KBR

61% of organizations have experienced **an Internet of Things (IoT) security incident** **

54% of companies have experienced **an industrial control system security incident.** **

The average cost of an attack is **$5 million,** with **$1.25 million** due to system down time and another **$1.5 million** attributed to IT and end-user productivity loss. **

Cyberattacks occur an estimated every **39** seconds.*

The Cost of Cybersecurity Breaches is at an All-Time High

KBR CYBER RANGE TRAINING

Defend against cyberattacks, better evaluate vulnerabilities and save money with KBR's advanced training

Combat Cybercrime with KBR Cyber Range Training Software

The KBR Cyber Range offers a hands-on experience to conduct cyber learning and exercises through an online curriculum. This virtual environment allows real-world cyber testing without impact to mission-critical systems. Utilizing digital battlefields, participants experience the same cyber threats and risks companies face every day and learn which tools are necessary to fight back and how to use them.

Notable features and capabilities:

- Training in static content and dynamic exercises

- Hyper-converged and software-defined computer and storage capabilities

- Secure and segmented environments

- Cloud management capabilities for automated deployment of environments

- Integrated access to IoT devices from autonomous vehicles to supervisory control and data acquisition systems

Learn how to:

- Act as the hacker

- Evaluate vulnerabilities

- Secure non-traditional computers

KBR advantages:

- Save money with consumable pay model so that participants only pay for what they use

- Real-life system training anywhere in the world

- More than 100 years of experience delivering federal market solutions and extensive scientific and programming expertise

Interested in learning more?

Email Brock Rabon at: **brock.rabon@us.kbr.com** or visit **KBR.com/CyberRangecom/CyberRange**

M5289-2019-KBR-12-2019