INTOSAI WGITA Virtual Seminar:
New Concern of IT Auditors

Isnaeni Achdiat

Senior Partner EY Indonesia; Senior Member of ISACA Indonesia Chapter

Thursday, 2 September 2021 (19.10 - 19.30)

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

Building a better working world

Profile

Isnaeni Achdiat

CA, CIA, CISA, CISM, CGEIT

- ✓ 28 years of experiences in EY Indonesia Consulting
- ✓ EY Asia Pacific Advisory Council Member
- ✓ Institute of Indonesia Chartered Accountants (IAI), National Council Member 2019 – 2024
- ✓ ISACA Indonesia Chapter, President (two consecutive terms) 2014 – 2018
- ✓ Founder, Media and Community AKUTAHU, A Social Enterprise promoting Knowledge Based Society & Positive Journalism in Indonesia
- ✓ University of Indonesia, Faculty of Economics and Business, Senior Lecturer
- ✓ Master Degree in Strategy and Finance, UI
- ✓ PhD candidate for Information System & Innovation.

EY

Building a better working world

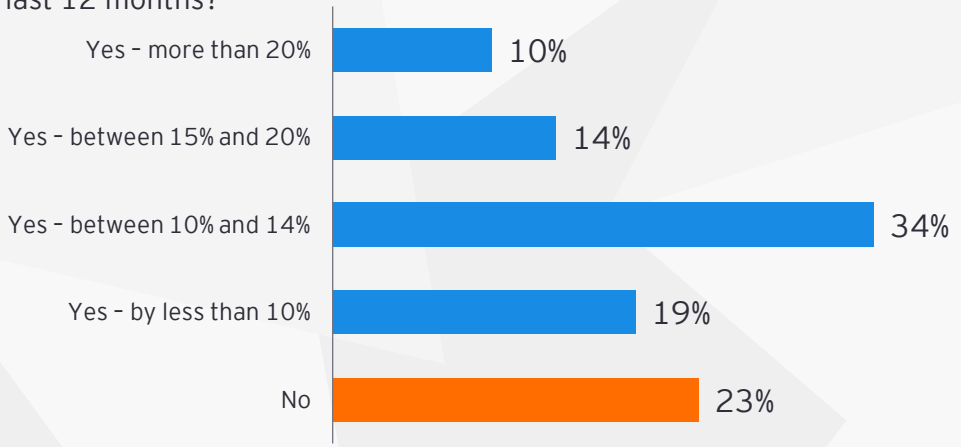
EY Global Information Security Survey 2021
Current Landscape of Cybersecurity

While cybersecurity goes hand-in-hand with information security, below are the key difference:

Terms	Objective	Key Process	Scope	Threat Example
Cybersecurity	Protect the cyber environment and organization	Preventing Cyberthreaths /Risk e.g. cyberattacks	All kinds of cyberthreats	Cyber crime/frauds, Cyber bullying
Information Security	Ensures confidentiality, integrity, and availability of information (in general, and broader sense)	Protects information from any form of threat	Digital and analog information	Unauthorized access or modification of data

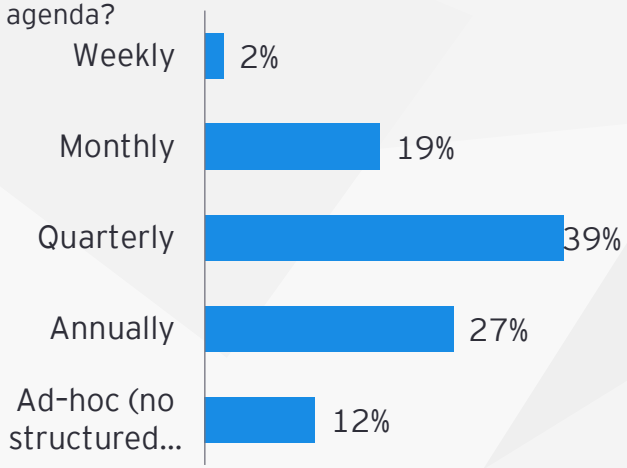
77% of companies saw increases in the number of **disruptive attacks in 2021**. Only 59% saw an increase in 2020.

Q. Have you seen an increase in the number of disruptive attacks over the last 12 months?

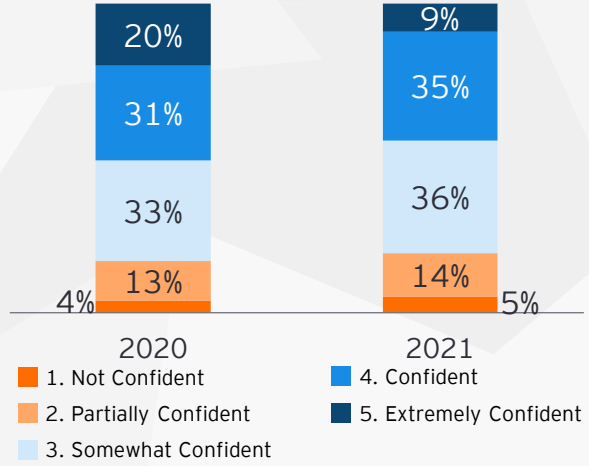


In 2021, quarterly cybersecurity on the Board agenda has **risen to 39%** (29% in 2020) and Boards are **less likely to be extremely confident** in cybersecurity than before.

Q. How often is cybersecurity on the Board agenda?



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



*From the EY Global Board Risk Survey 2021

"

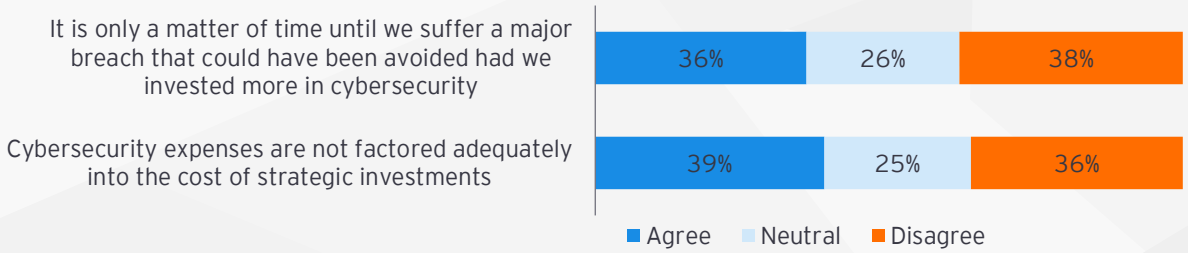
Increasing number of **cyber disruptive** attacks **corelate positively** with a more **frequent cybersecurity on board agenda** and **less confidence** on cybersecurity risk mitigation measure

This shows an **increasing attention and concern** from organization leaders regarding cybersecurity worldwide.

3 key current cybersecurity challenges
Challenge 1: cybersecurity organization is severely underfunded

Businesses spend between **2 and 5% of annual revenues on IT**, according to industry reports. Our GISS research suggests they spend just **0.05% on cyber**, on average.

1 Business are aware of the needs for cybersecurity investment, yet only **36% consider cybersecurity adequately into strategic investment**.



2 To support transformation, businesses should consider **sharing the cost** of cybersecurity across the business. However, just **15%** currently do this.

Q. How do you define your cybersecurity budget?

15%
The expense for cybersecurity is shared across business units, which define their contribution dynamically, based on use

19%
The budget is a fixed part of a larger corporate/organizational expense (e.g., 5% of IT/tech) and is defined cyclically

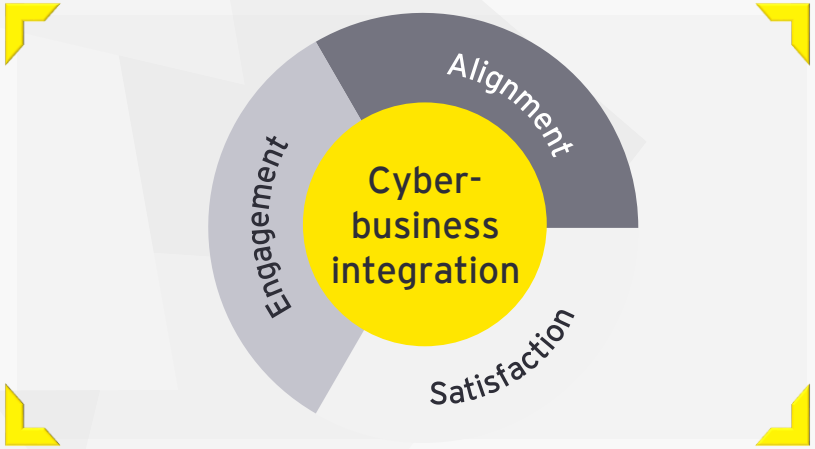
23%
The expense for cybersecurity is a fixed expense, shared across business units, which is defined cyclically

43%
The budget forms part of a larger corporate/organizational expense (e.g., IT/tech) and is defined dynamically

Steps to address the issue:
Transform the approach to business alignment

Alignment to business goals
- Map cyber strategy to business and IT strategy
- Establish risk profile to align to business goals and anticipate needs
- Apply appropriate levels of controls to protect the things that matter most

Engagement and communication mechanisms
- Service catalogue with engagement mechanism and cost chargeback
- Communication and governance channels (bi-directional)
- Performance reporting mechanisms

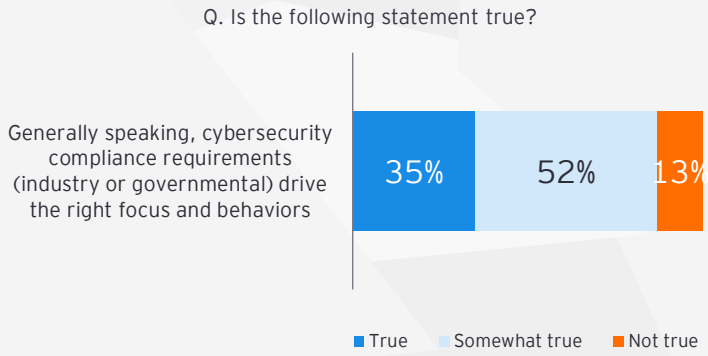


Satisfaction with performance and delivery
- Feedback loops from the business and key stakeholders
- Escalation paths when adjustments and attention is needed
- Recognition for exceptional performance and service

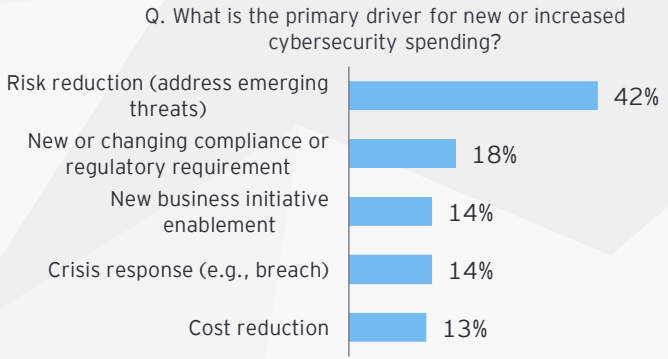
3 key current cybersecurity challenges
Challenge 2: Regulatory fragmentation is a growing headache for CISOs

The **global compliance environment is becoming more complex**, with regimes operating at regional and national levels. **Organizations in certain sectors must also manage industry-specific regulation**. Regulation is claiming time that CISOs do not have to give.

In 2020, **46%** of respondents said **compliance drove the right behaviors**; 5% said this was not true. Their assessment has become **more negative over the year.**

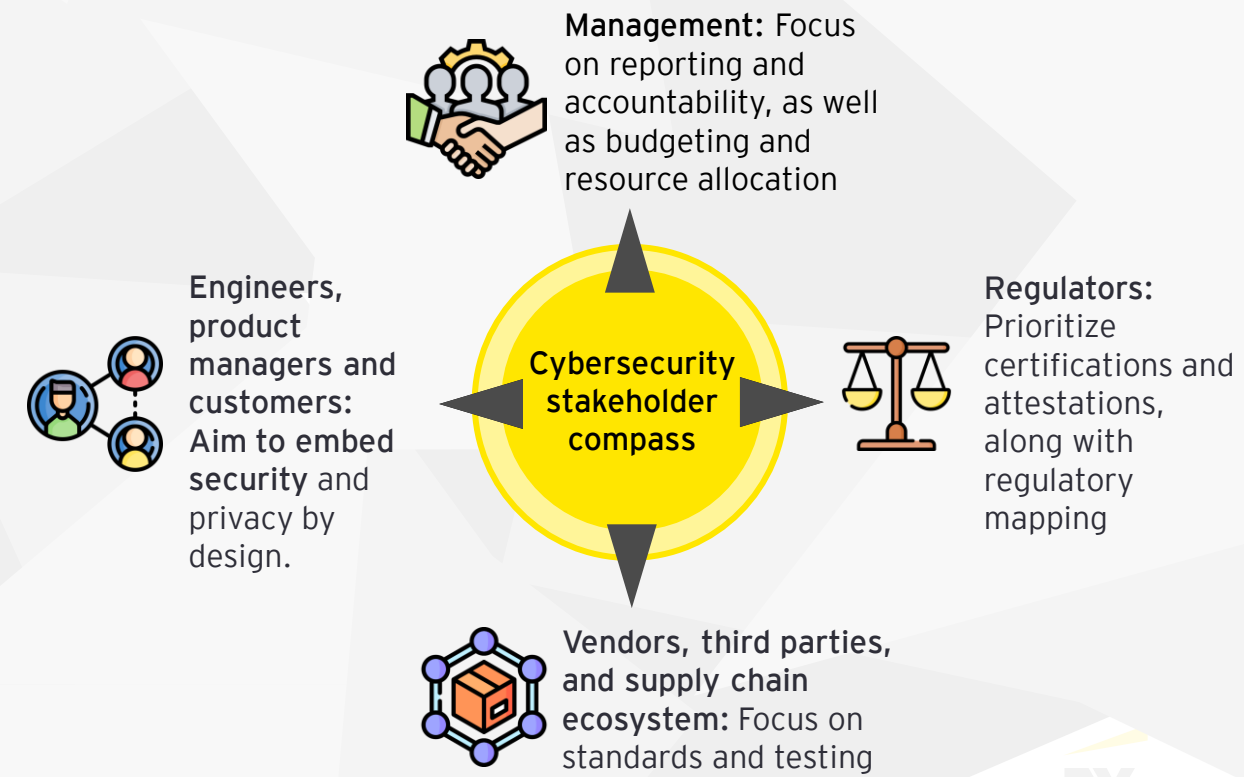


In 2020, **29%** described **regulation** as a **primary driver** of **increased spending**. It has since **fallen to 18%.**



Steps to address the issue:
Understand where compliance sits on a stakeholder compass

CISOs are familiar with the principle of "shifting left," striving to involve cybersecurity earlier on in transformation. Today, they need to understand how to navigate **four key stakeholder** groups.

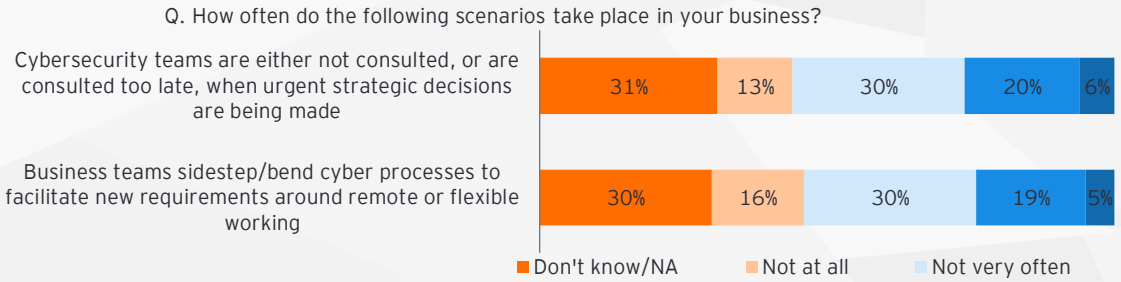


3 key current cybersecurity challenges

Challenge 3: Cybersecurity's relationships are deteriorating – when healthy relationships are needed the most

CISOs need to provide counsel at the earliest stages of decision-making. But **the relationships** between cybersecurity and other functions **lack positivity and strength**.

1 **Cybersecurity teams are not always consulted**, some say business teams sidestepping cyber processes. Even if it happens infrequently, **it represents a significant risk**.



2 **Communication is a growing problem**, though the **business recognizes core strengths**

3 Only **19%** of organizations **include cybersecurity in the design phase** of any digital transformation program

> "...CISOs still have more work to do in **communication barriers** by **talking in less technical language** for boards **to better understand potential business risks.**
>
> –Darren Kane, CSO at NBN Co Australia

Steps to address the issue:

Review your talent profile, but don't expect the impossible

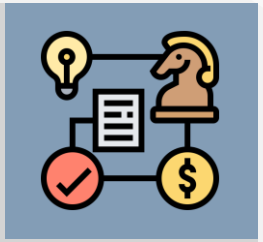
Here we outline some of the many cybersecurity executive profiles that have emerged in recent years. **The best approach is to build a team that balances a combination of broad disciplines, with the understanding that each has its own strengths and weaknesses.**

Cybersecurity executive profile	Area of focus	Strengths	Weaknesses
Security expert	All things security	Deep subject-matter expertise	Lack of business acumen
Tech advocate	Technology solutions and tools	Technology oriented	Siloed thinking
Risk and regulatory pros	Risk, controls, and compliance	Good for highly regulated sectors	Lack of technology acumen
Business transplants	Business integration	Business connectivity	Lack of technology and security acumen
Part-timers & job-splitters	Split between cybersecurity and other primary roles	Cost saving	"Jack of all trades, master of none"

Section 3: Action to be taken?

EY's findings suggest that CISOs should consider **three core actions** to strengthen their position within the business.

1 *Reassess your alignment with the business*



Focus attention on the elements of cybersecurity where many have been weaker in the past

- **a** *Strengthen engagement with stakeholders*
- **b** *Ensure alignment to core business goals*
- **c** *Assess business partners' satisfaction*

Cybersecurity teams have traditionally been strongest when it comes to **assessing their capabilities, identifying risk, and building roadmaps for the future.**

2 *Adopt a new stakeholder compass*

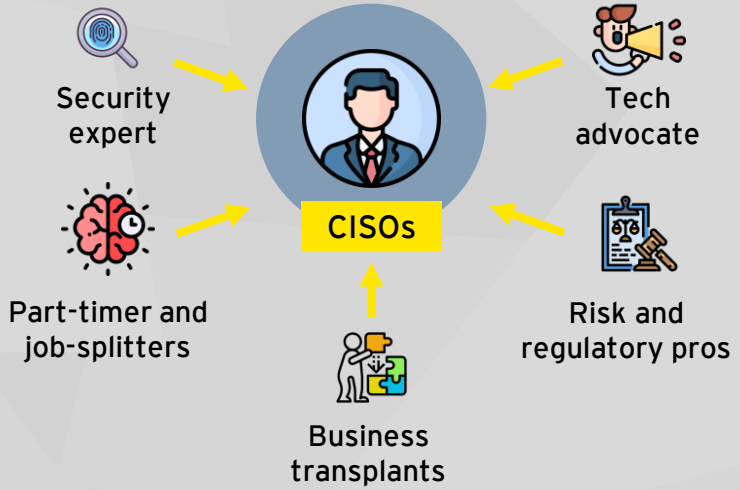
CISOs need to navigate to the four key stakeholder groups

Shifting	Meaning
North	Reporting, accountability, budgeting and resource allocation
East	Certifications, attestations, and regulatory mapping
South	Enhancement of standards and testing
West	Security and privacy by design along with certification and continuous testing

Positioning in the center of these four vital stakeholders, CISOs will be in the right place to take their function to the **next level of strategic influence.**

3 *Review your talent profile*

Responding the organizational challenges, CISOs need the support of versatile, multi-skilled professionals



There is no such thing as a **standard cybersecurity** profile. CISOs need individuals with advanced technical skills.

EY | Assurance | Tax | Transactions | Consulting

About EY
EY is a global leader in assurance, tax, transaction and consulting 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. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

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/id