Cybersecurity regained: preparing to face cyber attacks

EY 20th Global Information Security Survey 2017-18

Oil and gas sector results

EY
Building a better working world

Global findings

The Global Information Security Survey investigates the most important cybersecurity issues facing organizations today. It captures the responses of nearly 1,200 participants around the globe from over 20 industries. We base our findings and conclusions on those insights and our extensive global experience of working with clients to help them improve their cybersecurity programs.

The following findings are from the 40 participants from the oil and gas (O&G) sector, and suggest that while organizations continue to prioritize cybersecurity – and are making good progress in identifying and resolving vulnerabilities – they are more worried than ever about the breadth and complexity of the threat landscape.

EY Global Oil & Gas contacts

Jeff Williams
+1 713 750 5916
jeff.williams@ey.com

Jason Finlayson
+44 20 7197 7053
jason.finlayson@uk.ey.com

Piotr Ciepiela
+48 22 5578761
piotr.ciepiela@pl.ey.com

Bala Venkateshwaran
+91 124 6779507
bala.venkateshwaran@in.ey.com

Connect with us

Visit us on Linkedin

Follow us on Twitter @EY_OilGas

See us on YouTube

O&G key findings

1. Employee awareness and exploitation

78% consider a careless member of staff as the most likely source of an attack.

43% of significant cyber breaches were from a lack of end user awareness, exploited via phishing.

2. Strategy, information security and the board

87% have not fully considered the information security implications of their current strategy and plans.

46% feel the whole board is knowledgeable about information security.

3. Risk to reputation rising

60% have had a recent significant cybersecurity incident.

15% have a robust incident response program and regularly conduct table-top exercises.

4. Skilled cyber workforce essential to keep pace with evolving threats

50% say the lack of skilled resources is challenging information security's contribution and value to the organization.

95% say their cybersecuirty function does not fully meet their organization's needs.

5. Challenges on the rise with the Internet of Things (IoT)

17% feel it is very likely they would detect a sophisticated cyber attack.

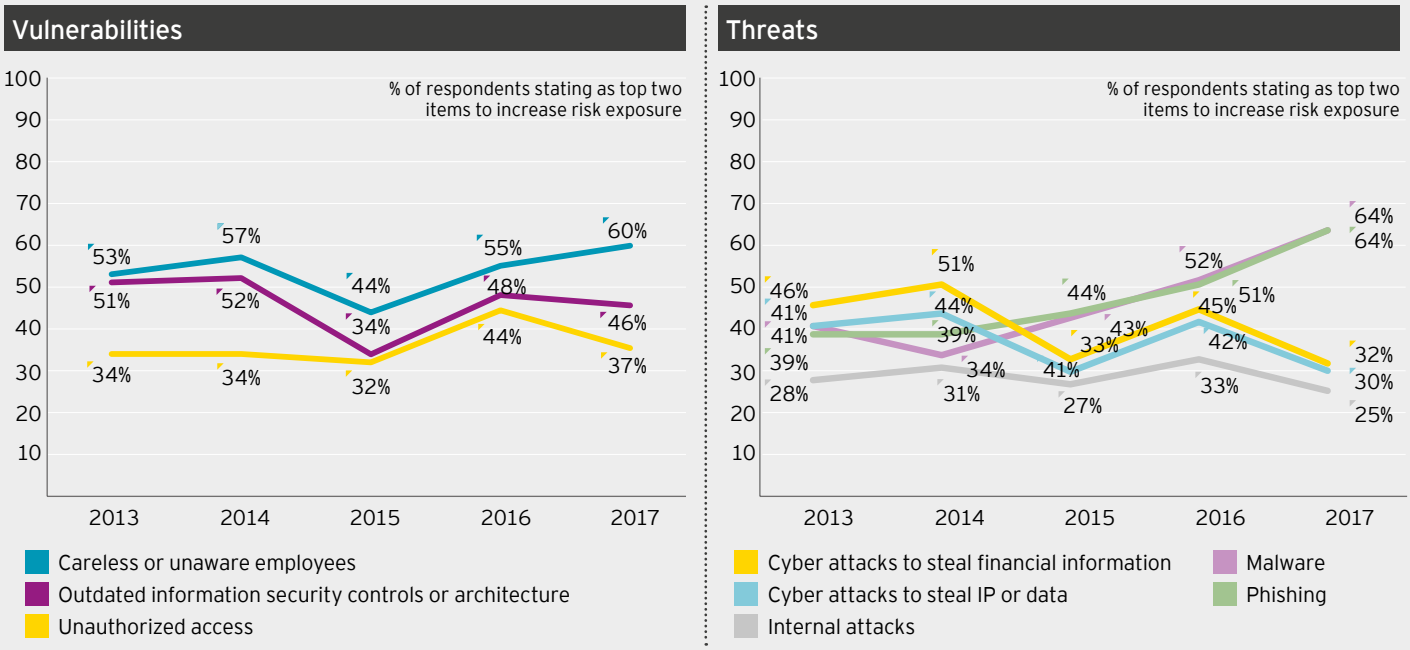
48% say it will be challenging to ensure that the implemented security controls are meeting the requirements of today.

6. Financial impacts, budgets and breaches

97% of the organizations' information security reports do not evaluate financial impact of every significant breach.

63% would not increase their cybersecurity spending after experiencing a breach that did not appear to do any harm.

Threats and vulnerabilities perceived to have most increased the risk exposure of the respondents, 2013–2017



Cybersecurity regained: building defenses that are fit for purpose

Sustained low oil prices are driving adoption of digitization across the O&G industry, ramping up the stakes for cybersecurity. Responses to cyber attacks must be multilayered, repelling the most common attacks, with a nuanced approach for advanced and emerging threat vectors. To protect critical information, an organization must not only address the security of the traditional IT and OT environments, it must also deal with the added complexities from the Internet of Things, while also integrating innovative digital business process disruptors, such as robotic process automation, blockchain and artificial intelligence. Never before has it been so important to ensure that security efforts are integrated into every facet of an organizations operations. We call this "cyber fusion."

- Defending against common attack methods means point solutions remain a key element of cybersecurity resilience, with tools including antivirus software, intruder detection and protection systems (IDS and IPS), consistent patch management and encryption technologies to protect the integrity of data, even if an attacker does gain access to it. Employee awareness is also a crucial frontline defense, building cybersecurity consciousness and password discipline to protect against the relentless malware and phishing campaigns.
- Defending against advanced attacks means accepting that attackers will get in and being able to identify intrusions quickly. A Security Operations Center (SOC) that sits at the heart of the organization's cyber threat detection and response capability is an excellent starting point, providing a centralized, structured and coordinating hub for all cybersecurity activities. SOCs are increasingly moving beyond passive cybersecurity practices into active defense – a deliberately planned and continuously executed campaign that aims to identify and remove hidden attackers and defeat likely threat scenarios targeting the organization's most critical assets.
- Defending against emerging attacks, such as the rise in cyber-physical threats, means recognizing that some threats will be unknown, especially in the O&G sector, where many are still in the early stages of their digital transformation journeys. Organizations need to build agility into their cybersecurity practices and approaches so that they are able to react quickly when the time comes. Organizations with good governance processes underlying their operational cyber fusion approach are able to practice security-by-design – building systems and processes able to respond to unexpected risks and emerging dangers.

Developing a cyber breach response plan

Organizations know it is only a matter of time before they suffer an attack that successfully breaches their defenses. Having a cyber breach response plan (CBRP) is essential to minimize the impact. An effective CBRP should encompass the whole organization. It should be regularly tested and when instigated should be led by someone within the organization with the experience and knowledge to manage the organization's operational and strategic response.

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.

How EY's Global Oil & Gas Sector can help your business

The oil and gas sector is constantly changing. Increasingly uncertain energy policies, geopolitical complexities, cost management and climate change all present significant challenges. EY's Global Oil & Gas Sector supports a global network of more than 10,000 oil and gas professionals with extensive experience in providing assurance, tax, transaction and advisory services across the upstream, midstream, downstream and oilfield subsectors. The Sector team works to anticipate market trends, execute the mobility of our global resources and articulate points of view on relevant sector issues. With our deep sector focus, we can help your organization drive down costs and compete more effectively.

EYG no: 07039-174GBL
ED None.

ey.com/giss
ey.com/digitaloil