Racing against time: Is your cybersecurity response regulation-ready?

28 September 2025

The better the question. The better the answer.
The better the world works.

Shape the future with confidence
聚信心 塑未来

Racing against time: Is your cybersecurity response regulation-ready?

28 September 2025

Starting from 1 November 2025, the *Administrative Measures for Reporting National Cybersecurity Incidents* (referred to as the "Measures") will officially take effect. The Measures require all network operators to report incidents promptly and accurately.

This requirement goes far beyond filing a report – it puts an enterprise's end-to-end crisis management capabilities to the test, spanning technology, operations and compliance.

EY insights: Three core challenges behind compliance reporting

The release of the Measures presents enterprises with three major challenges when responding to real-world cyberattacks.

Challenge 1: Making judgments and reporting under time pressure

The Measures impose strict requirements for reporting major incidents – sometimes within just a few hours. In practice, moving from "detecting anomalies" to "determining impact level, organizing valid information and submitting a compliant report" often requires cross-departmental confirmation and evidence gathering. When the time window is compressed, problems surface:

- Tech teams detect anomalies but don't know which ones require reporting
- Management lacks clear conclusions for decision-making
- Compliance and PR are left waiting for synchronized updates

Challenge 2: The "vacuum zone" in cross-department collaboration

Cybersecurity incident response is never a solo act by the tech team. The Measures require detailed reporting of incident handling, which demands coordinated efforts from technology, legal, PR and business functions.

Imagine this: during a ransomware attack, the tech team is recovering data, legal is assessing the risks of paying ransom and PR is preparing external statements. Without prior coordination or a clear workflow, departments act in silos – creating confusion precisely when unity is most needed.

Challenge 3: Is reporting a post-incident summary or a wartime front-line task?

The Measures emphasize "timely reporting", meaning it's no longer a slow post-incident summary but a front-line task embedded in the incident response process.

This shift requires enterprises to build a reporting mechanism that can be quickly triggered and seamlessly integrated into daily security operations. From incident detection, alerting, handling to final reporting, every step must interlock to meet the stringent timelines set by the Measures.

EY perspective: Compliance as the litmus test of incident response capability

The purpose of the Measures is not to increase the burden on enterprises, but to elevate cybersecurity from passive defense to proactive response. Compliance itself is not the end goal – it serves as a valuable catalyst for building stronger organizational capabilities.

Meeting these challenges requires more than simply investing in new security tools. Enterprises need to strengthen their teams' real-world readiness through structured drills and training, embedding response processes into the team's muscle memory. Ultimately, all these challenges point to one core question: When an incident truly occurs, can your team collaborate efficiently, make timely decisions and complete all required steps within the mandated timeframe?

The best way to answer this question is through incident response drills. These are far from theoretical – they place teams under simulated real-world pressure, helping identify blind spots in processes and refine collaboration mechanisms, turning response actions into instinctive team behavior.

EY services: Proactive foresight – role-playing Cyber Wargame exercise

Traditional cybersecurity incident response drills often follow a scripted, predictable format, where participants' actions and reactions are predefined. To bring realism and engagement to the next level, we have reimagined the approach with an immersive, scenario-driven "Cyber Wargame" that allows participants to act as themselves in a dynamic, evolving environment. Throughout the exercise, key information is revealed progressively, requiring participants to collaborate under pressure, make rapid strategic decisions and respond to unfolding incidents in real time. At the same time, various tools and technologies are used to enhance interactivity and engagement, making the entire cybersecurity drill more vivid and immersive.

The role-playing Cyber Wargame redefines traditional drill methods by blending card game and EY wavespace™ technology, enhancing realism, collaboration and immersive experience.

1. Participants play their everyday roles and experience simulated cyberattack scenarios firsthand
2. A customized storyline drives the scenario, simulating real attacks and responses to enhance interactivity and challenge
3. Virtual reality technology boosts realism and interactivity, allowing participants to fully immerse in cyberattacks and defense scenarios
4. Visualization tools improve team collaboration, enabling real-time updates and information sharing for greater coordination and efficiency

The EY cybersecurity incident response drills cover four key dimensions, helping your team identify weaknesses, optimize processes and ultimately transform compliance requirements into core security capabilities.

Type	Focus area	Target audience
Incident response execution drill	Assess the effectiveness of incident response processes, with a focus on cross-team communication and collaboration	Chief information security officer (CISO), incident coordinators, legal and compliance representatives, technical leads (applications, infrastructure), business function representatives (e.g., customer service, marketing and PR)
Leadership decision-making drill	Focuses on cybersecurity crisis scenarios, with emphasis on decision-making and external communication strategies	Senior executives (CXOs), CISO, legal director, PR director, government affairs lead, heads of affected business units
Technical drill	Evaluates the IT department's capabilities in detecting, containing, responding to, and recovering from security incidents	CISO, security team, infrastructure team, application team, operations team
Red teaming exercise	Simulates real-world attacks to validate the effectiveness of technical measures and processes, identify blind spots and enhance security operations	Incident response team leads, Security Operations Center (SOC) teams

Whether it's a cyberattack, system outage, supply chain disruption, reputational crisis or natural disaster, EY team can tailor drill scenarios that closely align with your business – you can choose from proven cases or customize based on your industry, organizational structure and risk profile.

Common cybersecurity threat types	
Remote work security	Insider threats
Ransomware, phishing and vishing	Supply chain risks
Secure development and risk management	Data breaches or leakage
Zero-day vulnerabilities	System outages
Cloud security threats	AI threats (deepfakes, data leakage)

Common business impact examples	
Privacy compliance risks	Social media trends
Regulatory scrutinies, investigations or penalties	Customer complaints
Data sold on the dark web	Negative publicity involving celebrities or brand ambassadors
Business disruption	Financial losses (e.g. coupon abuse, fraudulent promotions)

The most effective drills stem from the most realistic challenges. Through highly customized scenarios, immersive experiences, expert facilitation and in-depth debriefs, we help organizations simulate high-pressure, lifelike cybersecurity incident response exercises. Real-time, multi-event injections create an authentic sense of crisis and information overload, thoroughly testing the team's response strategies, decision-making efficiency and communication effectiveness. This enables organizations to pinpoint areas for improvement and transform compliance requirements into genuine response capabilities.

For more information, please contact us:

Kelvin Gao

Managing Partner
Greater China Cybersecurity Services
Ernst & Young (China) Advisory Limited
kelvin.gao@cn.ey.com

Lena Wang

Partner
Greater China Cybersecurity Services
Ernst & Young (China) Advisory Limited
lena.wang@cn.ey.com

Miao Xue

Manager
Greater China Cybersecurity Services
Ernst & Young (China) Advisory Limited
miao.m.xue@cn.ey.com

Emma Wang

Senior Consultant
Greater China Cybersecurity Services
Ernst & Young (China) Advisory Limited
emma.zt.wang@cn.ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

APAC no. 03024186
ED None

ey.com/china

Follow us on WeChat
Scan the QR code and stay up-to-date with the latest EY news.