IBM Newsroom

# IBM Debuts New, State-of-the-Art Washington DC Cyber Response Training Facility

**New federal agency-focused training helps address government cybersecurity mandates and pillars of the National Cybersecurity Strategy**

**Launches two no-cost cyber response training sessions for select critical infrastructure organizations**

WASHINGTON, March 6, 2024 /PRNewswire/ -- IBM (NYSE:IBM) today announced the official opening of the newIBM X-Force Cyber Range in Washington, DC. The range includes new custom training exercises specifically designed to help U.S. federal agencies, their suppliers and critical infrastructure organizations more effectively respond to persistent and disruptive cyberattacks, and threats posed by AI. The state-of-the-art facility is designed to help everyone from legal and mission-critical leaders, to the C-Suite and technical security leaders prepare for a real-world cyber incident.

According to IBM's 2023 Cost of a Data Breach report the global average cost of a data breach reached$4.45 million, with the US facing the highest breach costs across all regions. Organizations that formed an incident response (IR) team and tested their IR plan experienced faster incident response times and lower costs than organizations that did neither. In fact, the report found that high levels of IR planning and testing saved industry and government nearly $1.5 million in breach costs and 54 days from the data breach lifecycle.

"From national security threats to supply chain disruptions impacting the goods and services we rely on every day, cyberattacks on government and critical infrastructure can have ramifications that go far beyond the balance sheet," said Alice Fakir, Partner, Lead of Cybersecurity Services, US Federal Market for IBM Consulting. "The elite and highly customizable cyber response training we provide at our new DC range helps organizations and federal agencies better defend against existing and emerging threats, and also addresses federal mandates like those in the Biden Administration's Executive Order 14028 focused on improving the nation's cybersecurity."

Building on nearly a decade of experience operating cyber response training facilities globally, IBM facilitators at the DC range guide participants through full-scale breach scenarios – ranging from AI code poisoning and destructive attacks to deepfake and zero-day attacks. The experience is immersive and helps participants from companies and agencies work through challenges they would face in real time such as cross-team communication breakdowns, resource issues, and navigating new US

Securities and Exchange Commission (SEC) incident reporting requirements.

In addition to government agencies and critical infrastructure providers, businesses across all sectors can participate in cyber response training. Examples of the types of simulations that will be delivered through the X-Force Cyber Range in DC include:

- **Mission: Crisis Response:** In this challenge tailored specifically for federal government agencies, IBM facilitators test and guide teams through a series of cyberattack scenarios, exposing gaps in response plans within a safe environment, allowing federal agency stakeholders to learn best practices based on industry standards and real-world case studies. This federally focused scenario uses the CISA Cybersecurity Incident & Vulnerability Response Playbook, developed in accordance with EO 14028, to guide decision making in a realistic cyber crisis scenario. Private sector organizations can take part in a similar scenario, called the Business Response Challenge, tailored to their industries and unique security challenges.
- **Cyber Wargame**: In this hands-on scenario, participants uncover and investigate a cyberattack led by a cybercriminal organization against a fictitious corporation. The Cyber Wargame tests the organization's incident response process, communication, and problem solving by positioning technical and business teams in the middle of a realistic cybersecurity incident to see how they would work together to resolve it. This exercise can be run annually to help ensure IR plans and processes are regularly refreshed to meet the latest threats and business challenges.
- **Inside the Mind of a Hacker**. This exercise is designed to help participants understand the viewpoint of an attacker by demonstrating the types of tools adversaries are using today and the scope of modern attacks. The session includes relevant insights from X-Force threat intelligence to help participants stay informed and adapt to the latest cyber threats.

**Training Critical Infrastructure to Strengthen Response in Cyber Crisis**
Globally, nearly 70% of incidents that IBM X-Force responded to last year were against critical infrastructure organizations, according to the 2024 X-Force Threat Intelligence Index. Given the continuous stream of attacks targeting these organizations, and the critical role that defending critical infrastructure plays in America's National Cybersecurity Strategy, IBM will offer two free exercises at its new DC cyber range where select infrastructure providers will respond to simulated cyberattacks.

The first event will take place in the spring of 2024 and will host organizations within the chemical, energy (including electric, oil, gas, and renewables), and water industries. The scenario will be customized to cater to specific issues facing these industries. The second session will be held later this year. To learn more about attending one of the upcoming sessions for critical infrastructure organizations, visit here.

Since 2016, IBM's cyber range facilities have hosted more than 17,000 visitors including major banks, healthcare systems, and oil & gas producers across the globe.

**Additional Sources**

- Learn more about the IBM X-Force Cyber Range inWashington, DC.
- Book an information meeting.
- Read more about the upcoming free sessions for critical infrastructure.

**About IBM Security**

IBM Security helps secure the world's largest enterprises and governments with an integrated portfolio of security products and services, infused with dynamic AI and automation capabilities. The portfolio, supported by world-renowned IBM Security X-

Force® research, enables organizations to predict threats, protect data as it moves, and respond with speed and precision without holding back business innovation. IBM is trusted by thousands of organizations as their partner to assess, strategize, implement, and manage security transformations. IBM operates one of the world's broadest security research, development, and delivery organizations, monitors 150 billion+ security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide.

**Media Contact:**

Michele Brancati
IBM
Mbrancati@ibm.com

SOURCE IBM

---

Additional assets available online:


https://stage.mediaroom.com/ibmnewsroom/2024-03-06-IBM-Debuts-New,-State-of-the-Art-Washington-DC-Cyber-Response-Training-Facility