Ekaterina Kutsenko
Press Service
Deloitte CIS
Tel: +7 (495) 787 06 00
Email: ekutsenko@deloitte.ru

Deloitte Global report urges oil and gas industry to strengthen cyber security approach

New risks to industrial control systems call for a secure, resilient, vigilant approach

- *Need to bridge cyber-readiness gap grows with increased awareness of threat impact*
- *Robust cyber security platform essential for enhancing operational excellence*

Moscow, 29 May 2017 – A new Deloitte Global report released today, "*An integrated approach to combat cyber risk: Securing industrial operations in oil and gas*" calls for greater security around industrial control systems (ICS) as new technologies create increasingly complex challenges. The report shares insights gained from Deloitte's extensive field experience helping oil and gas companies go beyond safety in securing ICS.

The report highlights that despite the industry's growing adoption of evolving technologies such as robotics, digitization and the Internet of Things (IoT), it is still lagging with cyber security initiatives in ICS. To help make operational processes secure, vigilant and resilient, organizations will need to engage engineering and IT, and tailor technical solutions that are not always easily secured.

"The increasing sophistication of cyber criminals heightens the risk of catastrophic incidents, along with the magnitude of the impacts in terms of cost, safety, reputation and financial losses," said Paul Zonneveld, Deloitte Global Energy & Resources Risk Advisory Leader. "While the industry has escaped a major operational catastrophe thus far, this good fortune may not last unless companies expand their cyber security programs."

Understanding the risks

The ICS systems that are networked today were not previously designed to be connected. While digitization of operational processes in the oil and gas industry has brought new opportunities to improve productivity and drive down costs, the convergence of operational and business systems has also opened the enterprise to new cyber risks. The report dives into the following potential scenarios as examples of the changing landscape:

- **Insecure remote access communication**, allowing cyber criminals to hijack a process control system and push production to unsafe levels.
- **Improper testing of IT systems prior to deployment**, resulting in a system crash, and leading to disruption or shutdown of operations.
- **Poor security practices by a third-party contractor**, allowing a virus to migrate into the production environment, shutting down critical Supervisory Control and Data Acquisition (SCADA) systems.
- **Direct acquisition of unpatched technology without adequate testing**, introducing vulnerability and allowing adversarial communities to gain remote access.

Deloitte.

"As these examples illustrate, cyber threats can come from many directions, including internal actors aiming to sabotage production, competitors seeking to cause brand damage and external parties wanting to shut down operations," said Zonneveld. "While not every risk can be mitigated, it's important to know what type of controls are in place and where to focus improvement efforts."

Companies must find a way to reconcile the divergent points of view of IT and operations. A bowtie analysis, a common concept used in engineering for failure mode evaluation, can be a useful tool for bridging this gap, according to the report. Additional steps that can help secure the ICS include:

- **Conduct a maturity assessment.** This includes taking an inventory assessment of assets and facilities; determining if critical assets and facilities have well-known and exploitable vulnerabilities; and assessing the maturity of the controls environment for proactively managing these threats.

- **Build a unified program.** Oil and gas companies can build and implement a unified program through a multi-year, transformational effort. Each phase of the initiative should focus on moving up the maturity scale to create an ICS environment that is secure, resilient and vigilant.

- **Implement key controls.** While risk appetite will vary, there are several cyber processes that nearly every oil and gas company should have in place. These include awareness training, access control, network security, restricted and scanned use of portable media and incident response policies.

- **Embrace good governance.** A cyber security program within the ICS domain poses distinct talent management challenges. Organizations should develop awareness programs to bridge the gap between IT and ICS professionals, as well as a career development path for those wishing to specialize in ICS security.

###

About Deloitte

With over 244,400 employees, Deloitte has grown to be one of the largest professional services firms worldwide with a presence in over 150 countries. Deloitte offers unrivalled depth, breadth and quality of professional expertise to serve the needs of clients across various industry sectors.

Deloitte CIS is one of the leading international professional services firms that offers audit, consulting, corporate finance, enterprise risk, and tax and legal services leveraging professional experience of approximately 3,400 employees in 19 offices of 11 countries across the region. Today, Deloitte has offices in Moscow, St. Petersburg, Ufa, Yekaterinburg, Yuzhno-Sakhalinsk and Novosibirsk in Russia, Kyiv in Ukraine, Minsk in Belarus, Tbilisi in Georgia, Baku in Azerbaijan, Aktau, Almaty, Astana and Atyrau in Kazakhstan, Bishkek in Kyrgyzstan, Tashkent in Uzbekistan, Dushanbe in Tajikistan, Ashgabat in Turkmenistan and Yerevan in Armenia.