Creating trust in the digital world

EY's Global Information Security Survey 2015

Oil and gas sector results

EY's Global Information Security Survey investigates the most important cybersecurity issues facing businesses today. It captures the responses of 1,755 participants around the globe and across sectors. We base our findings and conclusions on those insights and our extensive global experience working with clients on improving their cybersecurity programs.

The following findings from the participants from the oil and gas sector show that organizations are making progress in improving the way they respond to today's cyber threats and attacks. But the results also indicate the need for considerable improvement as the world becomes more digital and attackers increase in sophistication and persistence.

Operating in a digital world invites new challenges and threats

Reputation protection involves a cyber strategy to support business transformation and financial controls compliance. As infrastructure becomes unmanned and remote, so increases the potential for destructive attacks, with cyber-physical impacts.

Operational excellence (OE) requires high safety and reliability standards so companies can minimize incidents impacting people, assets and technology. OE is a key focus area for companies with remote digital exploration and production or in politically fragile regions, as cyber threats increase with every additional technology connection.

Cyber enables digital transformation and allows for strategies to anticipate and address the specific threats and vulnerabilities in your digital world, applicable to your organization. More oil and gas companies have started or are refreshing their cybersecurity measures. Have you?

Is your cybersecurity ready to support your digital business?

Do you understand the specific threats and vulnerabilities in your digital world?

Have you done the work and thinking required to determine how that threat landscape applies to your organization and strategy?

Do you know how to set your risk appetite – the acceptable and unacceptable loss and harm from potential incidents – and how to prioritize cybersecurity measures around this?

Key findings

83% believe their information security fully meets the organization's needs

46% of organizations do not currently have a role or department in their information security function that focuses on emerging technology and its impact

40% of respondents say knowing all their assets is a key information security challenge

38% of respondents do not see managing the growth in access points to their organization as an information security challenge in the Internet of Things

47% of respondents do not have a security operations center (SOC)

40% of respondents say that lack of skilled resources is challenging information security's contribution and value to the organization

55% say an increase in funding is needed to protect the organization in line with management's risk tolerance

41% say it is unlikely they would be able to detect a sophisticated attack

39% of respondents do not have a threat intelligence program

Download our GISS 2015 report: *Creating trust in the digital world* **ey.com/giss2015**

Can you stop the attacks?

Organizations are familiar with good risk management principles, and the same can apply to cybersecurity:

Key risk management principles ...	... applied to cyber risk
1 **Focus on what matters most** Align to your unique business and risk culture	**Know your critical information assets** Identify critical business assets most vulnerable to cyber attack
2 **Measure and report** Include qualitative statements and quantitative measures	**Make cyber risk more tangible** Define cyber risk and underlying metrics clearly
3 **Comprehensive in nature** Cover all risk types, current and forward-looking	**Align with existing risk frameworks** Bring financial, operational, regulatory, customer, reputation and other frameworks together
4 **Allocation of risk appetite** Allocate based on the appetite of the business units and risk types	**Make cyber risk relevant to the business** Link organization-level risks to individual business units and their information assets
5 **Integrate with business planning** Prepare for regulators seeking evidence	**Embed risk appetite in investment decisions** Prioritize investment where critical, empower business to make informed local decisions

Cybersecurity is a digital enabler

Cybersecurity is not an inhibitor in the digital world; rather, it is the way to make the digital world fully operational and sustainable. Cybersecurity is key in helping unlock innovation and expansion. A tailored organization and risk-centric approach to cybersecurity will adjust the balance of the digital world back toward sustainability and safety to better protect your organization and build trust in your brand.

The shift to Active Defense

Understanding your critical cyber business risks and knowing what attackers may want from your organization enables you to establish "targeted defense," and assessing the threat landscape allows you to understand the most likely threat actors and methods they may use. All this information is crucial for your SOC and should be the basis on which it will support your organization.

Put in place a more advanced SOC and using Cyber Threat Intelligence to align operations that help enable Active Defense. This involves sending out intelligent feelers to look for potential attackers, analyzing and assessing the threat, and neutralizing the threat before it can damage your organization's critical assets.

Is Active Defense appropriate for your organization?

If any of the following statements apply, you should consider an Active Defense approach:

- We have an SOC but are still not finding evidence of advanced attackers.
- We have an SOC, but we still had a major breach.
- We have an outsourced SOC, but our intellectual property and business systems are not truly secure.

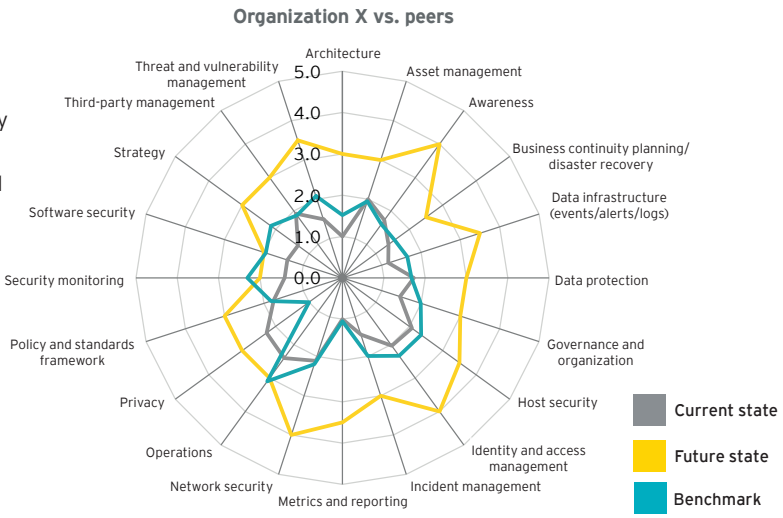
The road to improvement

Any organization will benefit from an objective assessment of its information security programs and structures:

- Understand your organization's risk exposure
- Assess the maturity of your current cybersecurity program and identify areas for improvement
- Build a prioritized road map for project investments and organizational change initiatives
- Collect information to create benchmarks against other organizations
- Determine whether your security investments have improved your security posture

This assessment needs to be broad and high-level as well as totally immersive in specific areas and components. Dashboard metrics will enable an organization to see what is needed to support the ongoing assessment, transformation and sustainability of the information security strategy.

An example of current state maturity benchmarking



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.

© 2016 EYGM Limited.
All Rights Reserved.

EYG no. 00343-164GBL

BMC Agency
GA 0000_04183

ED None.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

For further information, visit ey.com/GISS or contact your oil and gas advisory cybersecurity leader:

Americas

Simon Buesnel
T: +1 415 894 8562
E: simon.buesnel@ey.com

EMEIA

Trevor Niblock
T: +44 7983 813 954
E: tniblock@uk.ey.com

Asia-Pacific and Japan

Steve Lam
T: +65 6309 8062
E: steve-yk.lam@sg.ey.com