IN CONVERSATION WITH CYBERCRIME INVESTIGATOR AND CYBERSECURITY EXPERT UMMED MEEL

Ummed Meel is a CyberSecurity Expert, Ethical Hacker, Public Speaker, and Cyber Crime Investigator with an experience of more than 8 years. He has trained around 20,000+ Police officers from different states like Rajasthan, Delhi, UP, Himachal Pradesh, Haryana, Chhattisgarh, and other states. He has also trained CBI, BSF, CAPF, CDTI, CAG, BPRD, Air Force, and other LEA's (Higher Defence Organization) in India. He has given 100+ seminars in colleges, schools, and universities to encourage them to make their careers in the field of Cyber Security and Cyber Forensics. He works with Central Police, State Police, and other law enforcement agencies to investigate critical cybercrime cases across India.

Ummed Meel

Edited Excerpts

What are your thoughts about Cyber Crime? How does it impact businesses and overall society?

Any mischief or cheating which is either committed with the help of a computer or a computer network is termed as Cybercrime. Nowadays, hackers do not only target big companies to steal their databases but also individuals for cyberbullying, harassment, and financial fraud. In the last decade, cybercrime has increased exponentially. The main objective behind committing a cybercrime may vary. For instance, if hackers are targeting any online shopping website then their basic aim would be to hack the database, get into the website, and exfiltrate some critical information of users like their contact details, credit, and debit card details, etc. They can also target an individual in multiple ways like cyber harassment, defacement, extortion, etc.

Do you think that the Covid-19 Pandemic has increased the rate of Cybercrime? If yes, why?

Yes! Cybercrime increased a lot during the Covid-19 pandemic. From March 2020 to March 2021, cybercrime increased almost by 200 to 300% and the main reason behind this is the unlimited availability of digital devices and the internet. As the pandemic locked us in our homes, we started surfing the internet for endless hours a day.

If we invest so much time on the Internet, we try to explore more and more social media and OTT platforms. All these platforms ask us to register and fill in personal information like name, phone number, email ID, date of birth, and other debit & credit card details. Later, these details can cause cyber attacks or cyber incidents.

There are many small businesses that are emerging in the market. Do you think small businesses face the same Cyber risks today as larger companies faced in recent history?

Criminals are also targeting small industries in India to either make money or interrupt their ongoing business process to reduce the competition in the market. Earlier, criminals were only focusing on the big companies to steal their user's databases but after digitization in India, Cybercriminals have started focusing on small industries because every small business is moving towards digital transformation. They have started running their business online and accepting payments through online modes which attract criminals to hack the website & steal confidential data. Moreover, small industries do not focus on the security of their computer infrastructure because of the budget and resource limitations, which makes them more vulnerable to data breaches and cyberattacks as compared to the big companies.

Digital forensics and Cybersecurity go hand in hand. Elaborate how digital forensics is important to Cyber Security.

In information security, there are multiple domains and every domain has a significant role to play. There are two main fields in information security.

- Cybersecurity helps you to have multiple security services like vulnerability assessment, penetration testing, configuration review, secure architectural review, information security audits, and compliance checks. All these services can help you to keep your infrastructure and digital devices secure against any cyber-attacks.
- A Digital forensics team is a basic requirement for any organization to handle cyber incidents, analyze the incidents, and find out the root cause of a cyber-attack so that upcoming cyber attacks and cyber threats can be prevented.

Do you think India needs a strong cybersecurity policy considering the fact that recent technological developments are booming in the market?

To regulate the social media intermediaries, OTT, and other online service providers in India, we need to have a strong arrangement of law. Although, we have the IT Act 2000 but we also need Personal Data Protection and information security laws so that everybody can get an assurance that their personal information will never be misused by any service provider.

The government of India has released some guidelines for social media intermediaries that will make it mandatory for platforms such as WhatsApp to aid in identifying the "originator" of "unlawful" messages. The guidelines are:

- They have to register the complaint within 24 hours of the incident and set up grievance redressal mechanisms as well as assist government agencies in the investigation.
- The intermediary will also have to provide information or assistance to the authorized government agencies for "investigative or protective or cyber security activities.
- They need to appoint the Chief Compliance Officer, Nodal Officer, and a Grievance officer in India to deal with complaints. They would also need to publish a monthly compliance report mentioning the details of complaints received and action taken on the complaints as well as details of contents removed proactively.

Are there any digital rules that should be followed by all the people living in this online world?

Everyone should take some precautionary measures while using the internet or digital devices.

- If you are using a social media platform, always keep your profile private.
- Don't accept requests of any unknown person.
- Keep different passwords for different online accounts.
- Be careful while using internet banking or UPI. Never share your pin, CVV, or OTP passwords.
- Never share your confidential details like the screenshots or photos of your credit & debit cards on social media platforms.
- Use complex passwords that include numeric values, special characters, small and capital alphabets.
- Keep strong passwords on digital devices.
- Download applications from authorized and trusted app stores only.

Suggest some best practices and precautions that businesses should take to avoid cyber threats.

Every company should select a secured language framework and network to develop their web application, mobile application, and computer network. Multiple cyber security services like vulnerability assessment and penetration testing can help companies to identify the weak points and technical loopholes of any application or computer network. Companies can also conduct information security audits for the configuration review to check the secured installation of that framework, service, or application.

Companies can also organize webinars and seminars to spread awareness among consumers and employees regarding the kinds of attacks that can happen on their servers and applications. This can surely reduce the possibilities of future cyber attacks.

THE GLOBAL HUES®
WORLD MEETS MEDIA
Vol 1 | Issue 17 | November 2021

KEY TO INNOVATION
How will AI impact the Future?

Julie Sweet
Chair & CEO
Accenture

accenture
AN ACCENT ON THE FUTURE