Impact of Covid-19 on cyber crimes

Pramodkumar H N

Analyst and Certified Ethical Hacker (**ECC7843915620**)

Cyber Security

Abstract: **Cyber Security plays an important role in the field of information technology. Securing informationhas become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that comes to our mind is cyber crimes which are increasing immensely day by day. Various Governments and Companies are taking many measures in order to prevent these cyber crimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on the statistics and the mitigation of cyber crimes.**

Keywords: **Cyber Crime, Challenges, Statistics, Prevention.**

1. INTRODUCTIONS

As the Government/organizations around the world continue to trudge through the disruption caused by the COVID-19 pandemic, cybercriminals keep coming up with even more menacing ways of dragging them down. According to research conducted by Cyber security Ventures, cyber security experts have predicted that cybercrime will cost the global economy $6.1 trillion annually by 2021. With the pandemic serving as a catalyst, cybercrime is expected to soon become the world's third-largest economy.

While the ongoing pandemic has forced an unprecedented number of people to work from home and forgo the security of a well-developed IT infrastructure, cybercriminals have marked the unwary employees as the target of choice. Organizations were compelled to innovate and adapt so swiftly that the security didn't get enough time to catch up, leaving businesses vulnerable to the cyber threats looming across the horizon.

2. STATISTICS ON CURRENT CYBER THREAT LANDSCAPE

Owing to the COVID-19 pandemic and the sudden transformation to remote work culture, cybercrimes have risen like never before and are expected to rise even more as we move towards 2021.

Following are some outrageous statistics showing just how severely these cyber attacks are affecting the global economy:

As per the research conducted by Cyber Security Ventures (CSV),

➢ Within months of the first lockdown due to the pandemic, more than 4,000 malicious COVID-related sites popped up across the internet.

➢ A cyber attack incident will occur every 11 seconds in 2021. This is nearly twice the rate in 2019 (every 19 seconds), and four times what it was in 2016 (every 40 seconds).

➢ Cybercrime is expected to cost the global economy $6 trillion annually by 2021, as compared to $3 trillion in 2015. This will soon make it the world's third-largest economy, after the United States and China.

➢ CSV predicted that ransomware damages will cost the world $20 billion by 2021, which is 57 times more than what it was in 2015 ($325 million). This makes ransomware the most rapidly growing kind of cybercrime.

➢ According to CSV, 91% of cyberattacks are launched through spear-phishing emails, which infect the organizations/Government with ransomware.

3. WHAT CAN GOVERNMENTS/ORGANIZATIONS DO TO STAY SECURE?

As the rise in cybercrime is showing no signs of slowing down, it is essential for Governments/organizations to take the necessary precautions to avoid suffering any losses.

The three most critical aspects of any Governments / organization include its people, processes and data. By focussing their resources on protecting these three elements, Governments / organizations can arm themselves against all kinds of prevalent and emerging cyber threats.

Protecting People

“ Turn Your Employees Into A Cyber Threat Shield! ”

The best way of protecting your employees against cyber attacks is by educating them about the prevalent cyber security threats. Owing to cyber security unawareness, employees can unintentionally cause data breaches, leaving your company at risk. A report has revealed that implementing cyber security awareness training amongst employees significantly reduces human error, mitigating up to 90% of cyber risks.

With the dramatic increase in cyber risks due to the transformation to remote work culture, providing your employees with cybersecurity awareness trainingby Security professionals has become more important than ever. An organization cannot protect its finances, assets and reputation from cybercriminals without spreading awareness amongst its employees.

95% of cybersecurity breaches are caused by human error.

Cybersecurity awareness tools that helps in securing your workforce against various kinds of cyber attacks. Organizations can also implement a phishing incident response tools like Threat Alert Button to empower the employees to report any suspicious-looking emails immediately.

Protecting Processes

It is essential for an organization’s IT department to continually monitor, review and update all organizational processes. Employees should be made aware of the consequences of installing applications or software in their systems without the knowledge or approval of the IT department.

Any known vulnerabilities should be constantly monitored by the organization. Companies can provide protected and locked systems to the employees working remotely. This can be an effective way of restricting them from installing any malicious software.

Protecting Data

An organization must have a firm grasp on the data that it holds, processes and passes on. As per a recent study, companies share sensitive and confidential information with more than 500 third parties.

The first and foremost step an organization should take is to conduct an inventory and ensure any information is shared strictly on a need-to-know basis.

Secondly, make sure to encrypt all sensitive data including employee information, all business data and customer information. This ensures that the data becomes useless in case it falls into wrong hands. Also, always create regular backups of all your data and store it securely outside your network.

As the rise in cybercrime is showing no signs of slowing down, individuals and organizations alike are equally at risk. Therefore, it has become extremely important to take the necessary precautions and keep essential cyber security tips in mind for defending yourselves and your organizations against these threats.

4. CYBER CRIME STATISTICS BY ATTACK TYPE

It’s crucial to have a grasp of the general landscape of metrics surrounding cybersecurity issues, including what the most common types of attacks are and where they come from.

Some of these most common attacks include phishing, whaling,malware, social engineering, ransomware and Distributed Denial of Service (DDoS) attacks.

There are new malware and viruses being discovered every day.

Ransomware and Malware

- The average ransomware payment rose 33% in 2020 over 2019, to $111,605. (Fintech News)
- In 2018, an average of 10,573 malicious mobile apps were blocked per day. (Symantec)
- 94% of malware is delivered by email. (CSO Online).
- The average cost of a ransomware attack on businesses is $133,000. (SafeAtLast)
- 48% of malicious email attachments are office files. (Symantec)
- Ransomware detections have been more dominant in countries with higher numbers of internet-connected populations, and the U.S. ranks highest with 18.2% of all ransomware attacks. (Symantec)
- Most malicious domains, about 60%, are associated with spam campaigns. (Cisco)
- About 20% of malicious domains are very new and used around one week after they are registered. (Cisco)

Phishing

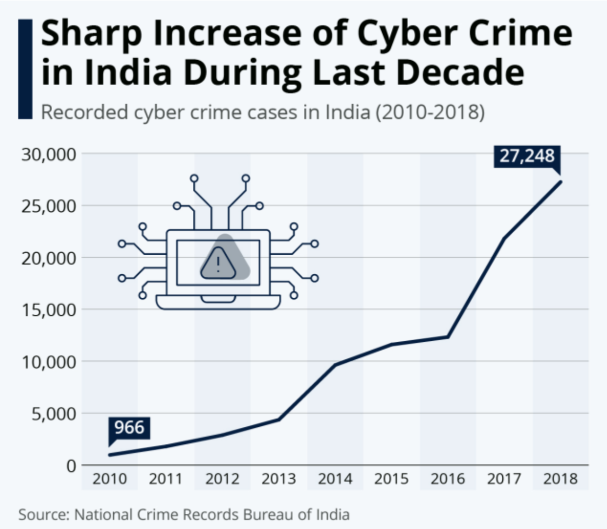
- After declining in 2019, phishing increased in 2020 to account for 1 in every 4,200 emails. (Symantec)
- 65% of groups used spear-phishing as the primary infection vector. (Symantec)
- 1 in 13 web requests lead to malware. (Symantec)
- Phishing attacks account for more than 80% of reported security incidents. (CSO Online)
- $17,700 is lost every minute due to a phishing attack. (CSO Online)

IoT, DDos, and Other Attacks

- By 2023, the total number of DDoS attacks worldwide will be 15.4 million. (Cisco)
- Attacks on IoT devices tripled in the first half of 2019. (CSO Online)
- Malicious PowerShell scripts blocked in 2018 on the endpoint increased 1,000%. (Symantec)
- The Mirai-distributed DDoS worm was the third most common IoT threat in 2018. (Symantec)
- 30% of data breaches involve internal actors. (Verizon)
- IoT devices experience an average of 5,200 attacks per month. (Symantec)
- 90% of remote code execution attacks are associated with cryptomining. (Purplesec)
- 69% of organizations don't believe the threats they're seeing can be blocked by their anti-virus software.(Ponemon Institute's Cost of Data Breach Study)
- 1 in 36 mobile devices have high- risk apps installed. (Symantec)

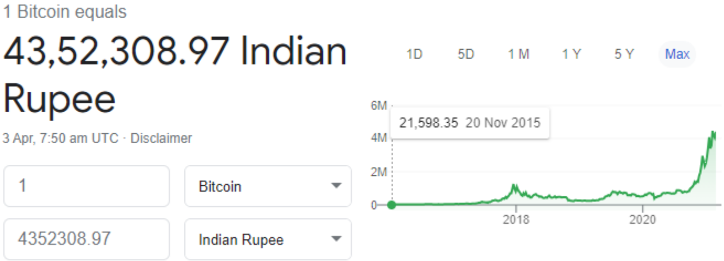
Government

- The U.S. government saw 1.2 billion records breached in 2018. (Purplesec)
- Manufacturing companies account for nearly a quarter of all ransomware attacks, followed by the professional services with 17% of attacks, and then government organizations with 13% of attacks. (Security Intelligence)
- The U.S. government allocated an estimated $18.78 billion for cybersecurity spending in 2021. (Atlas VPN)
- 3.17 lakh cybercrimes in India in just 18 months, says Indian govt.


Sharp Increase of Cyber Crime in India During Last Decade

Recorded cyber crime cases in India (2010-2018)

Source: National Crime Records Bureau of India


1 Bitcoin equals

43,52,308.97 Indian Rupee

3 Apr, 7:50 am UTC · Disclaimer

1 | Bitcoin

4352308.97 | Indian Rupee

5. STATISTICS OF CYBER ATTACKS IN INDIA

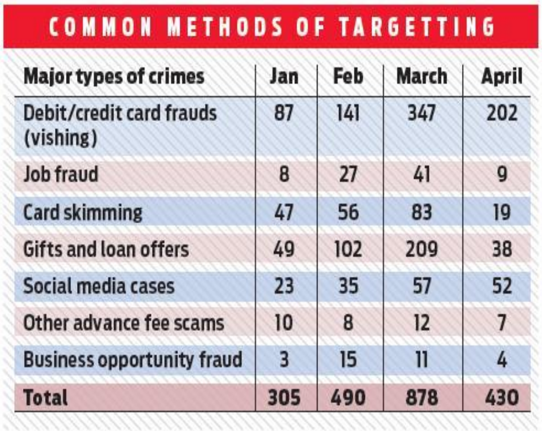
- " As per the data maintained, since its inception 3,17,439 cybercrime incidents and 5,771 FIRs have been registered up to February 28, 2021 in the country which includes, **21,562 cybercrime incidents and 87 FIRs in Karnataka**and 50,806 cybercrime incidents and 534 FIRs in Maharashtra ".

- With over 12,000 cases, Karnataka tops cybercrime list.(Deccan Herald)

- If you are a cyber crime victim, chances of your attacker getting a jail term is very less in India, especially in Karnataka where not a single case that went to trial in 2017 saw a conviction.(Deccan Herald)

The first two months of the lockdown saw a sharp spike in cybercrime, with a majority of them directed at elderly people and single women. According to City Crime Records Bureau data, March and April together saw 1,308 cyber crime cases with a jump in bank fraud and scams in which people impersonating government officials trick people into transferring money for welfare schemes or a government-run relief fund.

"Cyber attackers pretending to be bank officials make calls (vishing) or send emails or SMSes (phishing) to customers, asking them for their account numbers, credit or debit card numbers, CVV, OTP etc". From January to April, police registered 2,103 cases. "Six of every 10 cases we see are related to senior citizens".



COMMON METHODS OF TARGETTING

Major types of crimes	Jan	Feb	March	April
Debit/credit card frauds (vishing)	87	141	347	202
Job fraud	8	27	41	9
Card skimming	47	56	83	19
Gifts and loan offers	49	102	209	38
Social media cases	23	35	57	52
Other advance fee scams	10	8	12	7
Business opportunity fraud	3	15	11	4
Total	305	490	878	430

6. COVID-19 CYBERSECURITY STATISTICS

COVID-19 has impacted every industry and corner of the globe, and cyberspace is no exception. The global pandemic has paved avenues for cybercriminals to target many new victims: the healthcare industry, the unemployed, remote workers and more. Here are a few of the most impactful cybersecurity statics related to the pandemic.

- Since the pandemic began, the FBI reported a 300% increase in reported cybercrimes. (IMC Grupo)

- 27% of COVID-19 cyberattacks target banks or healthcare organizations and COVID-19 is credited for a 238% rise in cyberattacks on banks in 2020. (Fintech News)

- Confirmed data breaches in the healthcare industry increased by 58% in 2020. (Verizon)

- 33,000 unemployment applicants were exposed to a data security breach from the Pandemic Unemployment Assistance program in May. (NBC)

- Americans lost more than $97.39 million to COVID-19 and stimulus check scams. (Atlasvpn)
- In April 2020, Google blocked 18 million daily malware and phishing emails related to Coronavirus. (Google)
- 52% of legal and compliance leaders are concerned about third-party cyber risks due to remote work since COVID-19. (Gartner)
- Remote work has increased the average cost of a data breach by $137,000. (IBM)
- 47% of employees cited distraction as the reason for falling for a phishing scam while working from home. (Tessian)
- 81% of cybersecurity professionals have reported their job function changed during the pandemic. (ISC)
- Half a million Zoom user accounts were compromised and sold on a dark web forum in April 2020. (CPO Magazine)
- Cloud-based cyber attacks rose 630% between January and April 2020. (Fintech News)
- Remote workers have caused a security breach in 20% of organizations. (Malwarebytes)

7. CYBERSECURITY JOB STATISTICS

As rates of cyber attacks increase, so does demand for cybersecurity professionals and, thankfully, cybersecurity budgets continue to rise.

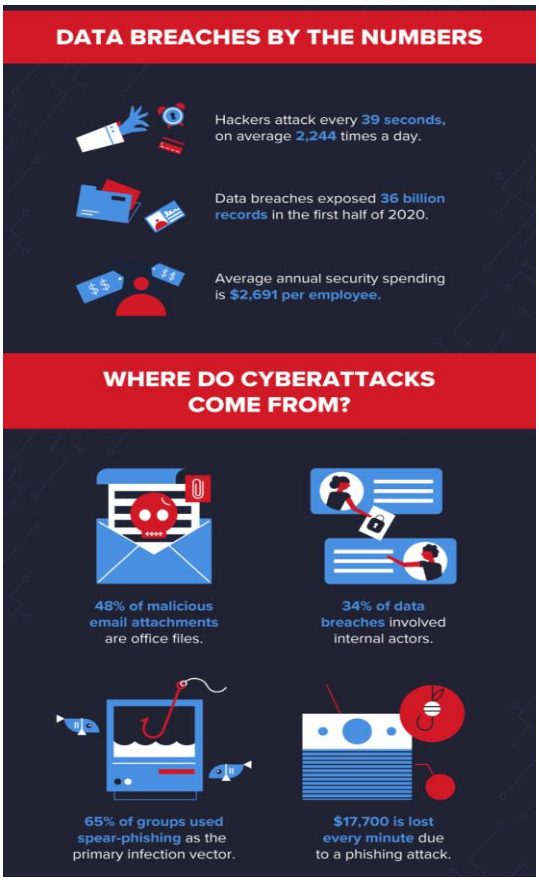
By 2021, there will be
4 million unfilled jobs
in cybersecurity globally.
Netsparker

However, the imbalance of the amount of skilled cybersecurity workers along with the high demand to fill cybersecurity positions has caused a cybersecurity skills shortage that sees no end in sight.

Interested in entering the field? Now is the time as the job field and average salary is only projected to grow. Looking for cybersecurity talent? Best of luck, it may be necessary to come up with creative cybersecurity skills shortage solutions — like outsourcing tasks, starting apprenticeships and partnerships with educational and military institutions to find fresh talent.

- 61% of companies think their cybersecurity applicants aren’t qualified. (ISSA)
- 70% of cybersecurity professionals claim their organization is impacted by the cybersecurity skills shortage. (ESG & ISSA)
- Since 2016, the demand for Data Protection Officers (DPOs) has skyrocketed and risen over 700%, due to the GDPR demands. (Reuters)
- 500,000 Data Protection Officers are employed (IAAP)
- More than two-thirds of cybersecurity professionals struggle to define their career paths. (ISSA)
- 61% of cybersecurity professionals aren’t satisfied with their current job. (ISSA)
- There was a 350 percent growth in open cybersecurity positions from 2013 to 2021.(Cybercrime Magazine)
- 40 percent of IT leaders say cybersecurity jobs are the most difficult to fill. (CSO Online)
- Cybersecurity engineers are some of the highest-paid positions started at $140K annually on average. (Cybint)

8. CYBER SECURITY STATISTICS FOR 2021



DATA BREACHES BY THE NUMBERS

Hackers attack every 39 seconds, on average 2,244 times a day.

Data breaches exposed 36 billion records in the first half of 2020.

Average annual security spending is $2,691 per employee.

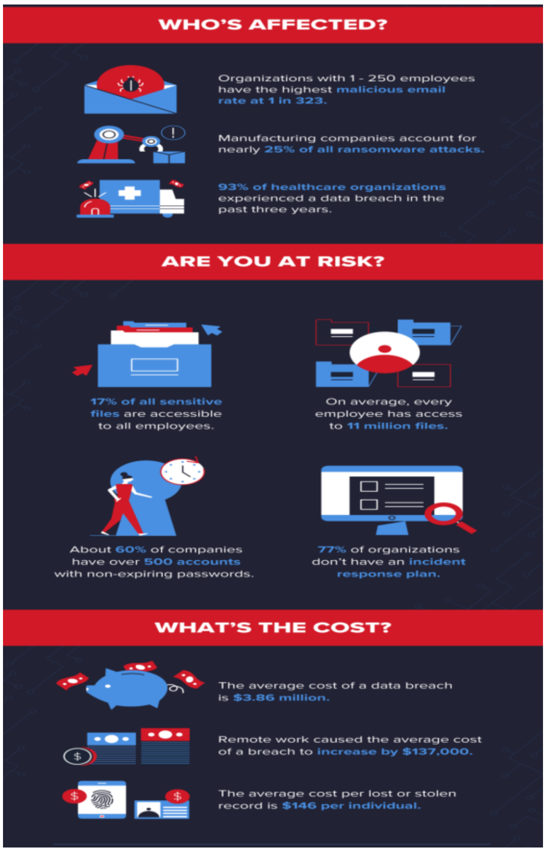
WHERE DO CYBERATTACKS COME FROM?

48% of malicious email attachments are office files.

34% of data breaches involved internal actors.

65% of groups used spear-phishing as the primary infection vector.

$17,700 is lost every minute due to a phishing attack.



WHO'S AFFECTED?

Organizations with 1 - 250 employees have the highest malicious email rate at 1 in 323.

Manufacturing companies account for nearly 25% of all ransomware attacks.

93% of healthcare organizations experienced a data breach in the past three years.

ARE YOU AT RISK?

17% of all sensitive files are accessible to all employees.

On average, every employee has access to 11 million files.

About 60% of companies have over 500 accounts with non-expiring passwords.

77% of organizations don't have an incident response plan.

WHAT'S THE COST?

The average cost of a data breach is $3.86 million.

Remote work caused the average cost of a breach to increase by $137,000.

The average cost per lost or stolen record is $146 per individual.

9. WAYS TO PREVENT CYBER ATTACKS (FEW LISTED BELOW)

" Every account you create

Every transaction you make

Every security best practice you fake

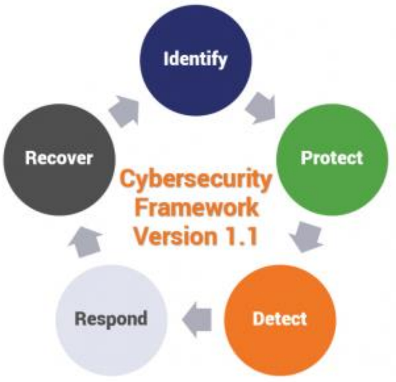
Every email you communicate

Hackers are watching you. "

Some of the best methods cybercrime prevention and control from a business perspective. Let's hash it out.

Step #1: Follow industry best practices and guidelines

Cyber crime prevention is not a one-size-fits-all approach. Organizations of different sizes have different needs, threats, risk tolerances, vulnerabilities, and capabilities. Luckily, governments, regulators, and even industry organizations have provided some general frameworks and security recommended practices for organizations to follow to reduce their likelihood of falling victim to cyber security attacks.



Step #2: Implement digital & physical security methods

We have previously discussed the idea of using firewalls, antivirus, network and server monitoring, and other forms of physical and digital data center security measures to create barriers for cybercriminals. Aside from hacktivists and nation-state actors who are trying to achieve ideal or political goals, many modern cybercriminals are simply looking for a way to make money. This could be through wire transfer scams or by stealing account information, personal data, or even intellectual property and proprietary research.

However, the more challenging your defenses are to get through and the more responsive you are to their attacks, the more work a hacker will have to do to accomplish their goals.

Step #3: Maintain asset lists, patches, and updates

While this should go without saying, cyber crime prevention involves keeping your company's hardware, software, and digital assets up to date through proper IT security asset management. A very easy and common way for hackers to get through a company's defenses is to simply take advantage of security gaps that exist due to outdated or unpatched IT infrastructure and software. While zero-day vulnerabilities — such as a Windows 10 cyber vulnerability for Microsoft Edge web browser users — could enable threat actors to take advantage of weaknesses that are unknown to manufacturers, the vulnerabilities they *do* know about are ones that companies will often issue updates or patches to fix.

Step #4: Manage SSL/TLS certs and keys for your domain(s)

When discussing how to prevent cybercrime, we'd be remiss to not mention the importance of using a secure protocol for your website in lieu of a nonsecure one. HTTPS, the secure version of hypertext transfer protocols for websites, is essential for every website regardless of content — even Google says so. This secure protocol is made possible through the use of SSL/TLS certificates — secure sockets layer and transport layer security — which authenticates websites and businesses and enables secure, encrypted communication through a process known as a TLS handshake.

Step #5: Train employees to identify and react to threats

Do you know what the biggest vulnerability in cyber security is for most businesses? If you guessed "employees" or "employee negligence," then you are correct. Employees (in house and remote) represent the most significant security risk to businesses and employee negligence is the leading cause of data breaches, according to research from Shred It. While I may not have a prize to offer, I can at least share some relevant insight on how to protect yourself from the numerous cyber threats that exist and seek to exploit your cyber vulnerabilities.

Cyber awareness training provides a basic understanding of cyber security best practices. Great training teaches employees — everyone from C-level executives to the janitorial staff — how to:

- Identify and respond to phishing and other email scams (hint: don't engage with them).
- Practice safe internet habits (such as creating secure passwords and not using them across multiple accounts).
- Familiarize themselves with your organization's cyber security-related policies and abide by them.
- Recognize social networking threats.
- Safely collect, store, manage, and send client and company data.
- Comply with government and industry regulations.

Your employees are your company's first line of defence. While automated cyber security protections such as firewalls, antivirus and antimalware solutions can help, they don't block every threat. This means that your employees need to be able to recognize and act quickly (and safely) to threats that make it through your network and other systems' defences. They also need to know how to not create risks by handling sensitive data and information appropriately.

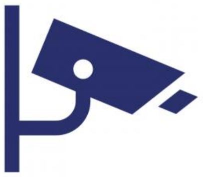
Step #6: Implement email security solutions and phishing simulations

Considering the rise in business email compromise, phishing, and other email-related concerns, the modern virtual mailbox represents a significant area of cyber security vulnerability. Unlike physical messages sent by a physical mail carrier, emails can contain a variety of threats from attachments containing malware (often Microsoft Office files such as Excel spreadsheets and Word documents) to embedded links that direct users to malicious websites.

Many businesses tend to rely on the anti-spam filters that come with bundled with their email platform or antivirus programs to protect their business's communications. However, there are additional third-party email solutions that you can use such as anti phishing platforms and email signing certificates.

Step #7: Monitor traffic and access to increase visibility

If you want to keep an eye out for danger, it's best to keep the lights on, pay attention to everyone coming and going, and make regular patrols. What many businesses do instead is turn off the lights, turn on the TV, and ignore everything else.



By always keeping their attention focused on something else and not paying attention to the traffic and things going on around them, they will miss important cues and won't be able to observe or learn from situations that occur.

Step #8: Regularly assess and test your systems

Vulnerability assessments, risk assessments, and penetration tests are simultaneously the best friends and annoying acquaintances of IT security experts everywhere. Although these terms are often incorrectly used interchangeably, these three methods of IT security they are related but separate functions:

- A vulnerability assessment helps to identify, assess, and prioritize any vulnerability in cyber security that may exist in your existing system.
- A risk assessment, on the other hand, is useful for evaluating potential risks for specific tasks or events.
- Lastly, penetration tests are your IT security team's way of testing to see how your defenses can be breached or compromised.

Step #9: Develop, implement, and enforce security policies

While analyzing, poking, and prodding your network and other IT systems is great, you still need to take it a step further and implement other protective measures in the form of cyber security policies. In the world of IT security, there are many types of security-related policies to choose from such as computer use policies, password policies, remote access policies, email/communication policies — the list goes on and on. Each of these policies has its own benefits and merits that should be considered.

10. CONCLUSION

These must-know cybersecurity statistics for 2021 demonstrate significant trends in the cybersecurity landscape. Ongoing security threats such as ransomware, advanced persistent threats (APT), nation-state hacker groups, and insider threats will continue to evolve their tactics to bypass security measures and compromise critical infrastructure. Business owners and consumers alike simply cannot afford to forgo investing in critical security measures and best practices.

Though not all people are victims to cyber crimes, they are still at risk. Crimes by computer vary, and they dont always occur behind the computer, but they executed by computer. The hackers identity is ranged between 12 years young to 67years old. The hacker could live three continents away from its victim, and they wouldnt even know they were being hacked. Crimes done behind the computer are the 21st centurys problem. With the technology increasing, criminalsdont have to rob banks, nor do they have to be outside in order to commit any crime. They have everything they need on their lap. Their weapons arent guns anymore; they attack with mouse cursors and passwords.

REFERENCES

[1] https://www.threatcop.ai/?utm_source=Cybercrime%20Expected%20to%20Rise%20at%20an%20Unprecedented%20Rate%20in%202021&utm_medium=Kratikal%20Blog&utm_campaign=Blog

[2] https://www.kratikal.com/blog/five-benefits-of-security-awareness-training/?utm_source=Cybercrime%20Expected%20to%20Rise%20at%20an%20Unprecedented%20Rate%20in%202021&utm_medium=Kratikal%20Blog&utm_campaign=Blog

[3] https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[4] https://securityboulevard.com/2020/12/cybercrime-expected-to-rise-at-an-unprecedented-rate-in-2021/

[5] https://www.profsandhu.com/cs6393_s19/Solms-Niekerk-2013.pdf

[6] https://www.varonis.com/blog/cybersecurity-statistics/