ENERGY TECH REPORT

IT Insights for the Energy and Utilities Industry

RESHAPING TODAY'S LANDSCAPE WITH TECHNOLOGY

CDW

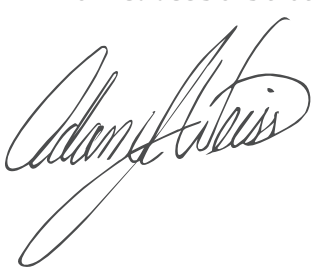
NEW CHALLENGES DEMAND UNIQUE I.T. SOLUTIONS

The energy landscape continues to shift as utility providers and oil and gas producers alike seek ways to streamline operations. They do this by leveraging the Industrial Internet of Things, cloud computing, predictive analytics, rugged networking and other powerful technologies.

Today's competitive environment makes it imperative to maximize your return on IT investment as well as protect your critical infrastructure from sophisticated and aggressive cyberthreats. Geographically diverse oil exploration operations, deep water rigs, pipelines and power utility lines — even the smartphone in your pocket — all require vigilance to ensure the cyber-resilience you need to boost productivity and gain new efficiencies. That means having the right IT tools and policies in place to enable secure access to data in the cloud, on the Internet and across the enterprise, wherever you deploy workers and equipment.

In this issue of *Energy Tech Report*, we take a deeper dive into the key technologies and trends shaping the industry. Our seasoned IT leaders and industry experts offer practical strategies and real-world applications to show you how to harness technology to build a more agile and profitable enterprise.

Better IT solutions make for better business outcomes. CDW E&U is here to help you navigate the technology maze and support your ability to make well-informed decisions that drive value and performance.



Adam J. Weiss
Area Sales Director

ONLINE RESOURCES

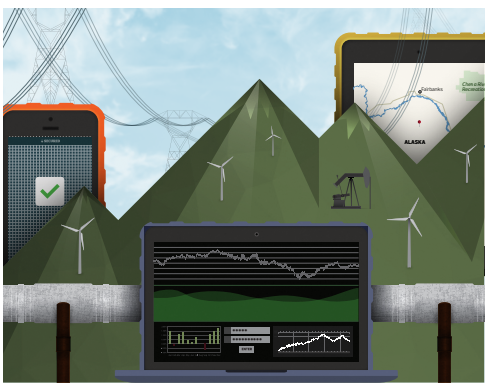
CAPABILITIES BROCHURE
"Powerful IT"
Find out how CDW E&U can help you maximize performance.
CDW.com/energycapabilities

VIDEO
"Ruggedized Networks Connect and Protect"
Ensure the reliable connectivity you need to increase efficiency and profitability.
CDW.com/energy

WHITE PAPER
"Delivering the Power of the Network"
Collect vital data and remotely monitor far-flung operations with ruggedized networks.
CDW.com/scadawp

WEBSITE
About CDW Energy & Utilities
Learn more about how CDW E&U can address your IT needs.
CDW.com/energy

CONTENTS



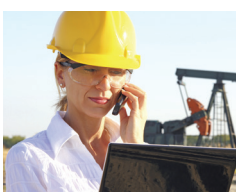
POWERFUL NEW ENERGY PARADIGMS

Track seven key technology trends that are reshaping today's energy landscape. 2

POWERFUL INSIGHTS

Three Strategies to Accelerate Data Access and Insights

Energy companies face vexing challenges capturing, processing, analyzing and storing unprecedented amounts of data, let alone quickly converting it into actionable insights. 6



PARTNER CORNER

Rugged Devices Deliver Reliability and Portability

Peter Poulin, chief marketing officer at Xplore Technologies, discusses how to choose the right rugged devices for your mobile workforce. 12

INFOGRAPHIC

Shining the Spotlight on Cybersecurity

With cybercriminals continuing to target E&U companies, it's critical to know the facts about safeguarding your data and infrastructure. 8

PARTNER CORNER

Smart Security Strategies in the Age of Hyper-connectivity

Cisco's Nicolaas Smit, director of the Energy Global Industries Center of Expertise, offers advice on how to protect your interconnected systems in the face of growing cyberthreats. 13

TECH TIPS

Connect and Protect High-value IT with Ruggedized Networking

CDW solution architect Aaron Pilcher discusses how and why you should take advantage of ruggedized networking to sharpen your competitive edge. 10

TREND WATCH

POWERFUL
NEW ENERGY PARADIGMS

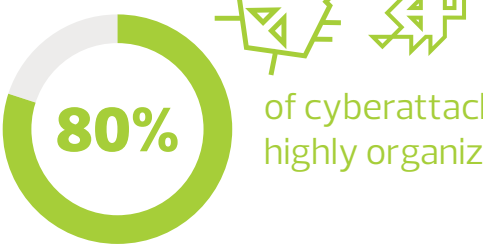
Digital technologies enable smarter power utility grids, more productive crude oil wells, safer oil rigs and the remote monitoring of thousands of miles of gas pipelines. Increasing in number and threat level, cyberattacks on refinery SCADA systems and power grids have raised industry awareness of the need for stronger cyber safeguards.

Oil and gas producers are turning to technology — sensors, supercomputing, predictive analytics — to enhance cybersecurity, boost production and improve operational efficiencies. Aptly referred to by some as the third Industrial Revolution, the Industrial Internet of Things (IIoT), supercomputing, mobile devices and apps, drones and 3D seismic imaging are creating powerful new energy paradigms to advance these goals. Fuel your purchasing knowledge by staying up to date on what's happening in the power utility and O&G pipeline. Here are seven important trends shaping the energy industry today.

1. Energy Industry Uniting Against Cybercrime

Cybercriminals are capitalizing on the proliferation of sensors and smart devices to target systems in critical energy infrastructure. Experts have identified that organized cybercrime rings are responsible for a majority of attacks. Taking down a regional power supply could have far-reaching impact on people and the economy.

Security analysts concur that collaborative efforts are needed to combat cyberterrorism and boost cyber-resilience. Energy companies, cyber-experts and government entities are joining forces to mitigate vulnerabilities and prevent cyberattacks. Cloud-based platforms make it easier for partners to collaborate and share real-time indicators on security incidents. By banding together to aggregate knowledge and data, the energy industry can more effectively protect against sophisticated cybercrime rings.



of cyberattacks are driven by highly organized crime rings.[1]

Cyber Value-at-Risk Components[2]

Vulnerability

- Existing Vulnerability
- Maturity Level of Defending Systems
- Number of Successful Breaches

Assets

- Tangible Assets
- Intangible Assets

Profile of Attacker

- Type of Attackers
- Type of Attacks
- Tactics and Motivations

2. Power Utilities Mobilizing with IT

Smart meters, remote asset monitoring and other mobile technologies are helping reduce costs and drive operational efficiencies for some power utility companies. Their remote field workers deploy with ruggedized notebooks, smartphones and GPS tracking technologies. They connect with a growing base of digitally proficient customers via bill alerts and energy saving tips, and even on social media. Mobile platforms and applications can greatly improve power outage recovery communication, real-time outage maps and texting options for consumers to report outages. Online self-service account management empowers customers and encourages participation in energy efficiency programs – while providing quantitative and qualitative advantages to the electric power utility.

UTILITY DIGITAL REPORT CARD

Utilities lag behind retail, communications and government in adopting digital technologies.[3]

26% of electric utilities offer mobile applications.

10% of customers at one large electric utility use mobile applications.

11% of social media users report using social media to communicate with their utility company.

64% of e-bill recipients are less likely to call customer service.

67% of consumers using digital channels are satisfied with their energy providers.

58% of consumers who don't engage online are satisfied with their energy providers.

3. Upstream Goes Digital in Oil and Gas

Oil and gas investments in Big Data, IoT, automation and supercomputing are cautiously rising. Full adoption of digital technologies will continue to move at a measured pace due to the steep capital costs associated with upgrading equipment on remote oil rigs, well operations and pipelines. As crude prices drop, industry leaders are proactively seeking ways to control costs by maximizing the value of existing assets, with an emphasis on well productivity. There is growing interest in digital investments, especially within the upstream sector, to support predictive analytics — which add business value by improving asset management and operational efficiencies.

O&G DIGITAL REPORT CARD[4]

Three out of five members of the O&G industry plan to increase digital technology investments.

90% believe more mobile technologies in the field would boost business value.

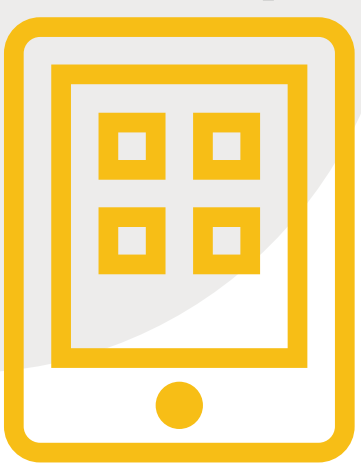
89% believe leveraging more analytic capabilities would boost business value.

86% believe leveraging more IIoT and automation would boost business value.

100% believe they must continue to invest in digital technologies or risk being left behind.

MOBILE APPS BENEFIT O&G

- Improved safety
- Real-time monitoring
- Environmental protection
- Regulatory compliance
- Capture efficiencies



4. Mobile Transformation for Oil and Gas

Across the board, industries involved in O&G production anticipate adopting mobile and Internet technologies by 2025. Transformational mobile tools for upstream and downstream processes support virtually all facets of operation, including remote pipeline inspection, location tracking, environmental assessments and monitoring of refinery equipment. In the past, workers manually tracked and transmitted critical data in workstations. Mobile apps now allow real-time and wireless data capture, so operators can make faster decisions and take corrective action when equipment and worker safety issues arise. Mobile apps also help meet O&G regulatory and monitoring requirements for improved compliance and environmental protection.

MOBILE USE GROWING[5]

There are approximately **5 BILLION MOBILE USERS** (businesses and consumers) worldwide. By 2020, mobile device users will surge to **OVER 6.7 BILLION.**

There are over **9.5 BILLION MOBILE DEVICES** in use worldwide. By 2019, the number of devices will reach **MORE THAN 14.8 BILLION.**

5. Attacks Double on SCADA Systems

Supervisory Control and Data Acquisition (SCADA) networks and sensors are used to connect scattered O&G sites and equipment, allowing producers to remotely control and monitor operations. Drill sites are almost uniformly located in inhospitable areas requiring ruggedized equipment and networks. Building SCADA networks requires planning to integrate disparate components and ensure a robust platform. Security risks rise as SCADA networks connect to cloud platforms and the IoT. Recent studies show SCADA attacks more than doubled last year, with refineries being a prime target. Any network vulnerability can potentially expose IT and O&G industrial systems to cyberattacks. Cybersecurity must entail vigilant monitoring and recovery plans for worst-case breach scenarios.

TIPS FOR SCADA SUCCESS[6]

- Choose a system wisely
- Get network integration right
- Prepare for environmental hazards
- Plan ahead for updates
- Watch for evolving security threats
- Realize some threats are undetectable
- Weigh interoperability considerations
- Be able to justify upgrades

DRONES HAVE MANY USES IN ENERGY INDUSTRY[7]

- Monitoring power lines
- Detecting gas pipeline leaks
- Scanning oil pipelines for structural weakness and leaks
- Inspecting wind turbines for cracked blades
- Open-air mining operation surveillance
- Pinpointing solar panel malfunctions

6. UAVs (Drones) Take Flight

Able to hover or buzz through the sky, equipped with high-resolution cameras and sensors, drones are taking flight in the energy industry. Military drones have long served defense operations. Commercial drones tend to be smaller and more nimble. The U.S. National Transportation Safety Board recently abolished a ban (no-fly zone) on commercial drone use. Several O&G companies have launched pilot projects after receiving FFA clearance to use drones. Drones potentially play a role anywhere that it's unsafe, inaccessible or cost-prohibitive to send people. Utilizing multispectral sensors, drones can capture data on gas and chemical contaminants undetectable to the human eye. They can quickly produce and upload high-resolution 3D images and geographic maps of vast areas to the cloud.

7. Rise of Smart Grids

Designed to remotely track energy use, smart meters are only one component of smart grids, which refer to a tapestry of wires, substations, transformers, sensors and switches built to gather and act on data for more efficient production and distribution of electric power. Growth in peak electricity demand in the United States exceeds transmission growth by almost 25% annually. Smart grids support projects to replace overtaxed infrastructures running up against physical limitations. Utility companies taking advantage of smart grid systems are able to adjust electricity prices based on demand. Unlike legacy systems, which are not equipped to handle the rapid fluctuations in wind and solar generation, smart grid systems more easily integrate renewable energy.

SMART GRID INVESTMENT IS EXPECTED TO REACH **$380.1 BILLION BY 2025.**[8]

[1] ibm.com, "IBM Opens Threat Intelligence to Combat Cyber Attacks," April 2015
[2] World Economic Forum, *Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats*, January 2015
[3] boozallen.com, "Digital Migration for Electric Utilities," 2014
[4] accenture.com, "Oil and Gas Digital and Technology Trends Survey 2015," April 22, 2015
[5] radicati.com, "Mobile Statistics Report, 2015–2019," February 2, 2015
[6] CDW, *Delivering the Power of the Network*, 2015
[7] frost.com, "Newest Oil & Gas 360˚ Research"
[8] prnewswire.com, "Global Smart Grid Vendor Landscape," June 3, 2015

THREE STRATEGIES TO **ACCELERATE DATA ACCESS AND INSIGHTS**

When it comes to data, more is better — as long as you have the ability to effectively use it. Businesses across the spectrum grapple with overwhelming volumes of data these days, but energy companies in particular have been inundated — thanks to multiplying numbers of sensors, advanced data-gathering techniques and the Internet of Things (IoT). Oil, gas and utility companies face vexing challenges capturing, processing, analyzing and storing this unprecedented amount of data, as well as figuring out how to speedily convert it into actionable insights.

Successfully meeting these challenges is critical, since the ability to leverage data to maximize operational efficiency and maintain competitiveness in the current era of drastically reduced oil prices is absolutely essential. Given the uncertainty in the market, traditional cost-cutting measures such as layoffs and capital expense reductions simply may not be sufficient to enable companies to survive, let alone thrive. This situation presents an opportunity for forward-looking oil, gas and utility companies to drive digital transformation, taking advantage of Big Data and analytics to position themselves for continued growth.

48% of oil and gas professionals named data as the area of Internet of Everything (IoE) they need to improve most to make effective use of connected technologies to drive insights and value.[1]

According to the Cisco white paper, "Attaining IoT Value: How to Move from Connecting Things to Capturing Insights," energy firms must adopt three critical strategies in order to capitalize on this mushrooming data:

1. Integrate data from multiple sources.

Oil and gas companies named "data integration" as their biggest challenge relating to data quality and analysis in a 2013 Accenture study. More than half reported that the format, completeness and accessibility of data posed problems. The challenge of integrating data from varied, highly distributed sources still looms large today. As cost, technical difficulty and potential regulatory issues make it impractical to copy all data to a centralized node for integration, interest has been growing in data virtualization.

Data virtualization treats widely dispersed data as one logical database for users and applications, supporting integration on demand. It eliminates the need to physically store integrated data centrally because it integrates data live and only when users need it. As a result, users have the ability to access and manipulate data whenever and however they like, regardless of how the data is formatted or where it actually resides.

The **46 million** smart meters in the U.S. today generate more than 1 billion data points daily.[1]

2. Automate data collection using fog computing.

Energy companies also need to decide where to put all the data they collect. Should they transmit it to the "center" of the network — an offsite location, such as the cloud or a remote data center — for storage and processing? Or, does it make more sense to analyze the data right where it's captured, at the "edge" of the network? The edge could be anywhere from connected wind turbines to connected oil platforms to smart streetlights to substations.

37% of companies surveyed across industries believe that within the next three years, most of their IoT data will be processed at the edge of the network on smart devices.[2]

In "edge computing," the analytics moves to the data, rather than vice versa, speeding the ability to gain valuable operational, safety and other business knowledge. Edge computing capability is enabled by a platform known as fog computing, which complements cloud computing by transferring some of the processing, storage and networking workload from cloud services to distributed local resources such as routers and mobile devices. By moving real-time data closer to users, fog computing offers a cost-effective opportunity to support speedy analytics as well as IoT applications that require low latency, such as safety.

Highly distributed IoT applications such as pipeline monitoring, connected oil rigs and the smart grid are logical candidates for edge computing, since inadequate bandwidth coupled with the high cost of the bandwidth available can make it difficult or simply infeasible to tap into the data they generate in real time. For example, a typical offshore oil platform generates between 1TB and 2TB of primarily time-sensitive data daily. If data is transmitted via a satellite connection with data speeds ranging from 64Kps to 2Mbps, it can take nearly two weeks to move a single day's worth to a central repository. Clearly, fog computing offers a more viable alternative for companies eager to act quickly on this data.

Fog computing can also deliver numerous benefits to utilities. For instance, taking advantage of intelligent routers embedded in substations can improve smart grid resilience and security, reduce latency and lower costs.

3. Analyze data for actionable insights.

The true value in Big Data lies in the insights gleaned through analysis, whether that analysis occurs in the center of the network or at the edge. Companies then need to apply this business intelligence to fuel process reengineering efforts and organizational change. Gartner predicts the ability of energy companies to use analytics to reduce operating costs and increase production rates may become an essential survival skill. IDC forecasts that half of oil and gas companies will have advanced analytics capabilities in place by 2015, with the goal of optimizing drilling, production and asset integrity.

Gas and oil companies themselves have high expectations for the potential of data analytics to improve performance, in conjunction with the IoE — the networked connection of people, process, data and things. In a Cisco survey, they named data analytics for faster, better decision-making the number one driver for investment in connected technologies, ahead of improved operational efficiencies and increased productivity.

It takes more than **12 days** to move one day's worth of oil platform data to a central repository via satellite connection.[3]

[1] eweek.com, "Fog Computing Aims to Reduce Processing Burden of Cloud Computing," November 2014
[2] Cisco, "Attaining IoT Value: How to Move from Connecting Things to Capturing Insights," December 2014
[3] Cisco, "A New Reality for Oil and Gas: Complex Market Dynamics Create Urgent Need for Digital Transformation," April 2015

INFOGRAPHIC

SHINING THE SPOTLIGHT ON **CYBERSECURITY**

In light of the fast-expanding number of increasingly malicious cyberattacks by ever-more devious cybercriminals, oil, gas and utility companies need to be hyper-vigilant about security. In fact, NSA Director Admiral Michael Rogers has predicted it is only a matter of "when," not "if," there will be a "traumatic" event caused by a cyberattack on energy infrastructure.

Energy company data and infrastructure are top targets

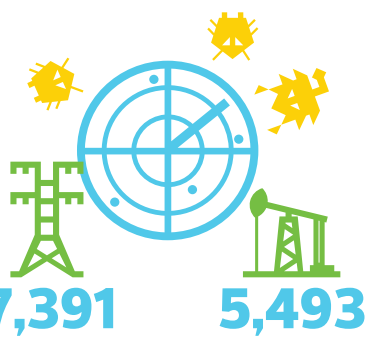
The fastest-growing sources of security incidents:[1]

Oil and gas

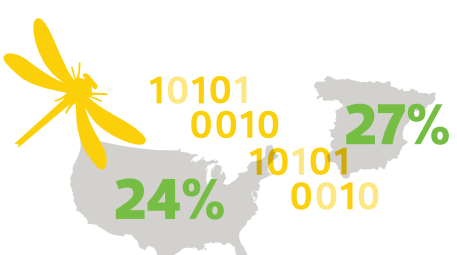
- **108%↑** Foreign nation-states
- **85%↑** Current employees
- **78%↑** Activists/hacktivists
- **69%↑** Competitors

Power and utilities

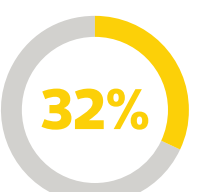
- **118%↑** Foreign nation-states
- **48%↑** Information brokers
- **40%↑** Activists/hacktivists
- **31%↑** Organized crime



The average number of detected security incidents in power and utilities companies climbed six-fold over the previous year, to **7,391** — the highest reported by any industry. Oil and gas incidents declined **16%**, from **6,511 to 5,493**.[1]



U.S. and European energy companies have been the primary targets of the ongoing cyberespionage campaign known as **Dragonfly** or **Energetic Bear**, which infects industrial control systems and steals data. Countries with the most active infections include **Spain (27%)** and the **U.S. (24%)**.[2]



of the **245** reported cyberattacks in 2014 targeted the energy industry, according to the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team.[3]

Easily crackable encryption puts more than **4 million** smart meters, thermostats and other Internet-connected devices at risk of cyberattack.[4]

Oil, gas and utility companies pay a high price for security — and lack of it

$1.87B

Cybersecurity spending on oil and gas infrastructure will reach **$1.87 billion** annually by 2018.[5]

$4M **$1.2M**

Estimated total financial losses related to security incidents in 2014: **$4M** for oil and gas companies and **$1.2M** for power and utilities.[1]

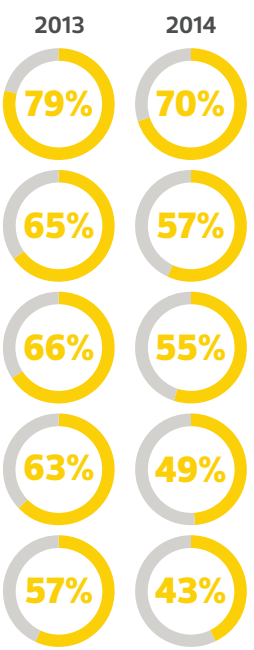
$5.7M

$3.7M

The average annual information security budget: **$5.7M** for oil and gas companies and **$3.7M** for power and utilities — nearly **4%** of the total IT budget for both sectors.[1]

Defensive strategies need to move front and center

Key security safeguards have weakened in power and utilities companies:[1]



75% of energy CEOs view cybersecurity as strategically important.[6]

Only **11%** of oil and gas companies are "fully confident" they can handle hacks appropriately.[7]

61% of oil and gas companies think it's unlikely or highly unlikely that they would be able to detect a cyberattack.[8]

Only **29%** of oil and gas companies report access to real-time cybersecurity insights.[8]

To learn more about how your organization can safeguard your data and infrastructure, visit **CDW.com/energy**.

[1] pwc.com, "The Global State of Information Security Survey," 2015
[2] symantec.com, "Dragonfly: Western Energy Companies Under Sabotage Threat," June 2014
[3] plantengineering.com, "Ensuring pipeline physical and cyber security," May 2015
[4] zdnet.com, "Flawed encryption leaves millions of smart grid devices at risk of cyberattacks," May 2015
[5] oedigital.com, "OTC15: Preventing cyber attacks," May 2015
[6] pwc.com, "18th Annual Global CEO Survey," 2015
[7] fox-it.com, "Cyber security: 60% of Oil and Gas Companies Do Not Have an Incident Response Plan in Place," February 2015
[8] explorationworld.com, "Cybersecurity and the Avoidable Disaster in Oil and Gas," May 2015

TECH TIPS

CONNECT AND PROTECT HIGH-VALUE I.T. WITH **RUGGEDIZED NETWORKING**

Between fluctuating prices, uncertainty about future resources and increased risk of cyberattack, energy companies need to find new efficiencies and innovative ways to improve productivity. With informed decision-making increasingly data dependent, the ability to strengthen your competitive advantage relies heavily on how effectively you deploy, manage and integrate a host of IT resources.

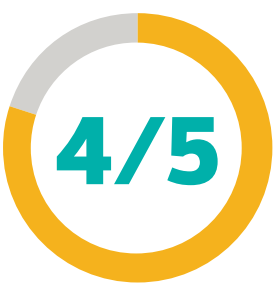
As a result, implementing a ruggedized network is essential, whether you're an oil and gas company with far-flung operations and widely scattered exploration sites or a utility expanding your smart grid. "Most electronic equipment is designed for typical indoor environments. But when you build networks under the ocean, in the desert or anywhere else out in the world, you don't have the luxury of filtered air or temperature regulation. That's when you need ruggedized, or hardened, networking equipment," says CDW's Team Lead – Enterprise Network and Solution Architect Aaron Pilcher.

Hardened networking components include switches, routers, wireless access points and other devices specifically designed to withstand harsh conditions such as precipitation, dust, intense vibration, and extreme variation in temperature and altitude. Designed with conductive cooling mechanisms rather than vents and fans, they are also engineered to operate maintenance-free for extended periods.

4 TRENDS DRIVE RUGGEDIZED NETWORKING EXPANSION

Four key trends are driving energy company investment in ruggedized networking:

1. **Widely dispersed exploration sites.** As existing oil fields mature, gas and oil exploration sites and equipment are becoming more scattered and remote. Field technology needs to be highly integrated with communications and IT to monitor and control operations as well as to support worker safety.
2. **More connected sensors.** Rising exploration costs and limited human resources boost reliance on growing numbers of connected sensors to transmit volumes of unstructured data from exploration sites to process, analyze and visualize via high-performance computing.
3. **The smart grid.** Utilities rely more heavily on automation to boost performance and rein in costs by using smart grid-connected meters to better manage consumer usage and demand, improve technician productivity and support faster repairs.
4. **SCADA and the IoT.** Companies increasingly seek to connect internal, enterprisewide SCADA networks to the fast-expanding IoT to enhance their ability to integrate and leverage data as well as enable collaboration between devices, people and systems.



Nearly **four-fifths** of oil and gas CEOs agree that digital technologies are creating value for their organizations when it comes to data analysis and operational efficiency.[1]

Pilcher points out that ruggedized networks enable oil, gas and utility companies to collect, transmit and analyze the data they need to meet two overarching goals:

- **Actively monitor equipment.** "You can make sure everything is in working order, whether it's remote drilling equipment or a smart grid," he says. "That leads to better performance, improved worker safety and cost savings."
- **Make smarter decisions faster.** "Companies can aggregate data to make more informed decisions at a faster pace. Essentially, that's the definition of the Internet of Things (IoT) — connecting the unconnected to drive smarter decisions faster," he says.

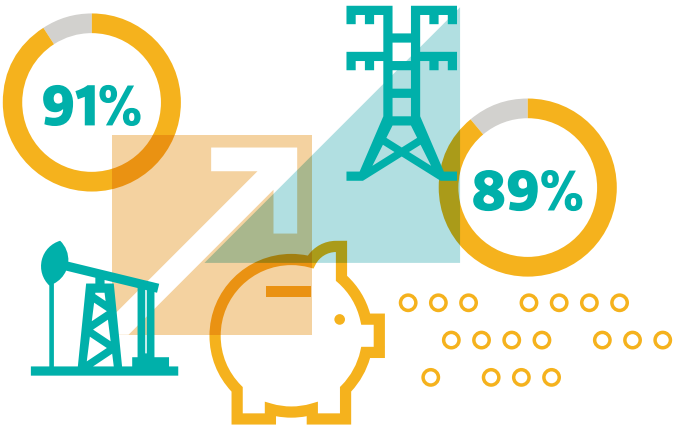
Along with delivering the benefit of increased connectivity, however, ruggedized networking introduces the need for an even greater emphasis on security. Although SCADA (supervisory control and data acquisition) networks have been used for decades in the energy industry, they have typically connected equipment within the enterprise. As SCADA networks more frequently connect with the growing IoT, security risk and data vulnerability balloon.

"This greater interconnectivity makes security absolutely critical," Pilcher says. "Often, the SCADA networks were designed without proper security because they were created for a non-networked or a closed-network environment. With interconnected systems, a firewall is no longer sufficient. You need multiple layers of network protection including perimeter security, device security, remote access security and user authentication solutions, among others."

There's little question that energy companies unprepared to take full advantage of ruggedized networking to integrate disparate operational and IT systems could miss out on valuable business opportunities. Since complex ruggedized networks are not off-the-shelf solutions, the key is to design secure, customized solutions carefully aligned with specific company needs and objectives.

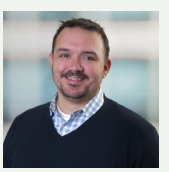
"You have to keep the end in mind, whether it's creating a safer or more sustainable environment, more effective processes or expanded connectivity," Pilcher says. "Effective planning is essential for ensuring optimal results."

The IoT is growing rapidly: **18.2B** objects are connected in 2015, and the number is expected to reach more than **50B** by 2020.[2]



91% of oil and gas companies and **89%** of utility companies expect their investment in IoT to increase over the next three years.[3]

RUGGEDIZED NETWORKING DEMANDS ROBUST PLANNING



CDW Solution Architect Aaron Pilcher offers these tips for optimizing performance with a ruggedized network:

1. **Plan carefully before you implement.** Invest time up front in thorough analysis and comprehensive roadmap development to prevent future problems.
2. **Deploy high-quality ruggedized components end to end.** Use hardened switches, routers, wireless access points, backhaul, storage and endpoints that meet appropriate use specifications and are designed to withstand harsh conditions and operate maintenance-free for extended periods.
3. **Focus on security.** Address heightened risk by implementing a multilayered security approach that incorporates perimeter security, remote access security, monitoring, endpoint security and other protective strategies.
4. **Partner with an expert.** Many internal IT teams lack experience in this specialized area. Highly knowledgeable, experienced guidance can help build a solid foundation for reliable connectivity and value-added performance.

To learn more about ruggedized networking, download our white paper, "Delivering the Power of the Network," at **CDW.com/scadawp**

[1] Pwc.com, "18th Annual Global CEO Survey," 2015
[2] Newsroom.cisco.com, "Connections Counter: The Internet of Everything in Motion," 2013
[3] Cisco.com, "Attaining IoT Value," 2014

PARTNER CORNER

RUGGED DEVICES DELIVER **RELIABILITY AND PORTABILITY**

Xplore Technologies Chief Marketing Officer Peter Poulin discusses why today's highly mobile energy workforce creates a growing demand for rugged devices.

Q: **What energy workforce challenges create a need for rugged endpoint devices?**

A: Devices used primarily outdoors, whether workers are inspecting a pipeline or on an offshore oil rig, are subject to extreme environmental elements. Along with rain, snow and humidity, a big challenge is simply temperature changes. In addition, device screens need to be readable in direct sunlight, and workers may need to use the device while wearing protective gloves. In explosion-prone areas, devices must be properly certified to ensure they will not cause a spark.

Q: **How does the highly mobile nature of field workers affect rugged device selection?**

A: Devices should provide both portability and mobility. That requires in-vehicle solutions that allow workers to mount, dock and safely secure rugged devices while they drive from site to site in their trucks, yet easily remove and use the devices when they're doing repairs, inspections or other tasks. A true mobility solution is not just about the tablet — it's also about the peripherals that support workflow. For example, rugged devices with hot swappable drives have a small backup battery inside so field workers who need power throughout a shift can quickly swap out batteries without having to power down their devices.

Q: **What other advantages do rugged devices offer over typical consumer mobile devices?**

A: Rugged devices are made with magnesium rather than aluminum frames. Magnesium is much stiffer and stronger, preventing the devices from bending — and the glass from breaking — if they're dropped. Gorilla Glass from Corning is frequently used because it's highly impervious to breakage. Research shows that although rugged devices typically cost more up front, over the five-year product lifecycle, the total cost of ownership is nearly half that of consumer devices due to replacement costs and lost productivity related to device failure.

Q: **What advice would you offer regarding selection of rugged devices**?

A: MIL-STD-810G testing and IP (ingress protection) ratings are the two standards that measure ruggedness, but the terms can be confusing. 810G is not a specification — it's a methodology for testing ruggedness levels using drop tests and other standards. It's important to look at detailed manufacturer specs to understand exactly how the test was conducted and whether the device can withstand the real-world conditions where it will be used. IP ratings indicate how much pressure it takes for water, dust or grains of sand to get into a device.

Before you deploy any technology, rugged or otherwise, you need to identify your goals and study the workflow of the workers who will be using the devices. That way, you can identify the necessary requirements and decide when it's worth investing in rugged devices and which features matter most.

XPLORE TECHNOLOGIES

As CMO of Xplore Technologies, Peter Poulin is responsible for strategic planning, business development, product marketing, brand building, channel development and demand generation. With more than 25 years of sales, marketing and general management experience, Peter has served in leadership roles across a broad range of startup and well-established organizations, including three years as Motion's CEO.

SMART SECURITY STRATEGIES IN THE AGE OF **HYPER-CONNECTIVITY**

By Nicolaas Smit

There's no ignoring two hard and fast facts.

Number one, forward-looking oil, gas and utility companies see digital transformation powered by the Internet of Everything (IoE) as an opportunity to achieve operational efficiencies and gain competitive advantage.

Number two, the exploding number of interconnected devices and applications substantially increases the risk that cyberattackers can steal or alter critical information, disrupt processes or damage equipment.

The good news is that security concerns don't need to inhibit pursuit of digital hyper-connectivity and the benefits it can bring. In fact, innovative approaches that integrate traditional physical security with multilayered cybersecurity solutions can boost efficiency, production and safety while also reducing costs.

To effectively address the entire continuum of cyberthreats before, during and after, security strategies should be:

- **Visibility-driven.** Solutions should deliver a real-time picture of the network, devices, data and applications that can be used to control the environment and mitigate threats.
- **Threat-focused.** You need the ability to detect, understand and stop threats, which requires continuous analysis and real-time intelligence across all technologies.
- **Platform-based.** An integrated system of agile, open platforms that covers your network, devices and the cloud enables end-to-end visibility with centralized management for unified policy and consistent controls.

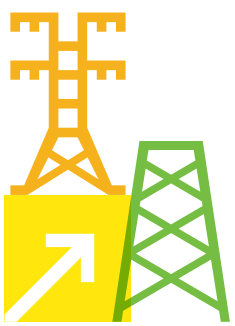
Embracing the IoE increasingly means converging information technology (IT) and operational technology (OT) systems, each of which have unique security management requirements. Comprehensive, integrated security solutions that are pervasive and applied in a unified way across the extended network don't simply protect against unauthorized access — they ensure your ability to securely capitalize on connectivity to increase business agility and improve performance.

PROTECT YOUR SYSTEMS, END TO END

Here are four steps you should take to safeguard your interconnected IT and OT systems:

1. **Establish the baseline.** Inventory all assets and their current state, and design defenses assuming that a successful attack is inevitable.
2. **Achieve visibility.** Ensure visibility of your assets, protocols, users, applications and traffic patterns on the control network so you know what is "normal."
3. **Implement controls and automation.** Prioritize your assets and systems, and build out defenses for the most critical ones first. Be sure to implement a combination of IT security and IACS (industrial automation and control systems) security.
4. **Strive for continuous improvement.** Test, review and update defenses and policies regularly, as threats and attack techniques constantly evolve.

Nicolaas Smit is director of the Energy Global Industries Center of Expertise at Cisco. He is responsible for identification, development and go-to-market strategy for the energy industry, including oil, gas and utility companies.



CONTACT CDW ENERGY & UTILITIES

To learn more about how we can help you achieve your IT objectives, contact your CDW Energy & Utilities account representative at **877.645.0685**

CDW.com/energy

@CDWCorp

CDW