Editor's Desk In Conversation

The Future of Cybersecurity: Insights from UPES Expert Nazia Aisha

By Kajal Mehra - December 4, 2024

223 0

In an interview with *TimesTech*, Nazia Aisha, Assistant Professor at UPES Online, delves into the critical importance of cybersecurity in today's digital world. She discusses emerging threats like ransomware and quantum computing, essential skills for cybersecurity professionals, and trends shaping the future of the industry. Highlighting the need for robust strategies, Nazia emphasizes the role of advanced education in preparing the next generation of cybersecurity leaders.

Read the full interview here:

1. To what extent is cybersecurity important in the modern age? In what way do you perceive the increasing dependence on digital systems as a threat to the increase of cyber-attacks?

Nazia: Cybersecurity is essential to the modern world, where digital systems cover nearly every aspect of our lives. From securing personal data in online banking to ensuring the integrity of critical infrastructure like power grids and healthcare systems, the importance of cybersecurity cannot be overstated. Hackers targeted the German steel giant ThyssenKrupp AGin February 2024,showing how a single cyber incident can disrupt production and bring an organization to a standstill. Moreover, the increasing adoption of digital platforms for commerce, communication, and operations amplifies the risks associated with cyber threats.

This dependence introduces vulnerabilities due to the rapid expansion of the attack surface. For instance, billions of IoT devices connected to the internet often lack robust security, providing easy entry points for attackers. The 8Base ransomware gang hit the UNDP in March 2024, proving that cybercriminals are not afraid to go big. Based on details uploaded to the hackers' leak site, the breach resulted in sensitive data being stolen. This included personal data, certificates, contracts, invoices, receipts, and more. It's crucial to acknowledge that as our confidence in digital systems grows, so must our investment in advanced cybersecurity strategies.

2. Which type of cyber threats are the most concerning?

Nazia: Among the various cyber threats, ransomware, supply chain attacks, and social engineering are particularly concerning. Ransomware in India has emerged as a pressing concern for businesses, institutions, and individuals. Over the years, there has been a surge in ransomware attacks, such as the PolyCab India Limited ransomware attack (2024) which affected its IT structure, AIIMS Delhi (2023) where patient data was compromised highlighting the dangers of cyberattacks in healthcare; supply chain attacks, such as the SolarWinds breach (2020), highlight the vulnerabilities present in third-party software, where compromising a single vendor can have a devastating impact on thousands of customers.

Social engineering attacks, like phishing, are still a big problem because they target people's instincts instead of technical weaknesses. These scams have gotten a lot sneakier, with some recent phishing attempts using AI to craft super-realistic fake emails. On top of that, AI-driven cybercrime and zero-day vulnerabilities are making things even trickier, as hackers use cutting-edge tools to stay under the radar and exploit software issues nobody knows about yet. Tackling these threats requires staying ahead with flexible and proactive defences.

3. Which skills do you consider essential for cybersecurity professionals?

Nazia: Cybersecurity professionals must possess a combination of technical expertise, analytical proficiency, and interpersonal skills to navigate the evolving threat landscape. Key technical skills include proficiency in network security, penetration testing, and cryptography, as well as experience with tools like SIEM (Security Information and Event Management) platforms for threat detection. The issue of incident response is another crucial issue, requiring the ability to analyze and mitigate breaches quickly. For example, organizations with strong incident response capabilities effectively contained the Microsoft Exchange Server attacks (2021) compared to those without well-defined protocols.

Equally important are soft skills such as communication and teamwork, which are essential for articulating complex technical issues to non-technical stakeholders. A thorough understanding of regulatory requirements, such as GDPR (General Data Protection and Regulation) and HIPAA (Health Insurance Portability and Accountability), is also vital for ensuring compliance while safeguarding sensitive data. As cybersecurity professionals operate in high-pressure environments, problem-solving, and adaptability are indispensable traits for success.

4. Which skills do you think are the most important for cybersecurity professionals of the future?

Nazia: Future cybersecurity professionals will need to master emerging technologies and adapt to a rapidly evolving threat landscape. AI and machine learning will be essential, as these technologies are increasingly being employed for both offensive and defensive purposes. For instance, AI-driven systems can help detect anomalies in real-time, while attackers use AI to craft sophisticated phishing scams. Additionally, expertise in quantum cryptography will become crucial as quantum computing threatens to make traditional encryption obsolete. Cloud and IoT security will also be important, given the rapid advancement of connected devices and cloud-based systems. Behavioural analysis skills, which help in understanding and mitigating social engineering attacks, will remain relevant. Finally, risk management and threat-hunting capabilities will be critical, as organizations shift from reactive to proactive cybersecurity strategies.

5. What are the different career opportunities one has after completing a course in cybersecurity?

Nazia: Cybersecurity offers a diverse range of career paths, catering to various interests and skill levels. Entry-level roles like cybersecurity analysts involve monitoring systems for potential threats, while penetration testers or ethical hackers focus on identifying vulnerabilities in security defences. Incident responders play a crucial role in containing and mitigating cyberattacks, often working under high-stress conditions.

Specialized roles like cloud security specialist and digital forensics expert address the unique challenges of securing cloud environments and investigating cybercrimes. For those interested in strategic leadership, positions like Chief Information Security Officer (CISO) involve shaping an organization's overall cybersecurity strategy. The rapid growth of cyber threats has also created opportunities in emerging areas such as threat intelligence analysis and IoT security, making cybersecurity a highly rewarding and future-proof field.

6. Elaborate on some of the major trends and issues that will challenge cybersecurity practitioners during the next decade.

Nazia: Over the next decade, cybersecurity practitioners will face several significant challenges. AI-powered cyberattacks will become increasingly prevalent, with attackers utilizing AI to automate and scale their operations. Furthermore, the emergence of quantum computing poses a major challenge to existing encryption standards, imposing the development of quantum-safe cryptographic algorithms.

Critical infrastructure security will remain a pressing concern, as attacks on sectors like energy, healthcare, and transportation continue to escalate. For example, recent cyberattacks on UK hospitals in 2023 disrupted patient care, underscoring the vulnerability of healthcare systems. Additionally, the rise of cyber warfare and nation-state attacks, as seen in the Red Echo Attack (2021) and Kudankulam Nuclear Power Plant Incident (2019) compromising sensitive systems at the nuclear plant will require governments and organizations to strengthen their defensive capabilities. Practitioners will also need to navigate the complexities of evolving regulations, balancing innovation with compliance in a globalized economy.

7. Considering the said need for more cybersecurity professionals, which positions do you think will be most relevant in the next 5-10 years?

Nazia: As the cybersecurity topography evolves, certain positions will gain prominence. AI security specialists will be critical for developing defences against AI-driven attacks. Quantum cryptographers will play a key role in designing encryption systems resilient to quantum computing. Cloud security architects will be in high demand, as organizations continue to migrate to cloud environments.

Other emerging roles include IoT security specialists, who will address vulnerabilities in billions of connected devices, and threat hunters, tasked with proactively identifying potential risks before they materialize. Cyber risk managers will also become more relevant, helping organizations balance security and operational efficiency in increasingly complex environments. These roles highlight the need for professionals with both technical expertise and strategic insight.

8. In your opinion, what extra skills or knowledge should be included in the curriculum of the degree in cybersecurity to prepare the students well regarding the ever-present threat?

Nazia: To prepare students for the challenges of tomorrow, cybersecurity curricula must evolve to include cutting-edge topics and practical training. Courses on AI and machine learning applications in cybersecurity and data forensics will be crucial, as these technologies play a growing role in both attacks and defenses. Quantum computing basics should also be incorporated enabling students to anticipate and address future cryptographic challenges.

Practical experience through simulations of real-world attack scenarios, such as ransomware incidents or supply chain breaches, can help students develop hands-on skills. Behavioural psychology modules can enhance their ability to counter social engineering tactics. Additionally, topics like blockchain security and regulatory compliance will equip students to navigate the expanding cybersecurity landscape. By combining technical, analytical, and strategic skills, a comprehensive curriculum can prepare the next generation of cybersecurity leaders.

TAGS Cybersecurity electronic news Future of Cybersecurity UPES

MOST POPULAR All More

Infineon OptiMOS 6 40 V family: Impressive RDS(on) combined with superior...
March 14, 2019

Techstreet Partners with IPC to Offer EMS Through Techstreet Enterprise
March 13, 2019

Are you ready to win Rs 1 Crore?
December 30, 2018

Taulia Enhances Platform with New AI Capabilities in a World First...
March 25, 2019

Understanding 5G New Radio Bandwidth Parts
November 8, 2018

Load more ›

Recent Posts

Turntide Tech Expands into Indian Market with Advanced Electric Mobility Solutions

Memory Market Outlook Innovations, and Strategic Insights Shaping the Future of Data Storage

NSDC International Acquires 10% Stake in Startup Stairs to Boost Drone, EV, AI, and Robotics Sectors

AAEON Releases the BOXER-8654AI-KIT

Industry Leaders Praise Digital Viksit Bharat, Stress Collective Efforts for Global Telecom Leadership