

SECON & eGISEC 2025: Key Security Challenges and Trends Unveiled

- Event Name: SECON & eGISEC 2025
- Event Dates: 19(Wed) – 21(Fri) March 2025
- Venue: Hall 3-5, KINTEX, Republic of Korea
- Website: [SECON 2025 - International Security Exhibition & Conference](#)
- Exhibitor List: [Exhibitor Digital Showroom | SECON & eGISEC 2025](#)
- Exhibit Category: Video Surveillance, Access Control, Smart City Security Solution, Social Security System, Homeland Security, Cyber Security, AI Security, Industri
- al Security/OT Security

The official media outlets of SECON & eGISEC, *Boannews* and *Security World*, annually select the core technology trends in the Korean and global security markets based on surveys and expert opinions. This year's key security issues are as follows.

[Expansion of Edge Devices]

Since the rise of ChatGPT, the AI market has advanced rapidly, bringing on-device AI into the spotlight. In 2025, edge devices with enhanced connectivity and scalability are expected to gain prominence.

Edge devices were highlighted as a key trend in the advanced equipment market. With real-time data processing, these devices offer superior security and speed, making them essential for addressing security challenges in smart cities, smart factories, and other interconnected environments.

[The Rise of the Converged Security Market]

The convergence of cybersecurity and physical security is now becoming a reality. With the rapid expansion of smart cars, smart cities, and other interconnected environments, traditional security measures alone are no longer sufficient to mitigate evolving threats.

As a result, the security industry faces critical challenges, including the development of integrated platforms, new security frameworks, and the standardization of emerging technologies to ensure interoperability.

[Expansion of the Zero Trust Security Model]

The Zero Trust model follows the principle of "Never trust, always verify." As network boundaries blur and cloud environments become increasingly complex, the demand for Zero Trust security strategies has significantly grown.

Government agencies and financial institutions have already successfully adopted customized Zero Trust frameworks, establishing them as an essential security strategy. With the release of the "Zero Trust Guideline 2.0" in December 2024, a maturity model was introduced, and in 2025, AI-driven automation is expected to further enhance data protection and access control.

[Intensifying Software Supply Chain Security Threats]

Software supply chain attacks continue to pose a significant security threat in 2025. These attacks infiltrate the software development process, causing severe damage to corporate trust and brand value. Organizations such as KISA (Korea Internet & Security Agency) and leading cybersecurity firms have identified this as a top security concern for the year.

As the frequency of attacks increases, governments and cybersecurity firms are ramping up preventative policies and technology development. Additionally, efforts are being made to strengthen SME security capabilities through vulnerability response training and Software Bill of Materials (SBOM) implementation trials.

[Cyber Fraud as a Service (Qshing) Threats]

With advancements in generative AI, cyber fraud techniques are becoming increasingly sophisticated. Cybercrime has now evolved into "Fraud as a Service (FaaS)," allowing criminals to launch attacks in various forms.

A particularly emerging threat is "Qshing"—a phishing attack that exploits QR codes, along with deepfake-based fraud. Further raising concerns, cybercrime marketplaces have emerged, facilitating the expansion of such threats. As these risks grow, both individuals and businesses must remain highly vigilant.

[Cybercrime Targeting Youth & Social Media Restrictions]

Cybercrimes targeting children and teenagers are on the rise. In the UK, online grooming crimes have surged by 89% over the past six years. Criminals exploit social media platforms to build trust before engaging in illegal activities, a tactic known as "online grooming."

In response, some countries are considering banning or restricting youth access to social media to combat such crimes. However, concerns remain about the potential for bypassing restrictions, highlighting the need for additional preventive measures.

[Cloud + Security = Industry Restructuring?]

The integration of cloud services and security is leading to new industry transformations. Cloud service providers are increasingly enhancing platform security, offering customized security solutions to boost customer trust and satisfaction.

However, concerns regarding monopolization have also emerged. With growing discussions about platform overdominance, many are questioning whether cloud security platforms and cloud service platforms can continue to coexist independently in the long run.

[The Hidden Risks of Old "New" Technologies]

AI and ChatGPT have become the latest buzzwords, much like cloud computing once was. However, just because a technology is widely adopted does not mean it is free from security risks.

For example, cloud services have suffered from "human errors," leading to unintended data leaks. Similarly, ChatGPT has raised serious concerns, as users often unintentionally expose sensitive information through interactions with the AI. These risks have prompted ChatGPT bans in several countries.

People tend to overlook security risks when technology becomes too familiar and convenient. However, even widely adopted technologies like AI and cloud computing still contain hidden security vulnerabilities that must be addressed.

Member of the Global **IFSEC** Group

전자정부 정보보호 솔루션 페어

SECON | eGISEC 2025

Now more than ever, dedicated efforts are required to address the various security challenges posed by these emerging threats. At SECON & eGISEC 2025, visitors will have the opportunity to experience these key security issues firsthand and consult with industry experts on-site.

As the only integrated security exhibition in Asia covering both physical and cybersecurity, the 24th SECON & eGISEC 2025 will take place from 19 – 21 March, at Hall 3-5, KINTEX, Korea. The event will span 28,000+ sqm, welcoming 30,000+ visitors and 400+ global leading physical and cybersecurity companies from 10+ countries.

Member of the Global **IFSEC** Group

전자정부 정보보호 솔루션 페어

SECON | eGISEC 2025

SECON & eGISEC 2025

19 – 21 March 2025, KINTEX, Republic of Korea

For any inquiries for 2025 event, freely contact

SECON & eGISEC Secretariat

Contact T. +82-2-6715-5400 / E. global@seconexpo.com / www.seconexpo.com