Consider cybersecurity liability insurance.
Step # 9. Nurture a culture of cybersecurity.
Step # 10. Re-evaluate cyber risk regularly.

Having a more reliable cybersecurity strategy in place can also improve business's reputation. Potential partners and customers will appreciate the emphasis on security, leading to higher loyalty and, thus, revenue.

How do we protect sensitive information handled and stored by third party vendor?

The growing number of third-party data breaches and the sensitive information they expose have negatively impacted consumer trust. Third-party breaches occur when sensitive data is stolen from a third-party vendor or when their systems are used to access and steal sensitive information stored on your systems. These third parties aren't typically under your organization's control and it is unlikely that they provide complete transparency into their information security controls. Some vendors can have robust security standards and good risk management practices, while others

may not. Therefore, we must at least do the following

1. Assess your vendors for before on boarding.
2. Incorporate risk management into your contracts.
3. Keep an inventory of your in-use vendors.
4. Continuously monitor vendors for security risks.
5. Collaborate with your vendors.
6. Talk about third-party risks.
7. Cut ties with bad vendors.
8. Measure fourth-party risks.
9. Follow the principle of least privilege.

Do you have the right data governance strategy to minimize cyber risk?

Data governance identifies important data across organizations and improves its value to the business. The most common areas covered by data governance are;

- Data Quality
- Data Availability
- Data usability
- Data integrity
- Data Security

And addressing all these points requires combination of people skills, internal processes, and appropriate technology. In our organization, we have created data governance framework that requires funding and management support. Another important thing in data governance is user engagement. They are the ones who consume data, understand and cooperate with governance rules.

Are your employees fully equipped with cyber technology and have all required certification?

The IT personnel trainings and certifications are vital to run information security programs successfully. Time to time, we arrange trainings for our employees. We also have 'allowance payment programs' for those employees who get industry standard certifications.

Why do we need to worry about information security?

In an increasingly interconnected environment, information is exposed to a growing number and wider variety of risks. Threats such as malicious code, computer hacking and denial-of-service attacks have become more common, ambitious, and sophisticated, making implementation, maintenance and updates of information security in an organization more of a challenge.

Implementing information security in an organization can protect the technology and information assets it uses by preventing, detecting, and responding to threats, both internal and external.

What do you think are the biggest cybersecurity threats right now, especially in perspective of Pakistan; and what do you suggest to tackle these threats?

The negligence from top management regarding information security is the biggest cybersecurity threat right now. Second is the employees' low levels of awareness and seriousness towards cyber security. Fortunately, Pakistan's National Security policy and Information Technology policy have addressed cybersecurity significantly and these strengthen cybersecurity posture.

People receive messages and emails that may be from malicious hackers, how can they be safe?

At first line defense, malicious emails carrying suspicious links should be stopped by fine-tuned technical controls. If malicious email bypasses the technical control then employees' cybersecurity awareness trainings should be strong enough that employee recognizes these types of emails and inform relevant teams to stop the spread of malicious code.

Do we need cybersecurity insurance?

Insurance coverage is important to protect businesses against the risk of cyber events. The cybersecurity insurance is gaining popularity Companies that purchase cybersecurity insurance today are considered early adopters. Businesses that create, store and manage electronic data online, such as customer contacts, customer sales, PII and credit card numbers, do need and can benefit from cyber insurance.

Are your information security and business priorities aligned?

We are striving towards it and industry regulations are helping us to achieve this alignment. The top management is now convinced and feeling that information security priorities should be aligned with business priorities.

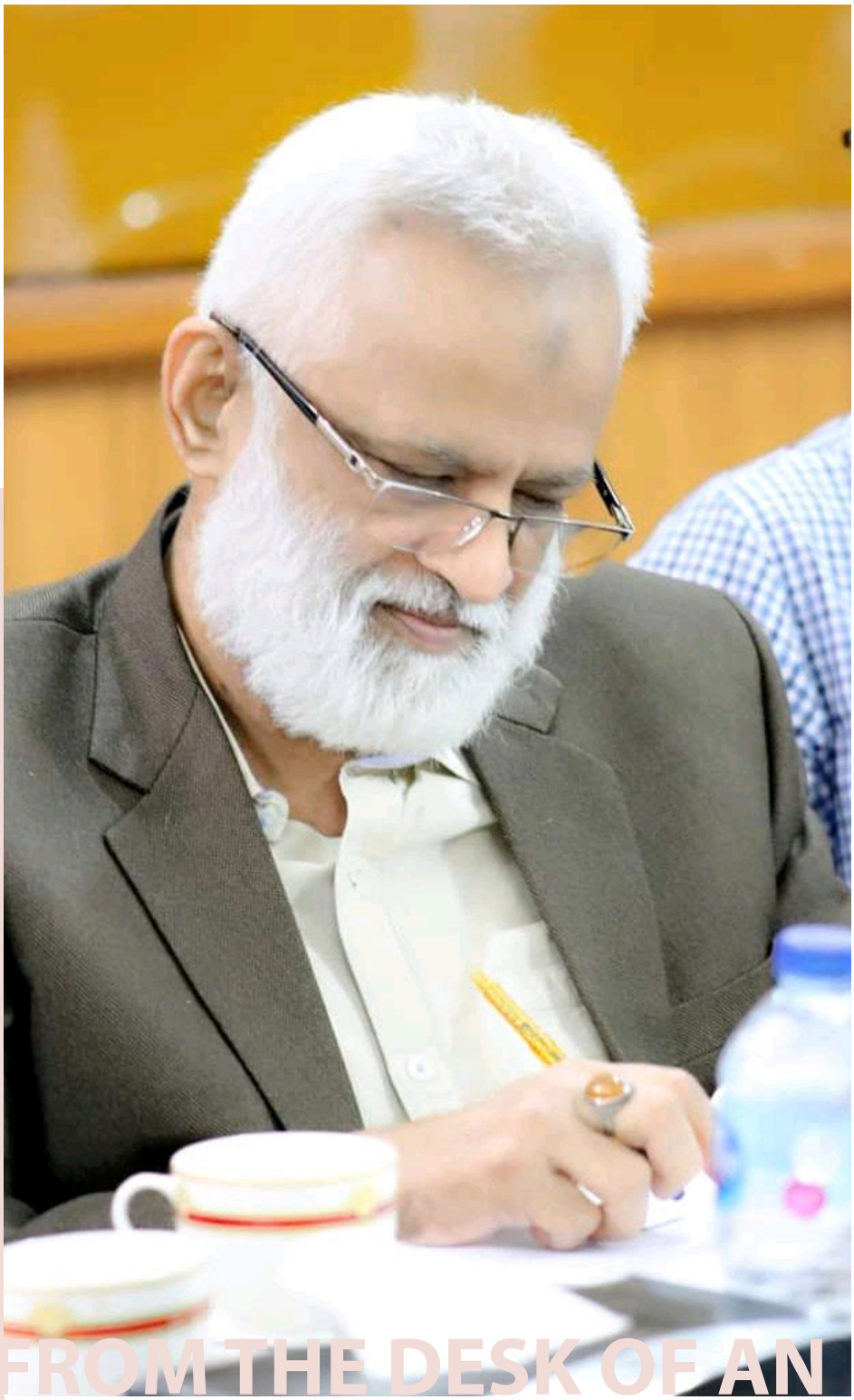
Do you think that people of Pakistan are well informed about cyber security and threats? If they are not well informed please advise?

The situation is improving. People of Pakistan have now started taking cyber threats seriously as online business has grown drastically due to covid situation. A mass awareness campaign should be organized by government to further cope with the situation.

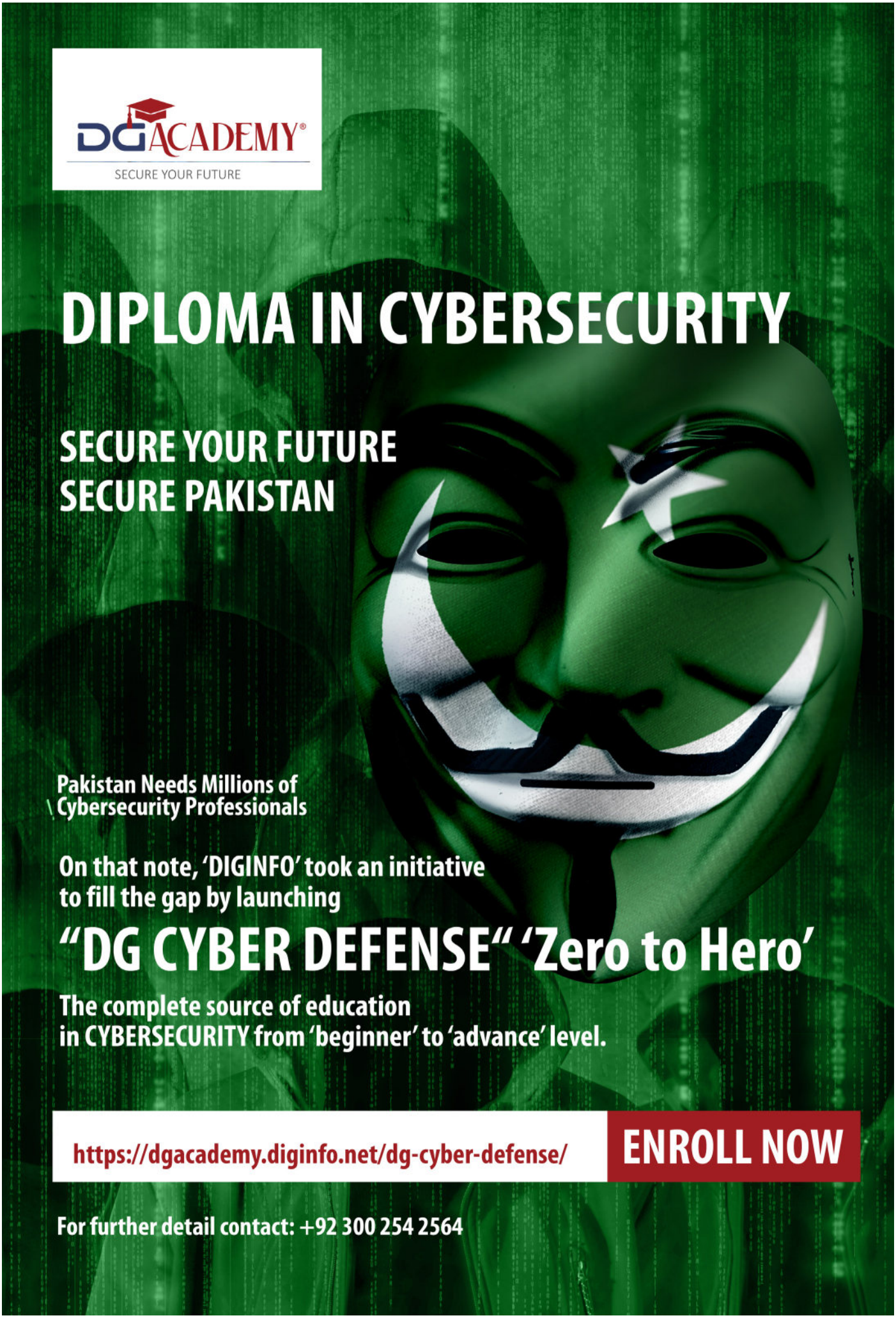
Please give some suggestions for our readers to what safe guard they adopt to avoid cyber mishappening?

Habits to stay cyber-safe.

- Keep your software updated.
- Keep your personal and private information lock down.
- Keep passwords complex.
- Backup your data regularly and encrypt it.
- Thinking twice before clicking on links or opening attachment if it is suspicious report it.
- Keep yourself on major security breaches.
- Install up-to-date end point protection.
- Verify requests for private information.
- Know what to do when you become victim.
- Be mindful of which website URLs you visit.
- Keep an eye on your bank statement.



FROM THE DESK OF AN EDUCATOR


DGACADEMY®
SECURE YOUR FUTURE
DIPLOMA IN CYBERSECURITY
SECURE YOUR FUTURE
SECURE PAKISTAN
Pakistan Needs Millions of
Cybersecurity Professionals
On that note, 'DIGINFO' took an initiative
to fill the gap by launching
"DG CYBER DEFENSE" 'Zero to Hero'
The complete source of education
in CYBERSECURITY from 'beginner' to 'advance' level.
https://dgacademy.diginfo.net/dg-cyber-defense/
ENROLL NOW
For further detail contact: +92 300 254 2564

Data of 500,000+ Students and Staff Exposed.

Ransomware Attack Behind The Scene.

The Chicago Public Schools revealed that data of more than 500,000 students and employees have been exposed as a result of a ransomware attack. The hackers targeted Battelle for Kids, a not-for-profit organization that handles student data.

A statement released by the school's administration says that the attackers gained access to full names, dates of birth, genders, school branches, classes, ID numbers and course information. However, home addresses, social security numbers, health and financial information remained safe from going into the hands of unauthorized persons.

Although the attack was launched on December 1 last year, the technology vendor Battelle for Kids did not notify Chicago Public Schools until April 26 this year. They issued a statement which reads like this: "In December 2021, Battelle for Kids was the victim of a cybersecurity ransomware attack. We immediately engaged a national cybersecurity firm to assess the scope of the incident and took steps to mitigate the potential impact." The students and employees who were affected by the breach have been informed of the incident and they will receive free identity theft protection together with credit monitoring from CPS.

The Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) have received the report of the crime. The investigation is ongoing but no headway has been made that could lead to the perpetrators of the crime. That's why experts speculate that ransom amount might have been paid by the technology vendor to avoid the attackers' next move that could be damaging. It has been noticed that when ransom is not paid, the criminals promptly publish the stolen data on public platforms.

Anyone can then gain access and misuse the data at will. Certainly, Battelle for Kids might have been endevoring to keep the data from reaching public eyes.

Although the scale of attack was huge, the act wasn't anything new. Cyber crime has entered into a new age where everything is getting darker and murkier. In the last month alone, a number of educational bodies were victimized. For instance, North Carolina A&T State University located in Greensboro suffered a ransomware attack which disrupted a number of facilities like the wireless connections, single sign-on websites, VPN, jabber, Qualtrics, Banner Document Management and Chrome River. The administration and the cybersecurity response team could not restore some of the services even to this day. A similar attack was launched on Florida International University. In both the cases the Black Cat group, aka ALPHV, stole personal information of students, teachers and other staff members. The group has also claimed to have gained access to contracts, financial information, SQL databases and email addresses.

A college of national importance with a history and traditions of more than 157 years was forced to close down after a malicious ransomware attack. The breach at Battelle for Kids followed soon afterwards. Security specialists believe that ransomware attacks are not just limited to educational sector. There has been nearly 70% rise in such attacks and a majority of them are aimed at small to medium sized organizations because they are not as well-protected as other larger outfits.

To limit the damage to a minimum, experts suggest a number of precautionary measures and careful handling of sensitive data. If organizations train all their employees and make them adhere to those small steps, then businesses and organizations would be safer.

GRC TOOLS

WHAT COMES FIRST?

Nowadays, because of increasing complexity in processes and operational procedures, organizations face countless challenges. And these challenges can come from any direction including regulation, technology, human resource management, processes and several others. That's the reason, organizations are in pressure to devise mechanisms for handling the wave of complexity. In recent years, all across the world, GRC Tools have become the mechanism of choice for addressing complexities of business environment.

GRC Basics The term GRC, an acronym for 'Governance, Risk and Compliance' first appeared in a research paper authored by the co-founder of OCEG (aka 'Open Compliance and Ethics Group). Although the paper was published in 2007, the term was referenced as early as 2003. The group defined the term as:

"A well-coordinated and integrated collection of all the capabilities necessary to support principled performance at every level of the organization. The capabilities include:

• Work done by internal audit, compliance, risk, legal, finance, IT, HR.

• The work done by the lines of business, the executive suite, and the board itself.

• The outsourced work done by other parties and carried out by external stakeholders."

The phrase 'principled performance' needs some explanation. It refers to an approach that helps businesses and organizations attain their goals while grappling with risks and uncertainty that prevails at the workplace.

Each of the terms also needs some elaboration:

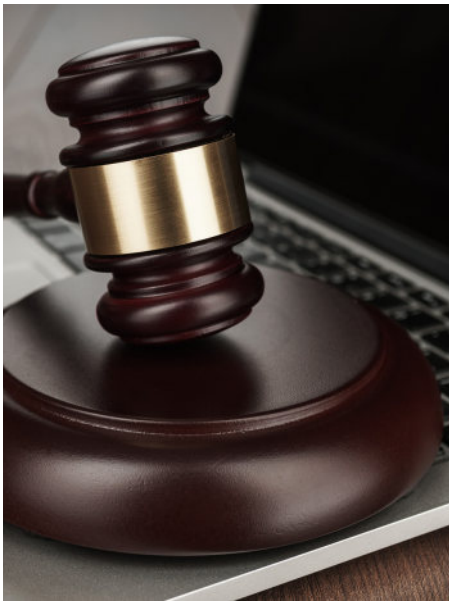
Governance:
Strategy and Policy, which help in determining the direction of the organization, are central to the Governance aspect of GRC. Then come, in order of importance, monitoring performance and controls and evaluation of outcomes.

Risk Management:
This activity consists of identifying and analyzing risks and then putting effective controls to ward off threats. Data breaches often create obstacles in the path

toward the goals of businesses and organization. Keeping vigilance against threats minimizes the risk of cyber attacks.

COMPLIANCE:

This aspect of GRC consists of ensuring standards defined by company policy are met and guidelines are followed. Compliance also makes sure that accounting and other related practices are also implemented.



Joanna Grama, director of cybersecurity and IT GRC programs for EDUCAUSE has summarized the function of GRC in a succinct way. She says, "Organizations develop a GRC framework for the leadership, organization and operation of the organization's IT areas to ensure that they support and enabe the organization's strategic objectives. The framework specifies clearly defined measurable that shine a light on the effectiveness of an organization's GRC efforts."

GRC DRIVING FORCES:

Businesses today have become increasingly conscious of GRC implementation. In spite of that awareness, the biggest challenge is to understand why and how to integrate cyber security and GRC tools into business operations.

SALES:

Of all the drivers for GRC, 'sales' head the list. In any organization, regardless of industry, checks and verifications are required for security frameworks and compliance with privacy standards in order to operate. Opportunities and obstacles both exist at the same time.Some of the obstacles from the compliance angle can be attributed to the following factors:

- Clients demand higher degree of security and assurance from organizations.
- Compliance with specific data protection or information security regulations/frameworks is required
- High risk of a potential breach and perceived lack of security process is implemented
- And some sales opportunities from compliance perspective:
- Tracking compliance to one or more industry-recognized frameworks. For technology companies, this could be ISO72001 or NIST800-53.
- Transparent and sharable audit reports that the sales team can leverage to demonstrate the organization's dedication to compliance and risk management.
- Centralized data repository or organizational controls that can be leveraged toward quickly answer security-related questions.

REGULATION:

Data, especially, personally identifiable data has the potential to generate business. At the same time, it holds great attraction for cyber criminals. To mitigate such risks associated with sensitive and personal information, governments are placing great emphasis on stringent laws and regulations. The unprecedented rise in cyber attacks together with growing awareness among individuals and civil rights organizations has shifted the focus on how companies manage information through the use of technology. As a consequence, processes, people and business operations have come into spotlight.

GRC BENEFITS:

GRC is thought of as a structured approach to achieve business goals by way of IT technology. In doing so, companies often meet compliance requirements while effectively managing risks and threats.
A clearly defined GRC strategy has a number of merits including better decision making, efficient investment decisions, elimination of silos and reduced fragmentation among various departments of the company.

GRC APPROACH:

The best way to implement GRC regulations is to adopt a holistic approach encompassing the entire organization. The OCEG ('Open Compliance and Ethics Group') has suggested an open source approach called the GRC Capability Model that combines various disciplines of governance, risk management and compliance with those of audit, ethics and IT into a unified approach. The model has four key components as proposed by the OCEG:

LEARN about the organization context, culture and key stakeholders to inform objectives, strategy and actions.

ALIGN strategy with objectives, and actions with strategy, by using effective decision-making that addresses values, opportunities, threats and requirements.

PERFORM actions that promote and reward things that are desirable, prevent and remediate things that are undesirable, and detect when something happens as soon a possible.

REVIEW the design and operating effectiveness of the strategy and actions, as well as the ongoing appropriateness of objectives to improve the performance of organization.

CONTENTIOUS DEBATE:

The logical order of GRC functions has remained a topic of hot discussion ever since the term was first coined some two decades ago. Researchers have been enquiring about what comes first. Governance, Risk Management or Compliance? The order of the GRC processes has to be understood to 'avoid silos' and 'improperly scoped' security mechanism. While establishing the GRC practices, a large number of researchers agree that 'compliance' takes the lead and influences 'governance' which then influences 'risk management.' With the agreement of experts and researchers, the contentious issue—which was more like a chicken vs egg debate—is resolved to a large extent.

Compliance: The function of compliance identifies and adheres to statutory, regulatory and contractual obligations together with internal business requirements such as directives that come from board of directors or any other decisions that are deemed necessary for the organization. To gain a comprehensive understanding of compliance needs, the workers need to work closely with the legal department, physical security teams, contracts management staff, and other key players. This involves interaction with various lines of business which offers an understanding of how the entire organization operates. Geographical considerations are also taken into account in this exercise.

With the knowledge that compliance is the key source of GRC function, we learn that 'Compliance' informs 'Governance' about the controls applicable to laws, regulations and frameworks. In response to the provided information, 'Governance' can enunciate policies and standards that are essential to meeting the defined goals.

In essence, 'Compliance' defines a set of controls that are essential to meeting the needs of a particular organization. The set of controls is often regarded as an organization's Minimum Security Requirement (MSR). MSR can be used by Governance team to enunciate appropriate policies and standards. Likewise, the Risk Management Team can also take guidance from the set of controls provided by 'Compliance' to determine the risk factors and take proper security measures by assigning weightage to different controls in order of importance and priority. It is a sort of hierarchy.

This assignment of weights to cybersecurity and data protection controls is indispensable for risk assessments and for determining an organization's risk tolerance threshold. This threshold helps the leaders and workers in analyzing the levels of risks that the organization can bear. In other words, the threshold help them define the risks that are acceptable and those that are not.

Governance: Once the controls are identified by the 'Compliance' function of GRC, the 'Governance' part gets into action to perform certain key tasks: a. Development of policies and standards to meet the compliance objectives. B.

Assigning ownership of controls to the concerned stakeholders. This function requires a RASCI (Responsibility, Accountability, Supportive, Consulted and Informed) Chart for effective implementation of the GRC model.

It is important to note that policies and standards are documented with details and clarity. This makes the task of implementation simpler and attaining of company objectives even easier. The cybersecurity and data protection documentation consists of 5 key components:

1. **Policies**
2. **Control Objectives**
3. **Standards**
4. **Procedures**
5. **Guidelines**

Risk Management: The last function of the GRC process is by no means the least although it follows both 'Compliance' and 'Governance' functions. Risk management is critical for maintaining situational awareness. It is also equally important for continuing to remain secure and compliant. It serves as the prime source to identify events of non-compliance that eventually lead to mismanagement of risks.

DOCUMENTATION IS KEY:

Most of the experts and cybersecurity specialists agree that documentation is indispensable to GRC. If documentation is not there or it isn't adequately managed, the GRC function collapses.

The GRC function demands regular and ongoing assessment of Governance, Risk Management and Compliance activities. Some experts compare it to a three-legged stool which will exhibit imbalance if one leg does not conform in size to the other two.

To sum up the debate, all three elements of the GRC function are necessary and complementary to one another. There may be a hierarchy to the logical order but all three coexist and are supportive.

The leadership holds the key to implement the function in the best possible manner to make sure the organization attains its objectives.

DIGINFO®

TRUSTED LEADER IN CYBER SECURITY

IS YOUR PASSWORD SECURE?

1. Make sure you are using a complex password
2. Regularly change your password
3. Use trusted professional Password Manager
4. Never use same password on other platforms
5. Never write your password anywhere
6. Never speak your password loudly
7. Never include personal information in your password

Contact us at +92-21-34325505,
Email : info@diginfo.net | www.diginfo.net

SCAN ME

Researchers Discover Backdoor WordPress Plugin

A Large Number Of Schools Uses It To Manage Websites

Researchers at website security service, Jetpack, have discovered a malicious backdoor lurking in WordPress plugin that a large number of schools use to operate and manage their websites. According to the investigators, the premier version of School Management Pro has had the flaw since at least version 8.9. They do not rule out the possibility of its existence in earlier versions. The backdoor plugin issue was assigned an identity CVE-2022-1609 and in terms of severity it was indexed at 10 out of 10.

Researchers at Jetpack said that they stumped upon the backdoor when support team members reported heavily obfuscated code on school sites that use the WordPress plugin marketed to schools for operating and managing websites.

After meticulous examination and deobfuscation of the plugin, the researchers learnt that the backdoor was deliberately placed in the license-checking part of the plugin giving outsiders the ability to gain control of the website.

The Jetpack post had this comment to offer, "The code itself isn't all that interesting: it's an obvious backdoor injected into the licesnse-checking code of the plugin. It allows any attacker to execute arbitrary PHP code on the site with the plugin installed."

The plugin is developed and marketed by an Indian software company, WebLizar. They market free and affordable themes and plugins for businesses around the world. Their free themes have been downloaded more than a million times. Meanwhile, their premium and free WordPress themes, besides the add-on plugins, have attracted more than 430k customers. Strangely, only the premium versions of the plugin were infected with the backdoor issue, whereas the free versions which were easily downloadable remained scot free.

After the revelation, the presence of backdoor has become public knowledge. It is obvious that attackers would be keen to locate a loophole for infiltrating the school websites and implant malicious code. That will open a doorway to ransomware accompanied by prospects of lucrative profits. Although the backdoor has been removed and updated versions have been issued, the vendor contended that "they do not know when or how the code came into their software."

In order to avoid being exploited by over-enthusiastic hackers, the best strategy for the schools that employ the use of plugin is to immediately shift to later versions. The researchers have recommended the plugin-users to update to the latest version (9.9.7).

Boundryless Cyber Laws

Tracking And Cracking Intruders

The internet has become an indispensable aspect of everyone's life. No task of daily life has been left out that doesn't rely on digital technology. The new technology has taken the world by storm. From businesses to not-for-profit companies and government entities, every organization seeks to have a web presence and relies heavily on it for communications. Businesses have shifted a large part of their sales and promotional activities online. This has resulted in an unprecedented rise in e-commerce. Governments, too, have also found it convenient to collect revenue through online facilities, further raising e-finance.

With the growth in online activities, there is an inevitable rise in cyber crimes. They have become a growing concern for countries all over the world. And their nature is as varied and as versatile as one can imagine. Both buyers and sellers are affected when hackers target an online sales business. And when the criminals turn toward organizations for ransomware, all hell lets loose. Besides these, there are countless other offences that are routinely added to a list of transgressions that can result in jail sentences or fine or both.

PUTTING HEADS TOGETHER:

Almost 25 years earlier, America Online Inc, in collaboration with US Secret Service and NY State Attorney General Dennis Vacco, sponsored a seminar on law enforcement in cyber space. This marked the beginning of an effort to bring cyber crime under rule of law. Back then, the participants pledged that all crimes that are being committed will be investigated and prosecuted. The day-long seminar comprising presentations and workshops focused on a variety of issues including consumer frauds, scams, computer trespassing, Trojans, harassment and pedophilia. A number of law enforcement departments and crime investigation cells participated in this gathering to form a united front against cyber crime. Soon after this meeting, legislation began to take shape and cyber space was brought under some control and regulation.

Since then, about 156 countries (80%) have enacted cybercrime legislation. Region-wise Europe takes the lead with highest adoption rate of 91%. The lowest rate was recorded in Africa at 72%. The cybercrime landscape is continuously evolving and creating wide gaps in skills. This poses a great challenge for law enforcement people to catch the perpetrators

and prosecute them. And when the criminals are beyond the borders, then the task becomes even more arduous.

GREATEST THREAT:

Back in 2012, FBI Director, Robert Mueller, testified at a hearing of Senate Select Committee on Intelligence that threats from cyber espionage and cyber attacks will overtake terrorism as the foremost threat facing the country. He reiterated, "Stopping terrorists is the number one priority but down the road, the cyber threat will be the number one threat to the country. I do not think today it is necessarily [the] number one threat, but it will be tomorrow."

The hackers did not wait long to vindicate the claim of FBI Director. Only a couple of days later, they relaeased a recording of a call between two agents of FBI and Scotland Yard investigating the Anonymous hackers group and LulzSec collectives. Analysts believed that this event pointed to the fact that at least one person's email at FBI was compromised.

PROBLEMS OF LAW ENFORCEMENT:

The trouble with cybercrime is that it knows no boundaries. The place is riddled with countless criminal activities and its expanse is vast—transcending all borders and posing acute problems for law enforcement. A criminal can inflict damage on a victim residing in the opposite corner of the world. The criminal can even choose multiple targets to inflict damage. That is not the end of this story.

The most troubling dimension is the law differs from place to place. Different culture, different sensibilities that can be poles apart, and contrasting behaviors in perceiving things all contribute toward complicating this affair. It is an uphill task to make universal laws that are acceptable to all countries. Even when laws, that have universal appeal, are made differences arise from time to time. In such cases prosecution and judgements drag on and on that it seems like eternity. In spite of efforts worldwide to bring some control to cybercrimes and legislate to make the space safer, the fact is the criminal is at an advantage. He can target and choose his victim at will. The victims can be individuals, business empires or government organizations even, stationed anywhere on earth. But his counterpart, the law enforcement, can rarely act beyond

the defined borders. That's why cybercrime has been increasing at an exponential rate.

ECONOMIC DANGERS:

With the proliferation of boundary-less cyberspace, risks and threats have leaped to an all time high. Attacks have grown in number and the methods of attack and the types of malware have also diversified. Attacks can range from phishing and doxing to distributed denial of service. Ransomware, that can make use of any type malware to achieve the goal of extracting maximum amount from victims, is the most dreaded of all attacks. The most infamous WannaCry ransomware attack in 2017 damaged more than a million computers worldwide. The damages ran up to $4b. Some hackers and hacker groups have elevated their technology skills to sophisticated levels. They are now offering their skills for hire in exchange of a certain percentage from the exploits.

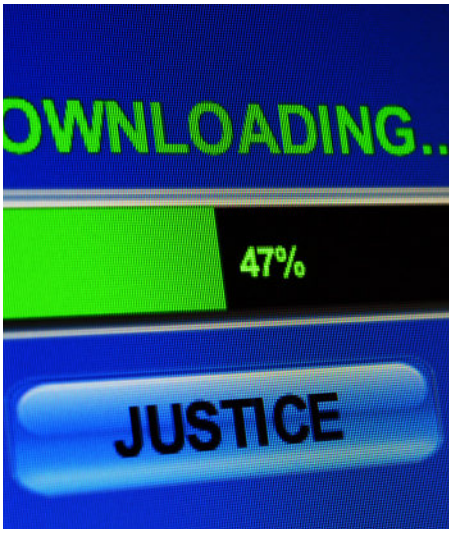
In the absence of effective laws to combat crimes of this nature, some large global businesses were forced to form an alliance to share threat information. The Retail Industry Leaders Association, RILA, includes members like Target, Nike, JC Penney and Walgreen and they have already started sharing information. The alliance's vice president for cybersecurity and data privacy recently said, "Collaboration between industry and government to share threat information is crucial in the fight against sophisticated and persistent cyber criminals."

SOME HEADWAY:

The world has come alive to the dangers of cyber crimes. Having a loose grip now means they will grow into uncontrollable monsters. Some societies are attempting to legislate and hit hard on transgressions—even those that were cast aside as minor deviations of behavior are now being considered as culpable. Strict penalties, including prison sentences, fines and other retributive measures, have been suggested for such behavioral abnormalities. For instance, in UK, cyber flashing has been banned. The perpetrators will face upto two years in jail for sending unsolicited images. This is part of the online safety bill, a landmark piece of legislation that aims to put a check on racist and sexist abuse, and a variety of harmful content. Prior to cyber flashing, upskirting was also included in the bill as a criminal offence. More recently, posting

threatening social media messages and hoax bomb threats have also been criminalized.

Under the revised law, tech firms will be duty-bound to protect users from damaging content. Earlier, tech firms used to take down content that was flagged to them as damaging but now they will be legally bound to prevent users from exposure to stuff like fraud, revenge porn and sale of hard drugs. Failure to comply would automatically result in heavy fines from authorities who will closely watch their performance. It was observed during surveys that Facebook and Twitter topped the list as hosts to such damaging posts.



BREAKING THE BARRIERS:

Legislation is one thing, prosecuting the criminals and bringing them to justice is quite another. Although stories of doom and gloom abound on the internet and its related technology, occasionally we get to hear some encouraging news. Such news fills our hearts with hope that the place will no longer be able to elude law enforcement. Some years back, the Australian police collaborated with Interpol and German police to arrest a gang of thirteen criminals exploited children. Of all the crimes that exist on the face of earth, the one that targets innocent and vulnerable children is the most heinous. As the criminals, taking advantage of openness and permissiveness, have shifted their activities online, the task to contain them has become a cross-border phenomenon.

There are other cases that fill with promise. In an extensive operation, codenamed 'Project Spade,' the investigation covered 94 states and a tightly knit network of criminals was dismantled resulting in the arrest of at least 348 hardened criminals. In another effort, the largest known network was broken into with the concerted efforts of Dutch and Australian police. The FBI was also on board in the large scale investigation of the group involving 45000 members. More than 300 people were arrested.

SOLUTIONS:

The internet has become an overwhelming necessity in everyday lives. All activities, including businesses and household activities, are now dependent on the new technology. This has dramatically altered the very nature of law enforcement agencies whose work was traditionally confined to borders. With cyber crimes on the rise, law enforcement people will have to involve themselves in cross-border activities. The only thing that serves as a barrier is sovereignty of states which does not permit external forces to launch operations freely on their territory. This is where coordination and understanding play their role. And that seems to be the only path that leads to a civilized society.

Russian Botnet for Disinformation Campaigns

Fronton Is Designed To Run On Social Media

A Russian IoT botnet, Fronton, has earned considerable infamy by its ability to launch disinformation campaigns on social media.

Botnet is short for robot network, and the term refers to an IoT network of interconnected computers which are infected with malware. Usually, one attacker or a team of attackers control the network and launch Distributed Denial of Service attacks.

Botnets usually target IoT devices to initiate their campaign because such devices have become ubiquitous and they are poorly protected. What's more they are always in the 'ON' mode which offers attackers the opportunity to gain access 24/7. That's why IoT devices have served as launchpads for some of the most devastating DDoS attacks.

Back in 2020, BBC Russia and ZDNet were the first to break the news about Fronton, the IoT botnet. Their source of information was the documents published by a Russian hacktivist group, Digital Revolution. The group had earlier claimed that they had hacked a subcontractor of Federal Security Service of the Russian Federation. Further investigation led the researchers to a Moscow based company, Zeroday Technologies. Working behind the scene was a hacker Pavel Sitnikov, who was arrested in March 2021. Charges were framed against him that he had distributed malicious software through his Telegram channel.

One security firm based in Virginia, USA, tried to learn more and found that Fronton also contains a web-based dashboard called SANA. Nisos, the security firm investigating about Fronton's operational features further explained:

"SANA creates social media persona accounts, including provisioning of an email and phone number. In addition, the system provides facilities for creating these newsbreaks on a schedule or a reactive basis."

This ability to create fake social media accounts from around the world, mimicking real life scenario, and use them in a coordinated manner is something difficult for any social media platform to detect.

When Fronton first came to light in 2020, it was assumed that the botnet was a fairly ordinary malware capable of launching DDoS attacks. But later investigations and in-depth analysis led researchers to realign their initial assumptions. Now, they believe that Fronton packs a lot of firepower behind its benign-looking facade.

Fronton is now known to have drummed up disinformation campaigns to create discension about immigration and covid19 issues. Reports also abound that support the perception that Fronton can even influence elections and democratic processes by moulding opinions in its favour.

Its role was highlighted in the events following Russia-Ukraine war. The neighbouring countries like Sweden and Finland now fear that Russia might try to invade their land just as it has done in Ukraine. Sensing that danger, both the countries of aligned themselves with NATO forces although historically, they have remained politically neutral for as long as one can remember.

Cyber security experts have now come to the conclusion that it is important to be ever vigilant when it comes to botnets like Fronton which can instigate upheavals in an otherwise peaceful and calm society.

Stealing Money From PayPal Users

New Bug That Allows Attackers To Steal Identified.

People around the world extensively use PayPal for money transfers. The heavy online traffic with billions of dollars constantly on the move is a great temptation for scammers. Every day new tricks are devised to fleece people of their hard earned cash.

According to new findings by a security researcher, there is an 'unpatched vulnerability in PayPal's money transfer service' which allows attackers to introduce malware. The malicious code then tricks users into clicking a link provided by the attacker. Once the user unwittingly clicks the link the attacker-generated transaction takes place and the user is deprived of his money.

This technique is referred to as Clickjacking or UI Redressing. It operates on the theme of coaxing a user to click a seemingly benign button or link resulting in downloading a malware. The rest of the actions like redirecting to malicious websites or disclosure of critical information is performed by the malware. The malware achieves this by projecting an invisible page or HTML element on top of the visible page. The user is led to believe that he is clicking the real page when, in fact, he is operating on the invisible rogue element sitting on top of the visible but inactive page.

This means that the attacker reroutes the clicks to a page of his choice where actions of their liking could be generated. The user unknowingly lands on a page that is owned and operated by another domain or application. These findings were reported by security researcher who identifies himself as h4x0r_dz. The researcher discovered

a problem while he was studying "www.paypal.com/agreements/approve" endpoint. He has reported the discovery to the security team at PayPal.

The researcher said, "This endpoint is designed for Billing Agreements and it should accept only billing agreement token. But during my deep testing, I found that we can pass another token type, and this leads to stealing money from a victim's PayPal account."

This implies that the attacker could embed the endpoint inside an iframe that sits invisibly on top of a legitimate page. All operations are done on this page while the real page is rendered idle and inactive. This forces the user to transfer funds to an attacker-controlled PayPal account by a simple click or a button.

Still alarming is the fact that the flaw could have had far more devastating consequences in websites that merge with PayPal for checkouts. This could enable threat actors to transfer huge amounts from PayPal accounts of users into accounts they use for such operations.

The researcher, h4x0r_dz, has issued a stark reminder, "There are online services that let you add balance using PayPal to your account. I can use the same exploit and force the user to add money to my account, or I can exploit this bug and let the victim create/pay Netflix account for me!"

DIGINFO®

TRUSTED LEADER IN CYBER SECURITY

HOW TO PROTECT YOURSELF FROM PHISHING ATTACK?

1. Never open email attachment from un-known sources
2. Never click on hyperlinks in email body from un-known sources
3. Always scan email attachment through latest and professional AV if email sender is well-known
4. Always check actual text of hyperlinks before clicking if email sources are well-known
5. If sender is well known make sure he actually sent this email by calling him

Contact us at +92-21-34325505,
Email : info@diginfo.net | www.diginfo.net

SCAN ME

Highlight of Pwn2Own Contest

Windows 11 Hacked Three More Times.

The Pwn2Own Contest marked its 15th annual event by returning to Vancouver where it had first started in 2007. The event started off as a small, browser focused activity and grew into one of the most well-known security competitions in the industry. In the early years, a successful exploit earned a McBook and $10,000. Last year, ZDI gave away millions of dollars in prizes alone.

In the 15th event more than $1.5 million were distributed for high impact security bugs conceived by high end programmers and ethical hackers. The event was managed by Trend Micro's Zero Day Initiative (ZDI) attracting hackers from across the world who competed ferociously to find bugs in products from a wide range of vendors including Microsoft, Mozilla and Apple's Safari.

Paricipants contested to win money or points. A team from StarLabs of Singapore, who took part virtually, was declared the champions with a total of 27 points for the vulnerabilities they discovered during the event.

A good number of well-known companies like Tesla, VMWare, Zoom, Microsoft and Teams, sponsored the event. They provided targets for the competitors. David Berard and Vincent Dehors from Synactiv discovered two unique bugs on the Tesla Model 3 Infotainment System.

Dustin Childs, senior communications manager at Trend Micro's ZDI, said, "The Synactive team was able to remotely take over the infotainment system, and they showed how they could stand outside the car and turn on the wipers, open the trunk, and flash the lights. The attempt that failed still demonstrated some interesting research, and we were pleased to acquire through a standard program submission."

On the third and final day of Pwn2Own Vancouver hacking contest, security experts hacked Microsoft's Windows 11 operating system using zero day exploits. Team Double Dragon could not demonstrate their exploit within the allotted time and failed in their attempt to hack the operating system. The other contestants, however, succeeded in the target and earned $160,000 after infiltrating Windows 11 three times and Ubuntu Desktop once.

On the third day of Pwn2Own contest, nghiadt12 from Viettel Cyber Security demonstrated a Windows11 escalation of privilege zero-day. Likewise, Bruno Pujos from Reverse Tactics and vinhthp1712 also demonstrated Windows11 escalation using Use-After-Free and Improper Access Control vulnerabilities. Finally, Billy Jheng Bing-Jhong hacked a system running on Ubuntu Desktop by employing Use-After-Free exploit.

The event ended on May 20, 2022 as 17 competitors claimed prizes and cash worth $1,155,000 for zero-day exploits chains demonstrated over three days from May 18.

During the event, the participants demonstrated six Windows 11 exploits, hacked Ubuntu Desktop four times and demonstrated Microsoft Teams zero-days. They have also informed the security specialists present at the Vancouver meet that several flaws exist in Apple Safari, OracleVirtualbox, and Mozilla Firefox.

Once vulnerabilities are exploited and brought into the knowledge of all concerned, vendors have 90 days to release the upgraded versions. After that period, Trend Micro's Zero Day Initiative publicly informs of the existence of vulnerabilities in the apps.

The Pwn2Own demonstrates about how talent from all across the world can coordinate to get even with the hackers, who seem to be in control and strike at their targets whenever they like and wherever they like.

DIGINFO®

TRUSTED LEADER IN CYBER SECURITY

PROTECT YOUR DEVICE FROM UNTRUSTED MEDIA

1. Never connect unknown media to your device
2. Never connect unknown charging or data transfer cable to your device
3. Set to always 'ask permission before connect' or 'peer to your device'
4. Always scan unknown media through latest and professional AV if you must connect it

Contact us at +92-21-34325505,
Email : info@diginfo.net | www.diginfo.net

SCAN ME

Massive DDoS Attacks on Sberbank of Russia

A Spate Of Attacks Cause Disruptions Of Service And Loss Of Business.

Sberbank is Russia's largest banking and financial services company. It ranks third in Europe with assets in excess of $570 billion. Lately, it has been battling the largest distributed denial of service (DDoS) attack in its history.

Cyber attacks are nothing new to Sberbank. Earlier in 2016, five Russian financial institutions were targeted intermittently for a couple of days. The country's bank regulator said that Sberbank was one of the targeted banks. The attackers launched a wave of attacks on the banks' websites , flooding them with malicious data known as Distributed Denial of Service (DDoS) attack. According to security firm Kaspersky, this was, until that time, the largest attack aimed at Russian banks. The security firm added that the floods of data normally lasted for 60 minutes but in one particular case, the flood continued for a full 12 hour period. Sberbank admitted that it suffered 68 similar attacks in the year 2016 but the one in November was the most intense. Webcams and other smart devices based in USA, India, Taiwan and Israel were all used in the attack.

Sberbank estimates that Russians have suffered close to 3.6 trillion roubles in losses to cyber attacks. The figure is so colossal, it seems like a parallel economy. The deputy chairman of the bank has said that private businesses and ordinary citizens are the greatest sufferers. The state security services are better protected.

Fast forward to May 2022, the conflict in Ukraine has added to the woes of Russian banks. In an address to a select gathering at a conference, Sergei Lebed, vice president and director cyber-security has said that thousands of hackers from several countries are attacking the banks almost incessantly around the clock. The security teams at Sberbank remain vigilant all the time—24/7.

Lebed informed the audience that the cyber criminals employed various methods to carry out the attacks. This included code injections, malicious browser exensions and Docker containers equipped with DDoS tools. DDoS attacks deprive customers of online services which ultimately leads to intermittent disruptions and loss of business to the company.

Sberbank's Security Operations Center has fought off and repelled the biggest attack in its history early this May. The DDoS attack was measured at 450+ gbps and over 27000 devices located Taiwan, USA, Japan and UK were used to generate the traffic.

Despite the success, Lebed has admitted that the attacks will likely continue because of the polarized political climate. Down the road, perhaps, the attacks may go down in number but they will grow in intensity and power.

This admission is vindicated by a recent Radware DDoS attack on a US service provider which lasted for 36 hours at 1.1 Tbps. This is a clear indicator that the hackers and groups of criminals are enhancing their levels of sophistication and getting smarter with each passing day.

DIGINFO®

TRUSTED LEADER IN CYBER SECURITY

HOW TO STAY SAFE ON PUBLIC WIFI?

1. Always use password protected Public WiFi
2. Never send sensitive information over Public WiFi
3. Never use credit card over Public WiFi
4. Always Pay attention to warnings
5. Never visit websites over Public WiFi where no SSL certificate exist
6. Turn off sharing while using Public WiFi
7. Always use VPN to access your sensitive systems wile using Public WiFi

Contact us at +92-21-34325505,
Email : info@diginfo.net | www.diginfo.net

SCAN ME

DG Cyber KIDS.

Empower every child with Cybersecurity Know-how

The new scenario, resulting from the pandemic involving work from home and study online has only exacerbated the already increasing incidences of cyber threats. DG Cyber Kids, a product of DIGINFO, provides resources for parents and teachers to educate children as they grow up in a world teeming with technological advancement. The initiative equips children with a sense of cyber safety and ethics. In the process, kids learn more about current terms that have become common like internet safety, bully response, technology balance, digital reputation and privacy.

We are relentless in our mission to improve security—not just for our customers, but for the entire community. We forgo the way information security has been done in the name of better outcomes for all. DG ACADEMY uses practical ways of educating the basics of cybersecurity to children.

DG ACADEMY®

PROTECT YOUR FUTURE


CYBER
MAGAZINE
DG MAGAZINE
The Ultimate Source of Cyber World
dgmagazine.diginfo.net
because...
CYBER
SECURITY
MATTERS
A Product of DIGINFO