A Product of DIGINFO®

CYBER MAGAZINE

Volume 6 I 2023

DG MAGAZINE

The Ultimate Source of Cyber World

TOP 5 HIGHLY PAID JOBS IN CYBERSECURITY

FRESH EXPLOITS OF BPFDOOR MALWARE
MALICIOUS CODE USING SOLARIS AND LINUX VULNERABILITIES

TOP 5 HIGHLY PAID JOBS IN CYBERSECURITY
A REPORT BASED ON RECENT SURVEYS

NEW RANSOMWARE EMERGES
VMWARE ESXi SERVERS UNDER ATTACK

CHINESE HACKERS INFILTRATE TELECOM GIANTS
AGE-OLD SOFTWARE FLAWS AT THE ROOT OF THE PROBLEM

dgmagazine.diginfo.net

CONTENTS

FROM THE EDITOR

Muhammad Saeed
Chief Editor

Publishing a magazine regularly taking, care to produce it in consistently high quality, is truly a thankless job. The team at DG Magazine has demonstrated time and again that the task they have taken upon themselves to accomplish will not remain elusive. The sixth volume which you are seeing right now is a statement of the passion at work.

In this edition you will read a handful of research based articles and plenty of news reports gathered from all corners of the world. The material, as always, is informative, enlightening and entertaining—appealing to a diverse set of people.

The articles featured here include one on GRC Tools and another shedding light on the current job market in the cybersecurity profession. And you will be able to read several others which will widen your perspective. On an equal scale, a number of news reports will tell you what is happening in this area of information technology. Particularly interesting is the report about the Cryptoqueen and her exploits. You will be surprised to learn how a young woman amassed so much wealth by persuading people to part with their money to satisfy their urge to have unrealistic profits.

The journal you have come to like so much is going to get better and indispensable for the professionals and enthusiasts alike. The motivation for our team to consistently produce quality stuff is the knowledge that the best gift one can give to loved ones is reading material that merits a place in libraries. Keep reading.

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.

EDITORIAL BOARD

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.

EDITORIAL BOARD

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.

TOP 5 HIGHLY PAID JOBS IN CYBERSECURITY

A REPORT BASED ON RECENT SURVEYS

As the number of cyber attacks increases with epidemic proportions, businesses and organizations are compelled to invest and allocate a sizable budget on human resources. Statistics indicate that the demand for cyber security professionals is registering an upward trajectory to keep pace with the alarming rate of breaches around the globe.

Ironically, hackers live on both sides of the divide. They are hunted not only by the law enforcement people but also by employers. In the latter case, they are generally known as 'Pen Testers' or 'Ethical Hackers'.

With unprecedented increase in breaches, hacking and cyber crimes of all sizes and intensity, businesses are forced to seek help from cyber security experts to protect them from attacks. As online business is expected to grow to a whopping figure of $248 billion by 2023, it is too tempting for cyber criminals to resist. To counter their attacks cyber security experts, or ethical hackers as they are sometimes called, have growing opportunities to market their skills in combating the crimes.

Those who are fresh out of school and those who have adequate experience may brace up for a new and exciting career that can infuse life in a dull routine of existence. Cybersecurity career is full of excitement and round the clock action. Professionals associated with this trade work on the battle front combating cyber threats in advance and building walls of defense for businesses to ward off incidents that can damage their reputation resulting in heavy losses.

A career related to cyber security is full of promise and is a sure path to successful and care free future. With growth in online business and simultaneous increase in criminal activity, the number of cyber security jobs too is increasing exponentially. Unfortunately, however, the number of positions to fill outnumbers the available professionals by a wide margin. According to some estimates, more than 3.5 million cyber security jobs will be on offer in the coming year but not enough skilled people will be around to fill those vacancies.

It has been reported that there will be a growth of 31% between 2020 and 2030 in CS industry. Compared to the growth of other industries, this is a far quicker rate. The cyber security job postings have grown by 95% in the past seven years. With this ever-increasing scope,

the industry offers great potential both to low-level CS jobs as well as seasoned and experienced professionals. It's a pathway to rewarding careers.

The post corona virus situation also is important for cybersecurity. The pandemic has provided a sound base for hackers and cyber criminals. A sizeable percentage of cyber attacks, almost 80%, revolved around Covid-19 and corona virus themes that included phishing, spam and malware.

The attacks launched by the criminals have assumed epidemic proportions. Ironically, this situation has only highlighted the importance of cybersecurity professionals, creating opportunities and prospects of bright futures.

SKILLS SET FOR CYBERSECURITY

People who possess a technical background, problem solving and communication skills have great opportunities to make their mark in the CS industry. A fair knowledge and understanding of the environment where hackers and cyber criminals operate is also required. To successfully thwart hackers' attempts, it is important to understand how cyber attacks take place and the methods and tools used by hackers.

Even without a technical background you can build a career in the industry with entry-level jobs. You can build technical skills as you progress. Soft skills are very important. Companies prefer individuals with specific skills over individuals with university degree. The best approach is to chart a career path leading to a position of strength and self-actualization. The next logical step is to add relevant skills to one's portfolio which will ultimately enable the candidate reach the goal.

CAREER PATHS

In cybersecurity industry, there are openings for "hacker" jobs as well. In this particular position they are known as Pen Testers. They are essentially "ethical hackers" whose job is to penetrate an organization's systems and detect vulnerabilities so that they can predict and prevent future threats. Businesses rely on Pen Testers to assess their systems. Their presence at the frontline means, they can feel the pulse and predict future cyber attacks. With that knowledge, they can prevent serious loss to the organization a breach can inflict.

Although this seems to be a very exciting and 'full of action' occupation but there are many more to vie for. In the broadest terms, there are two categories that cybersecurity jobs can be classified into: Analysts and Engineers. Each of these has its charms and attractions and each demands a specific skill set and fighting spirit, because the industry of cybersecurity is more like warfare. It is the spirit that matters most.

MONEY MATTERS

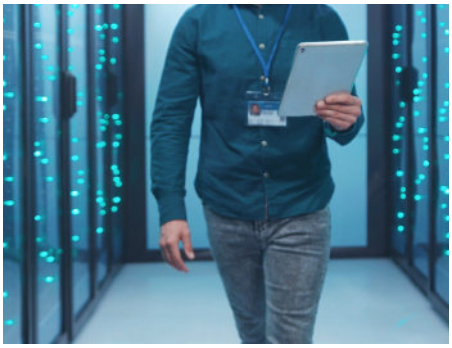
Freelance Bug Bounty Hunters
Brief Description:
Zero-day exploits have become an everyday phenomenon. From one per week in 2015, they have now risen to one a day. Age old flaws that create vulnerabilities are responsible for this situation. And hackers have capitalized on the weakness to create a burgeoning market for the bug bounty hunters.

Salary: US$ 130,000 per year to more than US$ 500,000 per year. Although the latter figures are rare, some freelancers do demand and get as much or even more.

Chief Information Security Officer
Brief Description:
The CISO's job is a senior level, executive position responsible for bridging the gap between security initiative with enterprise programs and business goals. The CISO is responsible for ensuring that information assets of the organization are safe and secure. The person in this position will see that a proper and effective response strategy is in place in case any incident occurs threatening the data of the business. A CISO is also charged with the additional responsibility of communicating and maintaining relationships with risk-related stakeholders.

Salary:
The salary packages, perks and additional benefits vary widely and depend on the size and type of business. Fortune 500 companies with offices located in big cities around the world may pay as much as US$ 380,000 per year to more than US$ 420,000 per year. This is on high end of the salary bracket, but on average, a CISO expects a package between US$ 150,000 per year US$ 200,000 per year.

Assistant to CISO
Brief Description:
A lot has been written and published about CISO but little is known about the newly created position of Assistant to CISO. In view of the volatile and fragile nature of cybersecurity job market, where number of positions outnumber the available cybersecurity professionals by a wide margin. This position is specifically designed for a person who will eventually assume the role of CISO. The responsibilities are nearly the same as those of the CISO but the deputy only acts according



to the plan and strategy determined by the CISO.

Salary:
At this stage, it is difficult to say how much the assistant to CISO may earn. Large companies are willing to offer compensations in the range of US$200,000 to US$250,000. On average, however, medium sized businesses and organization may offer much less in the range of

US$120,000 to US$160,000.

Software Security Engineer
Brief Description:
This job requires coding skills of the highest standard together with some leadership skill to lead a team of programmers and developers. A combination of both attributes is rare in the market. And when a candidate fits the bill, it usually means a senior management position together with handsome pay.

Salary:
Some companies offer even heftier packages than that of CISO. Professionals in this role have been known to claim as much as US$225,000 or more annually. And the figure along with the perks are getting even more attractive given the fact that fewer people are there to fill the available positions in the job market.

Cybersecurity Sales Engineer
Brief Description:
Alternating between two roles including that of coding and making an effort to increase sales of the company is a sure way to climb up the corporate ladder. If a person can write codes and, at the same time, can just as easily finalize sales deals, then it means value in

the job market and an assurance of a stable job.

Salary:
Some professionals who are measuring up to the requirements of both the roles are drawing packages in excess of US$200,000 a year. Yet others are putting in a lot of extra efforts to increase the number to still greater heights.

Cyber Security Architect
Brief Description:
Although some inexperienced persons are also accepted in this role, the position is one of those which often require prior experience. A lead cybersecurity architect constructs and monitors the implementation of an organization's network and security mechanism. The candidates for this position often have work experience in an enterprise architect's role. The person is well acquainted with architecture frameworks like MODAF and TOGAF.

Salary:
Entry level candidates who manage to land this job can get as much as US$80,000 annually. The compensation for mid-level and senior level jobs range from US$120,000 to US$130,000.

There are some other jobs like Computer Programmer, Database Administrator and Software Developer which can fetch somewhere in the range of US$70,000 to US$90,000.

Business leaders, especially those who work closely with the cybersecurity department, believe the prospects for jobs in this particular area of information technology are not only promising but exceedingly rosy as well. So, anyone who desires to build a bright career should look toward the cybersecurity area of organizations and acquire knowledge and skills to get there.

Vanishing Act of Cryptoqueen

INVESTMENTS OF ONECOIN BUYERS GOES DOWN THE DRAIN

The founder of OneCoin cryptocurrency, Ruja Ignatova, has entered the annals of crime by committing the largest ever scams that has so far exceeded 4 billion US dollars. With that feat of sorts, her name has been added to FBI's ten most-wanted list. And she has the distinction of being the only woman in the top ten, alongside murderers, gangsters, fraudsters and drug peddlers.

STERLING CAREER:
Ruja (pronounced roo-ha),42, is a Bulgarian of Romanian descent. She was born in Ruse, Bulgaria. Her family moved to Germany when she was only ten. She spent her childhood in Schramberg in the state of Baden Wurttenberg. In 2005, she earned a doctorate degree in private international law. After her studies, she worked briefly for McKinsey & Company. Her true claim to fame began with the launch of OneCoin—a cryptocurrency that supposedly competed with Bitcoin which is the first and most well-known of all.

With the success and unprecedented following of OneCoin, Ruja rose to become a self-styled 'Cryptoqueen.' In an event of June 2016, she stepped on the stage of Wembley Arena in front of a large cheering crowd and claimed that she had invented a cryptocurrency that will rival Bitcoin. She blatantly told the crowd that OneCoin was destined to become the world's biggest cryptocurrency.

REALITY CHECK:
The activity and immense interest that surrounded OneCoin could not have gone unnoticed. On one side were frenzied buyers driven by greed of making hard-to-believe profits and on the other side were skeptics who doubted the veracity of the cryptocurrency. Investigators, already smelling something fishy, got down to work as the self-proclaimed Cryptoqueen globe-trotted to address filled-to-capacity auditoriums, attracting investments in loads. According to estimates, from 2014 to the early part of 2017, OneCoin had amassed nearly US $4billion in payments.

All over the world, from Pakistan, Canada, Hong Kong and Brazil to Yemen, UAE, China, USA, UK and Germany, people were putting their savings on OneCoin, thinking that the cryptocurrency would transform their fate. Some estimates reveal that UK citizens alone invested nearly €30m in the first six months of 2016.

NO VALUE:
Although, OneCoin generated huge revenue, the coin by itself did not possess any buying power. But people kept on buying merely out of greed without really knowing that the OneCoin isn't what it is claimed to be. Unlike Bitcoin, which is backed by blockchain, OneCoin does not have any. Blockchain is a special type of database. It is a mechanism that records every transaction of the bitcoin. A lot of mathematics and technology goes into maintaining that database and it is something that has gained trust worldwide.

Unfortunately, OneCoin did not qualify as a cryptocurrency in spite of the claims that it is a rival of Bitcoin and that very soon it will consign its competitor to oblivion. The investors were not aware of this hard to swallow fact.

PONZI OR PYRAMID:
People learnt very late that OneCoin

was actually an investment fraud commonly referred to as a Ponzi scheme that distributes profits to existing investors by collecting funds from new investors. Ponzi schemes attract business with their lure of 'high returns and no risk.' Rarely, such schemes make any investments in lucrative projects. Instead, they rely on a steady stream of new investors. This scheme eventually collapses as new investors diminish and funds deplete.

There is some evidence that OneCoin also operated in the style of Pyramid schemes. Such schemes operate like multi-level-marketing schemes but in the pyramid scheme the product does not have a value of its own. The business model works on the premise that new members will be paid out on the condition that they recruit more members. The membership pool starts increasing exponentially once the chain referral scheme is triggered. A time comes when no further recruitment of members is possible. That's when the business becomes unsustainable.

MYSTERIOUS END:
In the early days and until late 2016, things were running smoothly for OneCoin and Ruja was riding the crest of success. Sometime in 2017, Ruja felt that FBI agents and other intelligence agencies were after her, she vanished without a trace. The last time, she was seen boarding a Ryanair flight that took her from Sofia to Athens. There is no news about her ever since. Speculations are rife though. Some say, she is idling on a luxury yacht somewhere in the Mediterranean Sea. Others say she might not be alive. Her brother Konstantin was arrested in Los Angeles and he has admitted to money laundering. But the Cryptoqueen remains elusive.

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 appeared 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, marginalization of silos and diminished fragmentation of 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—named as 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

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.

Ransomware Attack in New Jersey

THE ATTACK DISRUPTS A RANGE OF SERVICES

One of New Jersey's counties is reeling after a ransomware attack that left the systems installed at the local government offices in disarray. Somerset County is located just north of Princeton University and it has a population of more than 350,000. The administration has announced that the email system is down. And to prevent any further compromises, the systems have been disconnected and shut down. The county officials, however, have reiterated that only the email and IT systems were affected as a result of the attack. The emergency service systems and phone lines have remained safe. The damage, though limited, still required several days of restoration efforts.

In an effort to gain confidence of the citizens, the director of Public Information, Nathan Rudy, said that FBI has been notified of the incident and that investigations are under way to identify the criminals.

At the time of attack, the county had created temporary gmail accounts to provide access to critical services such as the "County Commissioners, Health, Emergency Operations, the County Clerk, Sheriff and Surrogate."

The administrator, Colleen Mahr, said that her county is in a position to perform most of the official tasks although the attack forced them to cancel a Board of Commissioners meeting. Mahr said, "We have activated our Emergency Operations Center and our Continuity of Operations of Government Plan. It is our assumption that this situation will remain in effect at least for the rest of the week."

In an update following the attack, the county administration informed that the County Clerk's office could not provide the services requiring internet connection. That is why land records, vital statistics, probate records and title searchers before 1977 were inaccessible to the citizens.

Mahr added, "We are working hard to ensure vital services the public depends on to be delivered, such as recycling, road maintenance, and transportation for seniors. Our IT department is working round the clock to evaluate the extent of damage and prevent further damage."

In this year alone, as many as 22 incidents of ransomware have been recorded in the US. But according to Rob Joyce, a senior National Security Agency official, fewer US organizations have suffered attacks this year. This situation is probably attributable to the ongoing war between Russia and Ukraine. His remark implied that most of the attacks on US installations often originated from this region and the hackers are now busy with tasks related to the turmoil in their region. As soon as the conflict will be over, the intensity and frequency of attacks may increase. This is a signal to cybersecurity professionals to brace up for a steady stream of onslaughts any time soon.

Cybersecurity Compliance in Public Cloud

ISSUES AND SOLUTIONS

Everybody is talking about cloud these days. There is so much buzz about it that it seems everything is happening in the cloud: moving, operating, storing and accessing. But few can precisely define what this amorphous concept really is and how it has morphed from plain, old computing to cloud computing. In short, it is a device or system that can be accessed through the internet. Once connection is established, anyone can access apps and services while also store data securely. Three key benefits of cloud make it a smart choice for computing.

1. The users are not required to maintain or manage it.
2. The size of the cloud—in terms of bytes and terra-bytes, of course—is humungous. There is virtually no chance of running out of capacity.
3. Users can access software and applications from anywhere on the planet. All they need is any computing device with an internet connection.

Benefits like these are too tempting to resist. That's why a shift to cloud based computing is happening for the past many years. Another factor responsible for the shift is the worldwide trend of home-based work instead of office-based operations. The covid pandemic has also stimulated this trend. It is easy to analyse the fact by simply observing the sales of hardware around the world.

Only a few years back, the sales of desktops and laptops reached 270 million. Tablets and pads registered sales of nearly 350 million. In comparison, mobile devices sold in excess of 2 billion.

The figures have spoken very clearly about the world preference and there is no denying the fact that the cloud has earned worldwide acceptance and users around the world have embraced it.

It would not be out of place to quote the words of Steve Jobs that he pronounced years earlier: "I don't need a hard disk in my computer if I can get the server faster…carrying around these non-connected computers is byzantine by comparison."

But it would be a misrepresentation of reality if someone paints a rosy picture about the cloud. With the increase in cyber crimes causing enormous damages—some of them running into millions of dollars—businesses and organizations felt a dire need for cloud usage. Since cloud computing provides various

advantages, such as 'improved collaboration, improved mobility, excellent accessibility and unlimited storage capacity, more and more organizations see tremendous merits in shifting to this mode of operations. This shift toward cloud has triggered a steep rise in cloud traffic and the amount of data stored there, engendering demand for regulations and compliance.

To begin with, cloud frameworks are put into place, which outline 'policies, configurations, rules and tools.' These are designed to manage the security of a cloud platform. Next comes cloud compliance—an area of operations that relates to regulatory standards of cloud usage. These standards are formulated in accordance with industry guidelines and laws that apply to all territories. For instance, cloud environments require well-defined password policies, encryption of critical data and configuration of security groups.

ISSUES IN CLOUD COMPUTING

Although cloud computing offers numerous advantages like accessibility, mobility, capacity besides excellent collaboration, security risks are also part of the package.

Here are some that cannot be taken lightly.

LOSS OF DATA:

This is the most common cloud security risk. It is also known as data leakage. When some information is being deleted, corrupted and rendered unreadable, it amounts to a loss of data. This usually happens when sensitive data is handled by someone else. In such a case data elements cease to perform at the optimum. The result: hard disk does not work properly or software is not updated.

BREACHES:

Breaches occur all the time. It is a known fact that at any given moment, someone, somewhere is preparing to launch an attack. Breaches are characterized by unauthorized access to sensitive and critical data by cyber criminals. Once they infiltrate and get access to data, they either steal it or implant a malware to blackmail their victims. Cloud computing too is exposed to this threat just as other computer systems at businesses and organizations.

DENIAL OF SERVICE ATTACKS:

DoS attacks have become common incidents. Hackers have developed a knack for attacking systems with busy traffic. Web servers of large organizations such as government organizations, media companies, banking sectors usually become the target. Companies are forced to pay out large amounts of money to restore their systems and the services which were denied to the customers.

INTERFACES AND APIs:

Cloud computing entirely depends on internet connection. It is essential, therefore, to protect interfaces and APIs. The latter constitute the easiest mode of communication with cloud services. Since these services can be accessed by third parties, there is a chance of hackers gaining access and causing damage.

VENDOR LOCK-IN:

When organizations need to shift services from one vendor to another, they encounter problems because vendors work from different platforms. The variation poses difficulty in moving one cloud data to another. That's why vendor lock-in is considered as one of the biggest security risks in cloud computing.

HIJACKING OF ACCOUNTS:

Hackers are now after cloud accounts of organizations and individuals. Once they steal the account details which may include bank account, email address and social media account, the hackers begin to use these to perpetrate unauthorized activities. Of all the troubling aspects of cloud computing, this stealth and strike activity is one of the most annoying.

SOLUTIONS TO PROBLEMS IN CLOUD COMPUTING

Here is a short list of some practices that can work as solutions to the array of issues that surround cloud computing.

RIGHT TEAM DELIVERS THE JOB:

Businesses and organizations that already subscribe to the services of a cloud provider or those looking to have one, must first have the right team to keep a watch and regulate cloud computing at the workplace. Employees with cybersecurity experience can ensure compliance of cloud regulations. Professionals with IT experience like network administrators, pen testers or cybersecurity engineers can provide valuable insights for successfully implementing cloud compliance.

RELIABLE CLOUD PROVIDERS ARE A MUST:

While it is a must to have the right kind of team to ensure cloud compliance, it is also useful to have a reliable and trusted cloud provider. A good vendor is helpful in meeting global compliance requirements like ISO27001, PCI DSS, HIPAA and FedRAMP Plus. Sometimes, it is a good strategy to procure services from different cloud providers which may prove efficient and economical for an organization.

THE SHARED RESPONSIBILITY MODEL:

When businesses, organizations or individuals subscribe to cloud, the security of space is shared between the service provider and the subscriber. An article on the subject uses the terms 'Security of the Cloud' and 'Security in the Cloud.' In the former case, it is the responsibility of the service provider while in the latter, the responsibility rests with the user.

CONTRACTS AND AGREEMENTS:

Contracts and agreements are often vague and clauses contained in the document are not stated clearly. It is, therefore, essential to understand what is written and if anything requires clarification or elaboration, prompt action is necessary. For instance, almost 63% of cloud providers do not state clearly that the customer's data is not owned by the provider. The ownership rights belong solely to the customer and the cloud provider can, in no way, claim ownership of uploaded data. Cloud computing carries tremendous benefits only if the users make sure that the well-defined principles are followed and compliance is strictly adhered to. That can save businesses a lot of headache that can come in the shape of fines, audits and other penalties that can affect smooth running of the business.

Austrian State Carinthia Halts Passport Issuance

RANSOMWARE POSSIBLE REASON FOR THIS EXTREME MEASURE

Large scale failure of government services was witnessed recently in the Austrian state of Carinthia as the infamous hacker group Black Cat launched a ransomware attack. The group is demanding US$5m in Bitcoin in exchange for decryption software.

Black Cat has also accessed sensitive data including personal information of citizens all across the state. In response, the state of Carinthia has halted the issuance of passports, though temporarily. The head of Carinthia's press service, Gerd Kurath, has reiterated that the state will not surrender to the demands of hackers because there is no evidence that the data has been stolen. Even if it were, the government had already backed up the data and stored safely elsewhere and it can be retrieved at any time. Interestingly, the hackers offered decryption software in exchange for an hefty ransom.

The news of this breach was first reported by HackNotice, a service that monitors trends and patterns to identify any trace of possible breach, leaks, hacks or any other data incidents. In one of their routine surveillances, they spotted footprints of a breach and reported the matter to the state administration. HackNotice has the technology to identify the time and date of breach, the of hackers or group responsible for the job and the location from where the attack was launched.

The administration of Carinthia initially said that the cause of failure of government services could not be verified. Later, when the incident became known through social media and other sources, the spokesman categorically stated that the demands of the hackers will not be entertained under any circumstances. However, the attack caused delays in payment of basic services and there were reports of leaked data from servers as well. In retaliation to the government announcement that the undue ransom demands would not be entertained, the hacker group, Black Cat, began releasing sensitive data on the dark web. Security expert Sebastian Bicchi has revealed through 'twitter' that 5.6 GB of the 250 GB stolen data have been leaked on to various sites accessible to anyone.

Although the state administration is firm and determined in the face of adversity, the fact is the citizens are in a quandary. The email service is down and the state website is continuously offline. The facility to trace COVID-19 patients is also not working. Consequently, there is no way to people suspected of contracting the virus.

The online facility to transfer social benefits was also temporarily in disarray. But it was restored in a few days.

The police and law enforcement are continually investigating and trying to locate the perpetrators. But the task is not an easy one. The criminals do not have a name or a face. Neither is their location precisely identifiable. The law enforcement is confined within a territory whereas the criminals are working in a boundary-less world.

The Rise of Malicious Browser Automation Frameworks

HACKERS UTILIZING FRAMEWORK FEATURES FOR THEIR ATTACK CAMPAIGNS

Researchers from Team Cymru have filed a new report informing cybersecurity professionals that threat actors are capitalizing on vulnerabilities inherent in browser automation frameworks that are offered for free. The team stated, "The framework contains numerous features which we assess may be utilized in enablement of malicious activities.,"

The team further added, "The technical entry bar for the framework is purposefully kept low, which has served to create an active community of content developers and contributors, with actors in the underground economy advertising their time for the creation of bespoke tooling."

The report has revealed that the command and control IP addresses of BlackGuard, Bumblebee and RedLine Stealer malware were connected to the subdomain (downloads.bablosoft.com) of BAS (Browser Automation Studio) developed by Bablosoft. This led researchers to believe that a number of malware operators were using the subdomain for post-exploitation activities.

The researchers added, "Based on the number of actors already utilizing tools offered on the Bablosoft website, we can only expect to see BAS becoming a more common element of the threat actors toolkit."

Investigations into the subdomain's IP address has revealed that the activity largely originates from Russian and Ukrainian locations. The open source intelligence has also indicated that Bablosoft's owner is based somewhere in Kyiv, the Ukrainian capital.

Several other hosts linked to cryptojacking malware like XMif and Tofsee have also been identified. Researchers observed that these hosts were communicating with a second subdomain of bablosoft, fingerprints.bablosoft.com to employ a service that was helpful in hiding the behavior of the the mining malware.

Mr. Shakeel Akhter
CIO Indus Hospital & Health Network

LEVERAGING TECHNOLOGY

COMBINATION OF EXPERIENCE & TECHNOLOGY WILL MAKE A DIFFERENCE

Mr. Shakeel Akhter, CIO Indus Hospital & Health Network, is an IT professional with 34+ years of experience. His work largely relates to Health Informatics. He is one of the pioneering members and one of the first employees of Indus Hospital.

His vast experience includes information technology, healthcare, software engineering besides development and implementation of applications in several industries and specifically in health care information systems. He was featured on cover page of 1st CIO magazine in 2008. He has also received the award for the ICT Best CIO (Private Sector) of Pakistan in 2009. His portfolio also includes title of Master (2020) and title of Legend (2021) at the Global CIO 200 Forum. Another award in 2016 for Best Innovative Idea in Pakistan serves as an icing on the cake.

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 cybersecurity 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 is 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 and 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 cybersecurity measures have you introduced and implemented in your organization?

Well, the only thing that is crucial for your organization is a strong cybersecurity 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 cybersecurity awareness which is the essential measure to bridge gap of cybersecurity 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 cybersecurity strategy at addressing business risks?

For addressing business risks, cybersecurity strategy is critical.

Steps to Assess and Mitigate Cybersecurity 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 cybersecurity 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 cybersecurity and threats? If they are not well informed please advise?

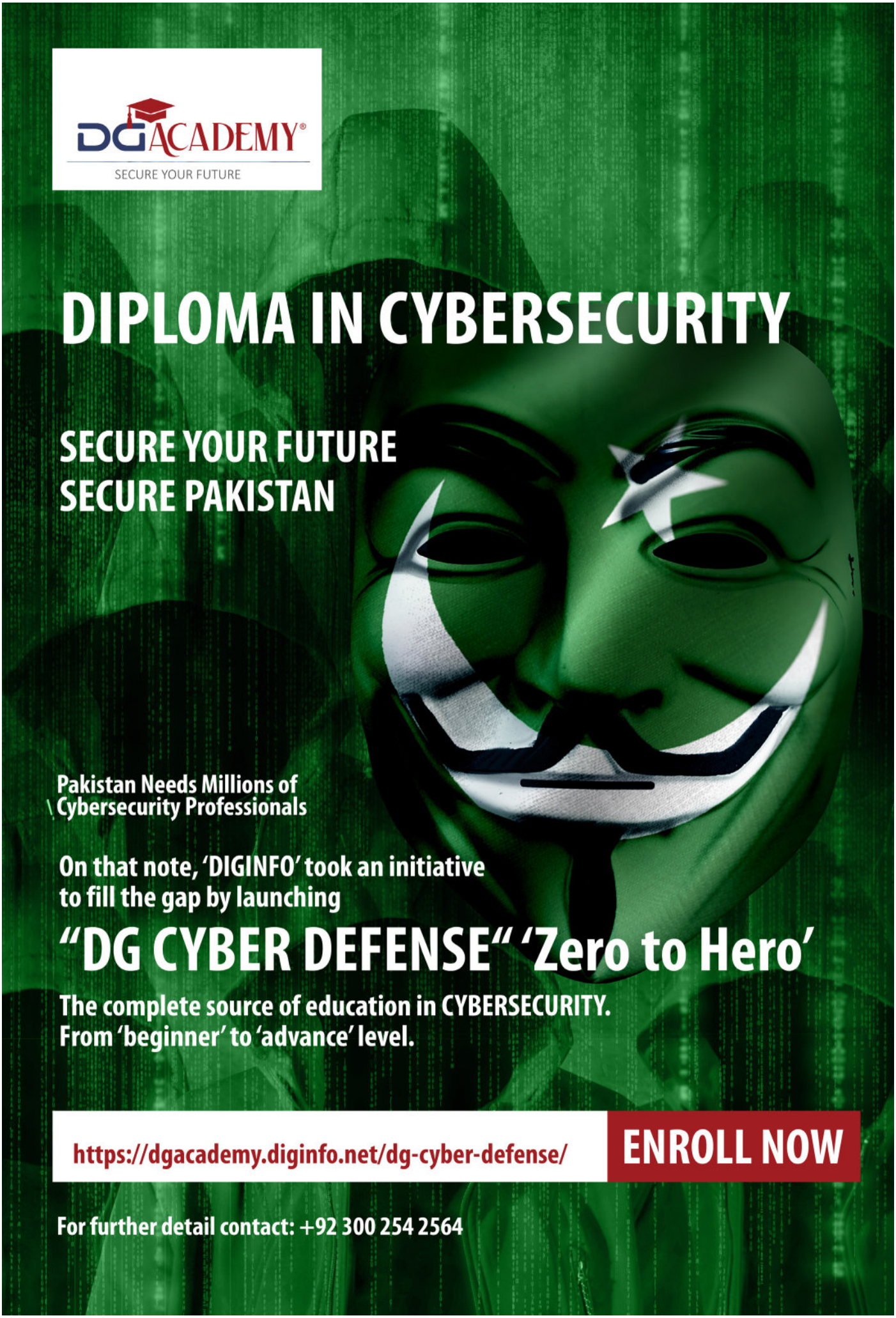
The situation is improving. People of Pakistan have now started taking cyber threats seriously as online business has grown drastically due to covid situation. A mass awareness campaign should be organized by government to further cope with the situation.

Please give some suggestions for our readers to what safeguards they should adopt to avoid cyber mishappening?

Habits to stay cyber-safe.

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

EXPERIENCE SPEAKS LOUDER THAN WORDS


DG ACADEMY
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

ROI FOR CYBERSECURITY BUDGETS

DEFENDING TECHNIQUES AND READINESS

Price Waterhouse Cooper published a report a good many years back stating that only 22% of CEOs believe there is enough risk to their data security to affect their key decisions. The rest of 78% do not even consider cybersecurity as necessary, let alone feel the urge to allocate permanent budget for it. In spite of a surge in attacks causing huge losses, closures and bruised reputations, the statistics stayed true for more than a decade.

The main reason for the grim outlook is lack of understanding even among the league of most CEOs. And there is another difficulty which contributes toward these statistical figures. It is not easy to quantify and justify the need for investment in this particular area of information technology.

CYBERSECURITY BUDGET DILEMMA

Figuring out cybersecurity budget for the company is a tricky affair. The first thing that comes to mind while doing so is ROI (Return on Investment). For instance, if a $100k annual investment can avert losses around $1million, then the spending is worth making but if the expected loss isn't as high, then the spending would seem like an extravagance. But what are the metrics to assess the losses?

It would not be out of place to quote Bruce Schneier, an internationally acclaimed security technologist and author of 14 books and several research papers.

He is referred to by the celebrated jouranal, The Economist, as technology guru. Schneier said:

"Cybersecurity (ROI and annualized loss expectancy) is considerably harder, because there just isn't enough good data. There aren't good crime rates for cyberspace, and we have a lot less data about how individual security counter measures—or specific configurations of countermeasures—mitigate those risks. We don't even have data on incident costs.

One problem is that the threat moves too quickly. The characteristics of the things we're trying to prevent change so quickly that we can't accumulate data fast enough. By the time we get some data, there's a new threat model for which we don't have enough data. So we can't create ALE (annualized loss expectancy) models."

PROACTIVE vs REACTIVE APPROACH

Most CEOs and COOs are reluctant to release cybersecurity investments because they believe the threats are not so serious to warrant heavy spending. They think that if that money is spent tasks other than cybersecurity then the money would return with profits. This tendency among the top decision makers of organizations forces them to adopt a reactive approach to cybersecurity. They are inclined to sit back and wait for an attack to happen. But they shy away from realizing that if the attack really happens, the damage would hurt the company in many ways. A ransomware attack can cost a company millions of dollars.

On the other side are companies who have taken a safer and more pragmatic approach. They have invested a chunk of their IT budget to devise several defense mechanisms to prevent an attack. Such a posture helps companies to mitigate the probability of attacks. Even if the cyber criminal successfully infiltrates the system and attacks with some kind of malware, the company is ready with a response strategy. Such readiness and preparedness are hallmarks of a proactive approach that can save millions of dollars.

A proactive approach aims to prevent an attack before it happens. Businesses and organizations may continue to allocate a budget to prevent an attack that may never take place. The top decision makers may consider the expense as unnecessary because of this reason but in case the attack is launched on the company and the cybersecurity team lacked the strength to face it then the losses may run into millions and may even threaten the very existence of the organization. There are examples in abundance where companies that paid little attention toward an effective cybersecurity policy could not recover from an attack and had to close their business down.

ESTIMATING COSTS OF CYBERSECURITY

It is not easy to estimate the cost of steering and running an effective cybersecurity program, because a number of variables are involved in the exercise. . The methodology used in measuring the costs, the size of the organization, the maturity index and several other factors have to be considered. In spite of the difficulty, some careful estimates put the figures between 5% and 15% of the overall IT budget. But some estimates are not as conservative. Kaspersky, for instance, has put the percentage around 30% of the overall IT budget. Evidently, this is highly unusual and it may only be true for a small percentage of organizations.

Although cybersecurity budget is expressed as a percentage of IT budget, the activities related to cybersecurity are not restricted to information technology alone. It has been observed that workers—not necessarily staffed by the IT department—are responsible for incidents. They are often seen to be reckless in using computer systems. Their inclination toward following precaution and safety measures is near zero. That's why training them is so essential nowadays, since everyone from the board members to the lower echelons of the workforce have access to the network. In that scenario, cybersecurity awareness programs including anti-phishing protocols, tabletop exercises, third party risk management, user monitoring controls form the basic components of cybersecurity program. Evidently, such activities require a sizable budget.

There are two other metrics for estimating the cybersecurity budget:

a) the average cost per employee which may range from $2100 to $2700 according to various estimates
b) the budget expressed as a

percentage of total revenue which may range from 0.16% to 0.54%.

A few well known financial institutions have declared their cybersecurity budget publicly presuming this might improve their rating as a safe and reliable organization. The worldwide investment bank, HSBC, has spent nearly $1 billion on cybersecurity in the years 2016 and 2017. Another institution, Desjardins, spent $150 million in 2020 and increased the budget by a two-third margin to $250 million in the following year.

MAKING A CASE FOR CYBERSECURITY ROI

Businesses often adopt a pragmatic approach before making any investment in new projects. The Chief Financial Officers routinely probe the prospects of investment and want to know about the rate of profit for every penny spent on a project. For instance, if a company invests $10 million in launching a new product, it expects $100 million in return. Likewise, if a company spends $20 million on procuring new IT system and on hiring staff, it expects $200 million in increases. But it is not easy to justify Return On Investments (ROI) on cybersecurity.

Experts believe that it is imperative to measure performance to justify a sizable budget for cybersecurity. They have identified key performance indicators an aim to install a proactive program. Threats are always lurking somewhere around the surface, and hackers can strike anytime. Companies that wait until incidents occur are only riding on the wave of a reactive approach which can lead to regulatory fines. In this case the costs for recovering lost or stolen data can be prohibitive. In contrast, a proactive cybersecurity policy depends on precautionary measures to avert any danger of attack. Moreover, this approach is distinctly marked by preparedness and readiness to face any challenges.

Here are some of the performance indicators which can mean a successful cybersecurity program which saves costs and hassles:

- Number of times hackers have tried to infiltrate the organization's systems.
- Number of unidentified devices linked to the organization's network.
- Number of unpatched devices that are exposed to attacks.
- Number of employees who are informed and trained about cybersecurity.
- Number of cyber incidents reported within the organization and the industry.
- Number of users within the organizations who have administrative access.
- Time it takes for the cybersecurity team to identify threats to the system.
- Time it takes for the cybersecurity team to respond to an incident.
- Time it takes to fully recover from an attack.
- Status of cloud security compliance and other security apparatus compliance in the organization.

CALCULATING CYBERSECURITY ROI

Quantifying the ROI for cybersecurity remained a challenge for a good many years. Several attempts to represent factors like risks, threats and compromises in numbers and figures by deriving equations did not meet with success. However, recent studies based on systematic and qualitative analyses led experts to identify the tools and technologies which will ensure optimum cyber-resilience for the money spent. After making this headway, cybersecurity experts developed a systematic methodology and model that calculates cybersecurity ROI.

After studying various methods used by different businesses to calculate risks, cybersecuritby experts took guidance from banking and insurance sectors where operational risk is defined as the 'likelihood' or 'frequency of events' multiplied by the 'severity of an

event.' Cybersecurity professionals used an analogous method for measuring ROI.

At the outset, Expected Loss (EL) is defined as 'Probability of a Successful Cyber Attack (PC)' multiplied by the 'Impact of Cmpromise (IC). This equation gives the dollar value for the expected loss. By figuring out the financial impact of Expected Loss (EL), the experts arrived at the following equation to determine the ROI of the project:

Cybersecurity ROI = [EL before project) – (EL after project)] – Cost of Project/Cost of Project

The unknown variable in the above equation is EL. That can be determined by defining two quantities: Probability of Compromise and Impact of Compromise.

Probability of Compromise = Threats x Vulnerabilities
Impact of Compromise = Assets x Losses in the event of Compromise

The 'Assets' in second equation may represent data assets, intellectual property, physical assets, factory equipment and machinery etc. Once these values are assigned mapping projects to preventive controls is done which yields reduction in probability of compromise.

A similar calculation is done to arrive at the value of reduction in the 'Impact of Compromise.' EL values are obtained by performing the calculation twice: one before commencement of the project and the other after the project is complete.

By supplying these values in the equation, we obtain a new one that is easily quantifiable:

ROI = [(PC x IC before Project) – (PC x IC after Project) – Cost of Project]/ Cost of Project

These calculations may not be precise and accurate because some of the variables involved in the equation are subjective in nature. Nevertheless they provide a basis for educated assessment and forecasting. That is required to have a meaningful cybersecurity strategy.

Chinese Hackers Infiltrate Telecom Giants

AGE-OLD SOFTWARE FLAWS AT THE ROOT OF THE PROBLEM

Hackers based in China, allegedly enjoying state sponsorship, routinely attack telecom giants around the world. According to US security agencies, the activity is a part of a larger espionage campaign that lasted well over two years. The programmers purportedly penetrated their targets by taking advantage of old and notable basic weaknesses in well known systems administration equipment. When they had a traction inside their objectives, the programmers utilized the compromised gadgets to acquire full admittance to the organization traffic of various privately owned businesses and government organizations, US authorities said.

The warning did exclude the names of those impacted by the mission, nor did it detail the effect it has had. In any case, US authorities called attention to the particular systems administration gadgets, for example, switches and switches, that programmers in China are remembered to have designated more than once, taking advantage of serious and notable weaknesses that really gave the assailants free rein over their objectives.

"These gadgets are frequently disregarded by digital protectors," the American warning cautioned. They "battle to keep up with and stay up with routine programming fixing of Internet-confronting administrations and endpoint gadgets."

The new warning is the most recent illustration of an extreme shift among US insight organizations from a culture of quietness and mystery. The associations currently regularly talk freely to give network protection direction. The new report is intended to help casualties distinguish and discharge programmers who have been invading their organizations for quite a long time.

What's more, it's something greater, as well: an advance notice about the requirement for better fundamental online protection for probably the main organizations on the planet.

High Gamble

Media transmission firms are very high-esteem focuses for knowledge organizations. These organizations fabricate and run on the greater part of the foundation of the web as well as numerous confidential organizations all over the planet. Effectively hacking them can mean opening ways to a significantly greater universe of valued spying open doors.

The United States has its own archived history of such assaults. The National Security Agency, for instance, when invaded the Chinese telecom and web monster Huawei, purportedly both to keep an eye on the actual organization and to take advantage of the systems administration and broadcast communications items Huawei sells around the world. Amusingly, that activity was provoked to some degree by proceeding with American feelings of trepidation that Beijing could utilize Huawei's equipment to keep an eye on American interests.

The programmer for-employ industry is currently too large to even consider coming up short. This is a defining moment of disturbance and change for the hacking industry. Be that as it may, the interest is setting down deep roots.

In the recently announced digital mission, the Chinese programmers supposedly took advantage of systems administration gadgets from significant merchants like Cisco, Citrix, and Netgear.

The weaknesses were all freely known, remembering a five-year-old basic defect for Netgear switches that permits aggressors to sidestep verification checks and execute any code they pick — an initial that considers a full takeover of the gadget and an unbound window into the casualty's organization.

The mission's prosperity is a sensational representation of the risk programming blemishes present even a very long time after they're found and unveiled. Zero-day assaults — hacks taking advantage of beforehand obscure shortcomings — sneak up all of a sudden and request consideration. Be that as it may, realized imperfections stay intense on the grounds that organizations and gadgets can be hard to refresh and get with restricted assets, staff, and cash.

Ransack Joyce, a senior National Security Agency official, made sense of that the warning was intended to give bit by bit directions on finding and removing the programmers. "To kick [the Chinese hackers] out, we should grasp the tradecraft and identify them past introductory access," he tweeted.

Joyce repeated the warning, which guided telecom firms to sanction essential online protection rehearses like staying up with the latest, empowering multifaceted validation, and diminishing the openness of inner organizations to the web.

As per the warning, the Chinese undercover work commonly started with the programmers utilizing open-source checking apparatuses like RouterSploit and RouterScan to overview the objective organizations and become familiar with the makes, models, forms, and known weaknesses of the switches and systems administration gadgets.

With that information, the programmers had the option to utilize old yet unfixed weaknesses to get to the organization and, from that point, break into the servers giving confirmation and distinguishing proof to designated associations. They took usernames and passwords, reconfigured switches, and effectively exfiltrated the designated organization's traffic and replicated it to their own machines. With these strategies, they had the option to keep an eye on for all intents and purposes everything happening inside the associations.

The programmers then, at that point, convoluted and erased log documents on each machine they contacted trying to annihilate proof of the assault. US authorities didn't make sense of how they at last learned about the hacks regardless of the assailants' endeavors to cover their tracks.

The Americans likewise excluded subtleties on precisely which hacking bunches they are denouncing, as well as the proof they have that shows the Chinese government is capable.

The warning is one more caution the United States has raised about China. FBI representative chief Paul Abbate said in a new discourse that China "leads more digital interruptions than any remaining countries on the planet joined." When gotten some information about this report, a representative from the Chinese government office in Washington DC rejected that China takes part in any hacking efforts against different nations.

DIGINFO®

TRUSTED LEADER IN CYBER SECURITY

PROTECT YOUR SYSTEM

Make sure antivirus, firewall, and ad-blocker solutions are patched and updated on a regular basis.

Never download pirated apps or software as they often contain malware.

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

SCAN ME

Fresh Exploits of BPFDoor Malware

MALICIOUS CODE USING SOLARIS AND LINUX VULNERABILITIES

New examination into the internal operations of the secretive BPFdoor malware for Linux and Solaris uncovers that the threat actor behind it utilized an old weakness to accomplish constancy on designated frameworks.

BPFDoor is a custom secondary passage that has been utilized generally undetected for no less than five years in assaults against media communications, government, training, and planned operations associations.
The malware was found as of late and revealed first by scientists from PricewaterhouseCoopers (PwC), who credited it to a China-based danger entertainer they track as Red Menshen.

Top ArticlesREADMOREMicrosoft Azure currently has classified VMs withephemeral capacity
PwC tracked down BPFDoor during an occurrence reaction commitment in 2021. Taking a gander at the malware, the specialists saw that it got orders from Virtual Private Servers (VPS) controlled through compromised switches in Taiwan. Ensuing, thorough examination from Craig Rowland, the pioneer behind Sandfly Security, and Kevin Beaumont showed the profoundly treacherous nature of the malware, which can practically sidestep most recognition frameworks.

BPFDoor can't be come by firewalls, it can work without opening any ports and needn't bother with an order and control server as it can get orders from any IP address on the web.

Utilizing a public endeavor CybersecuritycompanyCrowdStrike has noticed a danger entertainer that zeroed in chiefly on focusing on Linux and Solaris frameworks utilizing the exceptionally constructed BPFDoor embed on broadcast communications suppliers to take individual client data (for example call detail records, information on unambiguous telephone numbers).

CrowdStrike is following the secondary passage under the name JustForFun and credits it to a foe that they allude to as DecisiveArchitect. The specialists examined action of this foe a few times starting around 2019.

"DecisiveArchitect shows a serious level of functional security as a component of their strategies to make it more hard for protectors to recognize and explore their action using different safeguard avoidance methods" - CrowdStrike
In a report today, the scientists give insights concerning how protectors can recognize the BPFDoor embed and feature strategies utilized across Solaris frameworks.

They note that once DecisiveArchitect accesses a Solaris framework, it accomplishes root-level consents by taking advantage of CVE-2019-3010 - a weakness in the XScreenSaver part of the Solaris working framework (variant 11.x). Take advantage of code for the weakness is freely accessible for a considerable length of time and apparently DecisiveArchitect put forth no attempt to change it.

source: CrowdStrike
The danger entertainer begins utilizing the bug normally "inside a couple of moments of the JustForFun embed organization," as indicated by the specialists' perceptions.

CrowdStrike analysts note that on Solaris frameworks the danger entertainer utilizes the LD_PRELOAD natural variable to accomplish usefulness like the order line parodying seen on Linux has.

Be that as it may, beginning April 2022, DecisiveArchitect refreshed its strategies, methods, and techniques, and started utilizing the LD_PRELOAD ecological variable on Linux machines, too, to stack the BPFDoor/JustForFun embed in the genuine cycle/sbin/agetty.

"The satirize order line shows up in orders, for example, ps that might be utilized to explore dubious movement on the host," CrowdStrike The specialists feature that recognizing BPFDoor/JustForFun inserts on a Linux framework might end up being an overwhelming errand in light of the fact that the danger entertainer changes existing SysVinit scripts on the host to accomplish perseverance.

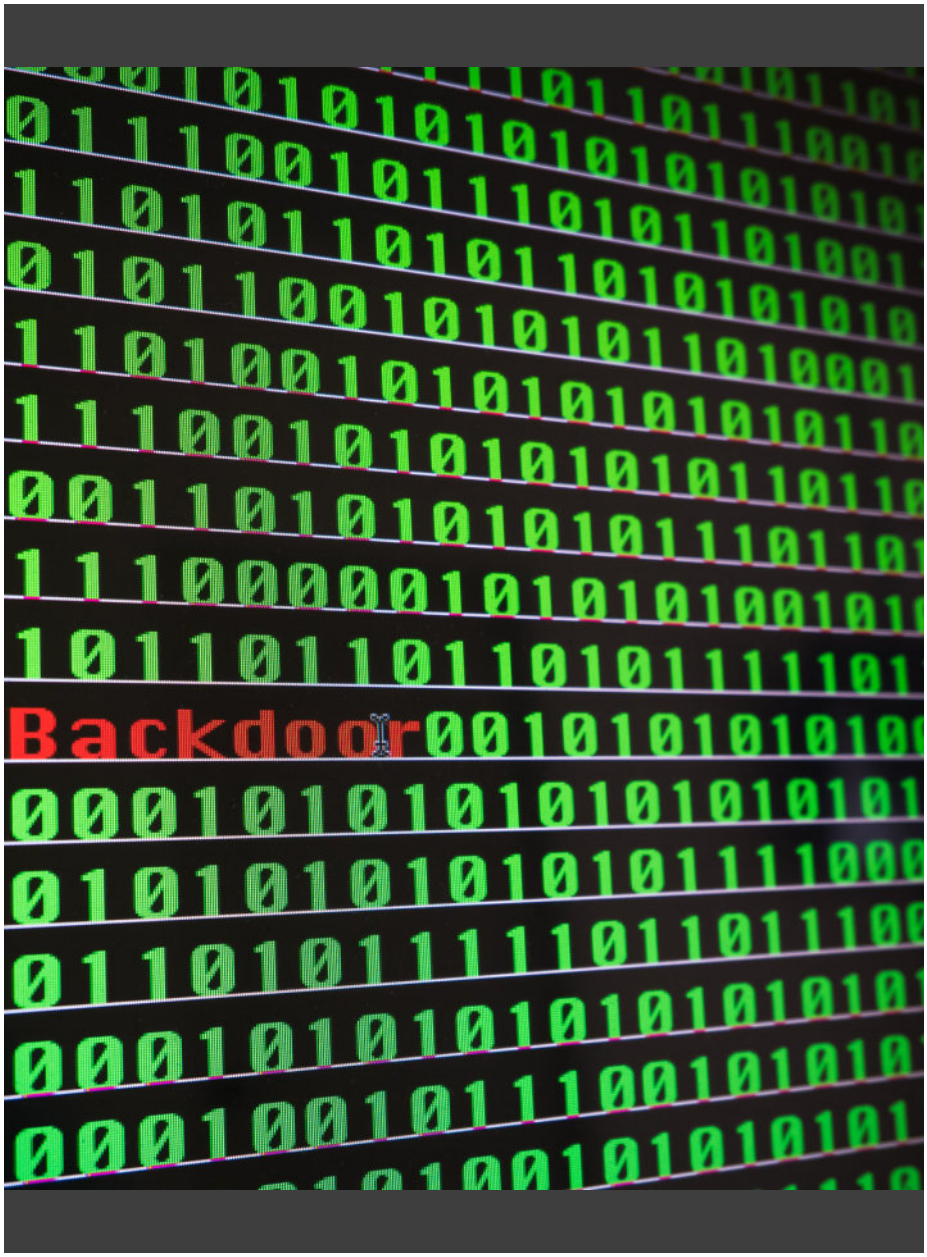
In that capacity, essentially auditing the lines of code in SysVinit scripts is probably not going to uncover the reference to the embed and all document references ought to be examined.

To make it considerably more hard to recognize, the document names and ways for the embed and the related steadiness related scripts are not quite the same as one framework to another.

CrowdStrike gives a bunch of orders that could end up being useful to safeguards examine whether BPFDoor is available on their organization by recognizing running cycles with a crude attachment

open: CrowdStrike's report today incorporates a rundown of signs of give and take for both Linux and Solaris frameworks, as well as two Windows scripts whose reason stays obscure right now.

The specialists say that the threat actor behind BFPDoor communicates with Windows machines during the beginning phases of the interruption however they distinguished no custom inserts for this working framework



CYBERSECURITY FRAMEWORKS

MAKING A CASE FOR VULNERABILITY MANAGEMENT

Businesses and organizations around the world invest considerable resources to install systems that manage their data. It is a paradox however that the systems deployed to deliver efficiency and ease of operation are fraught with risks and threats. In the past several years, cyber attacks have become a permanent feature of information and communications technology. If anything has remained constant in the cyber world, it is the steady rise of cyber attacks—not only in their intensity but also in their frequency. The technology application and level of sophistication are also on an upward trajectory.

The profession of cybersecurity emerged soon after the realization that every enterprise requires a permanent workforce to balance the effect of attacks. Cybersecurity has now become an ongoing and continuous battle between threat actors and ethical professionals. Experts working for cybersecurity of any organization constantly devise newer and more effective ways to counteract hackers' activities. In recent years, cybersecurity frameworks have become a routine form of best practices for vulnerabilities management.

CYBERSECURITY FRAMEWORKS.
Eminent cybersecurity organization routinely carry out researches to reach a best possible solution to neutralize the effect of breaches. Their continued pursuit of excellence led to creation of cybersecurity frameworks. These are fundamentally a set of predefined policies and procedures for a particular business or an enterprise. The frameworks are well documented for theoretical purposes and practical implementation.

Digital systems and data environments differ in their operational modes from one organization to another. Cyber security experts, therefore, devised different frameworks for specific industrial setups and business types. These frameworks are designed to mitigate vulnerabilities and misconfigurations inherent to any organizational network. In a nutshell, cybersecurity framework is a set of rules and regulations aimed at enhancing IT security.

IMPORTANCE OF FRAMEWORKS.
Cybersecurity frameworks aim to upgrade existing security posture and introduce new security protocols to improve the overall security apparatus. The frameworks also help organizations in understanding how their

organization or business fares when it comes to maintaining security standards. The frameworks are often well-designed and tested under different conditions, businesses and organizations can be sure of their reliability.

KEY PROCESSES.
Frameworks consist of five key processes that define the entire function. Any cybersecurity framework will follow these steps to make sure security is in a state of readiness and preparedness to face any challenges posed by the ever active individual hackers and notorious groups. The five processes are referred to as:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

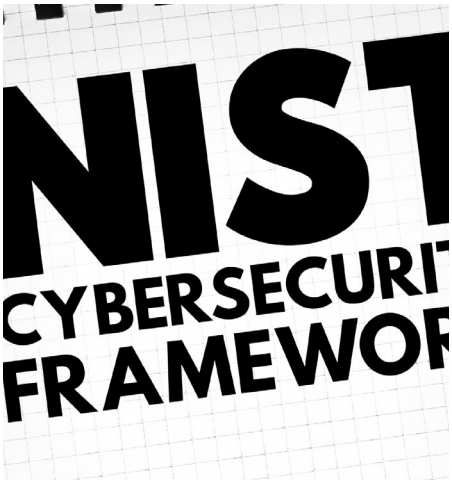
IDENTIFY: This process aims to pin point the vulnerable spots within the business or organizational environment. These spots could be physical IT assets of the company, resources or information.

PROTECT: To take care of cybersecurity in and around the business environment, this process takes up corporate access control, data security and maintenance. This step is considered as a proactive phase of the framework.

DETECT: This function is designed to explore and detect breaches by monitoring logs. Besides this, intrusion detection procedures are also undertaken at the network and device level.

This procedure is also marked by two other activities: security information and event management.

RESPOND: Once organizations detect that a breach has occurred, they need to invoke response procedures immediately. This phase is defined by an accurate assessment of the breach and a strategy to counter the attack. This is followed by removing the vulnerability and making amends for the damage done by the breach. Attempts to recover the lost or damaged data is also an integral part of this phase of framework. With the knowledge acquired as a result of the incident, the professionals handling the situation proceed toward mitigation, response planning and improvements. All this is done to make the security strong, if not impregnable.



RECOVER: This stage of cybersecurity framework strategy function is identified by recovery planning procedures. This includes disaster recovery and backup plans which contribute toward better and more robust security posture in the event of any other such incident.

TYPES OF FRAMEWORKS.
Dozens of frameworks are in use today. Every now and then, a new framework, with new principles and guidelines announces its arrival. Some of these are specific to a particular organization or business while others were built to cater to all types of businesses. Many of these, because of their applicability to all setups, have become popular and enjoy great following. Here are a few frameworks that are often seen at businesses—large or small:

- NIST Cybersecurity Framework
- ISO 27001 and ISO 27002
- SOC2
- NERC-CIP
- HIPAA
- GDPR
- FISMA

NIST CYBERSECURITY FRAMEWORK.
Former Presiden Obama is said to have passed an executive order which is known as popularly known as 'Improving Critical Infrastructure Cybersecurity.' The executive order emphasized the need for greater collaboration between the public and private sector for identifying, assessing, and managing cyber risk.

The NIST Cybersecurity Framework was established as a result of these deliberations. Over a period of time, NIST has acquired the status of 'gold standard' for measuring cybersecurity maturity, locating security gaps, and complying with cybersecurity regulations.

ISO 27001 AND ISO 27002.
International Organization for Standardization (ISO) formulated these certifications to validate cybersecurity programs, both within the organization and across third parties. ISO certifications have become internationally recognized sets of standards which allow organizations to prove to all stakeholders that they are adopting the right strategy to manage cyber risk. Having an ISO 27001/2 certificate is a fairly reliable indicator that the vendor adheres to mature cybersecurity practices and controls. But good things have demerits as well. The certifications are expensive

both in terms of resources and time consumption. That is why, organizations should opt for these standardization procedures only if true benefit, like the prospect of new business, is probable. The certification is also time restricted. It does not cater to evolving risks as opposed to continuous monitoring which can be more effective in detecting them.

SOC 2.
This framework, popularly known as Service Organization Control (SOC) Type 2, is trust-based and arguably the toughest framework to implement. It has over 60 compliance requirements together with comprehensive auditing process systems and controls.
The auditing is long and labour intensive, consuming at least a year to complete.
Businesses, like banking and finance houses where higher standards of compliance are required, prefer to install this framework because of its comprehensiveness and accuracy. In spite of the inherent difficulties, the framework is valued and depended on for effective third-party risk management programs. American Institute of Certified Public Accountants (AICPA) developed this framework to help partners and vendors manage client data securely.

NERC-CIP.
The steep rise in attacks on critical infrastructures in the United States prompted North American Electric Reliability Corporation—Critical Infrastructure Protection to design this framework. The aim was to assist organizations and businesses related to power supply and utilities to mitigate cyber risk and ensure reliability in operations of critical nature.
Multiple control factors are suggested in the framework to quantify and measure processes and aspects categorizing systems, critical assets, training employees, risk management, vulnerability management and incident response.

HIPAA.
The framework known as Health Insurance Portability and Accountability Act (HIPAA) was especially designed to strengthen cybersecurity profile of healthcare organizations. It facilitates healthcare facilities to implement controls for protecting information stored in databases. In addition to enforcing compliance of cyber best practices, it also helps healthcare facilities to conduct assessments for risks and threats in and around the data environment.
HIPAA compliance has become a benchmark of high standard facilities and remains a key driver for optimum performance.

GDPR.
The General Data Protection Regulation (GDPR) was designed and implemented in 2016 with a major aim to provide security to the private data of EU citizens. The framework is not restricted to EU citizens alone, in fact, it impacts all organizations and businesses that interact in any way with EU citizens or acquire and maintain their private information.
The framework consists of 99 articles related to compliance responsibilities of organizations. Besides data access rights, privacy policies, breach notification, there are several more aspects that this framework takes into account. Any discovery of a breach or a minor intrusion has to be reported within 72 hours. Delay means punitive action against the organization or business.
Harsh fines have been recommended for non-compliance. The fine may climb as high as €20,000,000 which may at first seem unrealistic. Yet the EU has no qualms about enforcing this rule.

FISMA.
This framework is associated with Federal Information Security Management Act (FISMA) and works closely with NIST standards. The framework is geared toward protecting systems that are managed by federal government institutions and organizations. FISMA regulations also serve the interests of vendors and third parties who are in any way associated with federal agencies. Over 800 guidelines have been provided for the protection of sensitive information. A categorization has also been incorporated according to the level of threats and importance of data.

SOLUTIONS:

Cybersecurity frameworks are now fully developed systems to play an important role in defending against unexpected situations. This ability gives cybersecurity professionals an edge over cyber criminals.

Businesses are now learning to invest in cybersecurity procedures. They are also beginning to understand that investing in cybersecurity ultimately benefits the organization by bringing in more clients and enhancing the reputation. In essence, it is a win-win position.

Russian Hackers Linked to Brexit Leaks

THREAT ACTORS PUBLISH EMAILS OF SEVERAL LEADERS

A new website that goes by the name of "Very English Coop d'Etat" has published leaked emails of several leaders who campaigned for Britain's exit from the European Union. The website is linked with Russian hackers. This was revealed by Google's cybersecurity officials and former head of UK's foreign intelligence.

Notable persons whose private emails have been released on public domains are former British spymaster Richard Dearlove, leading proponent of Brexit Gisela Stuart, pro-Brexit historian Robert Tombs and several others who campaigned for Britain's exit which was ultimately finalized in January of 2020.

Although the reports of email hacks could not be ascertained immediately, but two of the leaders confirmed that they were victimized by the hackers and that the action enjoyed support of Russian government. "I am aware of a Russian operation against Proton account which contained emails to and from me," said Richard Dearlove. He was referring to the privacy focused ProtonMail service.

Dearlove, who headed Britain's MI6 from 1999 to 2004, advised everyone to exercise caution with the leaked material because of the prevailing crisis following war between Russia and Ukraine. Pro Brexit historian, Tombs, stated in an email that he and his colleagues were aware of the Russian disinformation based on illegal hacking. Gisela Stuart, who was leading Vote Leave campaign in 2016, did not respond to emails seeking her comment on the leaks. Shane Huntley, the director of Google's Threat Analysis Group told Reuters that the "English Coop (sic) dEtat" website was linked to Russian based hacker group, 'Cold River.' Some technical indicators together with the group's attempts to highlight the incident led researchers to point the finger at 'Cold River.

Russian embassies in London and Washington did not respond queries through email. Britain's Foreign Office too did not respond to enquiries. Other Brexit campaigners, whose emails were supposedly hacked and published by the Russian group, chose not to reply. Lack of response from those who were victimized by the leaks could not conclusively establish the role of Russia based hackers. But Thomas Rid sees a stark similarity to past attempts that were linked to this group, purportedly having support of Russian government. Rid said, "It looks very familiar in some ways, including the sloppiness."

If the reports of hacks are true in any sense, then it would be the second incident in just three years. In a way Russian hackers have developed a knack of stealing emails from senior British officials and then publishing the stolen material online. Earlier in 2019, after one such incident targeting UK government institutions, British foreign minister, Dominic Raab, alleged that the hack-and-leak was an attempt by the Kremlin to influence UK elections. This charge was vehemently denied by Moscow. Thomas Rid said, "If the leak has newsworthy detail, then it is also newsworthy to point out that the material comes from an adversarial intelligence agency, especially in a time of war."

New Ransomware Emerges
VMWARE ESXi SERVERS UNDER ATTACK

A new ransomware has announced its arrival with an attack on VMware ESXi servers which are known to be vulnerable. The malware is popularly known as 'Cheers.' This is not the first time the enterprise class, type-1 hypervisor has experienced an attack. There were several in the past, the most recent being those launched by LockBit and Hive. VMware ESXi is not a software application running on an operating system, it is actually a virtualization platform that runs on bare metal and includes its own kernel. According to the website of the makers, 'VMware ESXi enables you to:

- Consolidate hardware for higher capacity utilization.
- Increase performance for a competitive edge.
- Streamline IT administration through centralized management.
- Reduce CapEx and OpEx.
- Minimize hardware resources needed to run the hypervisor, meaning greater efficiency.'

Large organizations use this hypervisor that installs easily on any server and partitions it into multiple virtual machines. The platform had its beginnings as VMware ESX which was essentially a Linux kernel. It had the ability to load specialized virtualization components including ESX, commonly known as vmkernel. VMware stopped making ESX after version 4.1 and replaced it with ESXi which does no use the vmkernel at all.

The threat actors prepare to launch the encryptor once they succeed in compromising the ESXi platform. The encryptor automatically counts the running virtual machines and shuts them down by executing an esxcli code. The encryption uses a pair of public and private keys to generate a secret cipher key which is later embedded in encrypted files. Further ahead, the private key that is used to generate a secret key is deleted from the cache to prevent recovery of data.

The ransomware also creates ransom notes while looking for files to encrypt. These notes are then stored in each folder. These notes carry information on tasks performed on victim's files and links to sites that display tor data leaks and ransom negotiation details. Every victim has a unique tor link for ransom negotiation.

Researchers at Bleeping Computers have carried out some studies to observe cheerscrypt ransomware operations. The leak site so far revealed only four victims and it has pointed to facts that are obvious to anyone in the business of cybersecurity. Here are some that are readily noticeable:

- Cheerscrypt ransomware is using double-extortion tactic to victimize a number of companies who are under their radar.
- The very existence of the leak site points to the fact that the ransomware is carrying out data exfiltration and using stolen data.
- The victims belong to semi-large size organizations, and it seems that the ransomware group prefers to hit companies that are in a position to pay comparatively larger ransom demands.

- If victims deny paying the ransom, the attackers claim to sell the stolen data to other threat actors. If nobody shows interest in buying the data, it gets posted on the leak portal.
- Each encrypted file has a '.Cheers' extension, however, files are renamed before encryption. If access permission is denied for renaming a file, the encryption fails yet the file is renamed.
- The encryption uses a pair of public and private keys to derive a secret key, which is added to each encrypted file. The private key used for generating the secret key is deleted to stop recovery.
- The ransom notes have revealed that the threat actors allow only three days to the victim organization to negotiate and reach a figure for payment as ransom. The ransom note comes with a threat that if the amount is not paid within the allotted time, the data would be sold to others who may further exploit to serve themselves. In case the second option too does not meet with success, the threat actors warn of putting up the data on dark web for everyone to see and serve their own ulterior motives.
- VMware ESXi is a virtualization platform used by large to semi-large organizations. Any malfunctioning or breach can mean large scale damage or disruption of operations. That is why it is attractive for threat actors. Organizations, therefore, should adopt a proactive approach and strengthen their cybersecurity defenses against ransomware attacks.

IAM AND PAM

CHALLENGES AND TRENDS

Cybersecurity is a continuously evolving profession. Just when you begin to think enough has been done for data security, a totally unexpected situation arises forcing you to think twice. Gartner's 2022 Summit recently held in Las Vegas was motivated by this common notion. The theme at work was that the best time to determine strategies for next generation of software is now.

The subjects that were discussed at the summit were many but invariably all of them related in one way or another to the main focus of IAM and PAM programs.
Although, IAM and PAM are used interchangeably, the former is a broader term encompassing activities related to access management. PAM, on the other hand, is a subset of IAM. Here, some users, like the IT administrators, get privileged identities allowing them to access data of critical and sensitive nature.

IAM. Identity Access and Management (IAM) is a term for the process of identifying people—or machines—who are given the right of access to specific resources maintained in an organization's database. Mostly, IAM concerns identities of human users, usually employees and customers who login to access services and products displayed online.

TRENDS. The Gartner's 2022 summit focusing on IAM strategies has emphasized one fact very clearly that the time to rethink about strategies, solving problems and management has arrived.

MACHINE IDENTITIES. Many companies are going through a transition period. They are revamping identity management to make use of machine identities as a key strategic move. This marks a significant shift from former ways of thinking and operational methods. The trend now is to move away from technical and security centric strategy to the broader application of IAM systems. The inclusion of machine identities is a radical change in treating the issue with the next generation of IAM strategy.

IDENTITY FIRST. Although identity is of fundamental importance to security matters, but the Gartner's Summit has emphasized that post-pandemic, identity now occupies the central position in the scheme of things including security infrastructure.

Some researchers even believe that the next generation of IAM strategy will not only concern itself with issuing identities but protecting them and their infrastructure against cyber attacks. The inference from this fact is that the trend will be marked by even greater focus on entire identity lifecycle in order to ensure protection at every stage.

IAM CONVERGENCE. As opposed to a choice between 'best' and 'one-size-fits-all' approaches, the teams managing the IAM strategies now adopt 'best in suite' approach. This new trend was made possible by convergence in the capabilities of different IAM tools. That is not the end of the road. There is room for more improvements and professionals are focusing on coordination between platforms and continued convergence.

CENTRALIZED DECENTRALIZED SECURITY. A new concept has evolved in recent years that IAM teams and security should go with centralized controls and decentralized enforcements of regulations. When this concept is executed in a proper order, it results in Cybersecurity Mesh Architecture (CSMA).

CeDeSec evolved with the realization that in a decentralized IT structure, teams require a single point from where they can exercise control. At the same time, the system can allow teams to use the tools and workflows suitable for their operational needs.
The Summit has observed that CeDeSec is easily attainable because security teams are already good at maintaining visibility and management across a variety of tools.

JUST IN TIME. The new order is Just in Time (JIT) access brokering. In this process, certificates are still used for authentication of users but every time the users log in a new certificate is issued. Since the certificate is lasts for a short period of time and often it is valid for only a single use, the chance of compromising the credentials is minimized.

Although this IAM strategy is a hugely effective security protocol, it requires a very efficient highly scalable system to for issuing and de-provisioning the identities once they have been utilized.

WORKING GROUPS. The latest trend is organizations are fast moving away from Crypto Centers of Excellence. And they are adopting machine identity working groups instead.

There are two key factors behind this shift. Crypto is no longer an IT term because the word is used for digital currency which has gained a wider following. The second reason is the idea that one team can manage everything related to CCoE is too unrealistic.

The common realization nowadays is for organizations to have cross-functional working groups which are suitably represented and participated by stakeholders from IAM, Security Teams, DevOps, Infrastructure and Operations, and Cloud Teams. Bringing these teams together on regular basis not only extends responsibility of machine identities but also helps in formulating newer and more effective strategies.

PAM. In contrast, PAM or Privileged Access Management relates to the technology that secures, controls and monitors access to sensitive data. PAM manages human and non-human accounts that require access to critical data. PAM includes activities like shared access password management, vendor privileged access management (VPAM), privileged session management and application access management.

A CLOSER LOOK AT PAM.
Hackers usually target privileged user accounts since they have exclusive access rights to private information besides the ability to change settings as required by the organization's conditions. If hackers succeed in compromising such accounts, they can inflict huge losses to organizational operations.

In return, they can make a lot of money by demanding ransoms to restore stolen data.

PAM is of critical significance because privileged accounts are surrounded by risks. A cyber criminal has his eyes fixed on privileged accounts: compromising an ordinary user account would only provide information of that particular user but compromising a privileged account gives the hacker a world of opportunities. It is like a jackpot. The hacker will not only have far greater access to an organization's sensitive data, he will also gain the ability to destroy the system.

PAM not only provides protection and defensive capabilities in an event of attack but it also provides solutions to malicious bugs caused inadvertently by organization's employees.

PAM is a key player in enforcing compliance with regulations. With PAM in full operational mode, organizations can record and log every activity related to sensitive information. This facilitates safety of infrastructures and sensitive corporate data which helps in simplifying audit and compliance requirements.

PAM also gathers and securely stores details of privileged accounts commonly referred to in technical terms as system administrator accounts. This special treatment is intended to reduce the risk of theft and misuse. Some platforms go further ahead and do not allow administrators to use passwords generated by their own discretion. Instead, the password manger of the PAM platform allots the passwords for a day or one-time password for the employee to log in for a given period of time.

PAM systems help organizations monitor the network and give an idea about the users who access the organization's sensitive data. It is one of the best ways for an organization to protect against threats. The threats are usually those of stealthy infiltration which can mean access and damage to sensitive corporate information. The access is often gained through privileged internal accounts.

CHALLENGES. PAM systems present an array of challenges during implementation and monitoring. Good organizations are cognizant of these challenges and they take care to manage them effectively by adopting best practices.

ACCOUNT CREDENTIALS. Making use of manual administrative processes remained a common practice. For instance the function to rotate and update privileged credentials is an inefficient and expensive process because it was prone to error.

TRACKING ACTIVITY. Some organizations, for unknown reasons, do not track and monitor privileged accounts' activity from a central point. The absence of monitoring often results in compliance violations which ultimately lead to a greater cybersecurity threat index.

ANALYZING ACTIVITY. A substantial number of companies do not analyze threats. They can't tell routine and normal activity from suspicious and damaging one. This situation alone is responsible for the failure in reducing occurrence of incidents.

CONTROLLING ACCESS. Some degree of difficulty has been seen in controlling privileges access control to cloud computing platforms. This has created operational snags and often exposes the organization to all kinds of threats.

BALANCING ACTIVITY. While implementing PAM tools, cybersecurity professionals should strike a balance between high security and ease of use. If the admins are not able to create accounts, revoke access or handle urgent situations with ease then the security is not in safe mode. Organizations should meet this challenge proactively and with determination.

Cybersecurity professionals have come to the conclusion that to achieve highest level of security, organizations should implement both 'identity access management' and 'privileged access management.' IAM systems cover large attack surfaces whereas PAM systems cover smaller surfaces. But PAM surface is more valued because it offers a chance to infiltrate and steal sensitive information. In any case, better organizations understand the fact and take steps to make sure that the security strategy they have adopted is fairly safe if not entirely impregnable.

ChromeLoader Malware Hijacking Users' Browsers

EXPERTS WARN OF A SURGE IN ITS ACTIVITY

A malvertising danger is seeing another flood in movement since its development recently.
Named ChromeLoader, the malware is an "unavoidable and relentless program ruffian that changes its victim's program settings and sidetracks client traffic to promotion sites," Aedan Russell of Red Canary said in another report.

ChromeLoader is a rebel Chrome program expansion and is regularly circulated as ISO documents through pay-per-introduce destinations and goaded virtual entertainment posts that publicize QR codes to broke computer games and pilfered motion pictures.
While it basically works by seizing client search inquiries to Google, Yahoo, and Bing and diverting traffic to a publicizing site, it's likewise eminent for its utilization of PowerShell to infuse itself into the program and get the augmentation added.

The malware, otherwise called Choziosi Loader, was first reported by G DATA before this February.
"For the present the main design is getting income by means of spontaneous promotions and web crawler seizing," G DATA's Karsten Hahn said. "Be that as it may, loaders frequently don't adhere to one payload over the long haul and malware creators work on their activities after some time."

One more stunt at ChromeLoader's disposal is its capacity to divert casualties from the Chrome augmentations page ("chrome://expansions") would it be a good idea for them they endeavor to eliminate the extra.

Besides, specialists have recognized a macOS rendition of the malware that neutralizes both Chrome and Safari programs, really transforming ChromeLoader into a cross-stage danger.

"Whenever applied to a higher-influence danger — like a certification gatherer or spyware — this PowerShell conduct could help malware gain an underlying traction and go undetected prior to performing all the more unmistakably vindictive movement, such as exfiltrating information from a client's program meetings," Russell noted.

DIGINFO®

TRUSTED LEADER IN CYBER SECURITY

FIREWALLS DON'T PROVIDE 100% SECURITY

Beware of email attachments and links.
Don't post personal information.
Always check privacy settings.

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

dgmagazine.diginfo.net

DG MAGAZINE

The Ultimate Source of Cyber World

A Product of DIGINFO®

Amber Estate, Main Shahrah-e-Faisal, Near Baloch Colony Flyover, Karachi 75350, Sindh, Pakistan. Tel No. +92-21-34325505, **Email : info@diginfo.net**