A Product of DIGINFO®

CYBER MAGAZINE

Volume 4 I 2022

DG MAGAZINE

The Ultimate Source of Cyber World

ATOMIC FACILITIES HEART OF NATION'S DEFENSE

CHALLENGES AND TRENDS
FOR SECURITY PROFESSIONALS

Ukraine calls for volunteers
to protect critical infrastructure

Is Cybersecurity
A Business Enabler or A Hindrance?

Samsung Hit By Flawed
Hardware Encryption

CONTENTS

FROM THE EDITOR

Dr. Ashfaq A. Mailk
Chief Editor

You are holding the fourth volume of DG Magazine. Already you might have noticed a significant change in its look. After toiling with three volumes, we went back to the design boards and revisited the page layouts. You might agree that the overall look and feel has improved. In a survey we carried out before actually adopting the fresh new look, we asked several people from different strata and a majority of them liked to read from present layouts.

In matters of content, we have adhered to our principled strategy. Simple language, authentic material backed by research, and enduring stuff. The topics we select are current and relevant to the industry. After studying the issue from cover to cover, our readers have been known to eagerly wait for our next feed.

As before, your favourite magazine is packed with informative articles on a variety of technical subjects. Besides these, you will also get to know a lot about what is happening around the world from our news reports—gathered and selected carefully. In particular, you will find substantial coverage on the events following the Russia-Ukraine conflict. On top of these, the entire magazine would be a visual treat as well.

Our next volume will be out pretty soon with all the regular features and several interesting additions. Until then, enjoy these pages.

EDITORIAL BOARD

Muhammad Saeed

Head of Editorial Board

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

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

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

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

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

Dr. Ashfaq Malik

Chief Editor / Member Editorial Board

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

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

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

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

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

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

Shahzad Saleem

Member Editorial Board

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

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

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

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

Adnan Masood
Member Editorial Board

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

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

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

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

Irfan Nabi
Member Editorial Board

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

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

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

CREDENTIALS

EDITORIAL

PRINCIPAL & FEATURE WRITER
Hamed Mohiuddin

ARTICLE 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 forward. Printed version is also issued every month.

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.

ATOMIC FACILITIES

HEART OF NATION'S DEFENSE

The primary objective of a nuclear facility is to provide effective deterrence. Nations do not have to have a common border to exhibit hostility against one another. Nowadays, missile technology has developed to an extent that warheads can be delivered at targets several thousands of kilometers away. Even those nations that do not have any common geographical territory can be in conflict.

The most paradoxical aspect of nuclear facilities is that they are supposed to provide impregnable defense but they need layers upon layers of security protocols to counter threats from internal and external forces. Since widespread destruction and unimaginable catastrophe can ensue as a result of any espionage activity, the security mechanism for nuclear facilities is elaborate and few can dare to break the streams of barriers surrounding nuclear plants.

GOING NUCLEAR

The United States was the country that took the lead to mark the dawn of nuclear age. The first nuclear test was conducted somewhere in New Mexico. The implosion type explosion that occurred on 16th July 1945 was the result of efforts by the Manhattan Project. Only days later, while the World War was still raging, the US chose to drop bombs in Japanese cities of Hiroshima and Nagasaki.

After the war ended, the US conducted a series of nuclear explosions from 1946 to 1958 on Bikini Atoll, a group of islands surrounded by reefs. These historical events were replete with human sufferings when the inhabitants of the islands were forcibly evacuated to other nearby islands. Later on in1970, three families with 100 residents were resettled in the Atoll but researchers working in the area found dangerously high levels of radioactive elements in the area. Seven years later, the inhabitants were carrying abnormally high concentrations of caesium-137 in their bodies. The families were evacuated from the islands three years later.

THE POWER OF DESTRUCTION

This brought to light the fact that nuclear weapons were most potent in terms of destructive power but that is not the end. Their harmful effects extended years beyond the time of explosion. The case of Chernobyl accident in 1985 is a case in point. Chernobyl had to be evacuated soon after the lethal and destructive accident released massive amounts of radioactive material. A National Geographic team visited the city in Ukraine and discovered that the place was teeming with wildlife and vegetation although it was completely deserted. However, unusually high amounts of radioactive deposits were found even after all these years.

Such cases establish the fact beyond a shade of doubt that nuclear weapons are dreadful and can bring suffering and mayhem of a colossal magnitude. But the race for it had already begun after the first explosion came to light. In less than five years, the spies of the then Soviet Union penetrated the top secret US facilities to make their own version of the bomb. The United Kingdom, France and China followed suit in quick succession.

Today, nine countries, including India and Pakistan, are known to possess stockpiles of nuclear warheads. Though Israel possesses several warheads but its weapons grade capability still remains unannounced. There are several other countries that operate nuclear plants for producing energy but a handful of these are surreptitiously pursuing technology advancements for acquiring weapons despite international pressure and threats of sanctions.

TO BE OR NOT TO BE

Nations are no longer independent in making a choice to go nuclear. World opinion counts and often matters in enforcing the will of powerful states. Dissent invariably results in harsh sanctions, boycotts and economic isolation.
The states that took lead in developing the weapon foresaw the situation we are facing in the early years. The United States believed and hoped to maintain a monopoly on the new weapons program for years to come. But the secrets the country so jealously guarded soon went into the hands of the rivals.

Seeing the danger of nuclear proliferation if more countries vigorously followed the nuclear option, the United States together with other powers negotiated for a Nonproliferation Treaty in 1968. Later on, when environment issues became the topic of debates worldwide and scientists started voicing concern at deteriorating condition of the lonely planet, Comprehensive Nuclear Test Ban Treaty was enunciated to discourage tests that are bound to have adverse effect on environment.

A book by Vice President Al Gore, during Clinton's tenure as president of United States, earned rave reviews for the awareness it created about the deteriorating condition and declining health of our planet. 'The Inconvenient Truth' maintains that world powers still possess stockpiles of nuclear weapons which can destroy the planet several times over.. And there are no signs that this mad race will ever cease.

Some countries defied the rules outlined by these treaties in spite of being signatories. Pakistan, India and Israel never signed the NPT and all three possess arsenals of nuclear warheads. Iraq, under the despotic leadership of Saddam Hussein, aspired to develop the unconventional weapons. Iran and Libya too have secretly pursued nuclear ambitions. North Korea has doggedly tolerated world pressure and sanctions to carry out test explosions.

In spite of these occasional examples, the world bodies have recorded more successes than failures to contain and limit nuclear weapons programs.

NUCLEAR PARADOX

Although the world has made strides in communications, transportations and weapons technology, there has been no large scale conflict after the World War. It is a paradox of sorts that an instrument meant for destruction on a large scale has ensured peace and played a pivotal role in avoiding conflicts. The nuclear capability had a stabilizing effect on the relations of super powers. Both sides realize that nuclear capability implies an assured ability to strike back with the same intensity and fire power. This makes prospect of war a very costly and unpopular affair. While human loss and property loss can be easily calculated the loss that is an outcome of unpopular decision is not easily quantifiable.

The fact that any aggression by a country armed with nukes will likely be met with the same lethal and destructive force is enough a reason to exercise restraint. Even those governments who were known to adopt an aggressive stance have mellow and conciliatory tone when it comes to dealing with nuclear strategy. A reckless and irresponsible attitude can mean huge losses and catastrophes.

KERNEL OF DEFENCE

Besides diplomacy and armed forces, nuclear facilities form the third pillar of defense strategy and the most important one. The primary function of nuclear facilities is to provide effective deterrence against potential adversaries.
This role of nuclear facilities is expected to continue but the altering geopolitical landscape and advancements in warfare technology may evolve the position of nuclear assets as the primary player of defense strategy.

Ukraine calls for volunteers to protect critical infrastructure

The country is reportedly asking volunteers to join digital defensive and surveillance missions.

In an unprecedented move, Ukrainian government has called for volunteers with hacking skills to help protect its network and internet infrastructure. On February 24, notices were posted on social media forums inviting volunteers to apply providing details of their skill sets. Based on their expertise, the volunteers would be divided into two groups. One of them would be dedicated to helping the government in safeguarding the country's critical assets. The other group would employ the skills to fight against cyber espionage.

The driving force behind this campaign is Yegor Aushev, the co-founder of Cyber Unit Technologies. Aushev is well-known in Ukraine for his work on promoting ethical hacking. He posted the invitation on the directives of a senior defense ministry official. The post read, "Ukrainian cyber community! It's time to get involved in the cyber defense of our country" and it has elicited a response from all across the country.

On February 23, several government websites experienced power outages because of Distributed Denial of Service (DDoS) attacks. Websites impacted as a result included the Ukrainian Ministry of Internal Affairs, Ministry of Foreign Affairs and Ministry of Defense. The presence of Wiper malware gave clues to who might have perpetrated this hostile attack.

On February 24, the second-largest city, Kharkive's network and telecommunication disruptions left many users without services.

Earlier, in 2015, an attack targeting Ukraine's power grid left countless Kiyiv residents without power supply for at least an hour. Later researches by cyber security experts linked the crime to Russian cyber attackers.

Aushev believes that the new initiative to enlist support of volunteers will be an effective strategy to combat perpetual assaults. The team assigned to work on defensive maneuvers would focus on protecting critical assets including energy, water supplies and other vital installations. The other team, forming a frontline of offense, would aid Ukraine's military in fighting cyber espionage and in monitoring forces hostile to the country.

Official website of Russian Parliament, MoD and Kremlin go offline

Multiple government sites, including one of President Putin, go offline.

NetBlocks, a global watchdog monitoring events related to cybersecurity and cyber attacks, conveyed that many websites of Russian government have gone offline among which is the Kremlin domain – President Vladimir Putin's official website.

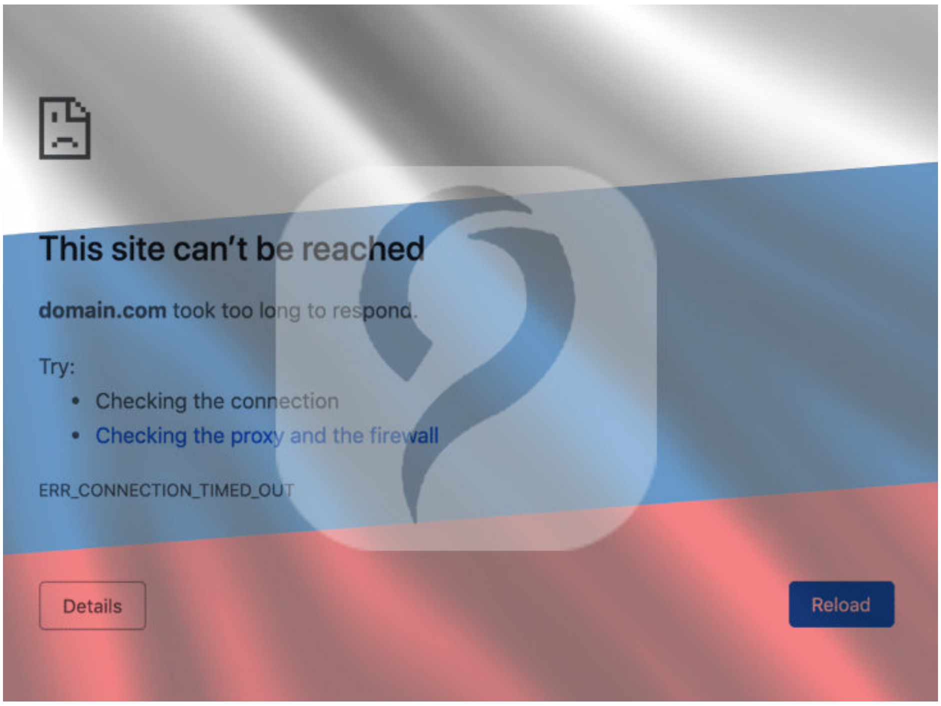
The organization, through a tweet, stated:

Confirmed: Multiple government websites in Russia including the Kremlin and the State Duma have fallen offline; the incident comes amid a spate of cyber attacks targeting neighboring Ukraine.

Besides the Kremlin (kremlin.ru) other websites that are offline include the one of Russian Ministry of Defense, and the official website of the Russian parliament (Duma). It is yet to be known if these sites became the victims of a cyber attack or it was the result of a malfunction. On the other side, it has been confirmed that many websites of Ukraine have been targeted with DDoS attacks together with malicious wiper software.

In a later development, the official website of Duma and Kremlin's domain are back online now but the website of Ministry of Defence is not operational so far.

Hackread.com also confirmed that these websites went off the net soon after the country launched attack on Ukraine. The site informed its users as follows:



This site can't be reached

domain.com took too long to respond.

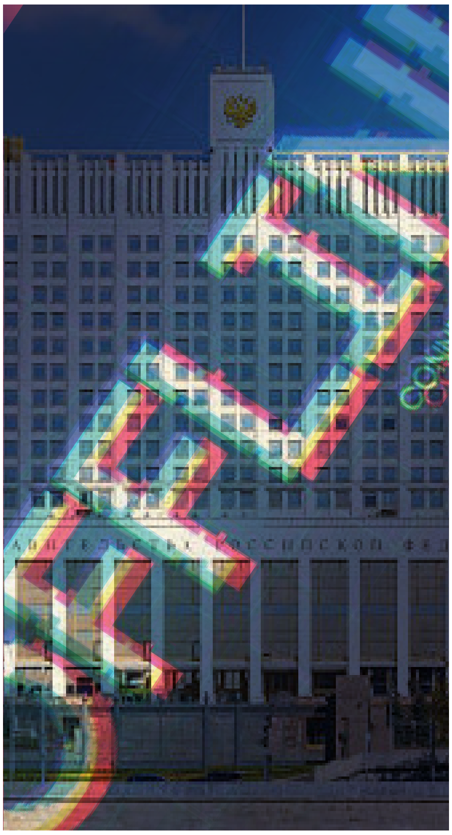
Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_TIMED_OUT

NetBlocks has also reported internet service interruption in Ukraine amid the entrance of Russian troops into the country. Nevertheless, Hackread.com is keeping eye on the situation, and in case or whenever the disrupted sites are back online, we will update this article accordingly.
Update (19:45 Thursday, Feb 24th, UK Time)

The official website of the Kremlin is back online and operating normally. However, the Ministry of Defence and Parliament websites are still down.
Update (19:55 Thursday, Feb 24th, UK Time)



IS CYBER SECURITY A BUSINESS ENABLER OR A HINDRANCE?

Whenever a discourse veers toward cybersecurity, two schools of thought immediately come to mind. There is one which has faith in having an independent and a dedicated cyber security department that keeps a close watch on suspicious activities in and around an organization's systems. And there is another which supports the idea that the entire exercise is needless—an extravagance that unnecessarily stresses an organization's budget.

IMPACT OF CYBER CRIME

The chain of events in the past many years has tipped the balance in favour of the first school. The latter group is fast losing ground. There is an overwhelming reason for this shift in world opinion. Over the years, cyber crime has escalated by leaps and bounds. And there are no signs of slowing down.

Cyber crime has great appeal for hackers. Three key motivators—all irresistible—drive the hackers to get on with their occupation. First, the job involving the task of infiltrating a computer system is fairly easy and the prospect of making money is on the high end. On top of it, there is a comforting feeling that they will not get caught or sentenced. Statistics speak of a very low probability of catching the perpetrators and bringing them to justice. Hackers can operate from anywhere in the world without being noticed or detected.

In spite of the ease the occupation affords, hackers are constantly upgrading their skills and level of sophistication. Researchers say that the technology these criminals employ is at par with that of top information technology companies. Just like their counterparts, the hackers have moved on to adopt cloud computing, artificial intelligence and encryption. By failing to enforce even the most basic precautionary measures at the workplace, businesses and organizations have, in fact, facilitated the criminals to perpetrate the breaches, in quick succession, without any resistance. On the other side, we see efficient employment of technology, automated software creation and monetization of their work.

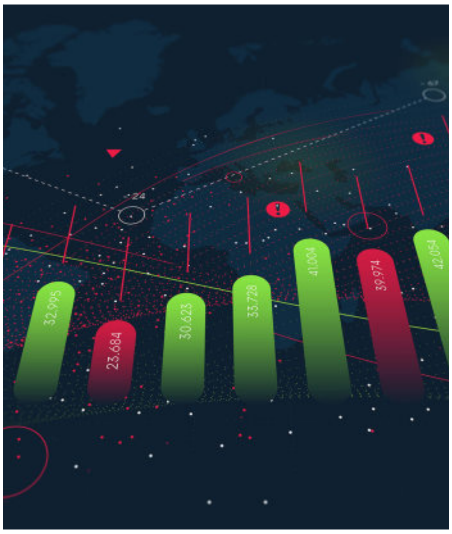
THE COST OF CYBER CRIME

Steve Morgan, Editor-in-Chief of Cyber Crime Magazine, writes, "Cyber crime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm." This is seemingly an endless list but if one takes into account the fact that the list may not be all encompassing, then the magnitude of losses goes far beyond anyone's imagination.

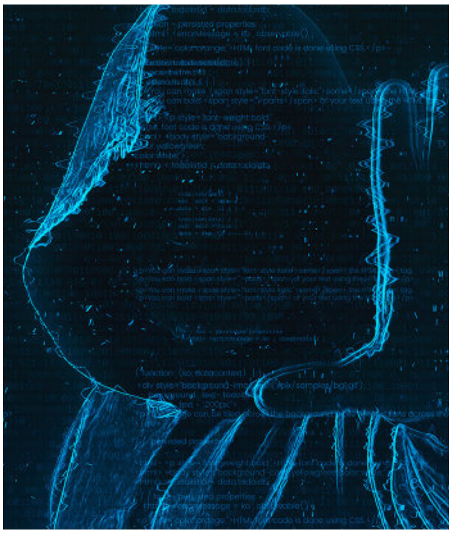
ECONOMIC IMPACT

Mc Afee and The Center for Strategic and International Studies (CSIS) have jointly worked on a research project and presented a report titled: Economic Impact of Cyber Crime—No Slowing Down. The report explores on how cyber incidents impact the economies worldwide. The researchers observed that the scale of crimes has assumed epidemic proportions. A few years back, in 2014, the losses were around $445 billion. Today, the figure has catapulted to $600 billion yearly, which is nearly one percent of global GDP. Only a few countries have GDPs exceeding that huge figure. The rest of the nations around the world contend with a markedly lesser amount.

In spite of that colossal figure, cyber crime ranks as the third most expensive of illegal activities. The first rank goes to government corruption followed closely by narcotics trade. Cyber crime ranks third in dollar value as a global problem incurring huge losses. Coincidentally, cyber crime is also third biggest economy exceeded only by those of United States and China.



SPIRALLING CRIME RATE



In the coming years, cyber crime is expected to grow in an unprecedented way because the hackers have turned their attention toward poorly secured Internet of Things (IoT) devices. They are using the devices to make inroads into sytems. IoT devices themselves are not valuable but since they are not fortified security-wise, they provide easy approach to personal information from where hackers can gain access to networks and sensitive data. Once hackers gain access to the systems through IoT devices, they can easily launch denial of service attacks which open opportunities of ransom earnings.

The use of artificial intelligence was also responsible for the phenomenal growth of crimes. Hackers were able to make use of the tools to create new and sophisticated malware and then identify targets and then move on to the cloud services. Cloud services provided hackers the facility to store malware and launch denial of service attacks from there. What's more, hackers can also search for targets on the cloud surface because businesses and organizations have moved on to cloud services to store a large part of their data including sensitive information. That is bait for criminals.

RESOLVING THE DILEMMA

The increase in cyber crimes is enough a reason to put to rest theories that cybersecurity is a hindrance in the smooth functioning of businesses and organization. If a dedicated staff is not maintained to keep an eye on the ever present threats of intrusions, cyber crime will grow like a snowball hurtling downhill. Having a cyber security department means having a force that is alert and vigilant to the dangers of attack. With CS staff working all the time, companies have a comforting feeling that even in case of an attack, the team will be on ground to contain the damage and do something as a remedy and attempt to recover lost or stolen data.

That leaves us with the only option. A cyber security department which is a team of professionals working round the clock and keeping a watch for any suspicious activity that may harm the system at the organization.

After establishing that cybersecurity is indispensable for a business or organization, we are now in a position to explore about how embedding it to business strategy can mean growth and profitability.

FROM A HINDRANCE TO CORE UNIT

Traditionally, the board members never accorded the importance to cybersecurity that it deserved. It was never considered as a requirement for the company. Instead, it was seen as restrictive and needless. But the events following COVID19 elevated cybersecurity to an indispensable position. The pandemic focing social distancing completely revolutionized the ways of conducting business. The staff were forced to operate remotely and physical offices suddenly turned into virtual hubs where colleagues communicated from their homes and meetings were conducted on apps such as Zoom. Cyber criminals took maximum advantage from the situation and increased the frequency of their attacks. In this scenario, maintaining a cybersecurity department became a necessity. Without an ever vigilant force, it was impossible to prevent and fight constant onslaughts which resulted in data theft and losses to the organization.

In spite of this transformation and change of heart, fewer than 25% of business leaders do no think of cybersecurity as a business enabler. They consider it as a barrier and a hindrance to smooth business routine. But such a stance is risky and exposes the organization to breaches and data loss. In contrast, when cybersecurity forms the core of business strategy, the chances of of bringing value to the enterprise drastically increases. Deep seated security speeds up agile implementations and resilience of operations.

Here are some more aspects that can enhance the value of cybersecurity and give it an attribute of 'Business Enabler.'

CUSTOMER FIRST

Every business relies on a customer base. The company would survive and thrive only when customers are satisfied and they choose remain loyal to the company. The news of cyber attacks and breaches travels fast and spreads just as quickly. It becomes a cause of bruised reputation and shattered confidence.

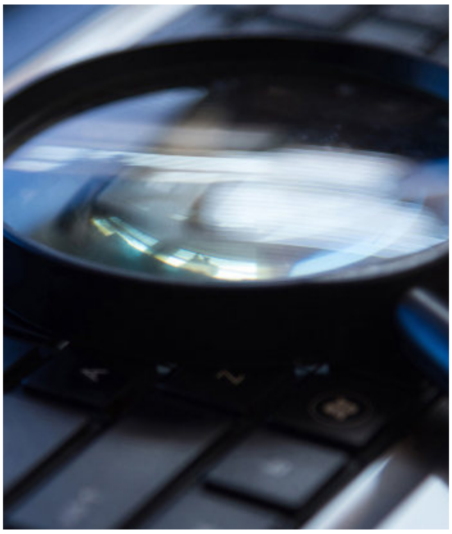
A strong security apparatus, that is both efficient in providing preventive measures and remedial strategy in an event of attack, gains confidence of customers. breaches shatter the confidence of customers and the company can no longer remain reliable. A global survey carried out by Vodafone has revealed that a strong cybersecurity can attract and retain customers which form the basis and strength of a business. According to the survey:

- 89% of businesses believed that customer loyalty and trust depends largely on improved cybersecurity
- 90% of businesses said that cybersecurity ehance business reputation in the market and this attracted customers
- 89% said that improved security acts as a competitive differntiator which helps in winning customers.

SHIFTING THE FOCUS

When companies place greater emphasis on prevention of attacks rather than threat detection and response, a restrictive environment evolves at the workplace. Such a place is not conducive for smart and talented work force to perform at their optimum. Restrictive checks and repetitive procedures hinder and distract employees from focusing on their tasks and give best results generating profits for the company.

The solution to the problem is to place the focus on detection and response instead of prevention. A defensive strategy hinders in creating an open environment essential for budding talent which brings innovation and continuous improvement.



SECURITY AND PRODUCTIVITY

Cyber attacks affect productivity by preventing employees from accessing their own system. A denial of service attack in particular can disrupt the business for a long time. By the time recovery attempts translate into success, huge losses are already on account.
A robust cybersecurity strategy excludes fear of attacks from the operational cycle. For sustainable operations, a dependable security mechanism works like a charm ensuring competitive edge helps in winning customers.

MORE CREDIBILITY, MORE BUSINESS

When a customer establishes contact with a service provider or purchases something from a seller, he reposes trust in the company. Based on that trust, the customer shares personal information assuming it will not be misused or shared with third parties. In case of a cyber attack and probable theft of personal data, all that trust and confidence vanishes in a matter of seconds. Although many companies recover from the aftermath of attack, but they fail to rebuild the confidence and restore the same relationship with the customer. According to a report prepared by PwC, highlighting concerns customers have about their data, 85% of customers won't make a purchase from a business if they have lost trust. Another report by OnePoll says that 86% won't do business with a business that has experienced a breach. The bottomline? More credibility, more trust. And more business.

INNOVATION: CENTRAL TO BUSINESS

E-commerce has opened a new opportunity for small businesses to compete with large businesses on online platforms. Businesses and organizations who have adapted to the new digital age are coming up with innovative products and services which help them in creating a niche for themselves. And to continue in this direction and to stay in business, companies will be bound to use best available technology. In a survey, 69% of c-suite executives thought that digitization is the mainstay of an organization's business strategy. And 64% agreed that cybersecurity is a key factor in ensuring the success of business models.

FINAL WORD

Gone are the days when cybersecurity was relegated to a dark corner of the enterprise. But now professionals and top executives have come to realize that cybersecurity is not only essential for businesses, it is key to its very existence. Times have changed and experience has taught great lessons. One of the lessons today is widely accepted: cybersecurity is a business enabler.

CYBER SECURITY

THREAT INTELLIGENCE

CYBER SECURITY MATTERS.

Focus the threats that matter to your organization

1. Cyber threat intelligence is information about threats and threat actors
2. Preventive measures based on real-time Threat Intelligence is real ROI
3. Cyber controls must be natively integrated to protect end to end
4. Empower your threat response by prioritizing the threats
5. Effective response to incidents depends on powerful threat intelligence echo system

Moscow Stock Exchange Under Attack.

Reports of attacks and counter attacks from the newest battleground.

Early on the morning of February 28, the website of Moscow Stock Exchange went down. As shareholders and brokers tried to log in, the website was inaccessible.

Initially, the Central Bank of Russia was reluctant in admitting of an attack but later said that the Moscow Exchange (MOEX) would remain closed on that day because the rouble plummeted to a record low against the dollar. Shares of Russian companies listed in London open market also experienced a downward slide to as much as 75%. Bloomberg reported that depositary receipts for Sberbank of Russia PJSC went down as much as 77%, while Gazprom PJSC dropped 62%. The Ukraine IT Army, a crowd-sourced group of hackers, enjoying support of Kyiv officials, claimed responsibility of the attack although independent observers could not ascertain this claim. The deputy prime minister of Ukraine, Mykhailo Fedorov, who was the guiding force in the formation of the IT Army, commented in a post on facebook in a celebratory tone, "The mission has been accomplished! Thank you!"

Companies like Cloudflare which track and monitor internet traffic around the globe, noticed that the wave of cyber attacks in recent weeks were all directed towards the east. Most of the attacks were targeting entities in Moscow. Cloudflare spokesman said that there was a marked increase in DDoS attacks whose origin could be traced back to Ukraine. He reiterated, "There was a large increase in bot traffic in Ukraine, also. These two things may be related, and cyber attacks remained relatively calm on .ua (Ukraine) domains."

On the same day, that is 28th February, the website of Russia's lender, Sberbank, also went offline. A spokesman for Netblocks, which monitors internet connectivity around the world, told Forbes, "We can confirm the Moscow Exchange is down, but we don't have the visibility into the incident's root cause or the extent of the disruption."

In the aftermath of Russian invasion of Ukraine, the pro west forces imposed sanctions to pressurize Russian economy. And to make matters even more complex for Russia, the IT Army of Ukraine planned a series of attacks on important businesses, government websites, critical assets and state organizations including banks and oil companies. That's why, when Sberbank's website went offline, Fedorov celebrated in euphoric excitement: "Sberbank fell!"

In retaliation of attacks on Russian websites, key Ukrainian government websites and banks were targeted. US and its allies, including Ukraine itself, blamed Russia for these cyber attacks. Recenly Romania offered to provide cyber expertise, threat intelligence and technology support "for as long as it is necessary." Florin Talpes, co-founder and CEO of Bitdefender said, "As proud Romanians and a company of global citizens, we stand with our northern neighbors who bravely fight for their future."

Samsung Hit By Flawed Hardware Encryption

Over 100 million Samsung Galaxy Phones Affected.

A group of scholars from a University of Israel have detailed the almost 'fatal' design flaws affecting about 100 million Android-based Samsung smartphones that could have resulted in the extraction of secret cryptographic keys. The said flaws have since been fixed.

Researchers investigating the cause of the flaws believe that they resulted from cryptographic design and implementation of Android's hardware-backed Keystore. A number of Galaxy brands like the S8, S9, S10, S20 and S21 flagship devices were affected by the flaws.

To gauge the vulnerability of software/applications used in these devices, these are tested in Trusted Execution Environments (TEEs) which are 'closed areas' making available a secluded space. Here, security-related critical operations are checked to ensure confidentiality and integrity of Trusted Applications (TAs).

Together with TEE, Keystore is a hardware-supported system in Android devices, that enables the construction and storage of encryption codes (keys) inside the parameters of TEE, which makes it harder to pick and copied from the device so that the primary operating system is prevented from having straight contact. Rather, the Android Keystore allows connection of Application Programming Interfaces with outside servers in the form of Keymaster TAs to execute within the domain, all cryptographic processes; including protected key creation, their embedding and handling for digital endorsements and encryption.

In Samsung mobile devices, the Keymaster TA runs in a TEE under using ARM TrustZone Technology. But the safety flaws detected in these devices show that an attacker, with fundamental read and write entitlements, can effectively get through to the secure element to have access to the hardware-protected private keys.

The detected issues are listed below :

In view of security researchers' responsible disclosure communicated in May and July of last year, appropriate updates for affected devices were issued accordingly. The detailed report of the flaws will be shared this August at USENIX's symposium on security.

According to the researchers, manufacturers such as Samsung and Qualcomm keep their designs and implementation procedures related to operating systems and TAs strictly confidential. They are of the opinion that such details should go through stringent audit and review process to be carried out by independent researchers and should not follow the hard route of dismantling and revamping of the proprietary systems.

Awais Ejaz
GROUP HEAD

Information Security & Governance at Allied Bank Ltd

FROM THE DESK OF CISO

My name is Awais Ejaz and I am working as a Group Head Information Security & Governance at Allied Bank Ltd. I am looking after Governance, Risk and Compliance pertaining to Information security requirements of the bank. Design, Development and Security Operations of the bank are also important areas of my job responsibility.

I am an active member of the PBA (Pakistan Bank's Association) – Cybersecurity forum and also member of different Information Security Groups.

Previously at ABL, I was heading the Networks & Communications division and was responsible for the overall design, architecture and operations of the Network Infrastructure.

I started my career from SYSNET Pakistan as a Network Engineer looking after the network deployments at HBL and PTCL. Later I joined Cyber Internet Services, an ISP and a DNOP (Data Network Operator) and was responsible for the Network Operations of the Central Punjab region.

I was responsible for setting up WARID's Enterprise data network and security architecture & design. During my stay at Cybernet I was involved in various projects for Network deployments and integrations with Mobilink, Total Parco, Pepsi, Unilever, Coke, Soneri bank, Saudi Pak etc.

Q&A QUESTIONS & ANSWERS

As you are aware that cyber threats are everywhere in the world and nobody or organization is safe, what is your opinion in this regard?

Cyber threats are everywhere and are rapidly increasing around the globe. The cost of cyber crimes has increased to 6 trillion dollars annually making cyber crimes as the world's 3rd largest economy after US and China. The digital transformation around the globe has added to this surge in the cyber crimes. If you look at the global threat landscape, following are the biggest cyber security challenges in 2022:

1- Supply chain attacks are on the rise
2- The cyber pandemic continues
3- Cloud services are a primary target
4- Ransomware attacks are on the rise
5- Mobile devices introduce new security risks
6- The next biggest threats would be arising from the IOTs (Internet of things)

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

In the murky moral universe of hackers, the line between good and evil intentions is often blurred. But the more we understand about the different types of hackers, their motives and their tactics, the better we can prepare for and prevent future attacks. It's true that some hackers are motivated by ethical or activist considerations, while Nation-state backed hacking campaigns on the other hand, aren't motivated by profit. They operate legally in their countries of origin; their purpose is to protect national security interests (including espionage and the propagation of fake news). As such they're often resourced directly by governments. But let's be clear: cyber crime is a vast, multi-billion-dollar industry and businesses need to get a firm grasp on it if they have any hope of preventing future attacks.

Without an effective cybersecurity program, your organization cannot defend itself against data breach campaigns, which makes it an irresistible target for cyber criminal. A lack of focus on cybersecurity can damage your business in a range of ways including:

Economic Costs
Theft of intellectual property, corporate information, disruption in trading and the cost of repairing damaged systems

Reputational Cost
Loss of consumer trust, loss of current and future customers to competitors

Regulatory Costs
GDPR and other data breach laws mean that your organization could suffer from regulatory fines or sanctions as a result of cyber crimes.

What cybersecurity measures have you introduced and implemented in your company?

The defense of any organization against cyber threats depends upon the robustness and effectiveness of their cybersecurity posture which comprise of People, Process and Technology. The bank has implemented a comprehensive layered security posture with controls like Next generation firewalls, Web & Email security gateways at the Perimeter, Controls like Endpoint Protection, Endpoint Detection & Response and File Integrity Manager are at the Endpoints. Database & Applications Security controls including Cloud based Web Application Firewall are also being implemented. Privilege Access management solutions are in place for monitoring and tracking of administrative activities.

Apart from these controls on Information assets, the bank has established 24/7 Security Operations Center for monitoring and management of cybersecurity incidents. The bank is PCI DSS certified for the last 3 years having strong processes and controls over cardholder data. We have recently formulated a cybersecurity awareness program and have plans to conduct this program for our staff and customers through a knowledge-based cloud platform as People is the weakest link in the chain of cybersecurity.

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

Dealing with non-state actors in cyber space is a challenge for states experiencing large-scale cyber attacks launched by such actors. Especially since more and more state actors seem to be hiding behind so-called independently operating non-state actors, it is important to get more clarity on how states could respond to such actors.

To protect the Organization's Information Assets from these Threat Actors, I would again lay emphasis on developing and implementing an effective and layered security posture strengthening your People, Process and Technology.

How do Black Hat Hackers Damage the System?

Black Hat hackers are criminals who break into computer networks with malicious intent. They may also release malware that destroys files, holds computers hostage or steals passwords, credit card numbers and other personal information. These threat actors typically engage in cyber crime operations and use hacking for financial gain, cyber espionage purposes or other malicious motives.

While hacking might have become a major intelligence gathering tool for governments, it's still more common for Black Hats to work alone or with organized criminals for easy money. The WannaCry ransomware released in May 2017 is one example. Within the first two weeks of its release, it infected approximately 400,000 computers in 150 countries. Fortunately, security experts released decryption tools within days of WannaCry's appearance and their fast response time limited extortion payments to about $120,000.

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

The main responsibility of the CISO is to provide maximum visibility to the organization in terms of its threat landscape. This is a continuous process and one cannot be sure about having complete information or visibility to oversee cyber risk.

Here Cyber Threat Intelligence (TI) plays an important part with relevant intelligence to the country and especially the financial sector to manage cyber risk.

Following are some key factors for managing cyber risk effectively:

1. Monitor the risk environment
2. Monitor data assets
3. Implement an incident response plan
4. Gain management support
5. Third Party / vendor Risk Management
6. Build strong external relationships
7. Enforce security protocols
8. Evolve with the technological environment
9. Ensure you comply with the relevant regulations
10. Invest in security awareness

How effective is your cybersecurity strategy at addressing business risks?

While developing cybersecurity strategy for the bank we had two considerations in mind. Firstly, we conducted a gap analysis of what is missing in terms of People, Process and Technology benchmarking international standards and Industry best practices. Secondly, the strategy had to be aligned with our business goals and objectives. Finally, a comprehensive strategy was an outcome both with short-medium term and long-term specific goals.

This whole process ensured that nothing was left out and provided us complete visibility of what was required at addressing business risk. We believe that we have made a rightful strategic plan which is effectively meeting business requirements against security risks.

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

In today's interconnected economy, companies rely on third-parties. It's increasingly common to outsource some parts of your business to vendors who specialize in that function, whether that be via a SaaS vendor, third-party service provider or contractor. These third parties aren't typically under your organization's control and it's 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. Some best practices for third party Risk Management include-

1- Adequate due diligence should be performed during the Vendor Onboarding process.
2- Make a practice of incorporating cyber risk into your Vendor Risk Management Program and vendor contracts.
3- Keep an Inventory of Your In-Use Vendors so as to understand who all your third-parties are and how

much is being shared with each of them.
4- Continuously monitor vendors for security risks by monitoring their security controls overtime.
5- Collaborate with your vendors to reduce risk and fix security issues quickly.
6- Talk about third-party risk by having leadership engagement on both the sides.
7- Cut ties with bad vendors – the ones with poor cyber hygiene.
8- Measure fourth party risk - as important as it is to understand your third-party risk, it's also important to know who your third-parties rely on. These organizations are known as your fourth-party vendors and they introduce fourth-party risk.
9- Follow the principle of least privilege. Many third-party data breaches occur because the third-party is provided with more access than they need to do their job.

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

Yes, we have a Data Governance structure in place and a strategy to minimize cyber risk.

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

Yes, our team is well equipped with the latest cyber technologies and the required certifications. Here i would like to make a point that with high turnover of cybersecurity resources, you need to have a hybrid model which includes your organization's staff combined with vendor outsourcing for relevant skillset and areas. This way you can effectively manage HR needs.
We have staff certifications including CISM, CISA, COBIT, CYSA, CEH, BSMS, SOC Analyst etc.

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

Globally, the continued combined impact of the COVID-19 pandemic, socio-political upheavals and ongoing financial stress is likely to increase the number of careless mistakes that employees make at work, creating more exploitable opportunities for cybercriminals. However, following are the biggest cyber security threats especially in the perspective of Pakistan

- Poor Cyber Hygiene
- Mobile Device Vulnerabilities
- Ransomware
- Poor Data Management
- Inadequate Post-Attack Procedures
- Configuration Mistakes

Recently some of our government organizations have been a victim of cyber attack. We need to considerably improve the cyber health of the government sector.

Following measures should be adopted to counter these cyber threats

Information Security Governance structure should be improved

Timely updatIng of all security systems and software

Conducting regular employee cybersecurity training

Reducing your attack surface by improving security controls

Threat Intelligence feeds relevant to the country

Backup and Recover your Data periodically

Managing Third Party Risk (Vendors)

Protecting your physical premises

Conducting Cyber Drills & Incident handling trainings

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

Banks and other Organizations should develop Information Security Awareness Programs and should conduct Awareness Campaigns to educate their Employees and Customers on regular basis about the latest and evolving threats.

Do we need cyber security insurance?

Yes. We need Cyber Security Insurance. State Bank of Pakistan has also mandated Banks for Cyber Insurance.

What do you think that people of Pakistan are well informed about cybersecurity and threats …if they are not well informed please advise ?

Cybersecurity is evolving in Pakistan. Cyber-attacks and Digital Frauds are also on the rise as digital transformation is taking place in the country especially in the last two

years of the COVID Pandemic.
I think people are not well informed about cyber threats as they should be. I believe mass level security awareness campaigns and programs should be conducted through Social, Print & Electronic media to provide awareness to the people.

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

Some best practices that can be followed to avoid cyber mishappening..

1. Keep your software and systems updated
2. Implement security controls like firewalls etc.
3. Make regular data backups
4. Activate multi-factor authentication
5. Ensure endpoint protection
6. Get appropriate cybersecurity knowledge
7. Control access to your systems
8. Create strong passwords and change them regularly
9. Secure your network devices and wireless connections (wifi)
10. Train your staff

FROM THE DESK OF
CISO

CHALLENGES AND TRENDS

FOR SECURITY PROFESSIONALS

Cybersecurity is an ever-changing landscape. New technologies and newer ways of handling emerging problems are constantly on the rise. With the wider application of Internet of Things(IoT) devices on global level and ever-increasing use of 5G technology, businesses all across the world are bracing to enhance their infrastructure. Another area they are focusing on relates to providing adequate training to all important decision makers of the organization.

With the passage of time, technology has taken a leap. The benefit of this enhancement has gone not only to the security professionals but also to malicious threat actors who create all the problems. The active involvement of these cyber criminals, who are now smarter and more knowledgeable than before, has made cybersecurity more of a complex nature. It is high time, therefore, to enforce strict measures against cyber crimes. This can be done in two ways and both are indispensable. First, proper measures should be installed to protect assets of the organization. Second, training should be given to all the workers to operate safely by remaining in combat mode all the time. They should be ready to respond to any threat in the shape of a cyber attack in a swift and befitting manner.

Cybersecurity Challenges

Here are a few challenges that affected the cybersecurity industry in 2021 and thereafter until recently

1. Remote Operations

The recent events brought on by the Covid pandemic have altered the way businesses operate. A large number of organizations has adopted work models that accommodate remote workforce. There is a constant increase in that number which is escalating the risk for cybersecurity.

It is plain to understand that security protocols can be enforced at a traditional office setting. But guaranteeing protection for remotely placed employees is not an ordinary task. It is a challenge because home based networks increase the chances of security breaches. The lack of control by a centralized authority is the key reason for distributed work environments.

2. 5G Challenge

Quite a few organizations and industries looked forward to the benefits the new 5G technology would bring. From cell phone companies to process industries, manufacturing plants to service based setups, every organization expected speed, responsiveness and enhanced operational efficiency.

But every new technology and every new application comes with a drawback. There are unknown risks and the nature of risks would only be revealed over a period of time when it has been used and tested on a large scale. At the same time, cybersecurity professionals need to be on guard and in a state of vigil. The potential threats can be unexpected and unfamiliar. Knowing how to handle can consume time and a lot of improvisation.

3. Phishing Attacks

Although phishing is one of the earliest, if not the earliest, forms of attacks, it still is a threat that cannot be ignored or downplayed. A spike in phishing attacks was noticed in the last quarter of 2021 coinciding with the Covid vaccine campaign.

Reports were circulating all around the world that fake vaccination emails are being sent out in bulk and online users are constantly being trapped as a result. This turned out to be a challenge for cybersecurity professionals.

Training employees to identify phishing attacks is apparently the most effective strategy to beat the crime, although enforcing access control also works well even when employees are working remotely.

4. Blockchain and Cryptocurrency

There is a growing acceptance for digital currency these days. Blockchain and cryptocurrency are growing rapidly and attracting a wide following. Transactions running into billions of dollars are routinely being done. Reputable companies like PriceWaterhouse Cooper have endorsed such transactions.

But since these modes of money exchange are based on digital technology, care has to be taken to make the transactions safe. Naturally some strict cybersecurity measures have to be adopted to protect people from identity theft, security breaches and several other threats. People dealing in such exchange of currency are careful to guard and protect their personal information. Organizations conducting such business should invest a decent amount to upgrade their IT infrastructure which would be of immense help in any event of cyber attack.

5. Internet of Things (IoT)

One of the latest in the fast developing IT industry is 'Internet of Things' which is essentially an interconnection of appliances via sensors that communicate.

The fascination for automation that has assumed epidemic proportions gave rise to connected devices which provide convenience and intelligent solutions to common everyday problems. But the presence of such devices inevitably means transmission and exchange of more data. As more data flows between devices, gaps form which allow cyber criminals to make an intrusion.

There is legislation that provides guidelines of use and protection for IoT devices, companies still need to invest a sizable amount to develop and maintain a minimal cybersecurity infrastructure and a dedicated work force to combat breaches. The Internet of Things cybersecurity act of 2020 may not be enough to provide foolproof security, but it is certainly the first step toward a more elaborate solution.
cybersecurity experts have outlined a number of other challenges confronting data and data management. The five above provide a good starting point for companies that really wish to provide a safe and secure work environment, free of snags and unexpected closures.

Cybersecurity Trends

Here are some trends that are commonly witnessed in the cybersecurity area.

Remote working

cybersecurity risks

The sudden and unexpected spread of Covid-19, acquiring the status of pandemic, has forced most organizations to redefine how they operate and conduct their day-to-day affairs. Most of the organizations have opted for a distributed workforce, operating from remote locations—often their homes.

In 2021, working remotely rated as the most discussed topic. It is a trend that demands new protocols and new guidelines for effective security because remote working poses new cybersecurity risks. Homes and outstations are far less secure as compared to centralized offices where all employees reach to perform their daily tasks. Centrlized offices are often protected by firewalls, routers and access restrictions. On top of these dedicated IT teams constantly monitor and look for any suspicious activity. A home environment is ill equipped to counter the sophisticated approach of cyber criminals who find it easy to make inroads from gaps created by a distributed workforce.

The trend that was seen in 2021 continues beyond that year. Organizations are now finding ways to face the challenges of distributed workforce. This entails identifying vulnerabilities and adhering to strict security protocols. Plus, guaranteeing documentation and monitoring.

Blockchain and Crypto currency

Blockchain and cryptocurrency are relatively new forms of wealth exchange. Although this mode of exchange has found wide acceptance generating business worth billions of, cyber criminals continue to target the activity generated by the trade. In this area, ransomware and malicious crypto mining are fairly common and businesses will continue to lose their money because of the transient nature of cryptocurrency and the raw state of security associated with it. Until proper regulations are ensured, cyber criminals will take advantage of the vulnerabilities and spread malicious crypto software like the Lemon Duck and MrbMiner which can incur huge damages by driving costs for pay-per-compute-time cloud services. In 2021, criminals racked up more than 406 million dollars in ransom as a result of attacks on cryptocurrency. With attacks in such magnitude, it is easy to see that cryptocurrencies and cyber criminals are closely linked.

The volatile value of cryptocurrency will continue to spur cyber crime involving the acquisition of cryptocurrency, not only ransomware but also with malicious crypto mining. Every time new server-side security vulnerabilities appear, threat actors take advantage of them to spread surreptitious crypto miner software to as many machines as possible and exploits capable of delivering those attacks persist in the wild indefinitely.

To prevent crypto miners from planting their feet in the network, organizations need to put in place a potent defense mechanism like MFA together with virtual local area network to segregate network segments. By adopting these measures, the security teams would effectively restrict the paths that will allow external and unauthorized persons to enter the company network from public internet facilities.

The Evolving Trend of 'Internet of Things (IoT)'

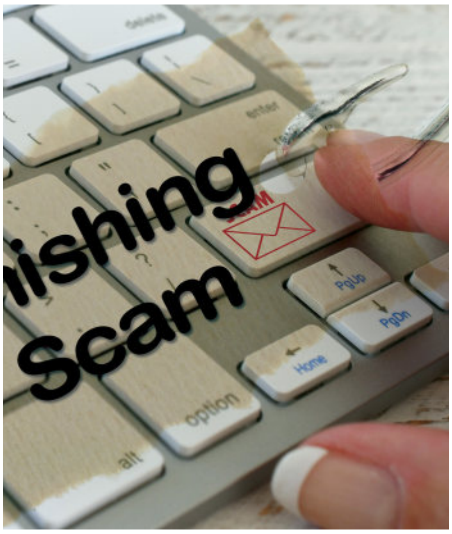
The constantly rising use of 'Internet of Things (IoT)' is creating new opportunities for cyber criminals. The 'Internet of Things' are actually physical devices besides than computers, servers and phones which are interconnected through the web. Smart devices like referigerators, wearable fitness trackers, , watches, appliances, voice assistants like Google Home and Amazon Echo all constitute IoT devices.

According to some estimates, more than 60 billion IoT devices will be running five years from now. This huge number will spawn a jungle of traffic. Cyber criminals who are always on prowl will be ready to pounce on any gap that they can find. Needless to say, it is easy to find a gap when the traffic is so dense and the magnitude so large. Moreover, IoT devices offer a number of potential entry points for criminals. As opposed to other devices like the laptops and mobile phones, IoT devices do not have processing or storage capabilities, which make it impossible to deploy firewalls, antivirus or other security apps. These are reasons that have elevated IoT to the status of 'one of the most discussed trends' of our times in the cybersecurity domain.

Phishing

Years earlier, it was fairly easy to identify a phishing message with its characteristic faulty language, plethora of typos and tall claims. But now, threat actors seem to invest some dollars on improving on their past mistakes to look more refined and believable. Phishing messages now direct their victims to link addresses which are marked as https:// which create a false sense of trust to make them appear as authentic. Sometimes, the messages are personalized and talk of specific details. Often, unsuspecting victims click those links to open the gates for the malicious actors.

The security team working in an organization should train the employees to recognize phishing emails. The common employee, after adequate training should have enough skill to tell the difference between what is safe and what is harmful.



A New Addition to Vulnerabilities Catalog

Microsoft's Email Platform, Zimbra, Under Stress.

If there can be a blood bank or a cryobank, then it makes sense to also have a bug bank. The US based Cybersecurity and Infrastructure Security Agency (CISA) is one such organization—a kind of repository where computer bugs, that can infect and damage systems, are catalogued and profiled.

The Known Exploited Vulnerabilities Catalog of US Cybersecurity and Infrastructure Security Agency (CISA) has been updated with the addition of newly discovered Zimbra bug zero-day flaw that was identified recently in the platform of Zimbra email.

The bug is classified as a cross-site scripting vulnerability that attacks open source e-mail platform. The bug, named as CVE-2022-24682 (CVSS score: 6.1), relates to the Calendar feature in Zimbra Collaboration Suite. Attackers use the feature to plant their malware by tricking users to download arbitrary JavaScript code. Just when the users unwittingly click the link, the malware takes control and the system launches itself on a disaster course.Zimbra's Versions 8.8..15 and older can get infected with this bug. More than 200,000 organizations over thousand government and financial institutions use the Zimbra's e-mail platform.

The Known Exploited Vulnerabilities Catalog is a repository of security flaws that are reported to have been exploited by online criminals in cyber-attacks. Federal Civilian Executive Branch (FCEB) agencies require all organizations that run and maintain a sizable system to patch these so that in case of any incident, the damage to systems can be fixed. In accordance with the Binding Operational Directive (BOD)22-01, once the flaw is added to the catalog, the agencies are required to address the recent vulnerabilities within two weeks.

Over 300 vulnerabilities were listed when CISA announced the Known Exploited Vulnerabilities Catalog. Another 50 have been added later on. The vulnerability was first discovered recently in early February by Volexity. Researchers, on a routine surveillance mission, identified a salvo of spear-phishing activity aimed at government and media bodies certain European countries. The attackers were leveraging the Zimbra bug to illegally gain access to mailboxes in order to infect the systems with the malware.

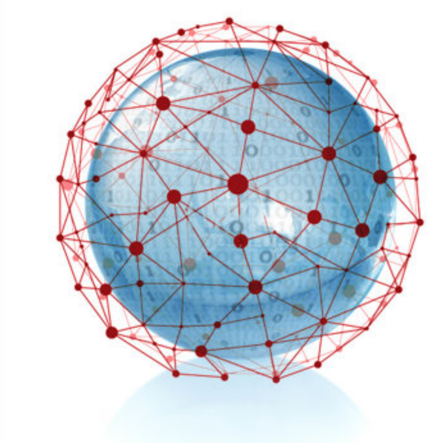
Researchers at Volexity believe that the attacker is operating under moniker 'TEMP_HERETIC.' The attacks are directed toward the open source edition of Zimbra's Versions 8.8.15 or older. Zimbra has launched a hotfix (Version 8.8.15 P30) to address the flaw.
This vulnerability has been identified with its technical code: CVE 2022-24682. CISA has added three more vulnerabilities to the catalog. All these vulnerabilities are specific to Microsoft programs. The codes and mode of action are listed here:
CVE-2017-8570 (CVSS score: 7.8) –Microsoft Office Remote Code Execution Vulnerability
CVE-2017-0222 (CVSS score: 7.5) – Microsoft Internet Explorer Memory Corruption Vulnerability
CVE-2014 -6352 (CVSS score: N/A) –Microsoft Windows Code Injection Vulnerability

DG ACADEMY®

SECURE YOUR FUTURE

PROFESSIONAL TRAINING & CERTIFICATIONS IN CYBERSECURITY AND INFORMATION TECHNOLOGY

DG ACADEMY aspires to be an educational leader in information technology especially in upcoming challenges of cybersecurity. With an infrastructure of this kind on our side, we hope to mold our students of today to become cyber security leaders of tomorrow.



DG ACADEMY CYBER SECURITY PROFESSIONAL PROGRAMS

- «DG Cyber Defence» ‹Zero to Hero› Training Program
- Training Program for Academic Institute and Cyber Professionals
- Training Program for School Kids
- Training Program for Industrial Cyber Security Professional
- Training Program for Cyber Security Management – (Role based Program)
- Training Program for Telecommunication Professional

We would love to help you secure your FUTURE Reach us at:

dgacademy.diginfo.net

SCAN ME

APPLICATION SIGNATURE

TECHNOLOGIES & TECHNIQUES

Ever since cyber crimes gained momentum, cybersecurity found a new and significant role to play in society. Not far back in time, the decision makers and policy writers gave scant importance to this area of information technology. But the viciousness of attacks and soaring costs of handling breaches forced everyone to go back to the drawing boards and redefine priorities.

Nowadays, cybersecurity is central to business and organizational activities. Thanks to the dependence on computer systems and internet for data storage, information exchange and communications.

Just as large and small department stores allocate a certain percentage for shoplifting losses, in spite of all the precautionary steps they take, like surveillance cameras, monitoring staff and security protocols, similar is the case with businesses and organizations who are bound to make an allowance for breaches and cyber incidents.

Cyber crime is so easy to perpetrate and so lucrative in profits that criminals find it hard to resist. Experts agree that no matter what organizations may do to avert cyber attacks, it is impossible to completely eliminate them. That's why decisions makers have now come to terms with the notion that it is imperative to maintain a regular staff for cybersecurity. That is a near surety to run a business or organization smoothly.

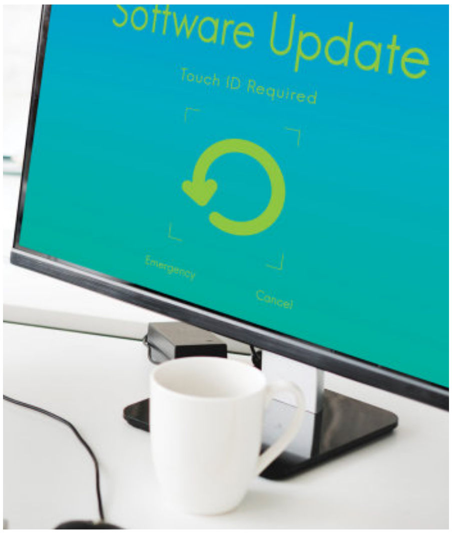
The turf of cybersecurity teams generally consists of devising preventive strategy, undertaking surveillance for suspicious activity and preparing for response in an event of attack.

Cybersecurity staff adopts a number of steps to safeguard their systems and to prevent any suspicious malware from infecting their data. Several protocols are in place and security personnel persistently ask the employees to follow these in order to have a secure workplace.

Cybersecurity protocols are plans and actions designed to offer safety from cyber incidents of all kinds like malicious attacks, breaches, ransomware and other such incidents. To make sure of a safe and snag-free operations, a variety of protocols and software are installed that work together to achieve the objective.

Application signature is one of these protocols. It is a unique pattern-based method of recognition which is used to identify application traffic. The process of identifying makes use of expressions or marks. Application signatures are familiar elements in the security domain. Cybersecurity specialists often make use of them while tracing viruses, worms, malicious content or cyber attacks.

Application signatures allow programmers to identify the author of app. They can also update the applications without having the need to create complex interfaces and permissions. In essence, application signatures are an assurance that one application can access any other application through well-defined IPC.



There is an array of applications like Next Generation Firewalls (NGFW), Network Visibility Appliances and Intrusion Detection and Prevention Systems which is used to identify the applications that are being accessed. This performance is delivered by these next generation software merely by examining network traffic. What's more, these applications can also tell if the browser is using a desktop version or a mobile version of the same app. They can also tell apart one program from another even if they are encrypted.

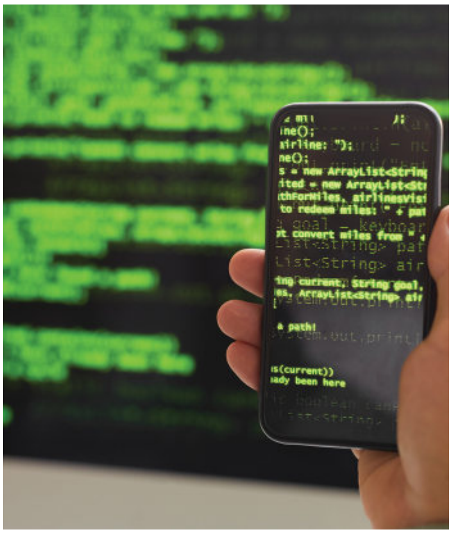
Application signatures are behind all these actions. Most of the time. There are other methods too like fingerprinting, or AI/Machine Learning but they are used alongside static signatures. .

Signatures are not standardized elements. They are generic in nature and are based on well-known codes such as XML, YAML, SNORT and other file formats. They can be static or dynamic. The former implies that they cannot be changed as often as possible. In contrast, dynamic signatures have the ability to learn and they can be created 'on the go.' Inherently, they are patterns or expressions which can be marked against data packets. When the data packets are matched with the signatures, they are labeled as 'matched.' The criteria for matching vary from vendor to vendor and from product to product. But one thing is common to all: most of the time, they rely on values from packet headers and payloads.

Application signatures have the unique ability to identify project files and protect apps on other remote computers. The signatures can have string values ranging from six to ten characters. If identical signatures are used for different apps, they will share same license information on remote devices.

Application signatures are being used widely to deliver a better and more secure environment for businesses and organizations. Their importance can neither be denied nor downplayed. Here are a few points that highlight their importance

Application signatures can be used to activate updates without the need to reenter activation code. In this both the original application and update files should have the same signature.



By using the same signatures for a group of applications on a single systems or remotely connected systems, license information can also be shared. The method enables the operators to activate a group of applications with a single code.

Machine code (MID) depends on application signatures. That's why operators can generate activation codes for protected applications. If a different project is loaded, a message will be reported informing 'MID code decryption error.

Caution should be exercised while changing the encryption key which is actually the Program Value ID. The change should only be done with a corresponding change in application signature, otherwise 'File damaged' error message will be generated.

When two or more applications are protected by same application signature, program ID, then same Site/MID code will be generated.

Businesses and organizations intending to give away free updates for a particular application, then same application signature and project settings should be used as for original application. This tactic will allow the update to unlock automatically.

In cases where updates require payment, application signature should be changed which will generate a different Site/MID code. A different Program ID may also be tried for these updates.

For applications with same application signatures, programmers should use same Program ID (encryption key). If a different key is used for apps sitting on the same computer, one of the apps will be decrypted in an erroneous way displaying 'File Damaged' message because both applications will share same license data and this is the reason one of them will be erroneously decrypted.

Digital assets including data and information need to be protected and safeguarded in the best possible way, given the frequency of cyber incidents and breaches. The management and decision makers are the ones who can take up the challenges and define their priorities. Devising best strategies and making an effort of continuous improvement ensure safe and secure workplace. And, therefore, profitability.

CYBER SECURITY

MAINTAINANCE

CYBER SECURITY MATTERS.

Measuring the Effectiveness of Your Security Controls

1. Cybersecurity Maintenance is to keep my security posture up-to-date throughout the lifecycle.
2. Maintain your Cyber Resiliency Metrics, Measures of Effectiveness and Scoring
3. It’s not about renewal of security control licenses
4. Choose correct benchmarking of your cyber controls

Espionage & Daxin

Chinese-Linked Malware Attacks Multiple Governments

Malware used for espionage activities are fairly different from other types commonly employed in cyber crimes. The capabilities of such malware include optimization for use against targets that are secured. This attribute allows the attackers to penetrate deep into a target's systems and exfiltrate data without even being noticed.

Researchers at Symantec Threat Hunter team have discovered a highly developed piece of malware which has been used in attacks since 2013 at least. They have dubbed this malware as Daxin. There are reasons to believe that it is China-linked. The inference is not based on any direct evidence but on the fact that Daxin is often deployed alongside tools that are known to be associated with Chinese threat actors.

Daxin is a backdoor malware which is capable of installing further malicious software. It can also perform network tunneling, relay across infected nodes, and hijack legitimate TCP/IP connections. Its level of sophistication and longevity is rare for a China-linked malware. Chinese threat actors usually worked on a simple idea: break in, achieve the objective, get out. They never had a tendency to remain under the radar for an extended period of time. Daxin is unique in that respect.

Although researchers at Symantec believe that Daxin has a narrow set of capabilities, it is an incredibly complex piece of code. It performs tasks it is programmed for in a superb manner. For instance, Daxin's ability to communicate is phenomenal. And yet it manages to lie low and stays undetected. It hijacks TCP/IP features by monitoring traffic while closely keeping track of patterns. Once this task is done, it snaps the connection of original recipient. This enables Daxin to perform key exchange in a unique way. And this unorthodox performance lets Daxin to be "both the initiator and the target of a key exchange."

Symantec researchers observe, "This mode of operations allows the malware to avoid firewall rules by hijacking legitimate traffic, and it also minimizes the chance that security teams notice any network anomalies."

Meanwhile, the US Cybersecurity and Infrastructure Security Agency (CISA) has informed that, "Daxin malware is a highly sophisticated rootkit backdoor with complex, stealthy command-and-control (C2) functionality that enables remote actors to communicate with secured devices not connected directly to the internet."

Once Daxin lodges itself in a system, it takes the form of a Windows kernel driver that activates a chain of elaborate communication commands. This action equips the malware with a high degree of stealth and the ability to communicate with other machines not connected to the internet. In short, the malware is recognized for its two key features—stealth and effective communications—besides others. This level of sophistication makes Daxin a very dangerous malware to deal with and nearly impossible to detect.

The researches at Symantec have confirmed that Daxin's technologically advanced code is most suitable for launching long running espionage campaigns. The malware permits the attackers to launch communications and information-gathering operations against a variety of businesses and organizations like telecom, manufacturing and transportation. Evidently, Chinese-linked threat actors would indulge in such activities only to serve strategic interests of their country.

The team investigating Daxin's continuous stealthy and clandestine activities has stated, "Most of the targets appear to be organizations and governments of strategic interest to China."

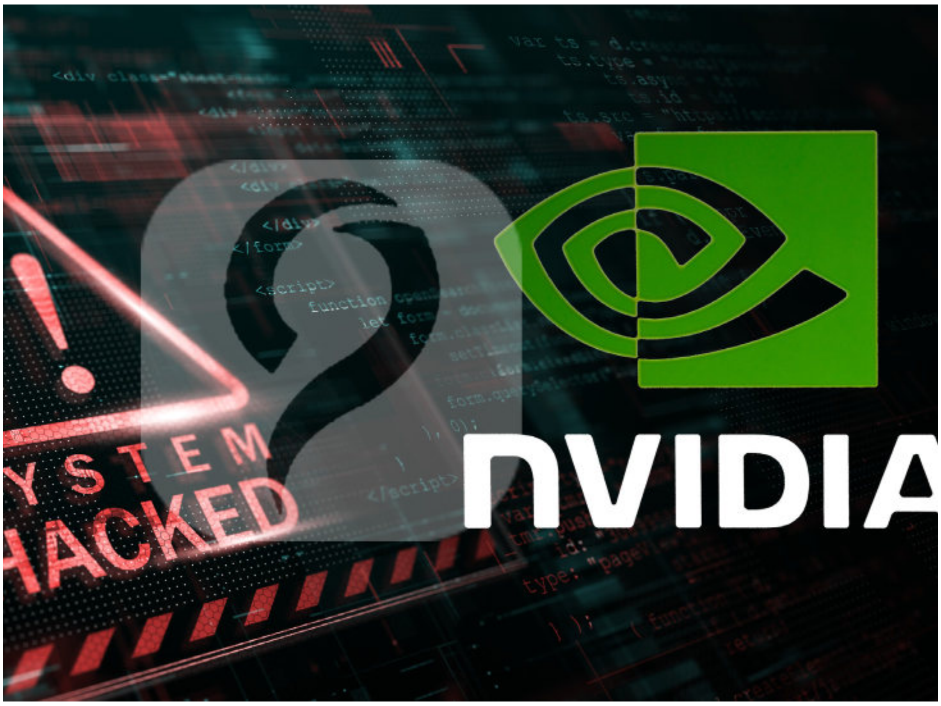
There is no doubt now that Daxin is the most sophisticated piece of malware ever detected by cyber security professionals. That it is capable of staying undetected, while undermining the systems it has infiltrated in, makes it even more dangerous. The researchers will have to work overtime to find an effective counter measure for this elusive code.

Nvidia Vs Lapsus$
A Case of Hacking and Counter Hacking.

Lapsus$ claims to still have a copy of the stolen data.

Ransomware has become a lucrative opportunity for hackers looking around for easy money. Since December last year, a seemingly new group has emerged whose objectives appear hazy. In just a few months, the hackers have recorded successes against a string of high profile companies like Microsoft, Nvidia, Samsung, Vodaphone and Ubisoft. The group likes itself to be known as Lapsus$.

Nvidia is a multi-billion dollar chip manufacturing company known for its GPUs which enhance gaming experience computer simulations. Its net worth, according to Reuters, is over $600 b.



Lapsus$ turned up under the prying eyes of investigators when they claimed to have attacked Brazil's health ministry early last December. The data pertaining to national immunization program went into the control of the group and Lapsus$ was able to demand a hefty ransom to return as much as 1TB of data. Ministry officials, however, employed the services of cyber security experts and retrieved the data and revamped the entire system. The ransom amount was denied.

A couple of months later, Lapsus$ chose to attack chip maker giant, Nvidia. On February 23, the company confirmed that a cyber incident has taken place and that some data relating to proprietary information and employee login has been compromised. The hacker's group started sharing the data openly as the news of breach began to spread. A large cache of 20gb, out of the stolen 1tb, was released online Shortly after learning about the incident, Nvidia promptly took steps to further strengthen their security protocols. In addition, the company engaged cyber security response experts and informed law enforcement agencies to contain the loss and redress bruised reputation.

In a communiqué to Bleeping Computer, Nvidia stated, "We have no evidence of ransomware being deployed on the NVIDIA environment or that this is related to the Russia-Ukraine conflict. However, we are aware that the threat actor took employee credentials and some NVIDIA proprietary information from our systems and has begun leaking it online. Our team is working to analyze that information.
"We do not anticipate any disruption to our business or our ability to serve our customers as a result of the incident…Security is a continuous process that we take very seriously at NVIDIA—and we invest in the protection and quality of our code and products daily."

Four of the researchers investigating the Lapsus$ activity have traced the attacks to a sixteen year old hacker who lives in Oxford with his mother. They believe the teenager is the mastermind behind the attacks.

Another teenager, living in Brazil, is also believed be to be a member of the gang. And there might be several more because at least seven accounts have been discovered that can be tied to Lapsus$ activity. The

Brazilian teen is blazing fast because the researchers tracking Lapsus$ activity were initially inclined to believe that it was automated.

Although money is a central motive of all ransomware groups, the methods employed by Lapsus$ do not support the idea that it is only money they are after. Researchers believe that notoriety is the other urge that drives this particular breed of hackers. One thing is clear, however. The teenagers are clever. They do not leave behind any evidence that would conclusively link them to the activity.

In retaliation Nvidia struck back to retrieve the lost or stolen data. The cybersecurity response team assigned the task to handle the breach, accessed the group's system through virtual machine left behind by Lapsus$ hackers in the device management program. Nvidia experts encrypted the stolen data and cut off Lapsus$ link to Nvidia's network. But Lapsus$ seemed to have another bow to their arsenal when they claimed that they possess copies of the stolen data.

The battle is showing no signs that it will end anytime soon.

WHY ONLY A DEGREE IS NOT ENOUGH TO GET A JOB?

[WHAT ARE THE MOST SOUGHT AFTER SKILLS IN THE MARKET?]

Richard Feynman, the maverick physicist and educator of 20th century, once said, "Never confuse education with intelligence. You can have a PhD and still be an idiot." This pronouncement has over time become a universal truth. Workers with a string of educational accomplishments are nowadays routinely outpaced and outsmarted by others who know how to go about their business. What could be the reason of this poor performance by degree holders? Lack of experience? Or something else?

THE PAPER CHASE

Obtaining a degree is no mean task. It requires investments in various categories. Time, hard work, and dedication. Money, too. Money returns once a person succeeds in getting the degree. That concept is hammered into the brains right from the beginning. All focus, therefore, is on getting hold of that piece of paper. Deeper understanding of the subject and developing of skills take a back seat.

Employers are now reluctant to rely solely on degrees when hiring a prospective candidate although degrees do feature prominently on the list of criteria. In particular, when the degree is not related to the job description and responsibilities, employers tend to look for other merits that can benefit the company as a result of hiring the candidate.

When two prospective candidates are nearly equal in terms of skills and demeanor, a degree plays a key part in tipping the balance in favor of the candidate who possesses it.

EXPERIENCE TELLS

In the mid-nineties, the possession of a degree nearly always guaranteed a job. This situation prevailed for a long time. In recent years, however, the number of students enrolled in degree programs has nearly doubled. That means twice as many candidates are competing for a position as in the final years of past century. A sort of credential inflation has spawned lately. The value of graduates in terms of salaries and perks is in sharp decline as the situation that prevailed for nearly five decades no longer exists. The formula of success that a degree afforded is no longer working.

There are certain things that cannot be taught at schools. Earning a degree, therefore, is not the end of the road. In fact, it is the beginning. Graduates must acquire extra skill, get experience, look out for specialized knowledge that relates to the job description and be alert to the ongoing changes in the market.

The possession of a degree is only for convincing the employer that the candidate has some minimum qualities that will prepare him for the challenging tasks ahead. Still, the employer would be inquisitive to find out if the candidate has some relevant experience and desired skills to launch him immediately into the work environment.

The bottom line is that students should focus on having a combination of educational degree and work experience. Some extra skills relevant to the job would be a great advantage.

LOGIC BEHIND THE TREND

According to a study, a steady rise has been noticed in the number of enrolments in universities. Students are inclined to believe that degrees offer higher growth potential and a wider choice in selecting a job of their liking.

Jobs that were filled by high school graduates are now being passed on to university graduates. Ten percent rise has been noticed in workers seeking lower managerial positions. All these workers invariably possess undergraduate degrees.

Researchers found that the trend in universities to produce more graduates has created a gap in average ability. The salary packages and perks that come with a job are on decline as a result of this trend. Employers saw an opportunity to draw benefits for their companies by employing degree holders in positions where a lesser qualified person would have done just fine.

It is a simple case of supply and demand in a free market. In spite of these economic drivers, universities continue to enroll students in their undergraduate programs believing that by imparting skills and experience their graduates would succeed in competing for jobs.

In almost every business around the world, there is a stiff competition which has generated a demand for higher educated individuals. That is why a wide variety of industries and businesses have made a shift to employ university graduates.

IN PURSUIT OF EXCELLENCE

In spite of the demand for degree holders, a large percentage of university graduates remain unemployed. Graduates in some courses have such a low demand that as many as two-thirds are unable to find a placement. These turns of events have forced students to find other ways that can secure a suitable job with a promise of career growth.

In effect, students are investing more time and more money on earning postgrad degrees. As a consequence, enrolments in Masters and PhD programs are constantly on the rise. Research related jobs, like those of college professors and economists require advanced degrees. Likewise, physicists, oil explorers, social workers, consultants and school administrators all require higher learning experience and longer commitments to education.

A majority of postgraduates, as much as 61%, who chose to pursue their studies after their undergrad programs, think that their degree helped in advancing their careers. Postgraduate programs instill skills and knowledge that are not attainable by undergraduate courses alone. Over a period of time, the standards and levels of education of undergraduate studies suffered a decline. As opposed to this, graduate courses are now considered as upgrades of undergrad degree programs.

In certain cases, specialized training and attendance in workshops are also required. For instance, the IT industry is ever changing and anyone who does not have his fingertips on the day-to-day affairs is living dangerously and under threat of losing his position. Sooner or later, he may have to relinquish his position and find some other occupation to make ends meet.

Although an undergraduate degree indicates basic skills and fundamental knowledge of the profession but employers are not content with that offering. They want more. Their wish list includes postgraduate qualification like a Masters degree or a PhD. These degrees are considered as signs that the candidate possesses the abilities to analyze problems and suggest creative solutions. Such candidates usually also have decent communication skills which go a long way towards improving outcomes for the organization.

After examining a shift in the preferences of employers, we can explore what the future of job market will look like and what attributes would be required for a desirable placement.

The Demand for Technical Skills

Health Industry

The spread of COVID-19 virus marked an unprecedented increase in demand for workers in the health sector. From doctors, nurses, and assistants to medical reps and multi-faceted practitioners, healthcare has assumed paramount importance in many countries. In places where the pandemic is disturbing routine lives, the demand for healthcare professionals is most acute. And the skills required are specialized. Professionals related to healthcare sector are angling to train themselves and acquire relevant knowledge to carve a place in the fast altering healthcare scene.

New Media Marketing

For several decades, marketing professionals resorted to conventional media to communicate with their prospective customers. With the advent of new media—social websites in particular—no marketing plan is complete without some activity at these platforms.

Digital marketing gained momentum when business saw an opportunity to attract customers online. Soon, mechanisms were developed for transactions that were safe and without any loopholes. After the pandemic, a large lifestyles and work routine experienced a transformation. More people were forced to live away from public place as social distancing became a norm. When a large section of population had to live and operate from home, more organizations shifted their businesses online. Digital marketing thus became the most in-demand skill. Currently it is the most sought after skill around the world.

Digital Marketing is a world in itself. A variety of skills are needed if one chooses to enter in this realm. The key skills include brand management, product marketing and digital strategy. The main objective of digital marketing is drive sales by maintain a visible online presence of brands together with an effective campaign to take the product to prospective customers. A person aspiring to go into the business can aim for positions like Marketing Representative, Social Media Manager, Creative Content Writer, SEO Marketer, Digital Marketing Expert and several more.

Coding Skills

Most of the top CEOs today, who are few of the richest people, have something to do with coding. They are related to this skill in one way or another.

In a few years' time, this skill climbed to the most desired skill. Many schools teach at least one form of programming language just as second foreign language is taught at lower levels of educational life. The top languages that one should focus attention on are Java, Javascript, Python, C#, C++, and PHP. To market oneself, a candidate should acquire knowledge and skills related to one or more of these languages. As a pre-requisite, mathematical and problem-solving skills are necessary.

User Experience Design

As web presence became a necessity for businesses, user experience turned out to be the key factor for driving products and claiming a sizable market share. Anyone using a website or an app would stick to it if navigating experience offers ease of operation and smooth transition from one page to another. A UX designer focuses on a typical browser's psyche, his attitudes and emotions towards a product being displayed, together with efficiency and effectiveness.

Basic attributes for becoming a professional UX designer include web design, design thinking, user experience testing and some knowledge of human psychology. Upon entering into this area of jobs, a variety of job titles can come to the fore including Product Design Consultant, User Experience Researcher, User Experience Designer, and UI Designer.

Data Analytics

Giant companies like facebook and google rely on data analysis to keep a watch on trends of website visitors. Digital marketing and advertising is heavily dependent on data analysis without which no effective strategy can be adopted.

Statistical Modelling, Data Visualization and Tensor Flow are the skills required for workers who intend to make Data Analysis their full time occupation. The positions they can look for may have attractive appellations: Data Scientist, Data Science Specialist and Data Management Analyst.

Cybersecurity

The growth of traffic on internet and mobile devices has lent great importance to cyber security. The Covid-19 virus, that has caused a pandemic around the world, is also a contributing factor in increasing traffic on the internet. When huge amount of data flows on networks around the world, it offers an opportunity to hackers to infiltrate in computers of businesses and organizations and steal sensitive data. The hackers can also induce malfunctioning in websites and demand ransom to make things right.

Millions of dollars are lost to such actions by the hackers. The bigger and more sensitive an organization is, the larger the loss will be. For a long time IT specialists handled such breaches and attacks on their own, but as the intensity and frequency of attacks increased, CEOs and top management felt the need for dedicated staff responsible for keeping an eye on suspicious activity and warding off intrusions in database of organizations. Over a period of time separate departments were created that were solely charged with the responsibility of providing security.

Further down the road, it was realized that cybersecurity is key to the survival and profitability of a business. The CISO (Chief Information Security Officer) was accorded a prime position in an organization. The CISO now is a board member and plays an active role in formulating company policies and business strategies.

THE FINAL WORD

We have seen that the value of degrees has changed in different times. There was a time when possession of a degree alone was enough to guarantee a top job. Then skills set bean to take precedence over everything else. Still at other times, higher qualifications like Masters, MPhil or PhD were sought after for key position in industries and businesses.

A pragmatic way to look at these things is to give due importance to every attribute. With unprecedented growth, lives have become extremely complex. To control and bring order, a combination of skills and a sound knowledge base are essential. While employers begin to look for these qualities, prospective candidates should also strive to enhance their skills after completing their studies and earning degrees. In the job market, these days are dictated by the doctrine of 'The more, the better' instead of 'Less is More.'

CYBER SECURITY

BEST PRACTICES

CYBER SECURITY MATTERS.

What is best to practice?

1. Crotical choice to finalize Cybersecurity Framework to follow
2. 'What needs to be followed' should brecede 'investment'
3. Recognize the importance of proactive management of Best Cyber Practice
4. Best Practices must be followed during each and every action
5. A governance framework with strong leadership is essential to effective enterprise wide cybersecurity
6. Prepare your checklist to be followed based on Best Cyber Practice

Communications Giant 'Viasat' Suffers an Attack.

The satellite communications company says cyber event is causing outages across Europe.

In a communication to the media channels and reporters, Viasat admitted to suffering a cyber attack which has caused outages in Ukraine and other neighboring countries in some parts of Europe on its KA-SAT network.

The staff at the company, responsible for addressing IT issues, is analyzing the network and systems to revive the services. This is being done to find out the root cause and prevent more such incidents from happening. Ongoing investigations being conducted by cybersecurity experts is assisted by government and its agencies.

Christina Phillips, vice president of public relations at Viasat, has released a statement which can be seen as a confidence building measure: "Our investigation into the outage continues, but so far we believe it was caused by a cyber event. We are investigating and analyzing our European network and systems to identify the root cause and are taking additional network precautions to prevent further impacts while we attempt to recover service to affected customers."

The time of the attack was the same as the beginning of Russian invasion of Ukraine. It was reported that there was an attack on KA-SAT infrastructure in Ukraine which continued to spread. SkyNet, a British news channel has reported that the impact was caused by a Distributed Denial of Service (DDoS) attack. As a result, several ISPs in European countries including Germany-based EUSANET experienced outages and disruptions in their broadband connectivity.

The KA-SAT network is not directly operated by Viasat. Instead, a third party oversees the operations on the network and extends the service through various distributors. Ukraine's military and security services have acquired different communication systems during the years before the conflict. These systems were run on Viasat's network.

The company has stated that clients who directly subscribed to Viasat's services remained safe from the disruptions. There is a possibility, therefore, that intrusion was made through third party systems which used the KA-SAT network.

To ascertain the real reason behind the broadband disruptions in various regions of Europe, Viasat has hired the services of Mandiant, a company well-known for investigating breaches instigated by state-sponsored hackers. No official from NSA, ANSSI or Mandiant was immediately available to confirm the news.

A Czech telecom executive, Stritecky, has absolved Viasat of the blame whereas some other point the finger straight at the satellite communication company. Amid these conflicting statements and confusing situation, the truth lies somewhere. We may have to wait until the investigations present a conclusive result and the real attackers are identified.

HYPOCRISY IN CS WORLD

'Saying something and doing otherwise might be a simple way to describe 'hypocrisy'. By extension, it also means having dual standards. We come to see examples of such behavior in abundance. Everywhere. And there seems to be no prejudice with respect to race, creed or citizenship.

US Under Microscope.

Some years back, Hillary Clinton, the then Secretary of State in Obama's administration, criticized the firewall approach—an oblique reference to Chinese attempts to gain control over the technology that is considered as a paradigm of independence, freedom of expression and democratizing. She said, "countries that restrict free access to information or violate the basic rights of internet users risk walling themselves off from the progress of the next century".

The world did not have to wait long to see the US government's own strong arm tactics. Only thirteen months after Clinton's moralizing sermon, the WikiLeaks revealed the hidden realities. Reports were rife that the government organizations were watching and 'snooping on private 'twitter' accounts.' This was an open breach of privacy. And civil rights organizations were in court to raise their voice and anger at the government's unilateral decision to intervene in private lives. Ever since, the cyber world has echoed with criticism about double standards in the US.

The situation went to a new low when the US domain name of WikiLeaks was denied any access. And to top it, Julian Assange's site was also denied the facility to raise money by employing PayPal, Visa and MasterCard services. This speaks a lot about how hollow the oft repeated phrase 'freedom of speech' really is.

Chinese Stance.

In the initial stages, the Chinese response to the disclosures was relatively mellow and was channeled through the Foreign Ministry which used soft words to comment on latest revelations. Edward J Snowden, a former CIA employee, alleged that the US government clandestinely monitored Chinese internet sites and several installations of sensitive nature. He has also spoken about 'Prism', a national security agency geared toward mining internet information from around the world, especially from regions which have some conflict of interest with the US.

But the recent remarks by Chinese Ministry of National Defense, to say the least, are upfront and aggressive. The officials of the ministry accused United States of hypocrisy over cyber surveillance activities and clandestine operations that are akin to interference. The officials further asserted that the WikiLeaks affair has vindicated Chinese stance and efforts to provide security on the internet.

Low Levels of Confidence.

The Pew Research Center, based in the US, is a nonprofit, nonpartisan and non-advocacy group. They inform the public about issues, attitudes, trends and behaviors that are defining the world. Their scope of work also includes studies on the behavior of people when they are online. The aim is to generate 'a foundation of facts that enriches public dialogue and supports sound decision making.' The methodology is largely based on regular polling to determine facts. In one of the reports, the Pew researchers published common perceptions related to privacy and security soon after Edward Snowden made the startling revelations.

The New York Times neatly summarized the findings as, "Americans say they want privacy, but act as if they don't." In other words, the people of US harbor concerns about privacy on the internet and trust no one online. Yet, they keep using the facility and whenever asked, they unwittingly share their personal information.

The Pew Research findings are sobering, to say the least. They speak of an increased distrust of online and phone communications after Snowden's revelations. Around 80% of those surveyed feel insecure while sharing private information on social media. Nearly 70% feel the same about chats, 60% about text messages, 58% about emails and 47% about cellphone voice communications. Users do not even trust landlines. Over 31% of the respondents felt uneasy about such communications.

A large number of survey respondents spoke of their suspicion when interacting with government companies or big online businesses. Yet, in spite of the distrust, more than half of those polled were ready to share their personal information for various reasons. A third of them believed that sharing information with the companies allows them to be efficient and provide quick service.

Almost 80% of the people, active on social networking sites, were wary of advertisers and third party businesses that had access to personal information shared on these sites. The survey brought to fore the grim reality that there isn't a single communications channel which can claim to have the confidence of its users.

The survey establishes without a shade of doubt that there is a widespread lack of confidence on communications channels. A vast majority of users thinks of online sites and phone communications as insecure. It is a paradox, however, that the same majority tends to use the channels. This points to the fact that internet users are caught in a psychological problem referred to as "cognitive dissonance." This state of mind is characterized by inconsistent thoughts and attitudes pertaining to attitude change and certain behavioral aspects..

There is a paradox here. People continue to use communication channels that they do not really trust. One answer could be the fact that there is no other alternative. And there might also be another reason. Most people are trapped into herd mentality. They would make choices that most others are making. The Greek philosophers of ancient times may have had a technical name for this fallacy: argumentum ad populum. In a nutshell, hypocrisy appears to abound when we observe people's behavior concerning the internet and its related technology.

Hypocrisy US-style.

Think tanks and government functionaries in the US constantly build a narrative that paints the country as the guardian and savior of internet freedom. They want the country to be seen as a defender and fighter against countries like Russia, China, Iran and Syria that are battling to bring the internet under some control. US leaders often speak out about US principles in a narcissist tone like Hillary Clinton did when she was the Secretary of state in the Obama administration:

"We are convinced that an open internet fosters long-term peace, progress and prosperity. The reverse is also true. An internet that is closed and fractured, where different governments can block activity or change the rules on a whim – where speech is censored or punished, and privacy does not exist – that ... is an internet that can cut off opportunities for peace and progress and discourage innovation and entrepreneurship."

Had the United States practiced what it preached, these words could easily have been considered as divine but that is not the case. The harsh and punitive actions against the founder of WikiLeaks, Julian Assange, and Edward Snowden are a testimony to US's attempts to gain control over the internet. The conclusion is immediate: when US interests are under threat, the country's machinery will employ all means to alleviate the threat and do everything to make sure that it never happens again.

More than a decade earlier, the United States formed Cyber Command, at Fort Meade, Maryland. It is one of the key units of Department of Defense and works closely with National Security Agency sharing the same leader. According to its official website, 'the Command has three main focus areas: Defending the DoDIN, providing support to combatant commanders for execution of their missions around the world, and strengthening our nation's ability to withstand and respond to cyber attack.' The About page further adds, 'The Command unifies the direction of cyber space operations, strengthens DoD cyber space capabilities, and integrates and bolsters DoD's cyber expertise.'

But the US government and its intelligence agencies have gone far beyond their stated goals. In just over a decade, the Cyber Command has developed capabilities to deploy cyber warfare against nations it unilaterally labels as 'rogue states.' To give credence to the unstated truth, we have an example. It is widely known that United States and Israel worked closely to launch a cyber attack on Iran's nuclear facilities through a virus called Stuxnet. These occasional cases of misconduct might be the tip of an iceberg. The full extent of subversive activities are still unknown or hidden. But the few cases that have come to light provide enough reason to believe that the US is committing actions that if countries like China or Russia are found to indulge in then they would be conveniently labeled as espionage.

Hypocrisy Euro-style.

Soon after the revelations on US government's NSA and UK's Government Communications Head Quarters, GCHQ, European General Data Protection Regulation (GDPR) was formed to standardize principles and provide guidelines for personal privacy protection. Now, it is regarded as the gold standard for personal privacy protection.

Documents released by whistleblower, Edward Snowden, the GCHQ mass surveillance activities were on scale few can even imagine. They collected information from 'every visible user on the internet.' The Cheltenham –based agency was gathering data from all sources including search engines, social media, online radio, news and a plethora of other websites. They built profiles by observing web browsing habits and stored data related to people's e-mails, texts and phone calls.

Last May, The Guardian, carried a lead story about a court ruling which observed that GCHQ's interception was an outright violation of right to privacy. The European Court of Human Rights has also ruled that the mass data interception was a breach of right to freedom of expression and that the regime for collection of data was unlawful. To sum up the whole affair, The Guardian put it in this way: "While Europol lags behind the US in terms of technological capacity, it is on the same path as the NSA."

Bottom Line.

The conduct of powerful states, who claim to follow democratic principles and a 'world order' that rests on freedom of expression, is unacceptable. They have themselves indulged in subversive activities. As a result, they have lost moral ground to ask for compliance from nations who attempt to bring the internet under their control.
Apparently, hypocrisy reigns supreme when it comes to the internet technology and cyber world. If this behavior is not corrected, the wonderful technology may eventually disintegrate and the world will lose the merits of having a single free internet.

Anonymous Exploits Flashing Pro-Ukranian Messages.

Anonymous hackers took the responsibility for the attack on Russian State TV channels.

Russian President Vladimir Putin was warned of unprecedented cyber attacks on Russia's critical assets, businesses and organizations. Anonymous, the online group of hackers, are openly supporting Ukraine over the conflict.

As the war entered its 12th day, the group has claimed that they had infiltrated Russian TV. To prove the claim, they shared footage of devastation in Ukraine which the Russian citizens could watch. The hacktivists are employing all kinds of tactics, carrying out attacks on government websites, banks, businesses and media. These include DDoS, defacement of websites, interruptions in TV transmissions and displaying of pro-Ukraine messages on these platforms.

The footage was broadcast on pro-Russian channels. It showed the devastation in graphic detail and highlighted the loss of civilian lives and extensive damage to property and infrastructure. The video beamed a written message that addressed Russians and told them that the war was incited by Russia's authoritative regime headed by Vladimir Putin and not by ordinary citizens. The purpose of this activity, the message further added, was to inform the general public of the true situation because the Russian government is blocking all news about war from reaching the common man.

The footage along with the message was first shown on several pro-Kremlin channels. Later on, according to the twitter account of Anonymous, all Russian state TV channels showed it when the group breached every channel.

The Russian radio channels are also reportedly affected by the activities of the group. The group made their way on the airwaves of Russian stations and broadcast Ukarnian national anthem. And the activities extended to Russian military radio as well.

After attacking the airwaves and TV channels, the hackers group went on to hamper the operations of an EV charging station in Moscow. The service of the station was immediately interrupted. As a result of the attack, messages against Putin and his regime began to flash. Images in support of Ukranian President Zelenskyy together with "Glory to Ukraine" could be seen on the screen.

The activities of Anonymous did not stop at that. The group claimed that it had attacked Russian Linux terminal and gas control system located somewhere in north of Russian Federation. Observers believe that Anonymous managed to make changes to the dates and they could also have induced variation in the gas pressure which may have resulted in catastrophe. However, prompt human intervention stopped this eventuality.

In yet another campaign, Anonymous took down the website of Chechen government which is an ally of President Putin. Chechen leader, Kadyrov, has deployed his armed forces along the border of Ukraine to show his solidarity with Russia.

The extent of war can be gauged by a tweet coming from Hanna Liubakova: "In the Mykolaiv region, a 78 year old man wanted to enroll in the territorial defense. Because of his age, he was refused to join. So he went to the checkpoint and threw a Molotov cocktail into the Grad multiple rocket launcher. The installation burned down. You won't break the spirit."

Earlier, in the wee hours of Feb 25, the aforesaid group posted an announcement: "The Anonymous collective is officially in cyber war against the Russian government. #Anonymous. #Ukraine." Soon after this, the group took down Kremlin's official website and warned that more attacks targeting Russia's key installations and infrastructure would follow soon.

On the opposite side, the Russian government labeled the campaign as 'fake news' and 'false information' about the war. According to The Independent, anyone who is caught with links to such propaganda would face a fine that may be as high as $15,000 and sentence that can lodge the culprit for as long as 16 years.

The Anonymous group has vowed to wage war against Russian government and its interests that these incidents will continue until the conflict is peacefully resolved.

More Exploits of Anonymous.

The group hacks and defaces Russian Space Research Institute Website.

It is an all-out war now. No opportunity to harm the interests of one another is left to chance. Everyone hears about attacks and catastrophes on the ground. And there are just as many on the cyber surface.

A prominent but loosely connected group—that goes by the name of Anonymous—has just added another bow to their victories. On March 3, the group hacked the website of Russian Space Research Institute (IKI), defaced it and leaked files that belonged to Russian space agency Roscosmos. As the Russian-Ukraine crisis continues, there has been a sudden increase in hacktivism targeting Russian installations. cyber attacks on Russian interests.

The hackers claiming responsibility of the attack called themselves 'vog3lsec' and they are affiliated with the prominent Anonymous group. The message was posted on one subdomain of IKI's website which is still offline, whereas as other subdomains like the one related to Department of Optical and Physical Research is active and accessible.

The group posted files drawn from Roscosmos, Russia's space agency. These files include forms, pdf's, and spreadsheets in both English and Russian. The content of these files dealt with lunar missions, as confirmed by 'Motherboard' that reviewed the data.

The hackers disclosed in a chat with 'Motherboard' that "they were using their own file sharing service where the files could be accessed only by providing a username and password…all I did was bruteforcing the password while keeping the username as admin… as they were using weak password, it didn't take much time for me to get the password."

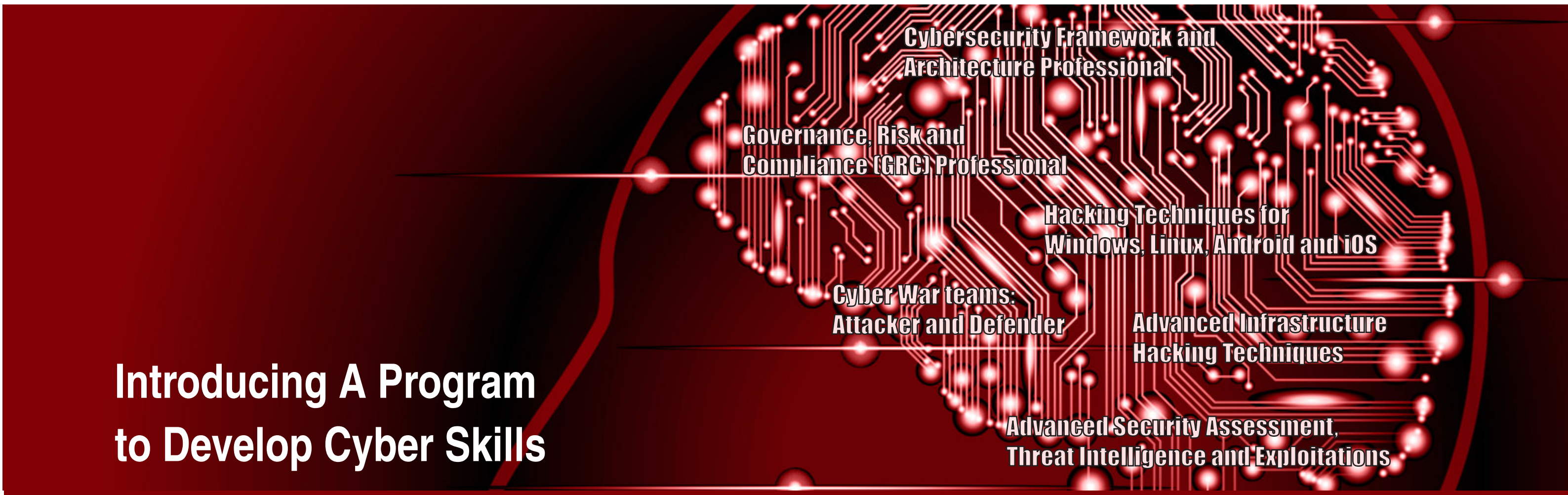
The leaked data reveals discussion on possible lunar landing site on the moon's south pole. This may not be significant achievement on the part of hackers because Russians have already announced proposed lunar landing sites. Motherboard could not ascertain the verity of these claims. And IKI also did not respond to requests for a comment.

A few days later, there was another claim from a group suggesting that they targeted 'Vehicle Monitoring System.' This time, however, the head of Roscosmos, Dmitry Rogozin came out with an immediate rebuttal that any of the Russian satellite control centres were hacked. He told Interfax, "Offlining satellites of any country is actually a casus belli—a cause for war." Researchers checked and confirmed that the new website does not show any signs that the space satellites were hacked.

When the iki website (url:uv.ikiweb.ru) was inaccessible, its archived version carried a message posted by the hackers and obviously directed towards the Russian officials. The language was profane and derogatory, to say the least; and it mentioned ISS at the end referring probably to Chief Ragozin's earlier remark that he had made about the partnership between Russian space program and NASA. He appeared to imply that the cooperation between the two space agencies could come to an end.

The breach at Roscosmos came only days after another hacker going by the name of NB65 claimed that he had shut down Russian satellite control systems. NB65 was also Anonymous-linked. Besides this another hacking group, operating under the guise of 'AgainstTheWest' claimed to have infiltrated the Rosatom nuclear energy entity. Yet another group, operating under the name of Anonymous Liberland released a large cache of data stolen from a Belarusian defense contractor. The claims, which could not be verified, were all denied by Rozogin.

In the midst of these claims and denials, the head of Russia's space agency warned that his corporation will eventually identify and apprehend these hackers and hand them over to Russian Security Agencies who would initiate criminal investigation against them and bring them to justice.


Cybersecurity Framework and Architecture Professional
Governance, Risk and Compliance (GRC) Professional
Hacking Techniques for Windows, Linux, Android and iOS
Cyber War teams: Attacker and Defender
Advanced Infrastructure Hacking Techniques
Advanced Security Assessment, Threat Intelligence and Exploitations
Introducing A Program to Develop Cyber Skills

DG Cyber KIDS.

Empower every child with Cyber Security Complexity

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

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

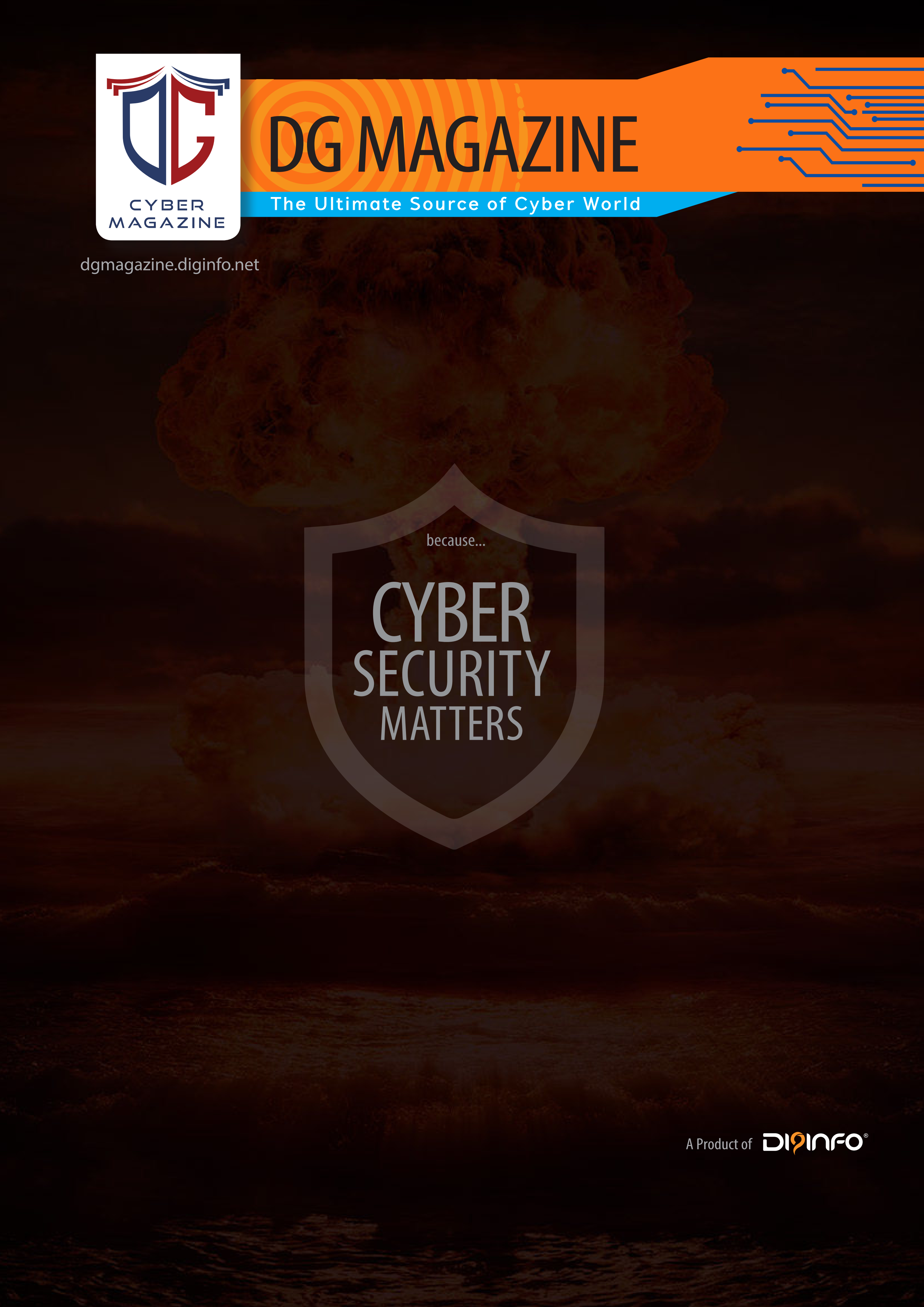
DG ACADEMY®
PROTECT YOUR FUTURE

CYBER
MAGAZINE

DG MAGAZINE

The Ultimate Source of Cyber World

dgmagazine.diginfo.net



because...

CYBER
SECURITY
MATTERS

A Product of DIGINFO