S.P MANDALI'S weschool Welingkar Education

YEAR 2022 | ISSUE 125

samvad

CYBERSECURITY

In collaboration with

InfoCratus
Empowering Excellence

WeChat

Prianshu Khandwala

LEAD INFORMATION AND CYBER SECURITY

UPL

MESSAGE FROM THE DIRECTOR

Prof. Dr. Uday Salunkhe
Group Director

Dear Readers,

It gives me great pride to introduce SAMVAD's edition every month. Our SAMVAD team's efforts seem to be paying off, and our readers seem to be hooked onto our magazine. At WeSchool, we try to acquire as much knowledge as possible and share it with everyone.

As we begin a new journey with 2022, I sincerely hope that SAMVAD will reach new heights with the unmatched enthusiasm and talent of the entire team.

Here at WeSchool, we believe in the concept of AAA: Acquire Apply and Assimilate. The knowledge you have acquired over the last couple of months will be applied somewhere down the line. When you carry out a process repeatedly, it becomes ingrained in you and eventually tends to come out effortlessly. This is when you have assimilated all the knowledge that you have gathered.

At WeSchool, we aspire to be the best and unique, and we expect nothing but the extraordinary from all those who join our college. From the point of view of our magazine, we look forward to having more readers and having more contributions from our new readers.

SAMVAD is a platform to share and acquire knowledge and develop ourselves into integrative managers. Our earnest desire is to disseminate our knowledge and experience with not only WeSchool students but also the society at large.

Prof. Dr. Uday Salunkhe,
Group Director

ABOUT US

OUR VISION

"To nurture thought leaders and practitioners through inventive education."

CORE VALUES

Breakthrough Thinking and Breakthrough Execution
Result Oriented, Process Driven Work Ethic
We Link and Care
Passion

"The illiterate of this century will not be those who cannot read and write, but those who cannot learn, unlearn and relearn." -Alvin Toffler.

At WeSchool, we are deeply inspired by the words of this great American writer and futurist. Undoubtedly, being convinced of the need for a radical change in management education, we decided to tread the path that led to the corporate revolution.
Emerging unarticulated needs and realities require a new approach in both thought and action. Cross-disciplinary learning, discovering, scrutinizing, prototyping, learning to create and destroy the mind's eye needs to be nurtured differently.
WeSchool has chosen the 'design thinking' approach towards management education. All our efforts and manifestations, as a result, stem from the integration of design thinking into management education. We dream of creating an environment conducive to experiential learning.

FROM THE EDITOR'S DESK

Dear Readers,
Welcome to the 127th Issue of **SAMVAD**!

SAMVAD is a platform for “Inspiring Futuristic Ideas”, we constantly strive to provide thought-provoking articles that add value to your management education.

We have an audacious goal of becoming one of the most coveted business magazines for B-school students across the country. To help this dream become a reality, we invite articles from all management domains, giving a holistic view and bridging the gap between industry veterans and students through our **WeChat** section.

In this issue of SAMVAD, we bring to you half a dozen articles focusing on ‘**Cyber Security**’ with a section called '**WeChat**,’ where we have got some exclusive insights of what is happening under the nose of our theme.

We worked together on this edition with InfoCratus Technologies, our official sponsor, which is a first-generation service provider to businesses across India and overseas. They have carved a niche name for themselves in the areas of management & cyber security consulting, auditing & advisory, corporate training workshops as well as technology risk management services.

Cybersecurity is the practice of protecting critical systems and sensitive information against digital threats. Cybersecurity measures, also known as information technology (IT) security, are intended to resist attacks against networked systems and applications, regardless of the origin of the threats. Globally, the average cost of a data breach in 2020 was $3.86 million. These costs consist of detecting and correcting the security breach, downtime and lost sales, and reputation and brand damage. Cybercriminals seek personally identifiable information, such as names, addresses, national ID numbers, and credit card numbers. They sell albums on digital underground markets. Customers lose trust, the government levies fines, and legal action may be taken when PII is stolen.

FROM THE EDITOR'S DESK

Disparate technology and a lack of in-house expertise may raise the complexity and cost of a security system. However, businesses with a comprehensive cybersecurity plan can combat cyberthreats more effectively and limit the duration and severity of data breaches.

We hope you have a great time reading SAMVAD!

Let's read, share and grow with us!

Best Wishes,

Team SAMVAD.

Index

Prianshu Khandwala

LEAD INFORMATION AND CYBER SECURITY

UPL

PGDM E-BIZ, WESCHOOL, 2005-2007

How has your journey been from the classrooms of Welingkar to the Lead Information & Cyber Security at UPL?

I started working as a cyber-security auditor at PWC after completing my postgraduate degree at the Welingkar Institute of Management. In this position, I was in charge of conducting ITGC audits (IT general control) audits or business process control audits. My grasp of business and how IT systems deliver financial statements has greatly benefited from this position. It provided me with a very detailed grasp of how the systems are linked, how the systems operate, and provided a foundation for understanding how IT systems contribute to organisational performance after I accepted a position with the Aditya Birla Group. When I worked for ABG, unlike a consulting business, I had the opportunity to collaborate with several of the group's firms, including, Hidalgo, telecom, and others in Sweden and India. It was a combination of manufacturing, services that assisted in the development of my skills, and knowledge of how business processes are interwoven with applications. There, I dove deep into information security.

After ABG I started working for Tata Motors and led application security. Applications currently generate genuine business value and are constantly evolving, thus they are most important. As soon as I become proficient in application security. I was given a new responsibility that required me to oversee cloud security and vulnerability management to the point where I had to approve any application that Tata Motors rolled out. I was

exposed to cutting edge technology such as IoTs and OT security. With respect to my stint at UPL Limited, I lead the Information Security practice along with privacy and as a part of information Security practice, OT or manufacturing security is also part out of my profile.Regarding my stint at UPL Limited, I manage both privacy and the information security practise, and as a part of the information security practise, OT or manufacturing security is also a component of my profile.

I believe that the security stack needed to be constructed from the ground up when I joined UPL, therefore I did that. We made significant investments in cutting-edge technology. What we observe is now the norm. We were one of the first firms to release cloud proxy and behavioural learning-enabled antivirus or anti-malware solutions, or what we now refer to as XDR capabilities.

We had a lot of cutting-edge solutions launched for SaaS apps as well because the company was highly demanding and many SaaS applications were being rolled out. This implies that even though you don't have control over the application, you can see everything related to it, including application traffic and access.

From 2019 to June '22, India recorded a whopping 36.29 lakhs of Cyber Security incidents. What steps has the government taken, and what strategies should businesses use to become resilient towards such digital attacks?

Cyber security measures are essential for safeguarding an organization's IT infrastructure in today's high-tech digital environment. Besides businesses, the government is also affected. A cyber-secure environment will be maintained, and the Indian government will mitigate risks associated with attacks. The cyber community can guarantee security, privacy, and digital rights. To take advantage of this opportunity, governments must take strict actions.

1.Adjust national frameworks: Developing national cyber strategies and legal and regulatory frameworks in cyberspace need to become more agile.

2.Cooperation between nations: COVID-19 has led to greater information sharing. All cyber issues need to be formalized and maintained.

3.Unify awareness campaigns: We

must educate more. Cyber incidents or one "bad click" can affect anyone, regardless of age and profession.

One goal, one team

A successful cyber defense requires teamwork and collaboration both internally and externally. There has been an increase in the effectiveness of cyber attacks against organizations and entire industries. According to the Global Risk Report 2022 from the World Economic Forum, cyber security failure has become a significant threat.

Here's the good news: Your organization can start building resilience with a few "power moves."

Work as a team in cyber security

You need a top-down approach to cybersecurity. Across the company, the industry, and public and private stakeholders, the CEO and board should champion a cyber security culture. Organizations need to create a security culture that involves everyone, from the board to the CIO and line managers. It will also take partnerships with supply chains, contractors, etc.

Performing tabletop exercises and updating Business Impact Analysis

For employees to be secure, they must undergo security training. However, resilience requires more. Board members can practice decision-making in cyber crises using tabletop exercises that simulate attacks to illustrate threat response and decision-making processes. Taking the appropriate action in the face of real-life threats can be prepared with tabletop exercises.

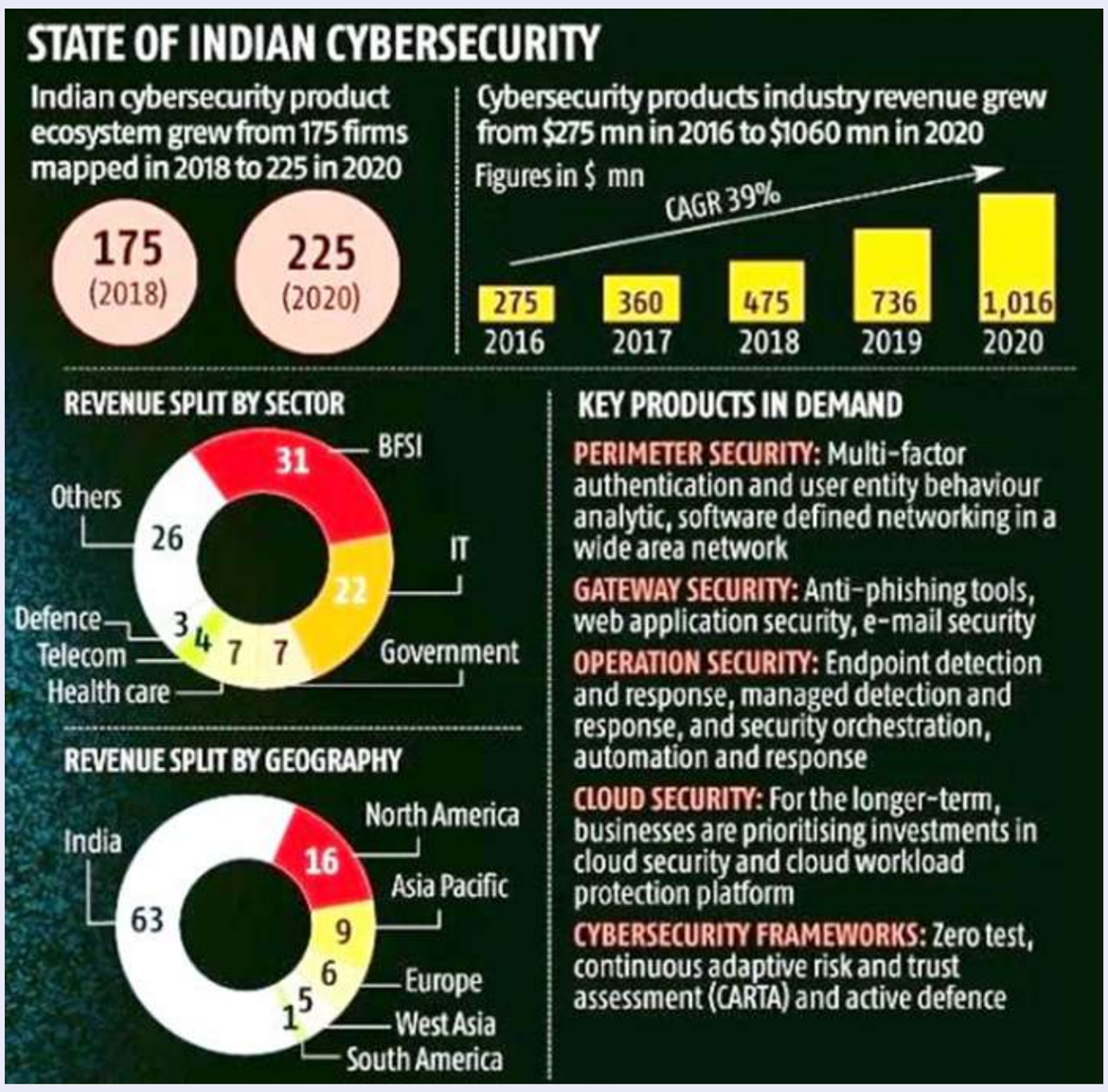
Establish relationships with law enforcement, government agencies, and info-sharing groups

Why shouldn't you share cybercriminal information about attack techniques and tools if cyber criminals do so? Staying ahead of cyber criminals may depend on sharing intelligence about cyber threats. Powerful hackers cannot be defended by companies alone. For example, governments, cyber security groups, industry peers, and organizations must collaborate to protect critical infrastructure providers from geopolitical and nation-state threats.

Collaborate on collective cybersecurity

Digitalization and connectivity make cybersecurity less of a responsibility for individuals and organizations.Businesses, i

industries, and governments must cooperate to protect themselves from global threats.



What are the most recent developments in ethical hacking, and how are businesses in India using ethical hacking and its techniques?

Due to ethical hacking, we have changed the way we view security. Nowadays, ethical hacking is an essential aspect of digital security.

Ethical hacking seems to be an oxymoron in cyber security, but it plays an integral role. Let's take a look at some of its recent developments.

There's always a solution to ethical hackers.

Almost every ethical hacker starts hacking computers early in their lives and develops the skills over time, but some have experience in network admin. Improve your network infrastructure with ethical hacking.

Penetration testing helps us identify system vulnerabilities before deployment and is simply the process of malware compromise. As a result of this approach, organizations can build more robust technical infrastructures.

Insight sharing

The most valuable insight ethical hackers can offer is determining how an attacker approaches a system, how sensitive data can be exploited, and where they can lead an attack. Ethical hackers may be able to fix gaps in security before cybercrime occurs quickly and someone's crucial information is compromised or destroyed if they imagine themselves as online attackers.

Several ethical hacking techniques can be used by businesses to protect and store confidential information.

Loophole analysis

When it comes to ethical hacking, it is essential to identify loopholes that criminal hackers can take advantage of. In addition to the security of data, other enterprise information must also be secured.

Proficiency in pen testing

It is also referred to as pen testing or penetration testing, which allows you to identify loopholes and vulnerabilities in an IT system or infrastructure. The ethical hacking training includes methods such as targeted testing, blind testing, internal testing, external testing, and testing of network servers or DNS services as part of the penetration testing.

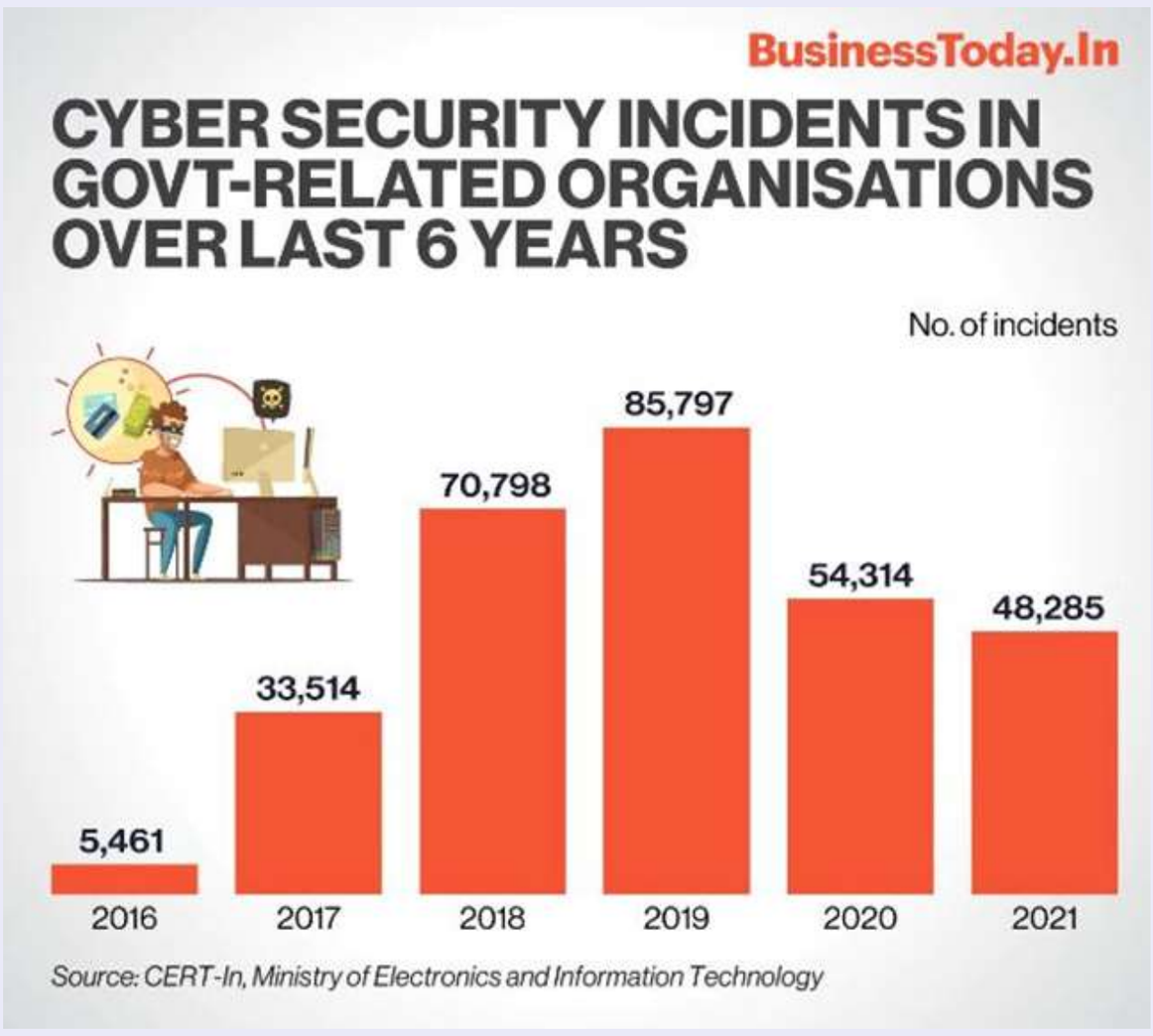
Knowledge of hacking tools

A mere interest in security measures will not ensure user protection. Even though most staff members are curious about safety methods, only a small percentage completely understand how to identify threats and implement security measures.

The tools and methods of identifying threats should be demonstrated and trained to the organization's staff by ethical hackers. Hackers are trained in using fundamental hacking tools, advanced methodologies, and technologies to protect organizations from cyber attacks.

Mitigation of loss in an attack

By using ethical hacking, ethical hackers can reduce the loss caused by an incident. Ethical hackers can find weaknesses and holes in IT infrastructure and mitigate losses in attacks. When vulnerabilities are identified in advance, they can be reduced in scope, reducing the exposure of more data, finances, and reputation.



GDPR and India: Where Are We Now? What kind of government policies and regulatory frameworks do we currently have and expect in the near future in our country?

Companies worldwide are evaluating how the EU General Data Protection Regulation ("GDPR") will affect their operations. A significant reason for these concerns is the high administrative fines associated with non-compliance with GDPR provisions. These fines can result in the loss of business for various

countries, such as India, due to non-compliance with GDPR provisions. An economic structural transition has taken place in India.

A NASSCOM report estimates that India exported 17.4% and 11.6% of IT/ITES services to the UK and Continental Europe in 2014. Given the critical IT-BMP services' importance to the economy, India must promote their growth.

India's ability to respond to global regulatory changes will largely determine business futures.

India must assess its preparedness and make effective changes if it wishes to remain a reliable destination for processing. Secondly, we will compare GDPR, the Information Technology Act, and the Rules notified under that Act based on the key provisions of GDPR, the Information Technology Act, and its Rules.

Rules around the collection and disclosure of sensitive personal data

A set of rules on security practices and procedures relating to sensitive personal data or information in the field of information technology was subsequently issued by the Indian central government under Section 43A of the Information Technology Act. Additional requirements have been imposed on commercial and business entities in India regarding the collection and disclosure of sensitive personal data or information similar to the GDPR and the Data Protection Directive, which require them to comply with these additional requirements.

The sectorial laws governing the financial services and telecommunications sectors require companies in regulated sectors to maintain the confidentiality of their personal information. These laws require companies to keep this information confidential and to use it only for prescribed purposes or as agreed upon by the customer.

Achieving compliance requires a combination of people, processes, and technology.

An effective compliance strategy is essential for today's highly regulated data environment organizations in India today to thrive. Those who do so will experience positive business outcomes and will undoubtedly benefit. The low adoption of data governance software and privacy protection needs to change - and change quickly. Companies must

gain better visibility into their data to comply with relevant data protection regulations. In the future, organizations in India can confidently embrace the new PDP Bill, once compliant, by adopting a people, process, and technology-centric approach.

What is the role of digitization and automation in cybersecurity?

Cybersecurity is a top priority for companies around the world and across industries. The world has become increasingly digital as technology advances, and organizations process all data types.

A growing number of companies are digitizing their operations, highlighting the importance of cybersecurity. Cybercriminals are becoming more sophisticated as their hacking techniques become more sophisticated, so a comprehensive cybersecurity program may not suffice.

The digital landscape constantly evolves, resulting in more sophisticated, costly, and threatening cyber-attacks. In what ways will organizations defend themselves against cyber-attacks? Automation may be the answer.

Here is more information about how digitization and automation contribute to cybersecurity

Cybersecurity automation benefits businesses greatly. Here are three reasons why enterprises are looking at cybersecurity automation as a means of enhancing security:

Lack of skilled workers in cybersecurity: The security technology industry is growing, but a small talent pool knows how to implement and use these technologies effectively.

Lack of standardization: Many security implementations fail as they depend on who implements them. For this reason, standards are the future of security implementations, which is why there is a growing need for standardization in security.

Expanded attack surface: There are a wide variety of new digital technologies used by businesses across all sectors, which increases their ability to expose themselves to threats and makes old cybersecurity techniques obsolete.

An effective digital transformation depends on cybersecurity.

The digital revolution has the potential to boost GDP by one percent a year over the next

decade, adding 2.5 trillion Euros to Europe's GDP by 2025. According to forecasts, German consumers will possess, on average, 9.8 connected devices by 2023. As a result, many smart living solutions could be developed. Digital interconnectedness, however, brings with it significant security challenges. Long-term confidence in digital transformation can only be sustained if cybersecurity is assured. As for digital platforms, they contribute to Germany's high productivity and economic growth through the ongoing digitization of industrial production.

What advice would you give aspiring professionals hoping to start successful careers in cybersecurity?

There are more available cybersecurity positions than qualified candidates, which makes it a booming field. From 2020 to 2030, the US Bureau of Labor Statistics anticipates a 33 percent increase in cybersecurity jobs. Cybersecurity careers can be advantageous. Cybersecurity professionals are in high demand because they provide organizations with security and help improve the world. They typically earn over $100,000 per year, assisting organizations in keeping their data secure.

Would you like to pursue a career in cyber security? To assist aspiring cyber professionals in launching successful careers, here are a few tips:

1.Start learning and doing.-A computer science degree isn't required, but you can start without certification or approval. Your investment in learning will yield great career opportunities.

2.Keep your options open.- Cybersecurity jobs range from technical to non-technical. This industry requires people with various skills, including communication, interpersonal, leadership, investigative, and an understanding of business. Cybersecurity is a challenge that requires leadership and collaboration between people, and its core challenge is risk management.

3.Expand your horizons.-Security careers require a wide range of tech experience. Having an excellent reputation for something else is what will make you good at security, says Tierney. A program such as this could help you learn the fundamentals of data networks. You will also be able to become proficient at administering multiple operating systems, or you could become proficient at several scripting languages (Python, Bash, etc.)."

4.Network with industry professionals. It's great to network online, but it's even better to network in person. Attend conferences, meet with current security professionals, and ask them for advice over coffee. Taking Tierney's words to heart, he says, "We should get to know as many people in your field as possible. Consider getting involved in an open-source project or community project. To be successful in networking, it is important to not only ask for help from others but also to offer them something in return."

Cybersecurity Digital Marketing Techniques

National Winner

Shivam Nikhare
(MMS), Marketing 2021-23
Jamnalal Bajaj Institute of Management Studies

Imagine you are Risk Manager 5 years down the line in a Mutual fund printing lakhs and crores of money every month for your investors and clients. You had a hectic day, slept well and wake up the next day to continue with the routine. The first thing that you do as soon as you wake is open the screen and checking for emails. You find out that you have won a voucher for Dubai trip. And now you need to enter the details of your bank accounts which you excitedly complete since you have wedding anniversary in the next month. The consequence is – "Dear HSBC User, you're a/c X9990 – debited Rs. 15,00,000 on 30 Sept"
This is not novel. Cybercriminal earns more than $ 1.5 Trillion every year. To represent some key statistics. The most affected continents are shown in the Figure 1.

Columbia is the worst affected country with approx. 94% of the countries being attacked atleast once in a year according to (CyberEdge 2021 Cyberthreat Defense Report)

Figure 2: Percentage of organizations compromised by at least one successful attack.

But only talking about data never helps. We need to come up with solutions as to how we digital marketing techniques to provide solutions to the customers about cybersecurity. So when we refer to the bible of marketing – "Marketing management by Philip Kotler", we

Figure 1

come to know that identifying TG – Target group is most important. This defines the trajectory of the budget allocation, branding, advertisements, and so on.

Here we know can identify that there are 3 key categories that uses cybersecurity solutions. They are

1. **Individuals** – Risk managers, auditors, analyst, underwriters

2. **Business** – Large enterprises, Insurance companies, hedge funds, mutual funds

3. **Government** – municipalities, military, PSUs and many more.

Now when you look at each of these categories, we can identify that each of them have different touchpoints so that we can be an opportunist by hitting them at the right point at the right time.

So the key techniques that we will recommend are

1. Educate and then Sell rather than focusing on selling

While we look at marketing, companies generally focus of selling the product by cold calling, giving sales pitch, email marketing and so on. Rather than doing this we need to create a dedicated blog so that we can teach them properly. As people get to know about the importance of cybersecurity, they will know that paying for the same would be beneficial for saving their data from data breach.

2. Freemium strategy

An experiment was performed by one of the company where the sales men were not asked to sell the product, but were asked to give it directly to the customers and ask them to give review after an interval – lets say a week. When customers

got the product for free they were happy and were excited to review different products.
So we need to apply a similar strategy in which we give the customers free trial on the basis of phone number or email id to protect them from threat and latter on leveraging this data for further promotions.

3. That extra efforts (Beyond customer expectation)
Since we are focusing of providing digital services, it is easy to copy all the differentiators in our strategy. While making posts and ads, we need to focus on what extra are we offering with respect to our customers. This can be highlighting money back guarantee, quoting 99.5% efficiency in cybersecurity, etc.

4. Credibility and trust
While targeting different digital channels, testimonials from old clients which can be municipalities, big companies, HNI clients, etc. can be displayed as it is shown that 72% customers say that positive reviews and testimonials help them trust more.

5. Leveraging AI and ML on social media
We need to exploit Artificial Intelligence and machine learning a lot. We can gather data from the activities of our customers as to how and which particular websites, software and online tools people are using in their day to day life. We can leverage them to create targeted ads. For ex. Using Instagram and Meta to create digital campaigns to target customers more willing in this area. Different analytics provided by these companies in the backend can help us optimise our ads.

6. Videos are future
It is said that attention of humans is decreasing day by day and we can only focus on a particular thing for 8 sec which is less that the attention span of gold fish. So creating content with 3D animations, using UI UX, amazing visuals would help us hook the customer to our product which would help us improve the sales. Also businesses looks at the amount of effort that the company is taking to develop their content. This content can be posted on YouTube, Instagram, Meta, and Other platforms which will help us show our efforts and technology advancement. We have to take this into consideration that people love videos rather than only content. The earlier we understand the better we will progress. At last we need to keep in mind that these strategies will help us sail through the digital marketing techniques to market our product. We should never think upon capturing the fear of the customers in an unethical

manner. We can educate them, help them understand the threats involved and then try to inform them about our services. This will help us improve the brand value along with trust in the hearts of people, organisation and government.

Blockchain to Drive Transparency in The Supply Chain

National Winner

PRIYA GUPTA & VEDASHREE R
MBA 2022-24
Symbiosis Institute of Digital and Telecom Management

Cyber hygiene, also known as cybersecurity hygiene, is a set of routine actions that businesses and individuals take to keep users, devices, networks, and data safe.

Attacks via the internet are becoming more frequent and more serious. Consequences of security blunders frequently make headline news and can be extremely damaging to the afflicted organization. Although there is a belief that only large, international firms are vulnerable but thousands of attacks against Small- and medium-sized businesses are frequently underreported. Also, there is a misconception that only the It security department or cybersecurity professionals are responsible for maintaining the IT assets instead it is the responsibility of each and every employee in an organization to be aware of taking necessary steps to prevent the same.

The threat of cyber-crime has emerged as a result of the introduction of new technology and the quick expansion of internet users. Unluckily, it's growing at a startling rate. To secure digital life in this situation, good cyber hygiene practises are required. Cyber hygiene practises play a key role in cybersecurity globally. A deeper understanding of user variations linked to good or bad cyber hygiene behaviour, as well as an enhanced understanding of what users do to promote good cyber hygiene, are urgently needed. Because of recent ICT breakthroughs and the Industrial Revolution 4.0, cybersecurity assaults are increasing (IR 4.0).

Common Cyber Hygiene Problems are as follows:

1) Bring your own device (BYOD) as a threat

Bring Your Own Device (BYOD) refers to employees using their own gadgets while on the job. Threats from BYOD are solely depending on

the user's interaction with employees' personal electronics. Increased productivity benefits organisation's productivity and decreased ICT spending. SMEs typically have more issues with the security of information systems (ISS) than bigger businesses. Due to staff mistakes and ignorance, this behaviour could endanger an organisation. BYOD issues may result in the theft of private legal information and accessing email attachments with viruses on devices, malware that could compromise a network, unintentionally recovering spam, and infections on personal devices.

2) Spear phishing

Attacks known as "spear phishing" are those that target certain people or groups with the theft of sensitive information by making claims about them or engaging with them using their names. They must use the web data at their disposal to learn more about the victim.

The high level of success of these attacks compared to other social engineering attacks is due to the difficulty in identifying and differentiating them from legitimate users when they attack a corporation from the inside.

3)Distributed denial of service(DDoS)

The distributed denial service saturates the attacking companies' network with traffic, eventually bringing it to a halt.

A domain name system recognised and attacked Distributed Denial of Service (DDoS) in 2016, which affected tens of millions of Internet Protocol (IP) addresses (DNS).

3)Ransomware attack

Cyber-malware called ransomware prevents access to data and related information. When a user clicks on the provided link in an email, it activates through that email and may occasionally need payment in order to access the affected data. When a user accesses particular websites or web pages, the system can also be filtered. Internal files are rendered inactive to the end user by this cyber infection, which also encrypts themselves and prevents them. Additionally, the server attached to that machine is affected, and occasionally the network settings for the entire system are locked.

4)Insider Threats

A risk to a company posed by employees, former employees, business contractors, or associates is known as an insider threat. These individuals have access to vital information about your business, and they have the potential to cause harm out of avarice, malice, or even just negligence. According to a study by Verizon, insider threats were to blame for 25% of data breaches.

This is a problem that is becoming

worse and could endanger consumers and staff or hurt the business financially. Insider risks are increasing in small firms as more employees have access to several accounts that contain more data.

Here are some things which can be done to create a comprehensive cyberdefense.

1)Changing the mindset

Vulnerabilities never become obsolete. Owners often concentrate their efforts on imagining the gains in productivity and customer satisfaction that can be gained by new technology while thinking about digital infrastructure. On the other hand, cyberattackers concentrate on identifying the ways that new technology use cases recycle the same flaws and vulnerabilities of the past. In fact, regardless of the technology involved, the challenges

<u>Simple recommended steps to maintain cyber hygiene are as follows</u>:[2]

Keep a log of every piece of equipment and Software to make sure it is patched correctly

Configure all the devices and control the entry and exit of the data

Make sure that any service agreements contain adequate security controls (including cloud services)

Create an incident response strategy

Often backup your data and verify that it can be restored and reduce administrative accounts

Infrastructure owners and operators can no longer be agnostic in the face of developing cyberthreats as the digital world grows more interconnected.

encountered by cybersecurity experts typically remain the same throughout time, such as authenticating individuals or protecting sensitive data from

unwanted access. According to a 2018 research from vulnerability scanning company EdgeScan, roughly 54% of the vulnerabilities it found in client networks that year first became known to the public ten years or more ago.

2)Create a cybersecurity culture

Employee cybersecurity training is a requirement. In its most recent annual Global Risks Report, the World Economic Forum found that 95% of all cybersecurity problems are caused by human mistake. Creating a culture of cybersecurity among employees will minimise this errors. Multi-factor authentication should be enforced. If these requirements are made, security will take precedence over all other considerations and should direct employee decision-making.

3)Building cyberdefence for organisations

Infrastructure owners and operators should begin by presuming that a cyberattack is imminent in order to construct effective defences. After that, they must create an integrated, unified cyberdefense that optimally safeguards all pertinent infrastructure assets. When determining what is pertinent, the asset owner frequently needs to be aware of what supporting infrastructure is also vulnerable—critical utilities, for example—and make sure that it is well safeguarded.

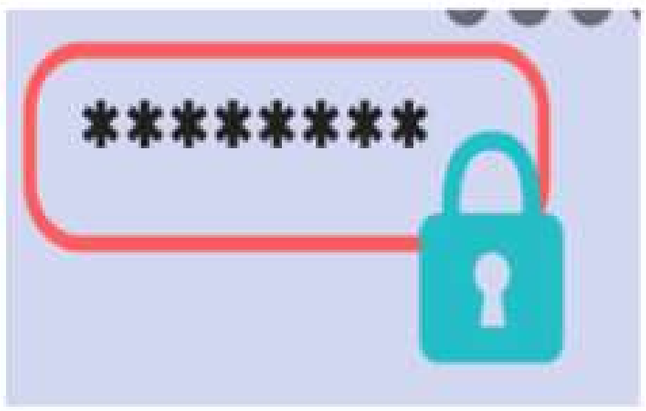
4)Developing an integrated defence

Every infrastructure network has a corresponding IT network where its proprietors and operators carry out daily operations including sending and receiving emails and producing reports. Similarly, to safeguard their data and technological assets, the majority of firms operating in an IT environment—and some organisations functioning in a linked infrastructure environment—have cybersecurity programmes in place. To defend both environments, one unified cybersecurity programme is more effective than two separate programmes.

It all comes down to habit and repetition when practicing excellent cyber hygiene. Making positive behaviors become habits should help you keep your client information and business data safe and secure in a remote working environment. These behaviors include enabling automatic software updates, running antivirus software on a regular basis, and often changing passwords.

Best practices for corporations in cyber hygiene

Use strong passwords



Keep your system up to date

Do not share everything on social media

3-2-1 backup strategy steps

Use backup strategies

Multifactor authentication

Use multi-factor authentication

Beware of Phishing attacks

Cybersecurity challenges and how do HR managers cope with them?

National Finalist

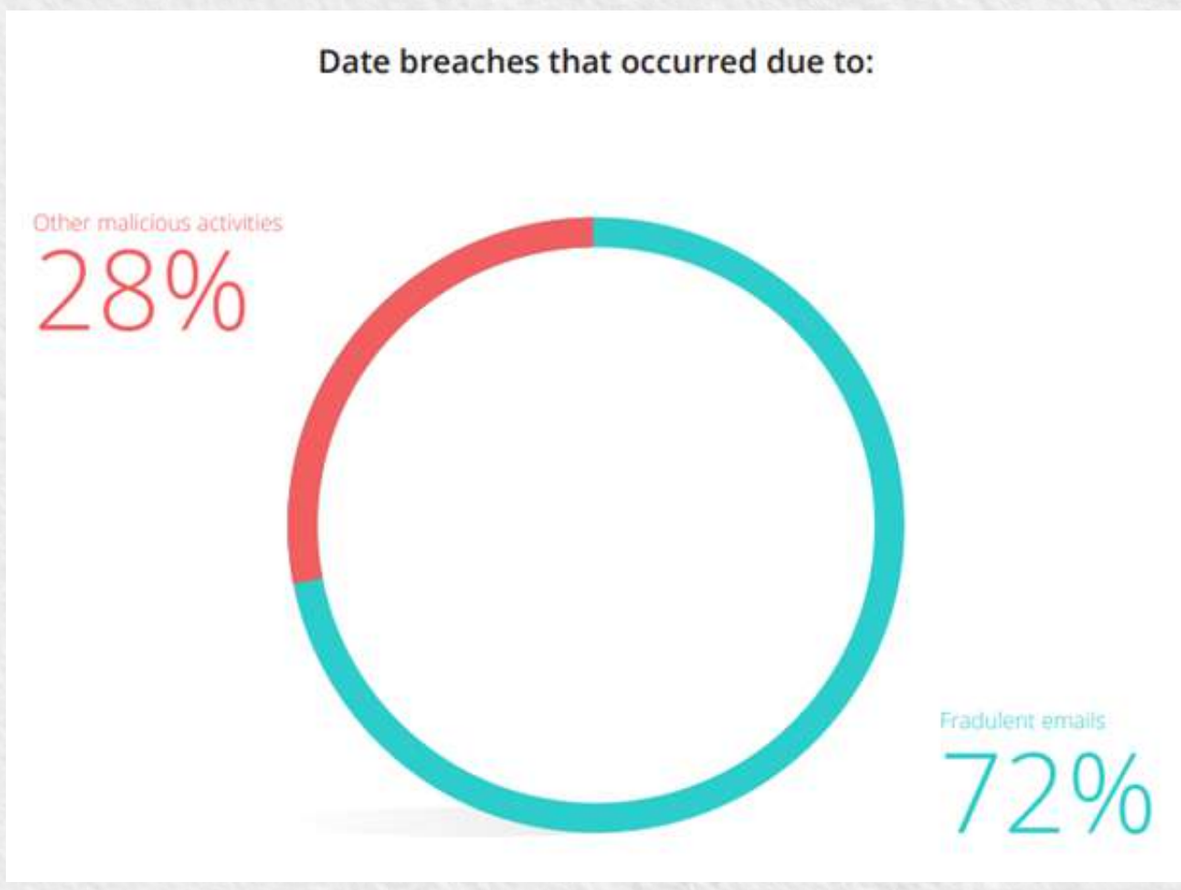
Nidhi Vajha
PGDM
Welingkar Institute of Management Development & Research, Mumbai

Security is handled via leadership or crisis. In the absence of leadership, we are left with a crisis.

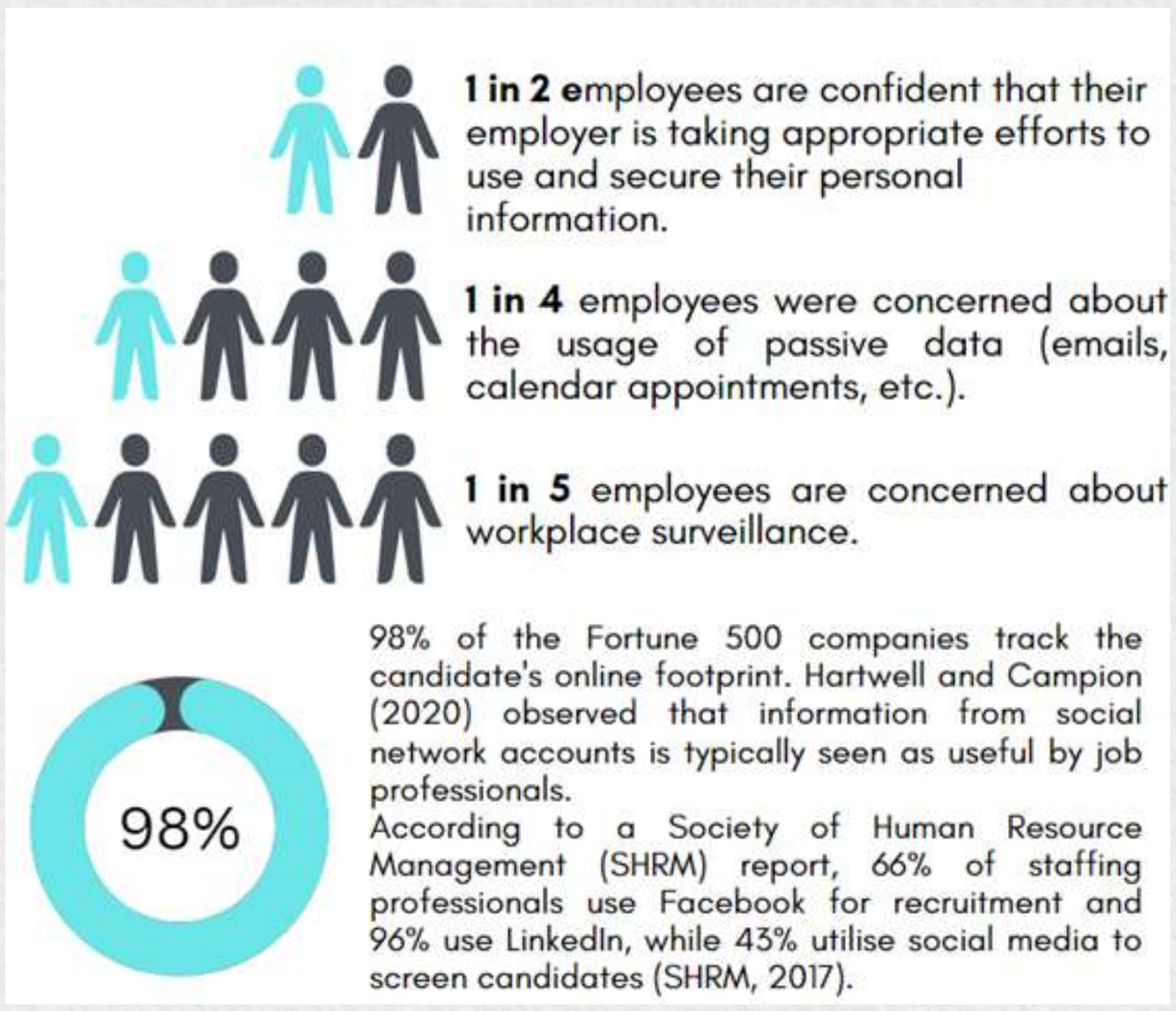
Security is a combination of technical and people controls, to reduce risk. Over the coming years, cybersecurity is assumed to be the second most important problem for global businesses. In the event of a security breach, a complete internet outage in a nation with strong connectivity would cause a daily GDP loss of 1.9%.

Human resources data is among the most valuable and critical data on many corporate networks. Employee social security numbers, dates of birth, bank information, home addresses, and other personal information are submitted to the company long before the employee ever joins. Data and security actions of employees are significant factors in an organization's overall cybersecurity. Attacks can be carried out by a number of techniques, including social engineering, malware, outdated/missing software updates which enable remote access to a system, ERP flaws such password breaches and SQL injection.

Although hackers and suppliers are a danger to an organization's cybersecurity, according to Mercer's 2020 Global Talent Trends Study, the staff's failure to adhere to data security rules is the largest concern. When employees open phishing emails, lose laptops, or put flash drives in that they shouldn't, they open themselves up to a lot of hazards. In Business Email Compromise (BEC) attacks, cybercriminals take over an employee's work email account and use it to send threatening emails to other employees. Naive employees believe the email and download dangerous files without thoroughly checking them.

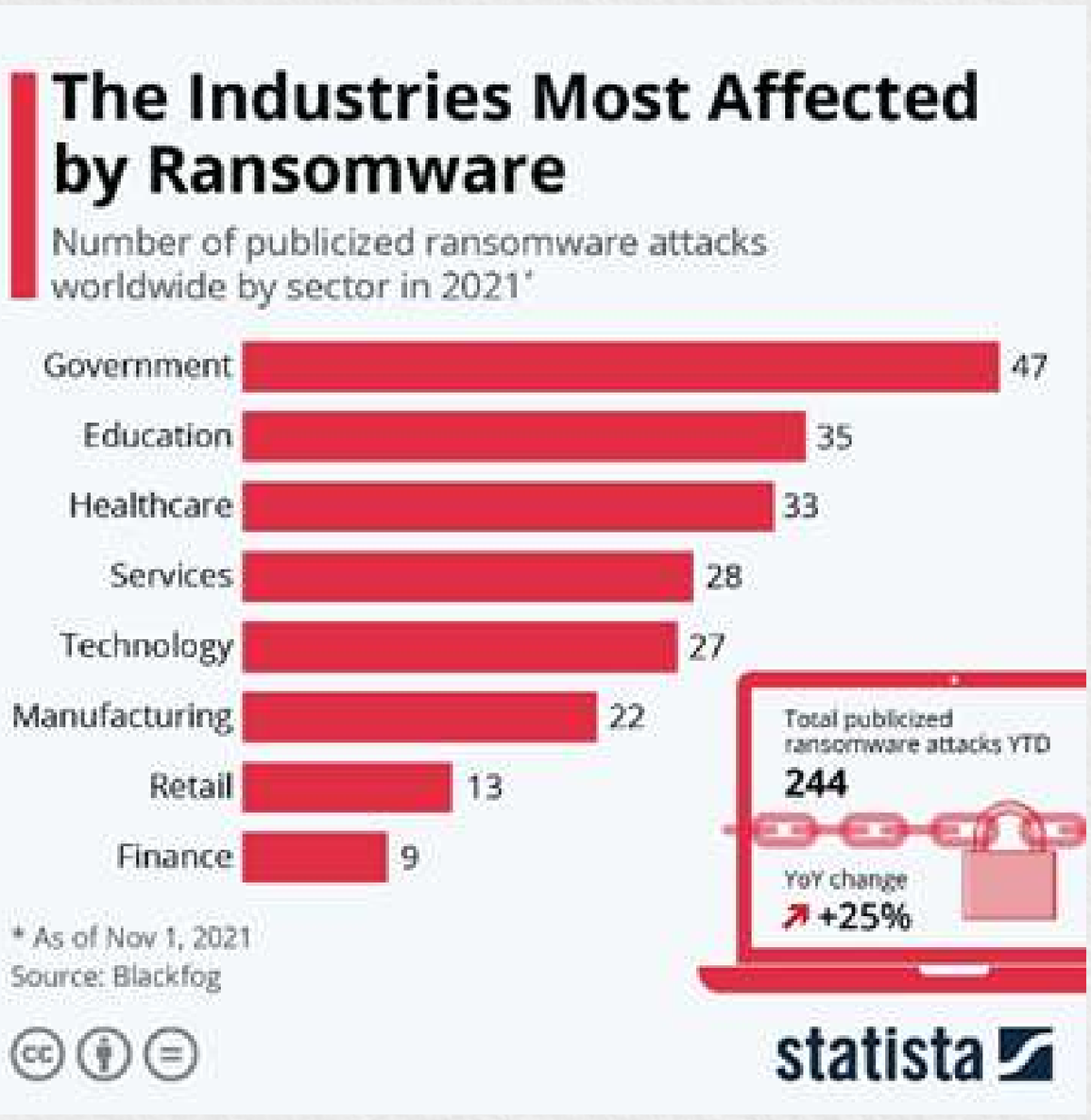


An online applicant tracking system, which preserves applicant information and enables organisations to process candidate applications more quickly, is thought to be used by 98% of Fortune 500 companies (Shields, 2018). Employees are concerned about having little to no control over how information is gathered, kept, and used. In a survey by the Society of Human Resource Management (SHRM), 66% of staffing professionals said they use Facebook for hiring and 96% said they use LinkedIn. 43% said they use social media in some way to assess potential employees.



Research from 2021 indicates that the government sector, followed by the education sector, is the most plagued by ransomware.

Optus, an Australian telecom company, disclosed this week that around 10 million customers, which accounts for roughly 40% of the Australian population had their data stolen, including names, birthdates, phone numbers, email



addresses, passport numbers, driving license numbers, and so on. The Australian authorities said that those whose passport and license details were stolen (approximately 2.8 million people) might face a considerable risk of identity theft and fraud.

In Q2 and Q3 of 2020, 22% of Fortune 500 organizations had active malware. 19 of the Fortune 500's 27 hardware, software, and IT services firms have been hacked.

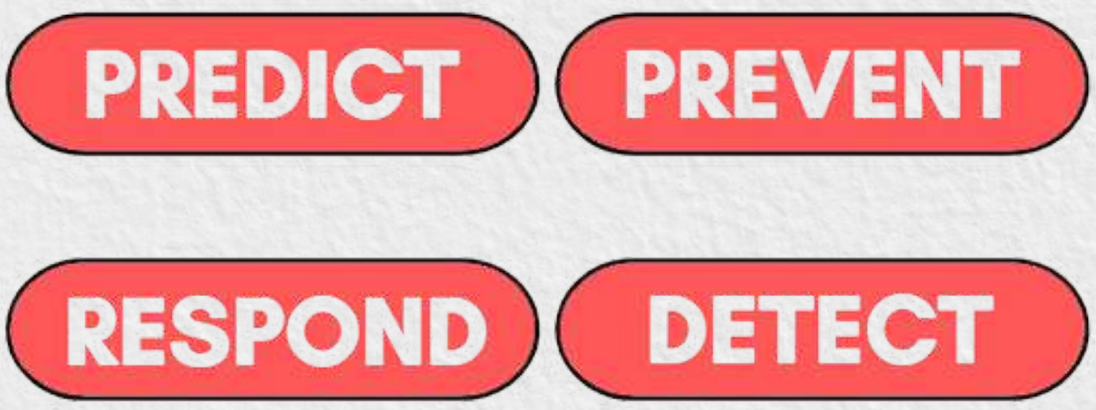
Bob Diachenko, a security researcher, discovered an unprotected database by data collecting platform "Adapt" in November 2018 which had over 9.3 million records of individuals and employer information, including their names, contact information, home addresses, social media accounts, job titles, and employer data such as organization description, size, and revenue. In response to incidents like this, the government stated in Budget 2022 that it would spend Rs 515 crore on

cyber security in FY 2022–23, of which Rs 215 crore would go to CERT-In, the Indian Computer Emergency Response Team, the organisation in charge of addressing cyber security issues.

Organizations are gathering information on their workers via their internet footprint. Employees post their social security number, phone number, home location, and birthdate online for a variety of purposes. Every time users fill out an online form with this information, a digital footprint is established that hackers may access. Hackers could be able to impersonate the employee, assume their corporate identity, and hijack the firm's databases if this information is combined with Dark Web resources. And this scenario is not an exception, but rather a daily occurrence. The digital traces we leave behind make it simpler for hackers to get beyond security safeguards and target business assets. According to a survey, 60% of departing employees steal employer information. The majority of breaches in 2016 (60%) had a financial gain as their primary goal, as indicated by the 2017 Verizon Data Breach Investigations Report (DBIR).

Employee mistakes led to a string of data breaches for the FDIC in the United States in February 2016, and one employee put Uber's self-driving car concept in jeopardy in 2017. Ex-employees obtained sensitive material faster than firms could discover and investigate the event. Data theft from an employer is quick and simple since it just takes a few minutes to copy crucial data to your device. However, it could be challenging to find a malicious insider on the company's network, and based on DBIR, data leaks might go undetected for months or even years.

ROLE OF HR:



A recruitment-to-retirement (R-to-R) approach should be used by HR, starting with educating potential employees about information security and privacy during the initial recruitment stage and continuing all the way up to the employees' retirements. HR should work with management to put effective policy communication and clarifying efforts into place. HR should collaborate with management to implement suitable policy communication and clarification initiatives.

Minimum risk awareness and responsible behaviour regarding electronic communication must all be included in yearly employee training. Furthermore, additional inspection should be considered for more sensitive roles, and data and access should be compartmentalised based on worker duties and responsibilities.

HR also contributes to relationships with other organisations by understanding and acknowledging the terms of their contracts and who will be liable for cyber security issues if the company experiences a breach. To decide how the risk will be managed if and when it arises, HR should work with the risk management department if the company has contracts with other employment agencies, contractors, and suppliers. As a result, human resources can play a predictive and preventative role in this situation.

The safety of HR data is essential because when data is shared with third-party partners, the business inherits the security—or lack thereof—of that data. Confidentiality may be prioritised by using robust cybersecurity procedures such as data categorization, encryption, backups, audits, storage, access control, etc.

Returning to the subject of information theft, HR is involved in termination planning and processes. In this case, HR should collaborate with other divisions, like IT, to create BYOD (Bring Your Own Device) regulations to restrict employees from exploiting remote access and carrying company technology home. In the event of a hack, HR should respond immediately to cut down losses. It is critical to identify losses that cannot be avoided to respond quickly and thoroughly.

The HR department of a company is in charge of meticulously implementing all policies and guidelines, as well as influencing workers' attitudes about cyber hygiene. They must ensure that staff follow security regulations, whether it is picking the appropriate password, maintaining email security, or detecting potential cyber dangers and frauds online.

The State of cybersecurity in the financial services industry

National Finalist

Vivek Kumar Garg
PGDM - General
T A Pai Management Institute

I. Introduction

Cybercriminals are drawn to the data of financial services companies because it may swiftly be monetized in grey markets, including the sale of customers' Personally Identifiable Information (PII). About 1 in 4 data breaches also involve hostile attacks. Accidents involving data may be disastrous, resulting in lost profits and the degradation of trust, company closures, regulatory fines, and consumer confidence.

Widespread impact along with high costs makes cybersecurity a critical priority for regulatory bodies. They're implementing tight security measures in the high-risk atmosphere. Regulators are strengthening cybersecurity policies and procedures through regulations, standards, recommendations, and frameworks to thwart assaults. The cost of non-compliance might be quite substantial. Still, several financial services lack regular compliance programs. Although financial services companies also invest on cybersecurity technologies, they frequently continue to ignore important recommendations made to protect against the most common security difficulties. They sometimes ignore that in a virtualized world, conventional security plans and in-premise security strategy are less adequate. Conventional security procedures must be backed up by cloud-based resources, technology, and cloud-enabled tactics that reduce the dangers of hostile assaults and mishaps. With the aid of this cloud-based financial services, companies can accomplish three crucial cyber protection methods, i.e., reduce cybersecurity risks, enhance regulatory compliance, and safeguard data.

Here are just a handful of the most damaging cyberattacks on financial services institutions in the past. Although they barely scratch the surface of the financial sector's cyber breaches, they illustrate the vulnerabilities faced by the organisations in the current era.

Exhibit 1

Attack Year	Organisation	Attack Method	Damage
2019	Capital One Group	A company's internal IT employee obtained access to servers through misconfigured web application firewall	Exposure of 106M credit cards
2019	First American Financial	Advantage taken by attacker due to a technical coding error	Exposure of 850M financial and personal records
2016	Equifax	Unpatched application vulnerability exploited	$4B loss; 148M accounts breached
2016	Bank of Bangladesh	Stolen SWIFT credentials used to transfer funds to Asian bank accounts	$81M loss
2016	Charles Schwab	Breached by an uninvited individual who acquired customer's credentials and then disclosing account names and numbers, stock market position and recent transactions	All customers
2016-2017	UniCredit (Italy)	Spy employee from other organisation gained unauthorised access to loan data	390k clients

Source: Ernst& Young

II. Cybersecurity challenges in Financial Services

Organizations face security challenges while delivering regional, international, or local financial services. They are deployment of multiple clouds, data security issues, evolving technological vulnerabilities, deliberate insider threats as well as unintentional insider threats, audit risk and consistent regulatory compliance.

1. I**nsider threats**: Many businesses do not have robust insider threat plans as their security measures are only intended to deter thieves

1./robbers. These breaches form 57% of the total breaches globally. Insiders have the potential to do significant harm, possibly catastrophic harm whilst camouflaging with the regular employees. Money transfers, illicit transactions, security code exploitation, and data dumps are a few harms. It happens when there is a weak identity and access management in place. Also, when Role Based Access Controls (RBACs) are poorly implemented.

2. Threats due to emerging technologies:
Transitioning of financial institutions to digital channels such as mobile transactions, internet banking, and the Internet of Things (IoT), expands their cyberattack surface. The more channels businesses offer their clients, the more possible paths cybercriminals have in getting past their security measures.

3. Increasing cloud dependence: Financial services companies are rushing to seize the advantages of cloud computing. Even though multi-cloud setups have many advantages, many financial services businesses are hesitant to use them. The concern of data breaches in third-party settings is still present. The main obstacle to the adoption of cloud services is that, while businesses can outsource business functionalities but cannot

outsource their data security responsibilities in entirety.

4. Data security risks:
Considering the constant threats, firms must protect the Personally Identifiable Information (PII) of its clients, private business communications and intangible property. Any loss of data results in a series of issues, including regulation scrutiny and lawsuits.

5. Phishing attacks:
These attacks happen when the user clicks on an unsolicited URL or open an attachment sent through an email. This gives an opportunity for the attacker to execute malwares such as ransomware, trojan, credential stealer and many more. This compromises the security of the system and can result in huge losses. Untrained users and weak IT security policies in place are the underlying reasons for such type of an attack.

A few more attack methods are explained in the below exhibit.

Exhibit 2:

1. Spear phishing
Employee in targeted organization receives email with the Carbanak backdoor as an attachment

2. Backdoor executed: credentials stolen
Upon opening attachment, employee activates the Carbanak backdoor

3. Machines infected in search for admin PC
Carbanak searches network and finds admin PC; embeds and records

4. Admin PC identified, clerk screens intercepted
Attacker watches admin screen to mimic admin behavior for the bank's cash-transfer systems

5. Balances inflated and inflated amount transferred
Attackers alter balances, pocket extra funds ($1k account enlarged to $10k, then $9k transferred)

6. ATM programmed to dispense cash
Attackers program ATMs to issue cash to waiting accomplices at specific times

7. Cash moved through channels by wire transfers, e-payments
Attackers use online and e-payments to receiver banks to transfer extracted funds

Exhibit 3:

Fraud and insider threats

- Internal and external threats
- Retail and nonretail threats
- Insider threats
- Market abuse and misbehavior

Cyber breaches

- Confidentiality
- Integrity
- Systems availability

Financial crimes

- Money laundering
- Bribery and corruption
- Tax evasion and tax fraud

Example: cyberattack on a central bank

- Bank employee's SWIFT[1] credentials stolen with the help of insiders
- Malware surreptitiously installed on the bank's computers to prevent discovery of withdrawals
- Funds routed from bank's account at a branch of another country's central bank to a third bank (on a weekend to ensure staff absence)
- Withdrawals were made at the third bank through multiple transactions that were not blocked until too late
- Attacks may have been linked to a known sanctioned entity

III. 5-Step protection strategy:

Step 1- Adopting a security framework

As a financial institution APRA CPS 234 is a mandatory obligation. ISO 27001 and NIST are other recommended frameworks to create a robust security roadmap.

Step 2- Assessing gap

Performing gap analysis to assess security posture to comply to adopted security standards.

Step 3- Strategy designing and building roadmaps to fill gaps

Hiring cybersecurity analysts, outsourcing to vendors, ensuring 24*7 security monitoring are a few

steps to ensure filling of the gaps.

Step 4- Building compliance

Cybersecurity being a continuous process, hence building a mechanism is essential to ensure compliance in real-time.

Step 5- Assurance

Seeking assurance to form security operations centre (SOC) to continuously control and monitor security in real-time. It also ascertains trust of clients and peers.

IV Best practices for organisations

1. Strong Encryption:

Data may be protected and obscured with encryption so that anybody or anything that isn't officially authorised cannot decrypt it and read it. A person or programme that requires access to decrypt the encrypted data, needs an appropriate secret code, often known as a "key". Key re-formats the data such that it becomes readable. This is how encryption offers a method that, if all other security precautions are ineffective, and data is in fact stolen, it becomes worthless and is totally safeguarded.

2. Threat modelling and compliance: Threat modelling assists financial organisations of all sizes in avoiding potential liabilities by eliminating abnormalities. Organizations may better understand their attack surface and data storage security effectiveness by using threat modelling. The development of threat models must take into account automated platforms, operations, and security. It is advised to incorporate threat intelligence gathered from organisations like OWASP, MITRE, and CIS.

3. Managing third-party risks: Financial institutions rely on a range of suppliers, partners, and vendors, and such connections expose the vulnerabilities of the institute. The enemies may easily locate the weakest link in the chain, regardless of how solid the security posture may be. Consequently, establishing a strong Vendor Risk Management Programme (VRMP) is highly advised.

4. Training:

The level of client trust in the security procedures is crucial to the success of financial institutions. The client wants to work with an institute that values the privacy of their information and money. As a result, it is strongly advised that security training is provided to both the customers and personnel. It is also recommended to provide training to customers on how to use mobile apps and internet banking securely. Additionally, giving company staff security training to lessen the attack vector.

V. Conclusion

In digital transformation era,

cyberattacks have advanced in sophistication and potency with the accelerated pace of technological advancement. The difficulty presents to solve the challenges simultaneously by constructing secure infrastructure whilst improving services. To protect themselves against complex cyber-attacks, financial institutions must strive for a sustainable cyber resilience plan.

Cyber Security - A Safe Warehouse for data operations

National Finalist

Puneet Jindal
Digital and Telecom Management
Symbiosis Institute of Digital and Telecom Management (SIDTM)

Introduction

The likelihood that your firm may be exposed to harm or suffer a financial loss as a result of a cyberattack or data breach. The potential loss or injury to technical infrastructure, technology use, or an organization's reputation would be a better, more comprehensive description.

Due to the increased reliance on computers, networks, software, social media, and data internationally, organisations are becoming increasingly susceptible to cyber-attacks. Data breaches, a typical cyber assault, can result from inadequate data protection and have a significant negative economic impact.

The prevalence of cloud services with lax default security settings, along with global connection, increases the possibility of cyberattacks coming from outside your company.

The networks that connect a business to the vendors it uses to manufacture and distribute its goods and services are known as supply chains. The flow of commodities, including all the procedures necessary to convert the raw materials an organisation consumes into the final items or services that the organisation offers, must be managed in order to effectively manage a supply chain.

Planning and overseeing the sourcing, acquisition, and conversion of raw materials, as well as logistics management tasks, are all included in supply chain management. Increasing competitive advantage is one of the main reasons businesses adopt a global supply chain management approach. However, a lot of the advantages that come with supply chains can also raise an organization's risk in terms of cybersecurity, business continuity, reputation, and quality.

Organizations increasingly rely on broad supply chains to do business as the globe grows more linked. For many, controlling the supply chain and the risks attached to it, however, is a costly and time-consuming procedure.

Organizations that don't effectively

manage their supply chain risks are frequently more vulnerable to cyberattacks, which may result in significant disruption.

Data Breaches

One of the most important cybersecurity risks that enterprises face today is data leaks. The likelihood is that in the upcoming years, both the frequency and the seriousness of these security events will only increase.

In addition to any regulatory or legal repercussions, a data leak or breach typically causes a company to suffer considerable financial loss and reputational harm. The average price of a data breach in 2021 was a staggering $4.2 million.

According to one piece of study, firms frequently take a long time to detect a data breach once it has happened, on average 197 days, even with the proper legal and compliance requirements in place. Even worse, when businesses have a data breach as a result of a supply chain security event, that number increases. According to IBM and the Ponemon Institute, it typically takes a business 280 days to discover a third-party data breach.

The likelihood that your data will be compromised or exposed increases the more sensitive data you share with third parties in your supply chain. Information that has to be safeguarded from unauthorised access in order to preserve the security or privacy of a person or organisation is referred to as sensitive data.

Unauthorized access via a business email account, hacking of an email provider, a lack of encryption, insecure websites, and incorrectly stored login information are some of the most frequent data breaches brought on by third-party providers. In extreme circumstances, third parties may even purposefully release private customer information outside the company, leaving your company open to supply chain assaults from hackers, rogue nation governments, and other cybercriminals.

Cybersecurity Breaches

This category is wide on purpose since there are a lot of recent technological developments that increase firms' susceptibility to cyberattacks along the supply chain in previously unheard-of ways.

Any modern gadget with an Internet connection poses a risk to the supply chain. For instance, the Internet of Things (IoT) typically refers to consumer electronics like smart thermostats or personal fitness trackers; in 2021, there were more than 10 billion active IoT devices globally.

IIoT especially refers to hardware that powers businesses on a much wider scale. IIoT includes all Internet-connected and Internet-

communicating devices, ranging from sensors and scales to engines and elevators, with the goal of enhancing production.

Malware and Ransomware attacks

Unfortunately, ransomware and malware assaults are getting increasingly frequent. These assaults are intended to steal data, alter internal data, or delete private or confidential information.

Any invasive programme that may enter your computer systems and cause harm, destruction, or data theft is known as malware. Viruses, worms, Trojan horses, and ransomware are among the most prevalent forms of malware threats.

The 2020 SolarWinds malware assault is among the most recognisable malware attacks in recent memory. Early in the year, hackers gained access to the Texas-based SolarWinds' network and introduced malicious malware into Orion, the company's popular software system used by about 33,000 of its clients to manage their IT resources.

Customers of SolarWinds who were using Orion received software upgrades in March 2020 that contained the malicious malware that the hackers had implanted. The hackers were then able to install more malware to spy on these businesses and organisations since the spyware had built a backdoor into the IT systems of SolarWinds' clients.

Ransomware is a common form of computer assault. By encrypting a victim's data, this type of malware enables the attacker to demand money in return for the decryption key. Most frequently, cryptocurrencies like bitcoin are used to trade money in return for a decryption key that can restore your data while obscuring the attackers' identities.

Real life examples

Kia and Hyundai cars

A network of thieves obtained customer and product information in 2016 to steal dozens of vehicles and smuggle them into the West Bank. The automobiles in the city may then be found using a list of licence plates. The data was used to identify the code of the keys and the address of the owner to steal a car. The hacker attempted to extract confidential data from the control system, including addresses and key codes for the stolen automobiles. Instead of the owner, hackers were able to access the automobiles' actual position and control system (Barth, 2016).

Wannacry Ransomware

The national healthcare system was attacked by the Wannacry ransomware assault in June 2017. (NHS). This malware affected over 150,000 machines across 150 nations. The result of this kind of attack was the rerouting of

ambulance services and the interruption of service at several hospitals around the system. Similar to a controller, the doctor also had access to the patient's data and medical algorithms. The patient's biometrics are measured as part of a continuous procedure to collect this data. The WannaCry ransomware assault prevented access to data, which had an impact on how the NHS operated because the controller was no longer able to access the data. The outcome of the therapy procedure is skewed as a result of such an attack (Smith et al., 2017).

Strategies from Attacks

Your business may adopt a variety of supply chain risk management best practises to shield your corporation and its clients from the cyber dangers mentioned above (and more). In order to better protect yourself against the aforementioned cyberrisks, try the following:

- Establishing compliance requirements for each and every one of your external providers, including producers, suppliers, and distributors.
- Clearly defining user roles and putting security measures in place will help you manage who has access to your systems and at what degree of clearance or permission. The least privilege principle governs this.
- Deciding on, articulating, and enforcing data stewardship principles; identifying who owns what data and what they are permitted to do with it.
- Giving each of your workers thorough security awareness training.
- Developing a single disaster recovery strategy in collaboration with suppliers in your supply chain network to ensure company continuity.
- Putting in place backup safeguards to protect your data backups.
- Upgrading your firewalls, anti-spyware, and antivirus software on a regular basis Additionally, you want to think about investigating more sophisticated cybersecurity methods like DNS filtering and network access control.
- Selecting a software programme that gives you a complete insight into your supply chain risks, like the Reciprocity ROAR platform, to enable you to spot dangerous conduct or anomalous behaviour right away.

Tata Steel D&I Challenge

Ashwin Sajayan

1. Firstly, Congratulations on winning How do you feel about it?

I feel immensely proud to be one of the top 10 finalists across India who got a chance to present in front of top leaders from the Tata Steel Jamshedpur corporate event. I also bagged a paid winter internship with the firm in my chosen domain for two months.

2. Could you brief us about this competition? What were the hurdles you faced and how did you overcome them?

The problem statement was regarding queer employability in India specifically in the manufacturing sector. There were three rounds where I had to create a compact presentation of my solution along with a video. After clearing the rounds, I made it to the top 10 finalists across India who were supposed to present it offline in front of a senior leadership panel.There were multiple hurdles that I faced during the competition.

As I was doing this alongside my summer internship and research project, it was extremely difficult to manage time and prioritize. To not let my internship suffer during day time, I used to pull all-nighters and work on my presentation post 10 pm. Another hurdle was my lack of knowledge in the D&I domain for which Dr. Shilpa Narayanswamy ma'am from the Operations department guided me and helped me out with her valuable suggestions. Competing with MBA as well as engineering students from top colleges like IIT, XLRI, and IIMs scared me at times but I overcame my fears and gave my best.

3.What were your key learnings and takeaways?

Inclusivity and Diversity are among the core values of all top companies today. Companies are extensively working and researching to enhance the employability of marginal communities in India. There's a huge untapped talent pool available in India within the queer community and we have to find ways to reach out to them. Lastly, it doesn't matter which college you're coming from, just believe in yourself and work hard towards your goal.

4. It's always difficult managing time between academics, personal life, and other opportunities. How did you manage your time?

Your hard work pays off. Plan out your schedule and accommodate all the important things you want to work on. I had to even skip classes for a few days as I had my final presentation in Jamshedpur but the college has been extremely supportive throughout.

5.What guidance or recommendations would you offer to juniors to help them land such a fantastic platform?

WeAchievers

Taking initiative and grabbing every opportunity is important. The opportunity might not come to you but you have to be alert and keep looking. Do not get demotivated by seeing competition from students from better colleges. You are as good as you believe. Work on your communication, presentation, and research skills. Take guidance from faculties from the college.

EDITORIAL TEAM

Sushmita Mudaliar
Chief Editor

Diksha Maheshwari
Co-Editor

Ashwin Sajayan
Co-Editor

TEAM SAMVAD

CREATIVE MINDS

Rohini Patial
Head

Shalini Balla
Deputy Head

Jyoti Honrao
Member

Maharshi Vyas
Member

TEAM SAMVAD

CONTENT CURATORS

Chandramohan Chauhan

Head Curator

Shrutika Shrivastava

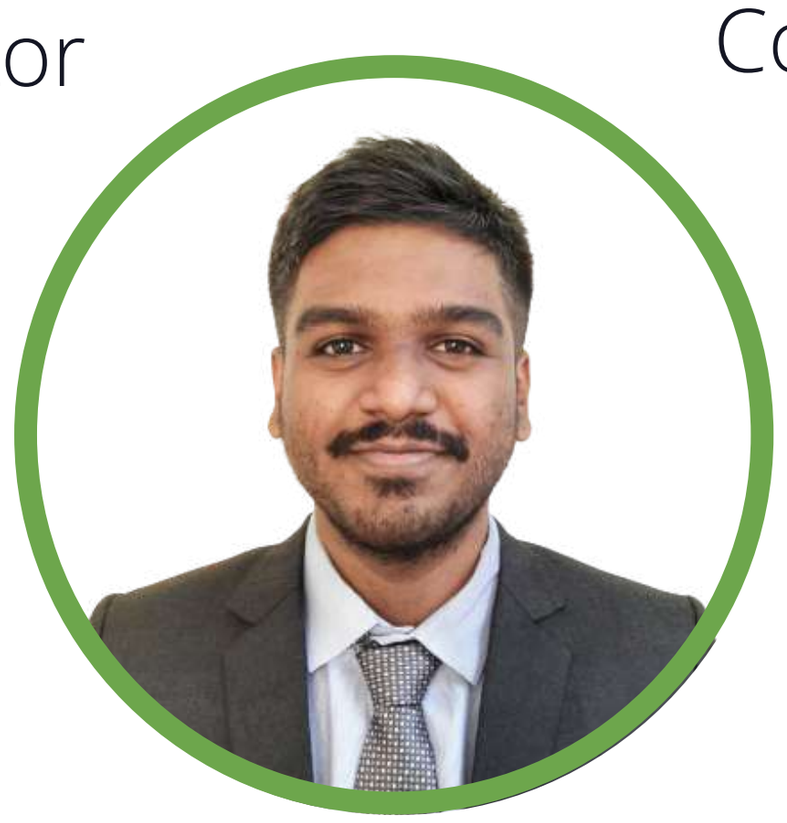
Deputy Curator

Neeraj Deshpande

Content Curator

Abhinay Yagnamurty

Content Curator



Sanket Aradhye

Content Curator

WECHAT MASTERS

Madhav Sharan
Head

Utkarsha Chaudhari
Member

Amit Dengale
Member

TEAM SAMVAD

PR PROS

Akansha Khatuwala

Head

Pritika Sarkar

Deputy Head

Jatin Gupta

Member

Charul Jain

Member

We invite articles for the next 128th issue of SAMVAD

The theme for the edition: **'GAMING'**

The articles can be from Finance, Marketing, Human Resources, Operations, or General Management domains.

Submission guidelines:

- Word limit: 800 - 1200 words.
- The cover page should include your name, institute's name, course details & contact no.
- The references for the images used in the article should be mentioned clearly and explicitly below the images.
- Send in your article in .doc or .docx format, Font size: 12, Font: Arial, Line spacing: 1.05' to samvad.we@gmail.com.
- Please name your file as: __<section name e.g. Marketing/Finance> Subject line: <Your Name>_<Course>_<Year>_<Institute Name>
- Ensure that there should be no plagiarism of more than 5%, and all references should be mentioned clearly.
- Clearly provide source credit for any images used in the article.<!--EndFragment--> </body> </html>

Follow us on

@samvad.weschool Samvad WeSchool SamvadWE

@samvad_we Contact Us: samvad.we@gmail.com