IDC Latest Research Shows 88% of Mining Companies Globally are Increasing Operational Technology Security Spending, but OT Security Risk Still Exist from Disjointed Management

SINGAPORE, March 13th, 2019 — IDC recently published a survey, *Operational Security Challenges and Approaches in the Mining Sector* which highlights that 88% of mining companies globally are recognising the threat of cybersecurity risk within mine sites hence an increase of investment in Operational Technology (OT) systems security, however poor management coordination still exists from disjointed management.

Technology addresses only one part of the OT related challenge, management of cybersecurity across enterprise and operational sites must involve coordinated management of business risk posed by the threat of attack across the operation.

Instrumentation and connectivity within mining companies is increasing not only within the enterprise but across operational sites through equipment automation, cloud, and mobility for example. This is creating the opportunity for improved efficiency, productivity and control, but also poses challenges to mining organizations. As equipment is connected, and systems integrated, companies are facing a far increased critical threat from a broadening attack surface.

Results from IDC's survey confirm that 78% of instrumented operations equipment is connected via wired or wireless networks. Mining companies recognize the associated risk and are increasing budget spend on OT security, but mining companies are not managing cybersecurity risk effectively operationally. More structure, adoption of standards, consistent processes and a single point of management accountability across all enterprise and operational security is required to ensure that as connectivity increases in support of business outcomes security systems in place within enterprise and operational environment can effectively manage the growing commercial and operations risk from cyber breaches.

As companies embark on technology led transformations to create integrated digital operating environments that are optimized and more productive (enabled by investments in cloud, IoT, AI, Advanced Analytics etc.), the security risk in operations will increase.

Furthermore, the survey showed that increased cloud and IoT investments are two of the top three drivers for increased investment in securing OT systems by mining companies. However, also in our survey 33% of mining companies globally highlighted the increased use of these disruptive

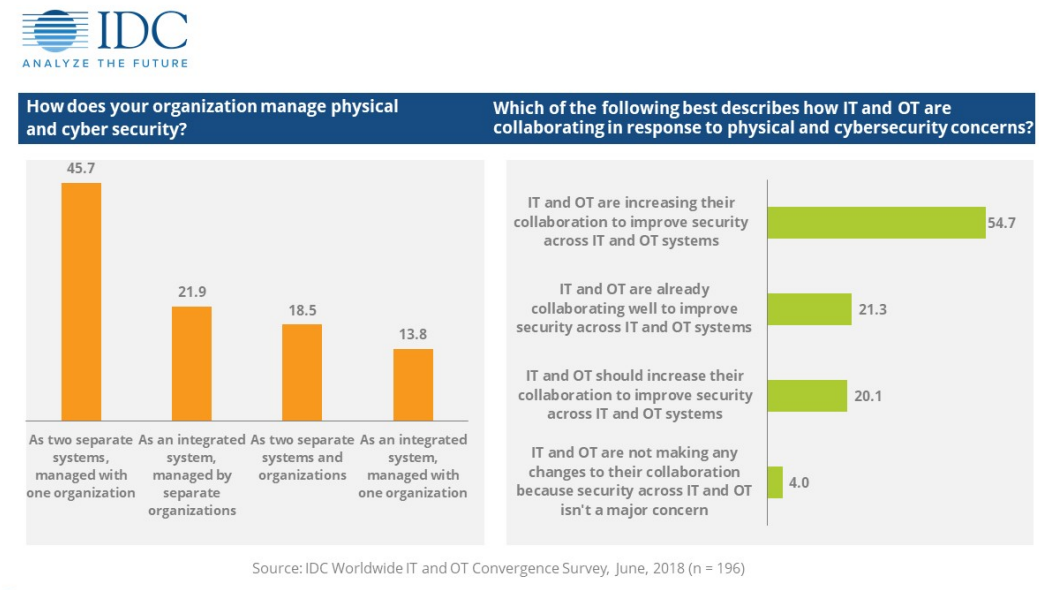
technologies as a major barrier to improved security for OT systems. Findings from the survey further highlight the risks we identified earlier to OT systems.

"This growth in technology led integrated digital operating environments is driven by management's need for improved insights into operations activities as a basis for improvements in productivity and yields and on a more consistently basis. Improved insights need increased levels of integration of OT and IT data. Ninety-six percent (96%) of mining companies have reported an operational focus on IT/OT integration as a strategic priority for investment over next 2-3 years, contributing to the growing exposure and risk in operations systems security," says Daniel Nimmo, Senior Research Manager at IDC Energy Insights and WW Mining.

In order to manage this growing and significant risk to the business, a coordinated approach to cybersecurity across the enterprise and operations is required. This should include common reporting lines for security strategy and execution across IT and operations security. According to the survey, 32% of mining companies confirmed that their lack of a holistic strategy across IT/OT systems security was one of top four barriers to their achieving higher levels of security across operations systems.

"Effective management of cyber security across mining operations is not simply a technology issue, the biggest challenges mining companies face in protecting their environments holistically and managing this risk relates to management and governance. IDC's research shows only 15% of respondents have a common management structure of IT and operational security. The lack of a single reporting line exacerbates the management of security on a consistent basis across the enterprise," adds Nimmo.

Figure 1



For more information about this report, please contact Daniel Nimmo dnimmo@idc.com or your IDC account manager. For media inquiries, please contact Alvin Afuang at aafuang@idc.com.

- Ends -

About IDC Energy Insights

IDC Energy Insights assists energy businesses and IT leaders, as well as the suppliers who serve them, in making more effective technology decisions by providing accurate, timely, and insightful fact-based research and consulting services. Staffed by senior analysts with decades of industry experience, our global research analyzes and advises on business and technology issues facing the utility and oil and gas industries.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,100 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a subsidiary of IDG, the world's leading technology media, research, and events company. To learn more about IDC, please visit www.idc.com. Follow IDC on Twitter at @IDC

For more information contact:

Daniel Nimmo
dnimmo@idc.com
+612 9925 2211
Emilie Ditton
editton@idc.com
+612 9925 2211
Alvin Afuang
aafuang@idc.com
+63917 7974586