IESBA Cybersecurity presentation

9 November 2021

The better the question. The better the answer.
The better the world works.

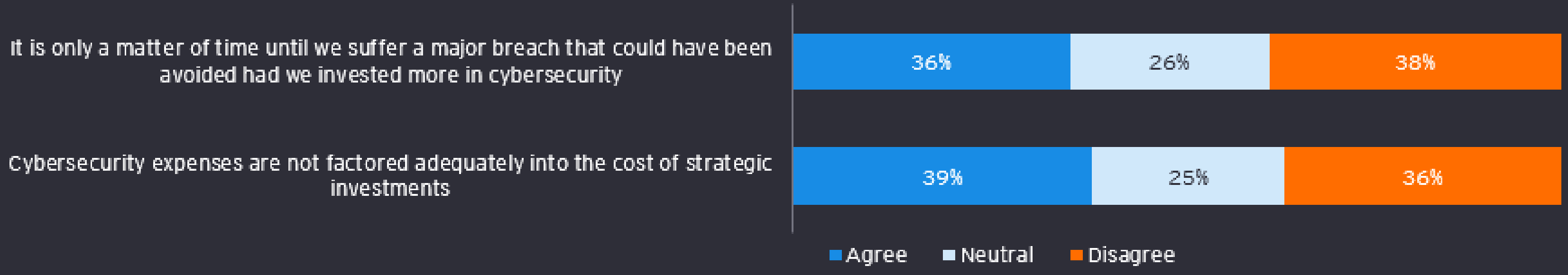
EY
Building a better
working world

Cybersecurity state of play - overview

- Cybersecurity risk continues to exponentially rise
- Cybersecurity is a people issue
- Increased quantity & magnitude of cyberattacks
- Budgets are tight / resource challenges
- Other trends
  - COVID 19 – rapid movement to cloud and remote work
  - Supply chain – protecting the ecosystem
  - Board / executive sponsorship
- Motives - Generally, three main motives of hacks are observed:
  - financial systems
  - intellectual property
  - intelligence

77% of companies saw increases in the number of disruptive attacks. Only 59% saw an increase in 2020

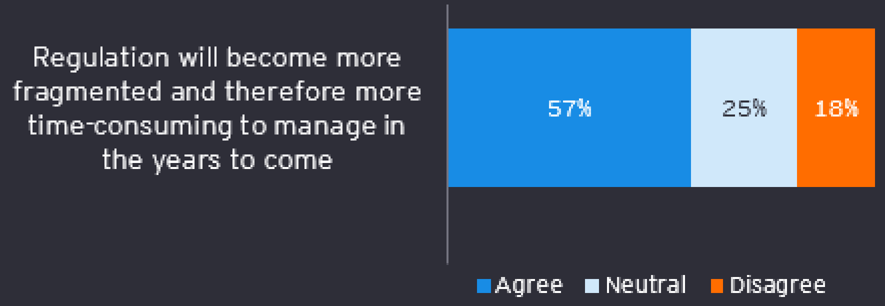
Q. To what extent do you agree with the following statements?



Cybersecurity state of play – digital disruption

- Digital transformation is affecting all organizations
- Technology adoption increases the available attack surface area
- Impact of Operation Technology (OT)
  - Perception of “air gap”
  - Critical National Infrastructure
  - OT convergence with IT - creating greater exposure
- Impact of Internet-of-Things (IoT)
  - Exponential growth in IoT connected to the digital ecosystem.
  - Disposable / inexpensive / numerous / static firmware / imbedded passwords
- “Shadow IT” is increasing
  - Bypassing IT department and enterprise security.
  - Shadow IT is generally not introduced for malicious reasons
  - Introduce insecure configuration and even data leakage
  - Not enterprise ready

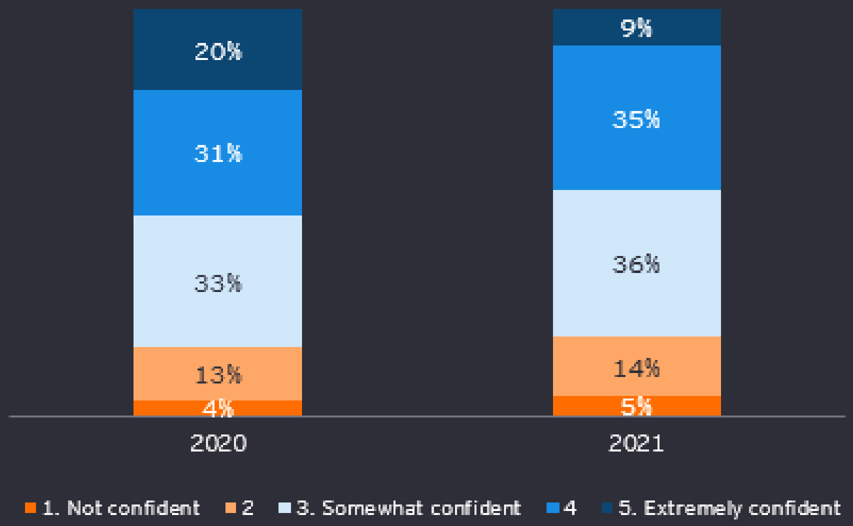
43% are more concerned than they have ever been about their company’s ability to manage cyber threats.



Cybersecurity state of play – threat actors

- State actors observed in Cyberattacks
  - Russia - cyberwarfare potential focused on Eastern Europe
  - China - intelligence and IP collection
  - North Korea – focused on financial services
  - UAE - spyware (i.e., Al Jazeera)
  - Others – generally national intelligence collection
- As long as Cyber is used as an offensive means, there wil not be any resolution to the issue

Q. How confident are you that cybersecurity risk mitigation measures can protect the organization from attacks?*

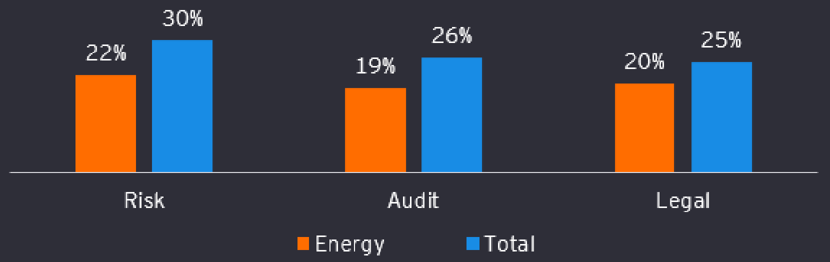


“cybersecurity defense right every single time, whereas attackers only need to get it right once”

Cybersecurity state of play – solutions

- Visibility
  - Asset management – cannot protect what you don’t know
  - Active scanning – quarterly seen as best practice
  - Each industry is at a vastly different level of maturity
- General awareness
  - Digital upskilling is required
  - Being aware and vigilant
- PAs Role in Cybersecurity
  - Cybersecurity is similar to audit
  - Pas positions are board members, senior execs, CFOs, controllers, etc
  - Regulations & standards are needed to help PAs move strategically towards the digital age
  - PAs need to understand cyber-regulations and ask the right questions, especially about risk
- Advocating Cybersecurity Hygiene in Businesses
  - Audit committees and internal audit groups for raising issues / awareness
  - Risk committees - can have challenges with cyber risk quantification

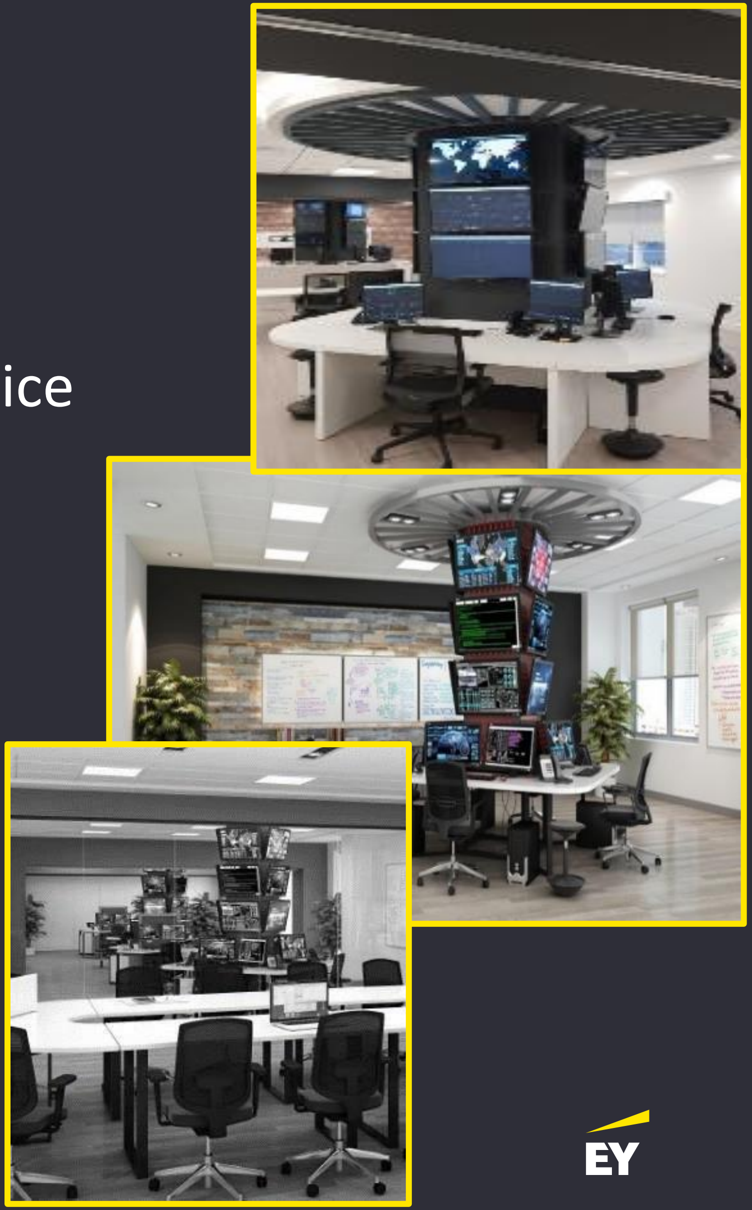
1. Energy organizations report more of a lack of trust relationship between organizational security teams and other business functions



(High trust relationships)

Cybersecurity state of play – managed services

- Current state –
  - provision of cybersecurity audits (ie. assessments)
  - clients are asking for Cyber services from their trusted audit partners
  - clients see Cyber as critical to their business
  - clients perceive cyber as a review function
- Service contract clauses – not practical to cease a critical service
  - presents a significant risk for a trusted service such as Cyber
  - especially when ongoing services are imbedded
  - hand over is complex
- Clauses make services unattractive
- Skill set shortages further stress the under resourced market
- Considered providing continuous 24/7 review or audit
- Benefit would exceed the auditor independence issue risk?



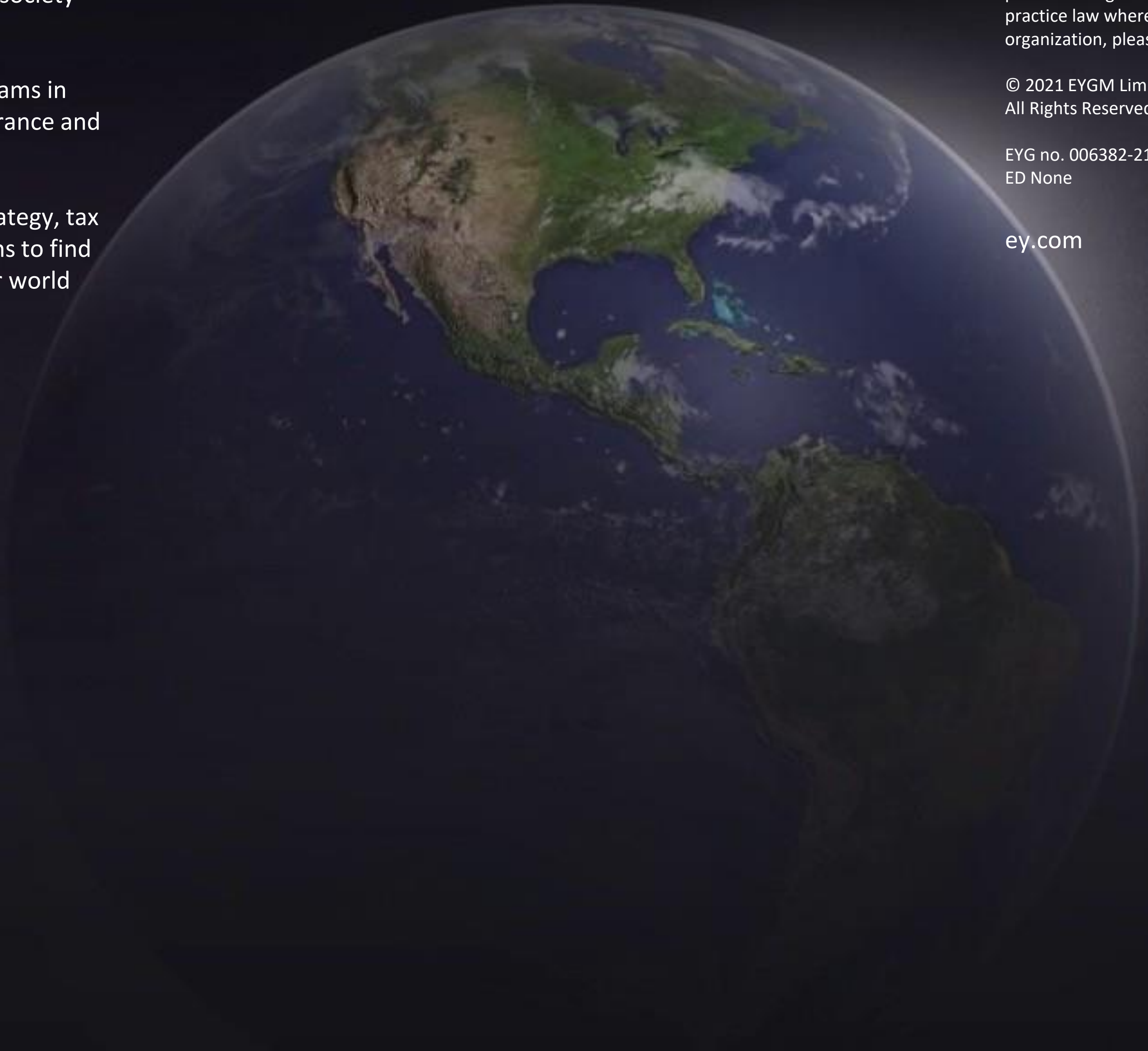
Questions?

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.



EYG no. 006382-21Gbl
ED None

ey.com