CDW PEOPLE WHO GET IT™

PROTECTING I.T. RESOURCES IN OIL, GAS AND UTILITIES

Energy companies must bolster their cybersecurity efforts as they face down a variety of threats.

EXECUTIVE SUMMARY

Oil, gas and utility companies have historically paid less attention to cybersecurity and IT than to physical security and operational technology, but there is a growing awareness within the sector that this imbalance is unsustainable. Cyberattacks on critical infrastructure have shown how vulnerable physical equipment and systems are and how much damage a successful attack can cause.

With valuable assets including customer data, intellectual property and networked heavy machinery, energy companies are prime targets for cyberattackers. As these threats grow both in sophistication and in number, leaders at many energy companies are understandably turning a more focused eye toward shoring up their own networks and systems. However, many organizations find themselves playing catch-up, a situation exacerbated by a shortage of experienced cybersecurity professionals who have the industry-specific knowledge needed to protect industrial systems from attack.

To effectively combat cyberthreats, energy companies must first assess their vulnerabilities and then implement a comprehensive cybersecurity strategy. This will, of course, involve the introduction of sophisticated new technical solutions into the IT and operating environment. But any good plan must also establish effective policies and procedures to ensure that these solutions perform as designed.

Advancing Threats

At many energy companies, cybersecurity efforts have long taken a backseat to physical security measures. IT and operational technology departments have frequently been kept separate from one another, with the latter often given preference over the former. Partly, this is a function of legacy, as many oil executives have backgrounds in exploration and extraction, rather than IT. But a simple bottom-line calculus also factors into the situation. While drills and pumps bring moneymaking natural resources to the earth's surface, firewalls and anti-virus software do not.

That calculus is quickly changing, however. While cybersecurity measures still cannot add to a company's revenue, they can certainly protect against losses. And with cyberattacks growing in both number and sophistication, executives at many energy companies are beginning to understand just how substantial those losses can be.

According to security firm Trend Micro's 2015 "Report on Cybersecurity and Critical Infrastructure in the Americas," 76 percent of security leaders say that attacks against infrastructure are becoming more sophisticated. In that same survey, 55 percent of respondents said they had noticed an uptick in the number of attacks over the previous year (with only 7 percent reporting a decrease), and 43 percent of respondents said they had detected cyberincidents that were specifically targeting infrastructure. Perhaps most concerning is the fact that the energy industry ranked second (behind only government) on the list of sectors facing malicious attacks designed to delete or destroy information, with 47 percent of organizations in the field experiencing such attacks.

At the same time that attack levels are rising, so are the costs of a successful breach. IBM and the Ponemon Institute estimate the cost incurred for each sensitive stolen record at $217, with the average total cost of a data breach at $6.5 million.

Energy companies, in particular, have a special set of vulnerabilities. Similar to enterprises in fields such as finance and healthcare, they store sensitive data, including payment information and personally identifiable information. But unlike companies in those sectors, many oil, gas and utility companies use their IT networks to control large physical systems. Add in the fact that energy companies' IT systems contain treasure troves of valuable intellectual property, and it is easy to see why a successful cyberattack against an energy company has the potential to be catastrophic in multiple ways.

Additionally, many energy companies operate in remote locations and harsh environments, making it more difficult to secure and monitor networks and equipment. Often, these enterprises' operations run 24 hours a day, seven days a week, making it impossible to detect network activity that occurs "after hours." Most critically, many companies in this sector manage powerful equipment that could lead to physical harm for workers or the general public if it were commandeered by attackers.

This multitude of potential targets within energy companies demonstrates how the industry is under assault from a number of different angles. For obvious reasons, energy companies are attractive targets for terrorists who want to cripple Western operations and generally wreak havoc by inflicting physical damage in a spectacular fashion. The sector is also vulnerable to antagonistic activists and nation-states. The trade secrets housed on company information systems (including oil exploration and refining techniques, and areas of future exploration) make them vulnerable to corporate espionage, as well as organized crime syndicates working on behalf of competitors. Finally, malicious insiders may target their own companies for any of the above reasons, or simply because they are unhappy with their employer.

Cybercriminals are currently using three popular methods of attack on the networks of energy companies: network-based attacks, watering holes and spear phishing. In network-based attacks, cyberattackers utilize platforms such as the Nuclear exploit kit to launch attacks directly against a company's infrastructure. A watering hole is a third-party website known to be visited by energy stakeholders (for example, the energy section of a major news website) that has been infected by hackers, allowing malware placed there by attackers to then spread to an energy company's own network. Spear phishing is a form of "social engineering" in which attackers send fraudulent emails purporting to be from a known contact of the victim. The recipient is then prompted to either click on a malicious link or provide confidential information.

The following notable attacks illustrate the potential consequences when cyberattackers target critical infrastructure:

Haifa: In 2013, the Associated Press reported that the northern Israeli city of Haifa had fallen victim to unknown, sophisticated cyberattackers who targeted a toll road there. Using a Trojan horse attack to take control of systems, the cyberattackers shut down the roadway for 20 minutes on one day, and then the next day locked down the tollway for eight hours.

Stuxnet: Widely seen as the world's "first digital weapon," the Stuxnet worm that sabotaged Iran's nuclear program was discovered in 2010. The worm attacks programmable

$5.7 million and $3.7 million

The average annual information security budgets of oil and gas companies and of power and utilities firms, respectively*

→ *TO LEARN MORE about how CDW can help companies in the energy and utility industries, check out our brochure on "Powerful IT."*

***SOURCE:** Verizon, "State of the Market: The Internet of Things 2015," February 2015

logic controllers (PLCs) used to control machinery, and it was introduced into networks via an infected flash drive. Partly because the attack targeted Iranian nuclear centrifuges, there has been widespread (and unconfirmed) belief that Stuxnet was the work of the U.S. government. Still, the worm demonstrated how mechanical systems can be just as vulnerable to cyberattacks as computer systems.

Baku–Tbilisi–Ceyhan Pipeline: This conduit carrying oil from the Caspian Sea to the Mediterranean Sea exploded in August 2008 in Eastern Turkey. An investigation revealed that cyberattackers had super-pressurized crude oil in the pipeline, causing the explosion. In addition, they shut down alarms, cut off communications and erased 60 hours of surveillance video. Published reports indicate that U.S. intelligence officials believe the Russian government to be behind the attack.

Lessons from Cyber Storm IV

Cyber Storm IV, the latest in a Department of Homeland Security series of exercises to test cybersecurity preparedness, ran from 2011 to 2014 and included large-scale simulated cyberattacks on critical infrastructure.

In a June 2015 report, DHS identifies four main trends:

1 **Cyber response and operating plans:** Participants found that to be useful, plans must be accompanied by training and education efforts. "Planners and stakeholders," the report states, "should champion training and education efforts to ensure that plans ... are widely socialized and understood across the relevant stakeholder set."

2 **Information sharing and communications:** Although the sharing of information is critical to reducing incident response times, the exercises revealed that many organizations lacked well-defined communication procedures. According to the report, "Organizations with stablished relationships and experience sharing information during steady-state or previous incidents coordinated far more easily during exercise play."

3 **Resource identification and allocation:** The response of some organizations was hampered by the fact that stakeholders did not know what resources were available or how to access them.

4 **Cybersecurity training, awareness and education:** Employee turnover and constantly evolving threats necessitate ongoing training, the report's authors write. "While exercises can increase player awareness of cyber-based threats, attack vectors and potential attack impacts, more consistent familiarity and exposure is needed."

Maroochy Shire: In 2000, the Maroochy Shire wastewater treatment system in Australia lost control of its supervisory control and data acquisition (SCADA) network. Pumps weren't running properly, equipment alarms weren't reported to network administrators, and sewage flooded local parks and rivers, killing marine life and filling the surrounding area with a lingering stench. Investigations revealed the culprit to be a disgruntled former employee of the company that installed the SCADA network.

The Regulatory Environment

Energy companies and would-be attackers aren't the only ones to take notice of vulnerabilities within the sector. Government agencies have also begun to show heightened concern over potential attacks, issuing new mandatory regulations and voluntary guidelines related to cybersecurity, energy and critical infrastructure. Agencies involved in the regulation of energy and utility companies include the departments of Energy and Homeland Security, the Federal Energy Regulatory Commission (FERC) and the Environmental Protection Agency.

In a 2013 Presidential Policy Directive, the White House listed the energy industry among 16 sectors whose assets, systems and networks are so vital that their incapacitation or destruction would have a debilitating effect on national security. "Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient," the directive states. "Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response and recovery."

In its 110-page Energy Sector-Specific Plan for national infrastructure protection, DHS outlines a roadmap for securing control systems in the energy sector, with these goals:

- Energy asset owners should be able to perform fully automated security monitoring of their control system networks, with real-time remediation.
- Enterprises should replace legacy systems and implement next-generation control system components and architectures with built-in, end-to-end security features
- Control system networks should automatically provide contingency and remedial actions upon detecting attempted intrusions.
- Energy asset owners and operators should work collaboratively with government and sector stakeholders to accelerate security advances.

In January 2015, the Department of Energy released guidelines for implementing the 2014 Cybersecurity Framework established by the National Institute of Standards and Technology. The guidelines recommend a seven-step process for implementing the NIST framework.

Step one, "Prioritize and Scope," involves the identification of high-level priorities and a determination of the scope of the systems and assets that need protection. "Orient," the second step, includes the identification of threats to and vulnerabilities of the enterprise's systems and assets. Step three

is "Create a Current Profile," which means mapping out current organizational cybersecurity practices, including an assessment of whether those practices are achieving desired outcomes.

In "Conduct a Risk Assessment," the fourth step of the process, organizations use threat and vulnerability data to estimate the likelihood and projected impact of cybersecurity events. Step five, "Create a Target Profile," involves the listing of desired cybersecurity outcomes. In the sixth step, "Determine, Analyze and Prioritize Gaps," organizations identify gaps between current and desired outcomes and create a prioritized action plan to address those gaps. The final step, "Implement Action Plan," includes both executing the plan and tracking its progress over time.

317 million

The number of new pieces of malware created in 2014*

In 2013, FERC approved Version 5 of the North American Electric Reliability Corp. (NERC) Critical Infrastructure Protection cybersecurity standards for utilities. The new standards go into effect April 1, 2016, and for the first time allow NERC to impose penalties for noncompliance. Analysts say that utility companies will need to take a number of steps in order to comply with the standards, including protecting critical infrastructure with robust firewalls and network segmentation, implementing patch management solutions and systems to classify data by security level, and identifying specific vendors and solutions that can meet the new standards.

Elements of a Security Strategy

The prospect of creating an entire cybersecurity strategy from scratch (or bringing an outdated or insufficient plan up to speed) can be overwhelming. Managers at many organizations may know that they need to improve their cybersecurity efforts, but they may not be certain where to start.

Typically, the first step is to assess an organization's current cyberassets and vulnerabilities through threat checks, penetration testing or other forms of risk assessment. In a threat check, IT administrators or outside consultants monitor the network to see whether it has already been compromised by malware or other types of attacks. Penetration testing is a more involved process, during which cybersecurity professionals assess an organization's vulnerabilities by attacking them directly with penetration attempts. Essentially, they act as hackers in order to see what sort of access determined attackers might be able to gain on a network, and what sort of damage they might be able to cause.

Once stakeholders within an enterprise understand their current vulnerabilities, they can implement the elements of an effective security environment and draft a plan for what to do before, during and after a cyberattack.

The elements of an effective security environment include:

Physical security: Most energy companies have no shortage

Securing SCADA Networks

The many moving parts of a supervisory control and data acquisition network can make managing security a daunting task. Energy and security experts offer these tips:

Monitor for abnormalities: Raj Samani, chief technology officer for Europe, the Middle East and Africa at Intel Security, exaggerates that protecting entire SCADA systems is easier than safeguarding his daughter's iPad, because security administrators can expect to see a very specific type of activity on them. "They shouldn't be running iTunes on them, hypothetically," he says. "Creating a baseline for what should and shouldn't run on them should be achievable."

Protect against internal threats: If a company does experience a SCADA breach, the most likely culprit is not an outside group, but a disgruntled current or former employee, says Tim Haïdar, editor in chief of Oil and Gas IQ. This means companies must studiously track who has access to different systems and revoke credentials when users no longer need them. "The most important thing about any company is its people," Haïdar says. "They're also the biggest threat to any company. Keep on changing the locks."

Plan for the worst: No security system is foolproof, and companies need to develop and test cyberincident plans in the same way that they test their business continuity plans, says Jim Guinn, global leader for cybersecurity practice in energy, mining, chemicals and utilities at Accenture. "This is not a one-and-done activity," he says. "The plan must be exercised annually, because threat vectors and attack surfaces change as technology evolves."

***SOURCE:** Symantec, "Internet Security Threat Report," April 2015

of fences, cameras and motion detectors to protect their far-flung physical assets. But it is worth mentioning these security measures within the context of cybersecurity, as well. In 2014, unknown attackers cut through major telecommunications cables and shot up transformers at a PG&E electrical substation outside of San Jose, Calif. The attack caused power to be briefly rerouted from the facility, and some media reports described the event as an attempted assault on the nation's power grid.

Perimeter security: Measures to defend the network perimeter include traditional firewalls and next-generation firewalls, unified threat management and intrusion prevention and detection. None of these tools is foolproof, and some security experts have compared firewalls to "hand washing" — a simple hygienic practice that can greatly reduce the risk of infection but cannot possibly catch every single threat. Intrusion prevention and detection tools create another layer of perimeter security, warding off attacks and alerting IT managers when the network has been breached. Unified threat management solutions typically incorporate these and other tools.

Authentication: Many security experts have arrived at the conclusion that a password alone is not a sufficient authentication measure for granting access to sensitive systems and data. More and more, two-factor authentication (using some combination of passwords, key cards, biometrics or other authentication factors) is becoming standard practice, especially for executives. However, authentication is a complicated issue for energy companies, because workers need to be able to quickly shut down certain equipment during emergencies, without going through a time-consuming multifactor authentication process.

Device and endpoint security: Individual machines must be protected with encryption, anti-virus and anti-malware software, as well as other security measures. The increasing presence of mobile devices on corporate networks — especially employee-owned devices brought into the enterprise through bring-your-own-device programs — makes endpoint security especially important, as organizations must ensure that no sensitive data lives on these devices.

Monitoring: Data logging, packet inspection and network traffic monitoring can all help organizations detect anomalous activity that could indicate an intrusion. For these monitoring activities to be effective, though, IT administrators must have a firm grasp of what normal network traffic should look like. This can be achieved by taking baseline "snapshots" of network traffic at times when there are no intrusions. To be confident in this baseline, organizations must first meticulously scan their networks for malware and purge the malicious programs from their networks. Otherwise, the traffic generated by these programs could be mistaken for healthy baseline traffic, leading to future malware going undetected.

An effective security strategy should include an action plan for before, during and after an attack.

Before an Attack

- **Discover vulnerabilities:** The easiest way to deal with an attack is to prevent it from happening in the first place, and attacks can be prevented if organizations continuously search their networks for vulnerabilities and work to mitigate them.
- **Harden systems:** Organizations should work to ensure that their IT systems are protected by the best possible cybersecurity tools.
- **Enforce security policies:** Even the best security plans won't work if they aren't followed. Organizations should provide ongoing cybersecurity training and work to ensure that all users, including upper management, are following policies designed to keep the enterprise safe.

During an Attack

- **Detect attackers:** Next to prevention, early detection of an attack is likely the most effective way to mitigate extensive

Expert Insight

Kevin Haley, director of Symantec Security Response, shares his expertise and insight on security for energy and utility companies.

Q: *What are the primary sources of cyberattacks in the oil, gas and utility industries?*

A: As with many industries, the energy industry is often a target for cybercriminals seeking financial gain or intellectual property. However, the energy industry has also found itself the target of cyberattackers intent on sabotage and hacktivism. That puts the industry in a fairly unique position of dealing with all four of these types of attacks.

Q: *Can you identify an example of a security challenge unique to the energy sector?*

A: The increasing number of connected systems and centralized control for industrial control systems means that the risk of attacks in the future will increase. Energy and utility companies need to be aware of these risks and plan accordingly to protect their valuable information as well as their industrial control systems or supervisory control and data acquisition networks.

Q: *Are most enterprises in this sector properly prepared to handle these sorts of attacks?*

A: There is no benchmark or rating that tells us how well an organization has prepared itself to defend against cyberattacks, but many companies become more aware only after they're breached — often, long after they have been breached. Unfortunately, many companies still do not employ even the most basic security precautions. At least 40 percent of spear phishing attacks could be prevented if companies blocked executable attachments and screensavers at the email gateway, for example. Additionally, three out of four companies have websites with unpatched vulnerabilities. Many companies are failing in the basics of protection.

damage. Intrusion detection systems, coupled with diligent network monitoring, will put organizations in position to respond to a breach as soon as possible.

- **Block access:** If network architecture has been designed with multiple gates and buffer zones between externally facing systems and more sensitive systems, attacks can often be thwarted before they reach critical infrastructure.
- **Defend systems:** Until an attack has been completely defeated, all available measures should be taken to further protect critical systems and other potential targets.

After an Attack

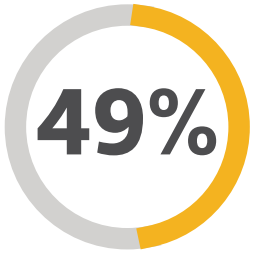
- **Determine scope**: Stakeholders should investigate to determine exactly which systems and machines may have been affected by an attack.
- **Contain damage:** Steps should be taken to ensure that malicious programs do not continue to spread.
- **Remediate:** Once the metaphorical dust from a breach has settled, the organization should conduct a thorough study of the attack. As far as possible, stakeholders should seek to understand how the attack was perpetrated, what vulnerabilities allowed it to be successful and how improvements to policies, procedures and technical solutions might prevent future attacks.

Mobile Security

Many of today's workers aren't content to be told by their companies which computing devices and software solutions they can use. They want to bring in their own mobile devices (and, increasingly, mobile apps) to solve business problems in their own ways. At their best, bring-your-own-device and bring-your-own-app programs can spur increased creativity, productivity and communication. But these types of programs also carry the risk of sensitive data residing on employee devices or on third-party apps.

A number of organizations are relying on the following solutions to support mobility in keeping it as safe as possible:

Mobile device management: MDM solutions allow IT departments to monitor, manage and secure users' mobile devices. While these tools add a layer of security to employee-owned devices, they are not foolproof. Data may still be put at risk, for example, if users employ unsecured connections to access business apps. Also, users may resist the level of access and control that MDM solutions give employers over their personal devices, including the ability to track location and wipe data.

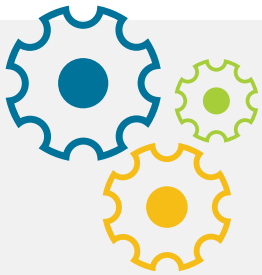


The percentage increase from 2013 to 2014 in the number of IoT connections established by companies in the energy and utilities sector*

Mobile application management: MAM tools, unlike MDM solutions, focus on securing software rather than hardware. They can provide enterprises the ability to control the provisioning, updating and removal of mobile applications, as well as the ability to monitor application performance and usage.

Client virtualization: In order to keep data from residing on users' personal mobile devices or on the servers of third-party mobile app providers, some organizations deploy client virtualization solutions. These solutions ensure that sensitive

Unlocking IoT Value in Oil and Gas



Internet of Things technologies have the ability to generate business and operational advantages for energy companies, according to "A New Reality for Oil & Gas," a 2015 Cisco Systems report. The report warns, however, that achieving these advantages will require many organizations to transform the way they do business.

The report notes that most oil and gas enterprises already have extensive experience with connected devices, and that the next step is for firms to focus on what the authors identify as the other three crucial components of the Internet of Things: data, people and processes.

In a Cisco survey, 48 percent of respondents identify data as the IoT area that they need to improve the most in order to make effective use of connected technologies. The report's authors argue that companies must learn to integrate data from multiple sources, automate the collection of data and analyze data to identify actionable insights.

In order to unlock the IoT benefits related to people and processes, the authors write, companies must eliminate barriers between their IT and operational technology departments. "These silos increase costs, limit business agility, and cripple [IoT's] ability to deliver business and operational benefits throughout the [oil and gas] value chain," they write. The authors also note that only 41 percent of survey respondents agree that their companies' operational strategies for IT and industrial control systems are closely aligned.

***SOURCE:** Verizon, "State of the Market: The Internet of Things 2015," February 2015

data remains on centralized servers. This also insulates applications from viruses that they might be exposed to on a device. Client virtualization is also typically far less expensive than building a custom mobile enterprise app. However, client virtualization has a number of potential drawbacks, including compatibility issues and difficulties working offline.

Encryption: Whenever sensitive corporate data resides on a mobile device (whether owned by an employee or the enterprise), that data should be encrypted. Encryption ensures that, even if a mobile device is lost or stolen, outsiders will not be able to access the data.

IoT Security

For energy companies, securing devices that make up the Internet of Things means safeguarding both the old and the new.

While the Internet of Things is a new concept for many consumers and businesses, energy companies have long relied on networked equipment to support operations. However, many of these systems are decades old and were not designed with cybersecurity in mind. Protecting networked equipment from cyberattack has only recently become a top priority for many organizations, in the wake of attacks such as Stuxnet and Dragonfly that brought new awareness to the vulnerabilities presented by industrial control systems.

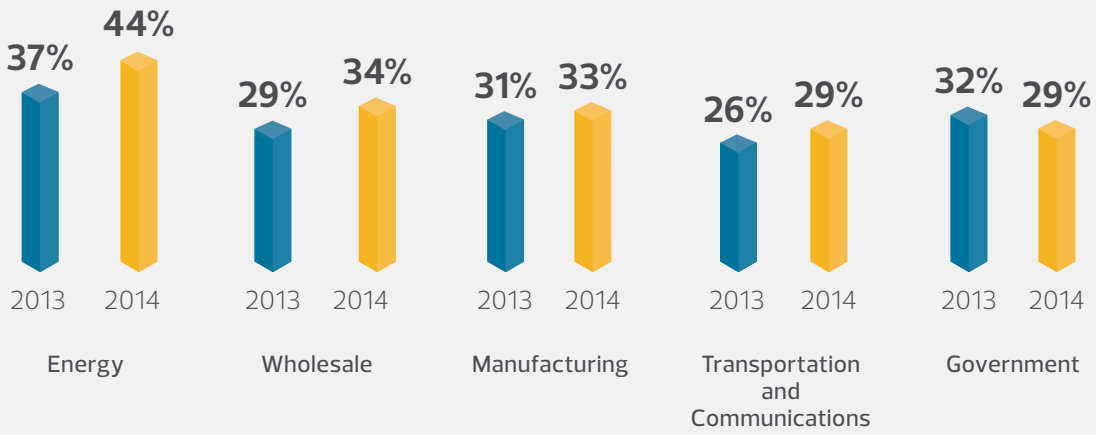
At the same time, energy companies face the same challenges as organizations in other sectors that are beginning to bring new IoT-enabled devices (including appliances, printers and wearable technology) into the enterprise. Many of these devices are aimed at the consumer market, rather than the enterprise market, and therefore lack enterprise-grade security features. While it is usually not difficult for an organization to keep any one of these products from creating new vulnerabilities, the projected influx of IoT-enabled devices presents a more significant hurdle. Cisco Systems projects that the number of physical items connected to the Internet could reach 50 billion by 2020, and each will have its own cybersecurity profile. It will be up to IT departments to ensure that these devices are incorporated into enterprise networks in ways that do not open up new points of attack for would-be intruders.

To the extent possible, enterprises should deploy devices that come with security features as part of their basic design. While IT departments in the past have been able to install security software on each computer operating within the corporate environment, the projected proliferation of IoT-enabled devices will make this approach impractical. It will simply be too expensive and time-consuming to install after-market security solutions onto every new device.

When IoT devices do not come equipped with adequate security, businesses should isolate them from other parts of the corporate network — especially for devices that are not critical to the business mission. There is no reason, for example, to have a "smart" refrigerator or coffee pot on the same network as critical infrastructure components.

Spearing the Energy Sector

In both 2013 and 2014, companies in the energy industry were at the highest risk of being targeted by spear phishing attacks.*



***SOURCE:** Symantec, "Internet Security Threat Report," April 2015

CDW: A Security Partner That Gets IT

Companies in the energy and utility industries face a daunting challenge. The security threats posed by hackers, rival companies, foreign governments, terrorists and others continue to grow in both number and sophistication. Meanwhile, the consequences for a security breach in these sectors can be catastrophic. In addition to protecting their intellectual property and customer data, these companies must also rely on their cyberdefenses to protect vast swaths of critical infrastructure. This is a burden that is unique to the energy and utility sectors, and it is a weighty one.

At many enterprises, leaders have a wealth of experience with oil rigs or power lines, but very little experience with information security tools such as firewalls or MDM solutions. For this reason, many enterprises within the energy sector choose to work with a security partner experienced in identifying, addressing and eliminating cyberthreats. CDW has partnered with oil, gas and utility companies for more than 25 years to optimize their IT infrastructure, and CDW's solution architects are specially trained to offer expert advice on cybersecurity.

Among the assessments CDW's experts can provide:

CDW Threat Check: Through partnerships with Cisco Systems, Tenable Network Security and Symantec, CDW offers a free malware detection scan, including a detailed assessment of an enterprise's network vulnerabilities, to help stakeholders determine their most critical risks. The process involves the use of a customized security appliance that passively sits on an organization's network, inspecting traffic for malware and bot activity and monitoring endpoint threats. The device also detects infected clients, identifying installed malware such as viruses, worms, Trojans and spyware, and will provide an actionable network vulnerability assessment.

Additionally, during inspection of inbound and outbound data traffic, the device identifies bots and their command-and-control servers. After the monitoring period, stakeholders meet with a CDW Threat Check engineer, solution architect and account manager to discuss the scan results. The team will also outline appropriate network, policy and software changes to help protect the organization from cyberattacks and data breaches in the future.

Penetration Testing: During penetration testing, CDW security experts take on the role of hackers, running creative, in-depth analyses to check whether security controls are operating as designed. The experts test IT systems and processes by attempting to gain access to corporate resources from the outside, helping to determine where holes and weaknesses exist in an organization's cybersecurity systems. Information gleaned from penetration testing allows CDW's experts to create tailored roadmaps, reports and recommendations aimed at protecting the IT systems and assets of an organization.

The CDW Approach

ASSESS

Evaluate business objectives, technology environments, and processes; identify opportunities for performance improvements and cost savings.

DESIGN

Recommend relevant technologies and services, document technical architecture, deployment plans, "measures of success," budgets and timelines.

DEPLOY

Assist with product fulfillment, configuration, broad-scale implementation, integration and training.

MANAGE

Proactively monitor systems to ensure technology is running as intended and provide support when and how you need it.

CDW® PEOPLE WHO GET IT™