BELA South Asia Virtual Roundtable

Hosted by Hindustan Coca-Cola Beverages

December 10, 2020

BUSINESS ETHICS LEADERSHIP ALLIANCE SOUTH ASIA

To preserve the integrity and authenticity of discussions held during our BELA South Asia roundtables, we always observe Chatham House Rules of confidentiality, which by virtue of this message, extends to the contents of this recap. We ask that each attendee and recipient of this message respect the privacy of fellow members of the BELA South Asia community. This document is not intended for distribution beyond those to whom it has been sent by Ethisphere.

Participating Organizations

- 3M Company
- Accenture
- Allstate
- Bayer
- Biocon Biologics
- Capgemini
- Cummins
- Diageo
- Dr. Reddy’s
- Dell
- EY
- Genpact
- GE
- Infosys
- JLL
- Mahindra
- Nissan Motor Corporation
- Nokia
- TATA Steel
- The Coca-Cola Company
- Uber
- Virgin Australia Group
- Western Digital Corp
- Zimmer Biomet

BUSINESS ETHICS LEADERSHIP ALLIANCE SOUTH ASIA

Thursday, December 10th, 2020

Roundtable Agenda

THANK YOU TO OUR HOST

HCCB HINDUSTAN COCA-COLA BEVERAGES PVT. LTD.

Coca-Cola

THANK YOU TO OUR PRESENTERS

Infosys Navigate your next

Biocon

EY Building a better working world

Opening Remarks | Preeti Balwani, General Counsel and Local Ethics Officer (LEO) of Hindustan Coca Cola Beverages

Topic 1 | The Ethical Aspects of Data Privacy
This session took a closer look at data privacy relating to contact tracing apps, personal data protection and the use of personal devices. Session leaders discussed the impact of India's data privacy legislation in 2021 and what companies should be prepared to address.

Topic Lead: Preeti Balwani, General Counsel and Local Ethics Officer (LEO) of **Hindustan Coca-Cola Beverages**; and Yogesh Goel serves as Vice President, Group Head Ethics & Compliance at **Infosys**

Topic 2 | Managing data breaches and reputational risk in a pandemic
COVID-19 has increased data security risks as the shift to employees working remotely provides significant opportunities for cybercriminals to target unwitting employees who are not prepared to handle sensitive data securely. According to EY's 2020 Integrity Report, cyber-attacks and ransomware (36%) and pandemics are perceived as the greatest risks to the long-term success of organizations. In this session, leaders approached this topic from a compliance and technology perspective and explored how companies are effectively preparing and managing this growing risk from a compliance and technology perspectives.

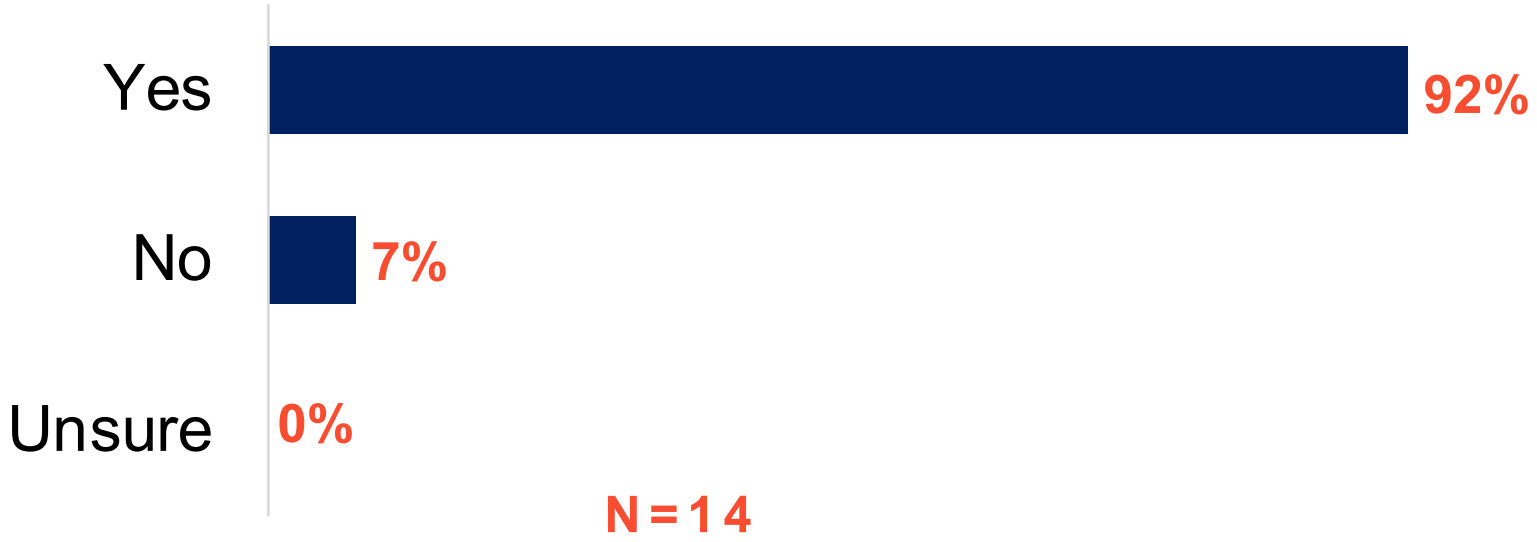
Topic Leads: Arpinder Singh, Partner, **EY India and Emerging Markets Leader, Forensic & Integrity Services;** and Karthik Kannappan Saravanan, AVP Legal, Deputy General Counsel and Global Head of Ethics and Compliance, **Biocon Biologics**

Topic 1 | The Ethical Aspects of Data Privacy

Preeti Balwani
General Counsel and Local Ethics Officer (LEO),
Hindustan Coca-Cola Beverages

Yogesh Goel
Vice President, Group Head Ethics & Compliance,
Infosys

Polling Results: Do organizations in India have robust cyber, data protection and privacy policies? (Single Choice)



Discussion Notes

More on this topic on the BELA South Asia Member Hub

- This year has seen a rapid increase of use of technology across the world. With a significant population of the workforce moving to working from home for the foreseeable future.

- Reopening does not seem to be an easy process and perhaps we may never be the same as we were in “pre-COVID” times, something that we now refer to as the “New Normal”.

- Today, it is of utmost importance that employers be mindful of protecting the data privacy of their employees and business contacts. The principles enshrined in several international and national instruments including Convention 108+ can only be derogated or restricted in a lawful manner.

- The good news is that data protection principles have the flexibility and allow the balancing of interests in different situations particularly in unprecedented situations like COVID-19. These principles are consistent and very much compatible and reconcilable with other fundamental rights and relevant public interests.

- Enterprises have adopted technology, developed alternate processes, and some have also taken aggressive measures to manage cost and sustain their business.

Discussion Notes

More on this topic on the BELA South Asia Member Hub

- If businesses are required by law to disclose certain data to government or public authorities for public health reasons, they are invited to do so under strict compliance with the law and with a clear understanding to return to “normal” processing (including permanent deletion) once the state of emergency regime is no longer applicable. We expect the government and public authorities to continue with the monitoring to safeguard our society. It is extremely important that businesses take compliance seriously when disclosing such information to government and public authorities.

- Upside: What is the area that provides some optimism in all of this? Technology. Tech will help the industries most affected make a come back in the coming years. Every business is becoming a digital business, industries are looking to digitize their services, this is a great opportunity for tech to come together and help other areas in need.

- Technology is giving us the chance to experiment new ways of doing things. Our definition of systems are data, application, cloud, network and architecture

Discussion Notes

More on this topic on the BELA South Asia Member Hub

- Organizations should think about ways to eliminate bias when handling algorithms and personal data. In this new CoVID (and soon to be post- CoVID) setting this information can be easily compromised

- Data protection laws are expanding around the world and this is something companies need to brace for, especially in India as how personal data is handled by companies and the government will be in the limelight for sometime.

- The notion of informational privacy has become salient in the past decade; although India has privacy jurisprudence going back several decades.

- The impending Personal Data Protection Bill aims to protect the informational privacy of individuals by creating a preventive framework that regulates how businesses collect and use personal data, as opposed to protecting informational privacy with a view to the consequent harms caused by the violation of such privacy. In doing so, it focuses primarily on regulating practices related to the use of data.

- Challenge: Everyone is making cuts to stay afloat. There are more redundancies, terminations, etc. The trends across Asia suggest that, for example, employees responsible for data privacy and protection are no longer at those companies and neither have those responsibilities been re-assigned.

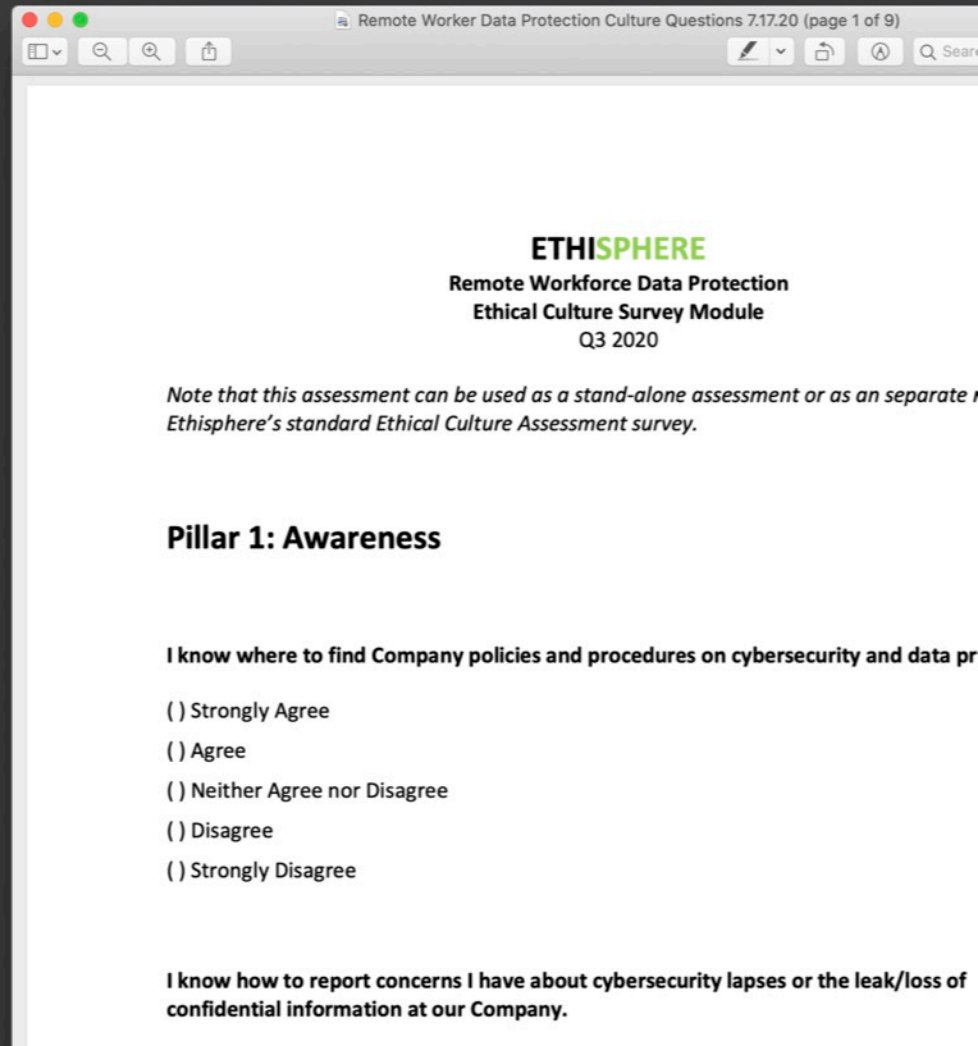
Discussion Notes

More on this topic on the BELA South Asia Member Hub

- It has been argued that the new Bill may pose consequences for innovation in the Indian economy
- Data: According to the recent 2020-2021 BELA South Asia survey, “The Impact of Remote Work on Compliance in India”, about the majority of respondents have reported that they feel comfortable with accessing policies and following it remotely, there’s about 25% that still feel the need to work around cyber controls to get the job done.
    - Participants revealed that laptops and smart phones are the main devices used, even though 100% of respondents said they received laptops or company devices, we still have 36% using a personal laptop, 40% using a smartphone due to comfort and convenience. If for example a platform is disabled or blacklisted like Zoom, employees will turn to a personal device in order to access this platform for their call.
    - As it relates to remote investigations, data collection and protection remain high priorities (68%)
    - Data-enabled actionable compliance: 53% use red flag alerts, which are part of data protection, and it seems that it is being used to track the movement of data and confidential info

Introducing the Remote Worker Data Protection Culture Module

- Has your newly-distributed workforce put your data at risk?
- Module available to current clients
- 20 questions
- Built to run as a stand-alone assessment OR module to standard ethical culture survey


Remote Worker Data Protection Culture Questions 7.17.20 (page 1 of 9)

ETHISPHERE

Remote Workforce Data Protection
Ethical Culture Survey Module
Q3 2020

Note that this assessment can be used as a stand-alone assessment or as an separate
Ethisphere's standard Ethical Culture Assessment survey.

Pillar 1: Awareness

I know where to find Company policies and procedures on cybersecurity and data pr

( ) Strongly Agree
( ) Agree
( ) Neither Agree nor Disagree
( ) Disagree
( ) Strongly Disagree

I know how to report concerns I have about cybersecurity lapses or the leak/loss of confidential information at our Company.

Remote Workforce Data Protection Culture Assessment Handout

Ethisphere's Eight Pillars of Ethical Culture

Ethisphere's Eight Pillars of Ethical Culture provide quantitative measurements into employee's awareness of where to go with concerns, level of comfort in speaking up, and to what extent they feel supported throughout the organization.

Pillar 1: Awareness of Program & Resources

Familiarity with the assets and efforts of the compliance and ethics function.

7 Questions

Pillar 2: Perceptions of the Function

Perceptions of the assets and efforts of the compliance and ethics function.

5 Questions

Pillar 3: Observing & Reporting Misconduct

Comfort in reporting misconduct, the reason for doing so, and potential reporting barriers.

22 Questions

Pillar 4: Pressure

Strength and source of pressure experienced to compromise standards to hit goals.

3 Questions

Pillar 5: Organizational Justice

Whether the company holds wrongdoers accountable and the awareness of discipline.

3 Questions

Pillar 6: Supervisor Perceptions

Supervisor's conduct and communication; comfort approaching with concerns.

5 Questions

Pillar 7: Perceptions of Leadership

Perceptions of the conduct, values, and communications of senior leadership.

2 Questions

Pillar 8: Perceptions of Peers & Environment

Whether employees and their peers feel personally responsible for the Company's ethics.

3 Questions

Setting the Stage: Ethisphere's Ethical Culture Benchmark Data

1 million+
Responses Received

90
Companies Around the World

>5 million
Represented Headcount

***Figures as of 11/15/20.**

Notes and Suggested BELA Resources

- **2020 South Asia Ethics Summit Video Replay**: BELA South Asia Community Survey: Preliminary findings of the impact of remote working on compliance in India – discussion led by Erica Salmon Byrne, EVP and Chair, BELA: https://bela.ethisphere.com/resource/saes-2020-remote-work-day2/

- **Improving Cybersecurity for Remote Workers**: Ethisphere, a champion of The Cyber Readiness Institute, shares CRI's Cloud FAQ: Improving Cybersecurity for Remote Workers.
    - This FAQ is designed to help senior management of small and mid-sized enterprises (SMEs) become familiar with cloud terminology and understand the basics of how the cloud can improve cybersecurity for your remote workforce: https://bela.ethisphere.com/resource/cri-cloud-faq/

- **Policy on Messaging Apps and Ephemeral Communications**: Shared by a BELA member, this is an anonymized version of a policy on the use of text messaging and other ephemeral communications technology for business communications: https://bela.ethisphere.com/resource/policy-ephemeral-comms/

- **2020 BELA South Asia Roundtable Recap, hosted by Accenture**: The impact of the pandemic on technology and data privacy: https://bela.ethisphere.com/resource/bela-south-asia-virtual-roundtable/
- **2020 BELA South Asia Magazine**: Appropriately themed, "India's Unified Force During an Era of Disruption" explores how leaders across the country tackle issues such as employee health and safety, data protection, policy management and the transition to a remote work setting, while dealing with one of the world's largest lockdowns: https://bela.ethisphere.com/2020-bela-south-asia-magazine/

Topic 2 | Managing data breaches and reputational risk in a pandemic

EY
Building a better working world

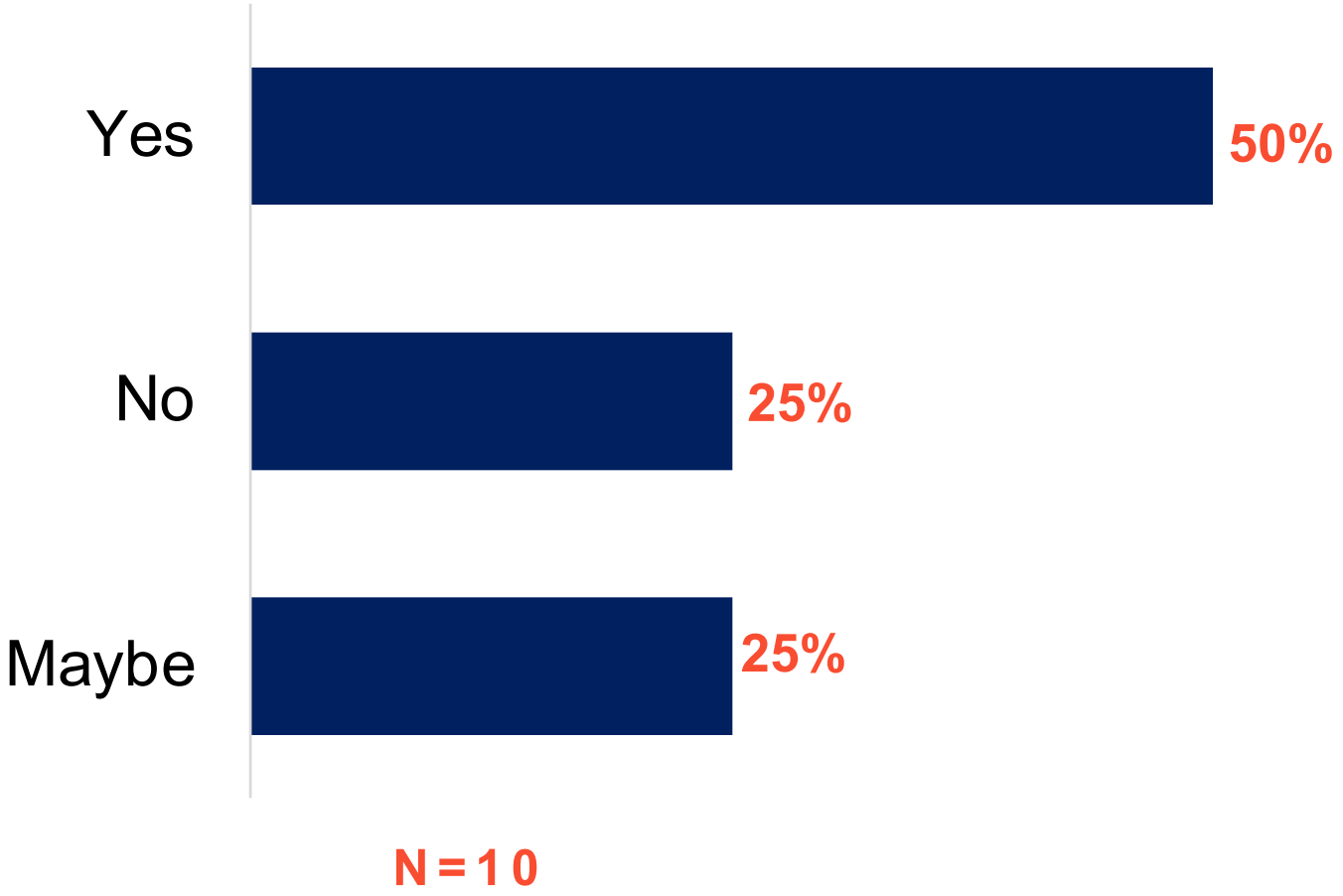
Biocon

BUSINESS ETHICS LEADERSHIP ALLIANCE SOUTH ASIA

Arpinder Singh
Partner,
EY India and Emerging Markets Leader,
Forensic & Integrity Services

Karthik Kannappan Saravanan
AVP Legal, Deputy General Counsel and
Global Head of Ethics and Compliance
Biocon Biologics

Polling Results: Do you believe cybersecurity is a priority for organizations' top management? (Single Choice)



Discussion Notes

The full presentation is available on the BELA South Asia Member Hub

- 6.4 billion is the number of fake emails sent worldwide-every day
- India ranked 3rd most vulnerable country in terms of risk of cyber threats in 2017
- India tops globally with the highest number of detected spam-bot
- 80% of cyber breach incidents resulted in the exposure of customers' personally identifiable information (PII)
- Subtle signs of cyber attacks:
    - Theft of IP – similar new product launched by competitor
    - Mergers & Acquisitions (M&A) activities disrupted
    - Operational disruption, without a clear cause
    - Operational disruption, without a clear cause
    - Unexpected share price movement
    - Oddities in payment processing or ordering systems

Discussion Notes

The full presentation is available on the BELA South Asia Member Hub

EY is hearing from clients that they are quickly adapting to the uncertainty by:

- Conducting rapid risk assessments and reprioritizing cybersecurity projects
- Leveraging third parties to provide staff augmentation and subject matter resources for emerging cyber risk areas
- Pre-installing and configuring laptops, tablets and encrypted drives for employees to use while working from home
- Developing simple teleworking policies and procedures and well as rolling out virtual security awareness training for employees new to teleworking.
- Redeploying cyber personnel to man round the clock help desk support, enabling teleworkers with technology support and expertise on subjects like VPN use or securing personal devices.
- Review data breach insurance and similar policies for coverages and exposures.
- Ensure an adequate bench exists to manage cyber incidents

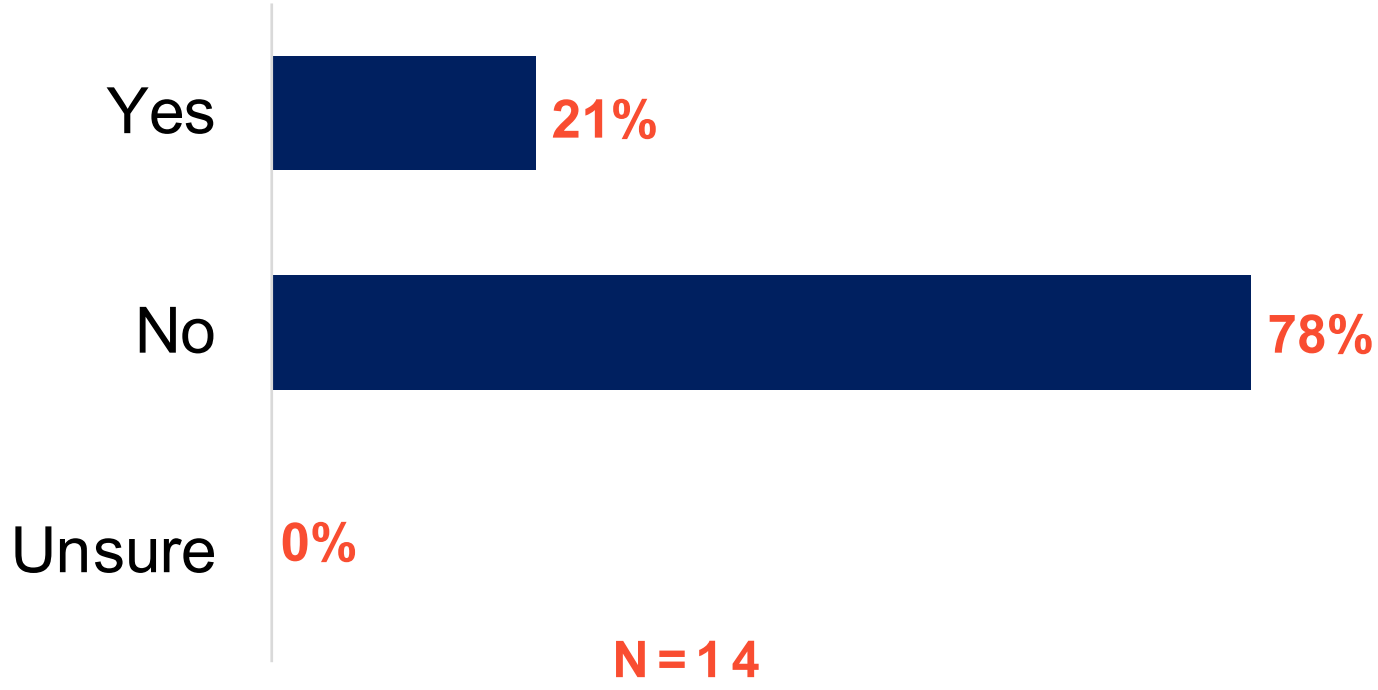
Discussion Notes

The full presentation is available on the BELA South Asia Member Hub

The Biggest impact of COVID 19 – Recognizing the elephant in the room:

- Current state of IT, and how companies are managing in the post COVID world and how managing in new environment with the risk and control owners remote and distracted their own business priorities.
- In a recent (April 2020) study undertaken by Risk management Society (RIMS) that surveyed 200+ risk professional on question that is considered as biggest impact of COVID 19, 49% of the responded stated “Mobilizing a remote workforce”.
- It is worth noting that, this is highest percentage followed by other impacts such as Customer demand shock (16%), financial pressure (15%) and supply chain destabilization (14%).
- Managing the remote work force was the No.1 biggest impact.
- It is no surprise, companies had to rapidly take steps to de-centralize their workforce, move employee to other corporate office and everyone had to work from home immediately overnight.
- These unexpected turns of events, immediately put pressure on the IT to have only the hardware, Software and infrastructure to support this massive shift but also the communication and training plan to help employee adopt to their new work environment

Polling Results: Do organizations in India have robust cyber, data protection and privacy policies? (Single Choice)



Discussion Notes

The full presentation is available on the BELA South Asia Member Hub

What Steps Can Companies Take to Avoid a Potential Cyber Attack or Data Breach? Biocon Biologics Explains:

Steps	Description
Executive buy-in	• In order to create an optimal cybersecurity policy, support has to come from the top levels of the organization. • Security must become a core part of the organizational culture
Understand your risk profile	• By knowing your industry and its attack vectors, what is valuable to your organization and how to protect those assets, security personnel can effectively create, support and promote cyber security initiatives
Take threats seriously	• Many organizations understand the full extent of the damage that can be done during an attack as well as the aftermath. • However, many companies choose to ignore the possibility of such an attack happening to them, or they are willing to accept the risk of not taking adequate precautions due to cost or complexity.
Policy enforcement	• Policies can be as simple as a strong password, but should ideally go well beyond passwords. • Security policies should be documented and automated wherever possible to avoid human error or omission. • Circling back to Executive Support, policies should be a part of the culture that everyone chooses to follow. • Keep things in simple terms that non-IT executives and users can understand.

Discussion Notes

The full presentation is available on the BELA South Asia Member Hub

What Steps Can Companies Take to Avoid a Potential Cyber Attack or Data Breach? Biocon Biologics Explains:

Training	• Security awareness and policy enforcement is crucial in order to create a security culture within an organization. Awareness of policies, security and other, should be of paramount concern to all organizations. There should be specialized training for those that deal with the most sensitive data in the company
Employee Screening	• Not all possible employees possess the same moralities as the business owners and stakeholders. • Employees should not only be screened to ensure that their skills meet the requirements of the positions but, more importantly, that their beliefs closely match those of the organization. • Remember that people are often the weakest link in a security chain
Offline backup Of critical data	• Data is the lifeblood of an organization. • Data loss is often as damaging, monetary and brand, to an organization as a data breach. • Many organizations never fully recover from data loss events, some go out of business entirely. • A copy of critical data in a secure offsite location is one small step that should not be overlooked.

Assess, Benchmark and Improve Your Cybersecurity Program

Does your **cybersecurity program** align to top guidance and standards? Here are way to assess the weaknesses and strengths of cybersecurity controls across your company – or that of your third party partners – and implement a road map for improvement: https://ethisphere.com/what-we-do/cybersecurity/

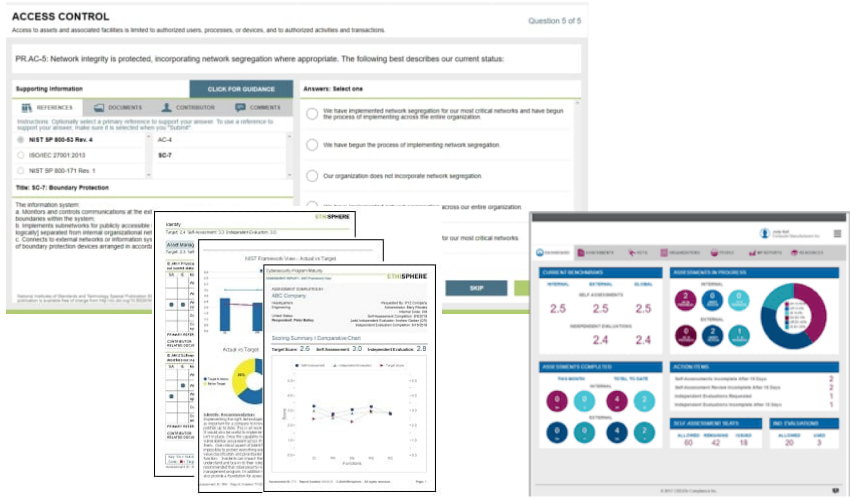
How it works:

Start-up call with our executive SME Craig Moss (about 30 minutes) to discuss our measure and improve approach to reducing compliance risk.

You complete the selected maturity assessment (approximately 45-60 minutes depending on topic) in the secure Ethisphere platform and immediately receive an auto-generated report with your maturity score (0-5 scale). The report also includes a target score showing the desired maturity level and a benchmark score showing the aggregated average score from other companies.

Maturity and risk review call with Craig (30 minutes) to review your self-assessment and discuss the risks your company faces related to the selected risk topic.

- **Priority Improvement Workshop led by Craig** (60-90 minutes). Using our proven change management methodology, Craig will lead a workshop to review your maturity level, identify the most critical risks and discuss your current plans in the area. Craig will work with you to define a quantifiable 6-month improvement goal and identify the milestones needed to achieve the goal. Finally, Ethisphere curate appropriate resources from the BELA Member Hub that can best support your goal.



**Note: Assessments on Anti-corruption and Trade Secret Protection and Confidential Information are also available*

Notes and Suggested BELA Resources

- **LinkedIn: 2020 South Asia Ethics Summit Video Replay**: In this session, Amyn Thawer, Head of Global Compliance & Integrity, **LinkedIn** shared his views on digital transformation and promoting integrity during a time of disruption: https://bela.ethisphere.com/resource/2020-saes-keynote-linkedin/

- **Pfizer: 2020 South Asia Ethics Summit Video Replay:** Sandeep Seth, Director, Corporate Compliance, Pfizer, Nikunj Savaliya, Company Secretary, Bayer CropScience Limited explain how analytics and digital transformation will establish greater compliance effectiveness: https://bela.ethisphere.com/resource/saes-2020-digital-transformation-day1/

- **EY 15th Global Integrity Report 2020** The COVID-19 global pandemic has shocked the world, impacting life for families, communities and organizations on every continent. Amid the turmoil, businesses and governments are faced with new and significant decisions that pose difficult ethical dilemmas https://bela.ethisphere.com/resource/ey-global-integrity/

- **BELA South Asia Webcast Series | EY's Global Integrity Report 2020 – Spotlight on India:** In India, in specific, the disruption caused by the pandemic has impacted businesses across the country. From cybersecurity to data privacy—compounded by a myriad of ethical challenges—India continues to battle the repercussions of the pandemic: https://bela.ethisphere.com/resource/global-integrity-report-2020-webcast/

2021 Upcoming Projects and Working Groups

2021 Cybersecurity and Data Privacy Survey
Launch Date: January 2021

Working Group
- Tripti Roy, Chief Information Security and Data Protection Officer, TATA Steel
- Piya Haldar, Director, Ethics and Compliance, Honeywell
- John Chung, Regional Compliance Counsel, Intel
- Anubhav Kapoor, Group Vice President, Cummins

2021 India Business Case for Compliance

Working Group
- Atul Kumar, Chief Ethics Officer, SBI
- Sandhya Sharma, VP, Corporate Governance, Mahindra
- Sandeep Seth, Director, Corporate Compliance, Pfizer
- Rajeev Chopra, Managing Director, Legal, Accenture

Revised India Supplier Toolkit: June 2021

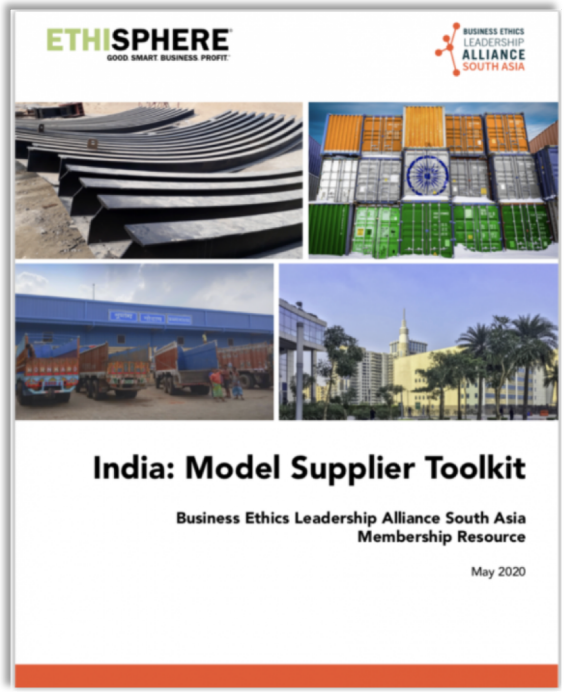
Working Group
- Sujata Nabar, General Manager, Diageo India
  Sheetal Raina, Ethics Advisor, India, The Boeing Company
- Seshadri Govindan, Ethics & Compliance, 3M
- Satyajit Nandi Third Party Compliance, Dun & Bradstreet

2021 BELA South Asia Magazine

Contributors:
- Dell
- Bharti Airtel
- Novartis

Interested in contributing? Reach out to aarti.maharaj@Ethisphere.com

BELA South Asia Resources



India Model Supplier Toolkit

2020 BELA South Asia Magazine

BELA South Asia Panel Sessions

All resources for the BELA South Asia community are available on the member hub here:
https://bela.ethisphere.com/south-asia/

Thank You!

BELA South Asia Contacts:

Aarti Maharaj
Managing Director, BELA South Asia and BELA Asia Pacific
Aarti.Maharaj@Ethisphere.com

Kevin McCormack
Executive Director, BELA
Kevin.McCormack@Ethisphere.com

BUSINESS ETHICS LEADERSHIP ALLIANCE SOUTH ASIA