Oil and gas cybersecurity: time for a seismic shift?

by Ken Allan and Sean Sutton

Oil and gas companies function on the leading edge of technology, with operations, networks and telecommunications systems encircling the world. Unlike other industries, oil and gas facilities include remote land locations, offshore oil rigs and oceangoing supertankers all needing to be connected to operations centers around the world, global financial markets as well as local retail locations via satellite, cable and fiber.

With the digital evolution of oil and gas information technology (IT), operational technology (OT) systems, networks and processes, many of the underlying security design principles have been strained by fundamental business economics, such as:

- Improving efficiency
- Reducing exploration costs
- Maximizing returns

However, as oil and gas organizations have joined the race for global interconnectivity, they have opened their doors to an increased cyber threat, often without even realizing it.

EY's recent *Global Information Security Survey 2014* looked at how organizations deal with cyber threats by considering the following aspects:

1. **Activate** – how well have they established the solid foundation of cybersecurity within their organization?
2. **Adapt** – how dynamic was their approach? Organizations are constantly changing, cyber threats are evolving and cybersecurity needs to adapt to changing requirements.
3. **Anticipate** – were organizations adopting a proactive approach and developing tactics to identify a potential cyber attack before it happens?

EY
Building a better working world

The results suggest that 61% of oil and gas organizations believe it's unlikely or highly unlikely that they would be able to detect a sophisticated attack. Only 13% believe that their information security function is fully meeting the organizational needs, and 29% have no real-time insight on cyber threats.

This presents a conundrum as oil and gas companies continue to spend large sums of money on securing their digital infrastructure and maintaining their security capabilities. It raises a question: has investment focused on the right areas, or are cyber threats evolving faster than organizations can adapt and respond?

Security budgets are static despite increasing cyber threats

With total budgets remaining flat in recent years, competing priorities and budget constraints mean oil and gas companies are addressing only the top one or two priority areas each year. This places huge importance on how spend is prioritized and means that these companies have a limited ability to keep pace with cyber threats evolving outside their priority areas.

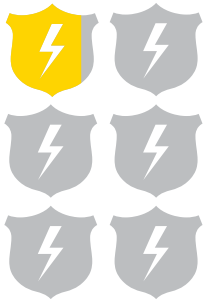
The survey also showed the majority of current spend is being allocated simply to maintain existing security capabilities. This is not to suggest that maintaining fundamental security capabilities, such as patching, antivirus updates, and user identity and access management, is not important. It is, but it does not advance a company's security capability. If you are not advancing, then you are standing still, which in the context of an evolving cyber-threat landscape means that your cybersecurity capability is actually diminishing.

It may also suggest that many organizations have not historically seen their cybersecurity posture improve as spend has increased.

Although cyber threats continue to increase, IT security budgets are staying relatively static. Security departments often still focus on purchasing the latest security tools instead of investigating and evaluating the underlying business behavior and/or root cause of the security challenges they face in order to better prioritize finite budgets. In the oil and gas sector, budget constraints are often further compounded by a separation of roles and responsibilities for operational technology (OT) security and cyber security. OT security often falls outside of the remit of a chief information security officer or chief information officer and this can lead to duplication of security spend, resource effort and misalignment of priorities.

61%
of oil and gas organizations believe it's unlikely or highly unlikely that they would be able to detect a sophisticated attack.

29%
have no real-time insight on cyber threats.



13%
believe that their information security function is fully meeting the organizational needs.

Although there is obviously a technology layer to addressing cyber threats, adopting new security technology is only one part of the solution. Other key parts are:

- Better business alignment
- Clearer understanding of existing corporate risk profiles and how they are dynamically linked to business events
- Efficient management of traditional security controls
- A strong security culture embedded within the organization

The cyber-threat landscape is evolving at an ever-increasing pace. This means where organizations are slow to recognize that they are either underspending on security or spending inefficiently, they increase the likelihood that the gap between their security capability and the threat landscape will extend to a point where the cost to "catch up" is at best significant and at worst prohibitive.

Security metrics are still too focused on "lag" indicators and don't provide a forward-looking perspective

In parts of oil and gas companies, the ability to read future indicators is paramount to success — for example, within a company's trading arm. Understanding historic events is important, but this is not the only indicator for commodity or energy traders when they are looking to buy or sell at a given price on a given day.

Security departments tend to report "lag" indicators when they are asked to provide the business with the likely cyber threats in the future that they should prioritize. These types of indicators do have some value, but they provide only a retrospective commentary on events, acting as historical indicators of performance or compliance rather than meaningful insight into future threats, risks of business initiatives or an evolving threat landscape.

The issue is that cyber threats continually evolve along with the factors that influence them. These factors are external to a given organization and are therefore not influenced by what that organization does, yet they are intrinsically linked to the decisions that same organization makes on a daily basis.

Oil and gas companies need to look at integrating "leading" indicators with their lag indicators to enhance their ability to proactively adapt their security posture to minimize cyber threats before they come to pass. In turn, being able to look at future threats more effectively can enhance the process of prioritizing security spend against those areas that will become more important.

Organizations that do this well also find they become more effective in building investment cases for additional budget since they are better able to articulate the threat, justify the risk and show how the budget can be reprioritized.

Most organizations are breached, but whether they know about it is a different matter

There is a growing body of evidence suggesting the majority of large organizations have been breached and either have threat actors operating undetected within their environments or have failed to identify the breach when it occurred. In some cases where a breach has been discovered, forensic investigation has revealed that the breach occurred months earlier and that the threat actors had likely traversed the environment targeting specific information or assets. It is often only at the point when data is being removed from the environment that an organization identifies the malicious activity and is then able to respond.

Several high-profile reports in the media over the past few years relate to state-sponsored activity within critical national infrastructure. This has included infiltration and mapping of power and distribution networks, breaches in operational technology security at nuclear facilities, and infiltration of oil and gas infrastructure, in particular, refineries and trading operations.

Not only has the threat from nation states, organized cyber criminals and hacktivists increased, but a rapidly expanding underground cyber economy is putting pressure on organizations while the intrinsic value of oil and gas assets, intellectual property and sensitive data has climbed. All of this raises the risk of cyber threats.

This situation is further compounded by the static nature of security investment within the sector, the limited ability to address prioritized areas and the lack of critical security capabilities, such as security operations centers, cyber threat intelligence and advanced malware protection.

Oil and gas organizations have the broad experience necessary to manage and support complex operations linked by large-scale networks and with many points of ingress and egress. They should apply this experience to securing these environments by:

- Implementing security-monitoring capabilities
- Enhancing response plans
- Working more closely with public sector security bodies and security partners
- Leveraging the strong health and safety culture that already exists to instill a true security culture

In this regard, the oil and gas industry has an advantage over other industries. However, this broader experience must be better utilized if companies are to adapt to the changing threat landscape.

Working together is vital to building future protection from cyber threats

The next phase of cybersecurity within the oil and gas sector needs to recognize the value of joining these resources together: using working groups to share and disseminate threat intelligence; using the experience and capability of consultancies to drive change and improvement programs; and leveraging security-vendor technology to underpin different aspects of cyber threat monitoring, alerting, defense and response. This would be a seismic shift, but one that would put oil and gas companies at the forefront of cybersecurity measures.

EY has market-leading experience in both oil and gas and cybersecurity. Our global network of security professionals works with our clients and third-party suppliers on all aspects of cybersecurity to drive a combined holistic view and approach.

For further insights on cybersecurity, visit ey.com/cybersecurity to find timely and topical publications designed to help you understand the issues and provide you with valuable insights.

Get ahead of cybercrime: *EY's 2014 Global Information Security Survey 2014*

Cyber Program Management: *identifying ways to get ahead of cybercrime*

Cyber threat intelligence – *how to get ahead of cybercrime*

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no. DW0463

EMEIA Marketing Agency
1001665

ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com