ENERGY INDUSTRY

OUTSIDE THE (BLACK) BOX

PROTECTING CORE OPERATIONS

Accenture Security

SECURING CORE OPERATIONS IS KEY TO THE CONTINUED RESILIENCY OF OIL AND GAS COMPANIES

Although oil and gas executives express confidence in their cybersecurity strategies overall, 60 percent still view cyberattacks as a bit of a black box. But as the mandate to protect oil and gas core operations goes critical, cracking open the black box is imperative.

Considered critical elements of national infrastructure, oil and gas companies are enticing targets for hackers and other cyber criminals. And yet, research shows that oil and gas players are confident in their ability to keep these systems safe.

To gauge the effectiveness of current enterprise security efforts and the adequacy of their existing investments, Accenture surveyed 2,000 top enterprise security practitioners representing companies with annual revenues of $1 billion or more. The resulting High Performance Security Survey showed that nearly three-quarters of the energy industry respondents say they are highly confident their cybersecurity strategies will achieve favorable outcomes. Specifically, they view preventing operational service disruptions and safeguarding the company's information and reputation as strategic mandates for achieving required business outcomes. What's more, between 75 percent and 80 percent of executives say they are achieving these goals.[1]

In spite of their confidence, however, oil and gas companies are falling behind other industries. According to the same Accenture survey, energy players consistently operate below the global average in terms of cybersecurity performance. In fact, the recently released Accenture Security Index ranked oil and gas companies second to last in a cross-industry evaluation of high-performance cybersecurity capabilities with an overall ranking of 27 percent, meaning these organizations exhibited high performance in only nine capabilities on average. Additionally, oil and gas organizations ranked last in all industries in the cyber incident communications capability (22 percent).[2]

Energy executives also express much lower confidence in their companies' ability to secure the enterprise compared to the global, cross-industry total. For example, only 28 percent claim to know their organization's frequency of breaches, while 41 percent of global companies say the same. What's more, just 30 percent have confidence in their ability to monitor for breaches – a critical capability in any cybersecurity strategy.[3]

And only 18 feel confident in their ability to identify high-value digital assets and business processes.

That's nearly ten points below the global average, which begs the question: how confident can an organization be about protecting cyber assets it can't identify?

As more oil and gas players embrace new Operational Technology ("OT"), cybersecurity risks will continue to proliferate. The introduction of digital automation solutions in Information Technology ("IT") and OT networks to improve productivity, boost operational uptime and enhance safety and quality increases a company's attack surfaces, providing new openings for adversaries.

DEFENDING DIGITAL

Digital operations are key to oil and gas companies' future growth. Process automation improves productivity, increases operational uptime, and enhances safety while focusing the attentions of skilled workers where they are required most. Intelligent, connected devices increase operational efficiency by enabling real-time decision making. And more advanced solutions like mobile worker applications, virtual and augmented reality, and 3D modeling are also beginning to produce measurable benefits from the wellhead to the boardroom.

As investments in OT go up, the need for Industrial Control System ("ICS") security increases as well. Oil and gas companies have long relied on the inaccessibility of their critical infrastructure through air-gapping or other "old school" forms of protection. But such measures are no longer enough.

Each new digital application increases the company's attack surface, leaving energy companies with a real cybersecurity conundrum: how to balance the benefits of digital operations while keeping the business safe and secure?

MAPPING THE SECURITY LANDSCAPE AND RECOGNIZING INSTITUTIONAL OVERCONFIDENCE

Accenture's High Performance Security survey shows that approximately one in three breach attempts succeed; security teams identify fewer than two-thirds of them in real-time (often taking months or even years to do so); and energy players underperform the global cross-industry average in cybersecurity, at times significantly. But energy executives remain highly confident in their ability to execute their cybersecurity strategies. Three-quarters say their organizations view cybersecurity as a board-level concern that their top executives support financially and culturally. And nearly two-thirds say their organizations have completely embedded cybersecurity into their cultures.

Despite their confidence, many energy players admit they lack the ability to monitor for cyberattacks and remain unaware of better ways to protect their organizations. In fact, a concerning 60 percent of oil and gas executives surveyed claim that cybersecurity is a 'bit of a black box' – meaning that they struggle to understand when and how cyberattacks might occur.[4]

This conflict is at the heart of the challenge facing cybersecurity executives in oil and gas. Businesses must address their changing security requirements – or risk significant disruptions in production and increased safety concerns.

OPERATIONAL COMPLEXITY

Some of this apparent cognitive dissonance likely arises because of the complex cybersecurity landscape oil and gas executives must defend. Operational technology produces massive amounts of data each day, which needs to be stored, analyzed and applied in near real-time to verify productivity, efficiency and safety. However, many OT solutions are ancient in digital terms; with design lives that span decades rather than years and fail to support even basic security protocols such as data encryption.

Nevertheless, the need for real-time data and remote accessibility is driving companies to connect these devices to each other, to the internet and even to corporate networks. While great for operations in the short term, these newly connected, often unprotected Industrial Internet of Things ("IIoT") devices are attracting ambitious hackers looking for alternate attack vectors into operations and back-office systems – a virtual treasure trove of client data, intellectual property and other information.

COMPLIANCE ISN'T ENOUGH

Companies can also confuse the achievement of compliance program goals with the actions required to protect the business from breaches. And the opaqueness of compliance programs themselves may contribute to the problem. For example, when asked which factors negatively affect compliance, 70 percent to 75 percent of energy executives gave all the listed factors the same highly negative ratings – indicating a failure to prioritize factors that pose the greatest risk.[5]

When an organization believes that everything has the same impact, programs tend to lack focus. While security control frameworks and compliance programs often prove extremely helpful in defining foundational thinking, they many times fail to reflect real-world dynamics.

Just as adhering to generally accepted accounting principles does not ensure protection against financial fraud, cybersecurity compliance alone will not protect a company from motivated threat actors.

Overconfidence can also result in a lack of willingness to seek better solutions. For example, when offered additional cybersecurity funding, roughly half would use it to double down on their current strategies, namely protecting the company's reputation and company information. Far fewer (under 25 percent) would use the cash to protect against financial losses—a huge consideration in most major hacking incidents—and just 23 percent would invest it in staff training; another area that tends to pay outsized dividends.

Factors Negatively Affecting Compliance

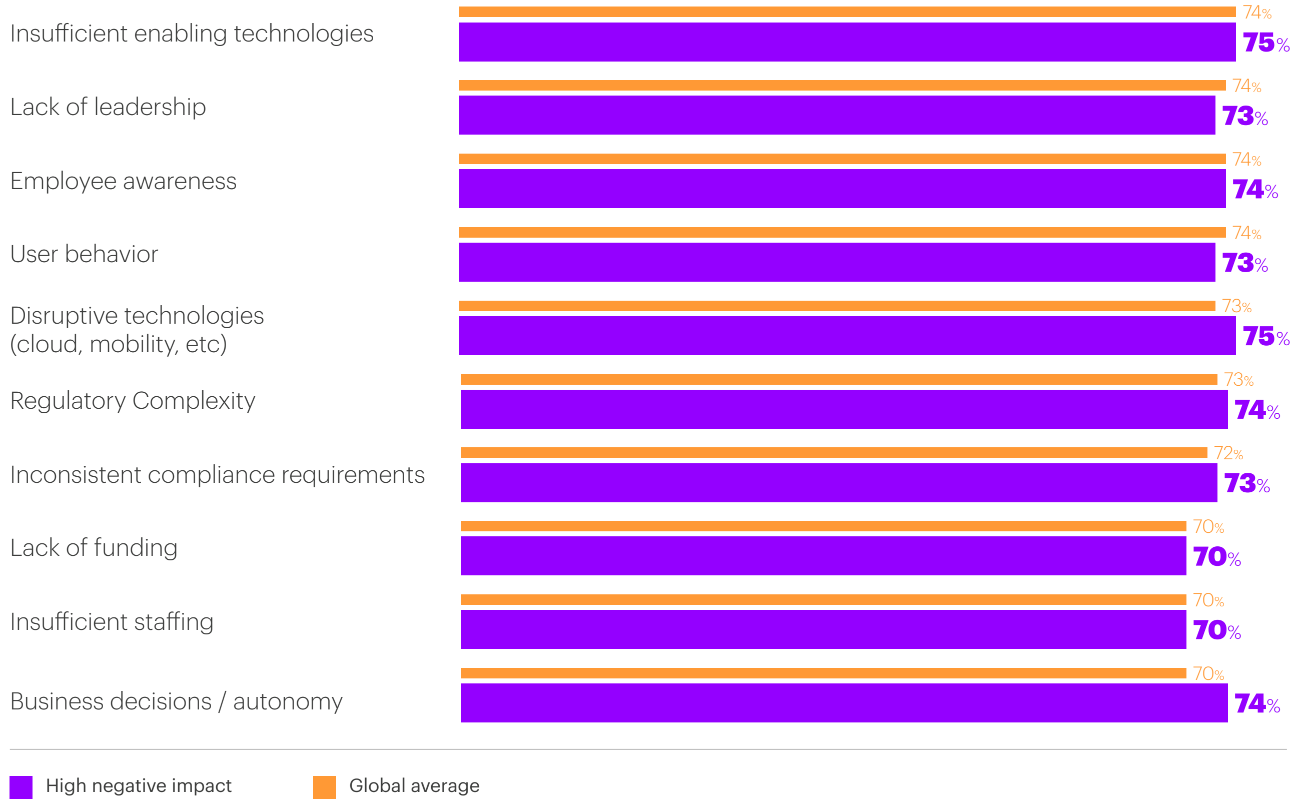

Fig 1. Energy executives indicate that every factor has a high negative effect on compliance, which shows an inability to prioritize based on greatest risk.

CRACKING THE ‘BLACK BOX’ – AND CONFRONTING CYBERSECURITY REALITY

Energy companies seeking to instate high-performing cybersecurity strategies likely have to reboot their approaches. Instead of pursuing standard “point solutions” that often fail to deliver enterprise-level impact, they need a robust approach that assesses threats across the length and breadth of their organization. The goal is to identify and reduce the enterprise’s business exposure by focusing on safeguarding priority assets.

A number of tools can crack open the black box or make it more transparent, including improved analytics, better incident response planning, and approaches that test the effectiveness of strategic plans and processes over time to identify and address any gaps.

DEFINE CYBERSECURITY SUCCESS

To reframe their cybersecurity perspectives and establish a new definition of success, oil and gas organizations need to understand what is happening on their networks – both IT and OT – and have plans in place to safeguard their businesses in the event of an attack. Start by answering several critical questions:

- Have we identified all priority business data assets and their locations?
- Can we defend the company from a motivated adversary?
- What are the potential ramifications of a successful cyberattack in terms of environmental, health, safety and productivity?
- Do we have the tools and techniques to react and respond to a targeted attack?
- Do we know what adversaries really want and what we really want to protect?
- Where should we make our cybersecurity investments based on potential risk?
- How often do we “practice” our plan to improve our responsiveness?
- Are we using the data and other outputs from our cybersecurity strategy to improve our program over time?

Energy security organizations need to improve the alignment of their cybersecurity strategies with the enterprise’s business imperatives. And while many firms are clearly making progress in compliance and risk management, security programs should continue to improve their ability to detect and deflect advanced attack scenarios.

CYBER DEFENSE FROM THE INSIDE OUT

Organizations often fail to limit internal access to key information, and do not regularly review contract workers with administrator-level access or monitor for unusual traffic or activity on the organization's networks, all of which can have severe cybersecurity consequences. However, better investments in cyber defense including advanced analytics on both industrial control systems and corporate networks can help identify issues that companies might otherwise miss and provide the data cybersecurity executives need to identify and prioritize high-value assets and processes.

Oil and gas companies should also look at how they can better use the tools that they already have. Most already have an arsenal of cybersecurity tools at their disposal, but fail to use them effectively. Through improved training and system integration, they can make better use of their technology investments.

CYBER INCIDENT MANAGEMENT PROGRAMS FOR OT AND IT NETWORKS

With oil and gas executives reporting an average of 96 attempted breaches in the last twelve months, it is no longer a matter of if cyberattacks will happen, but when.

One in every three attempted cyberattacks succeed.

This means that cyber incident management programs should be an essential aspect of any comprehensive cybersecurity program. Nevertheless, many incident management programs focus solely on the enterprise and fail to plan for potential cyberattacks on OT networks – a big problem where safety is concerned.

Virtually every energy business has invested in comprehensive environmental, health and safety (EH&S) programs designed to prevent and remediate safety and environmental issues in production operations. But many have not made the link between safety and cybersecurity, even though a successful cyberattack on an ICS environment could result in the same level of impact.

Like EH&S programs, cyber incident management focuses on identifying potential cybersecurity risks and developing comprehensive processes and procedures for dealing with potential issues when they arise. And as OT and IT become more integrated, it's essential that these programs encompass both enterprise and operational control networks and identify responsible personnel from both organizations.

(CAREFULLY) TEST SECURITY PERFORMANCE

To assess their ability to deal with high-impact threats, whether internal or external, oil and gas companies should "pressure-test" company defenses. Doing so can help leaders understand whether they can really withstand a targeted, focused attack. Organizations can engage "red teaming" external hackers in a real "sparring match" with their cybersecurity team to quickly determine whether it is up to the task.

Although testing is important, it comes with its own risks especially in OT environments. For example, a red teaming exercise of an offshore platform's ICS network could cause operators to lose control of production – inadvertently causing an event with devastating environmental, health and safety repercussions.

Leadership should work closely with operations personnel and technical leadership to understand the capabilities and limitations of their technology infrastructure. Leaders can convene a committee consisting of OT and IT personnel to develop the organization's testing strategy, and set clear rules and limitations for the red team to follow. By involving both the OT and IT organizations in security testing, companies can get a better picture of their cybersecurity program's effectiveness while limiting its potential impact on business and production operations.

MAKE SECURITY EVERYONE'S JOB

Organizations should make state-of-the-art cybersecurity an organizational mindset — one capable of continually evolving and adapting to changing threats. To foster a culture of cybersecurity and move closer to a state of digital trust, organizations should emphasize an adaptive, evolutionary approach to addressing all aspects of security on an ongoing basis.

This means investing in education and training for IT and OT staff alike so that they can step beyond their comfort zones and collaborate across the organization. Together, they can help devise security strategies that make sense in both business and operational contexts while encouraging deeper engagements with enterprise leadership on a day-to-day basis. Doing so requires IT to speak the language of OT, and vice versa.

REFERENCES

1. "Building Confidence," Accenture High Performance Security Report 2016 for Energy, Accenture, December 2016.
2. "The Accenture Security Index," Accenture, February 16, 2016. https://www.accenture.com/us-en/insight-accenture-security-index
3. "Building Confidence," Accenture High Performance Security Report 2016 for Energy, Accenture, December 2016.
4. Ibid.
5. Ibid.

CONTRIBUTORS

James Guinn, II,
Global Managing Director, Accenture Security – Energy, Chemicals, Utilities and Mining

Luis Luque,
Managing Director, Accenture Security – Global ICS Practice

For more Accenture insights on the oil and gas industry:

Accenture Energy
www.accenture.com/energy

Accenture Energy Blog
www.accenture.com/energyblog

Connect With Us
http://accenture.com/energy

Follow Us
https://twitter.com/AccentureEnergy

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and crate sustainable value for their stakeholders. With approximately 394,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit it us at www.accenture.com.

ABOUT THE ACCENTURE GLOBAL HIGH PERFORMANCE SECURITY RESEARCH

In 2016 Accenture Security surveyed 2,000 executives from 12 industries and 15 countries across North and South America, Europe and Asia Pacific. The survey objective was to understand the extent to which companies prioritize security, how comprehensive security plans are, how resilient companies are with regard to security, and the level of spend for security. The survey aimed to measure security capabilities across seven cybersecurity strategy domains identified by Accenture: business alignment, cyber resonse readiness, strategic threat intelligence, cyber resilience, investment efficiency, governance and leadership, and the extended ecosystem. More than 50 percent of respondents were key decision-makers in cybersecurity strategy and spending, including security, IT and business executives at director level and above at companies with revenues of US $1 billion or more.

DISCLAIMER

This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.