BCG

THE BOSTON CONSULTING GROUP

Cybersecurity – Beyond just compliance

FIBAC Panel discussion

NOVEMBER, 2017

What do these people have in common?

... are distinguished, experienced executives

Gregg Steinhafel

Target

President and CEO

Atiur Rahman

Bangladesh Bank

Governor

Dido Harting

TalkTalk

CEO

... serve very respectable, well-known companies

What do these people have in common?

... are distinguished, experienced executives

Gregg Steinhafel

Target

President and CEO

Atiur Rahman

Bangladesh Bank

Governor

Dido Harting

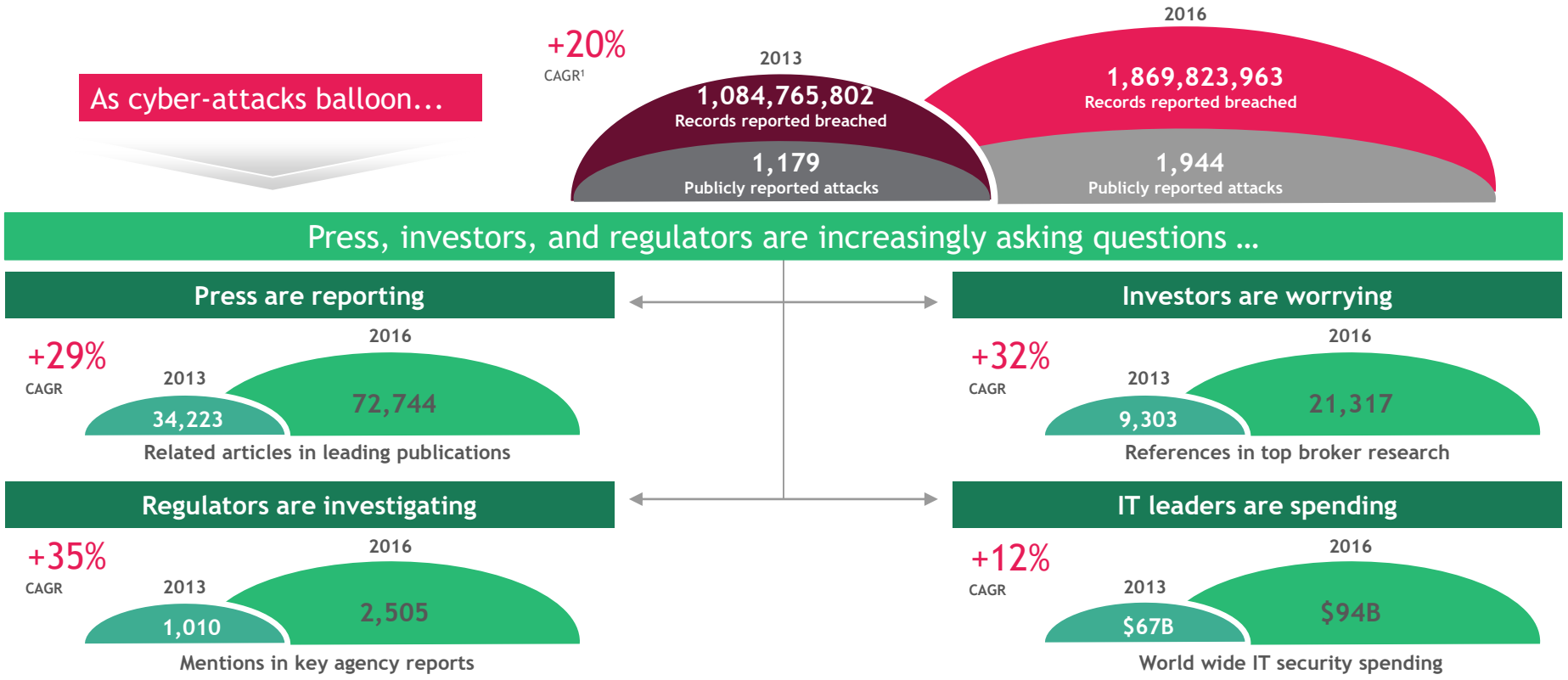
TalkTalk

CEO

... serve very respectable, well-known companies

Had to resign in the aftermath of a cyber attack on their organization

Cyber Security is increasingly top of mind



1. 20% CAGR is for records breached;
Note: Data forecasted through year end 2016. Source: BCG, Nov 2016

It is a CONSTANT war.... with potentially existential threats

Catastrophic Risk

All customer data is deleted … and so are the backups

2014: Code Spaces, a software collaboration platform, is put out of business by an attacker who deleted the company's data and backups

Financial Risk

An (almost) billion-dollar digital bank heist

2016: Cyber criminals use the SWIFT network to steal $101M from Bangladesh Bank, but for a typo, $951M could have been stolen

Reputational Risk

Front page headlines, Fired CEO, $400M in lost sales

2013: Despite heavy cybersecurity investment, hackers breach Target Corp's defenses and steal 40 million credit card numbers

Source: Press reports and BCG analysis

The titanic problem:

Cybersecurity is not just a technology challenge

Typical focus of attention:

Technology

Often neglected but equally important:

Organization

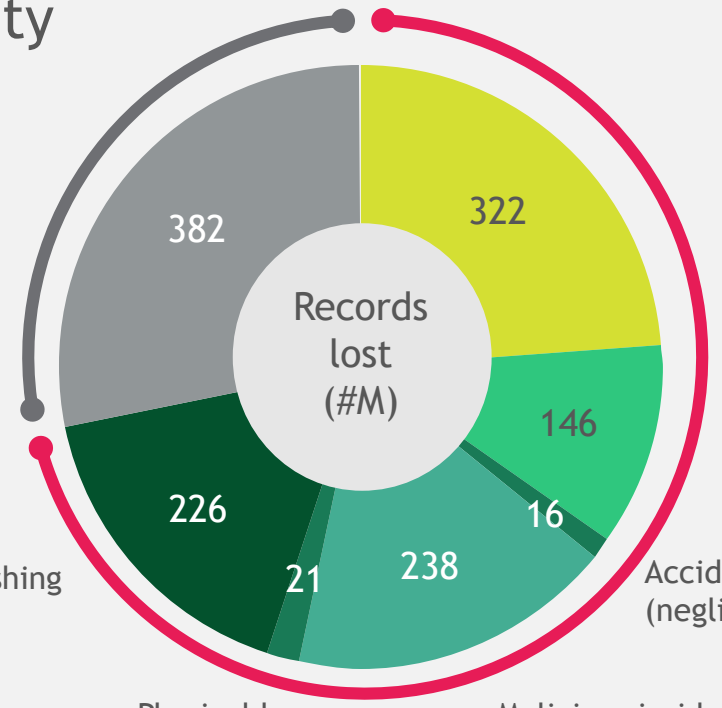
Process

People

The neglected factors differentiate: 72% of breaches are caused by organizational, process, and people failures

Inadequate security Technology
28%

Organizational, process, and people failures
72%



Source: Study of major data breaches: Building a Cyberresilient Organization (BCG Perspectives)

A comprehensive approach to Cybersecurity requires coverage of all three dimensions

Technology

Network monitoring

Intrusion detection capability

Big data/signal mining

Data Leakage Prevention

Lateral movement detection

Advanced Persistent Threat detection

Encryption

Multifactor authentication

Process

Standard & emergency operations processes

Decision & escalation processes

Whistle blowing processes

Identification of information assets

Data classification & access clearance

People/behavioral monitoring

Vendor Mgmt. and monitoring

People/Organization

Organization design

Roles and responsibilities

Substitutes function

Short hierarchies and open communication

Skills

Ownership and empowerment

Development and reviews

Talent identification

"Defense-in-depth" covers all these elements -- internally and at the perimeter

Source: BCG

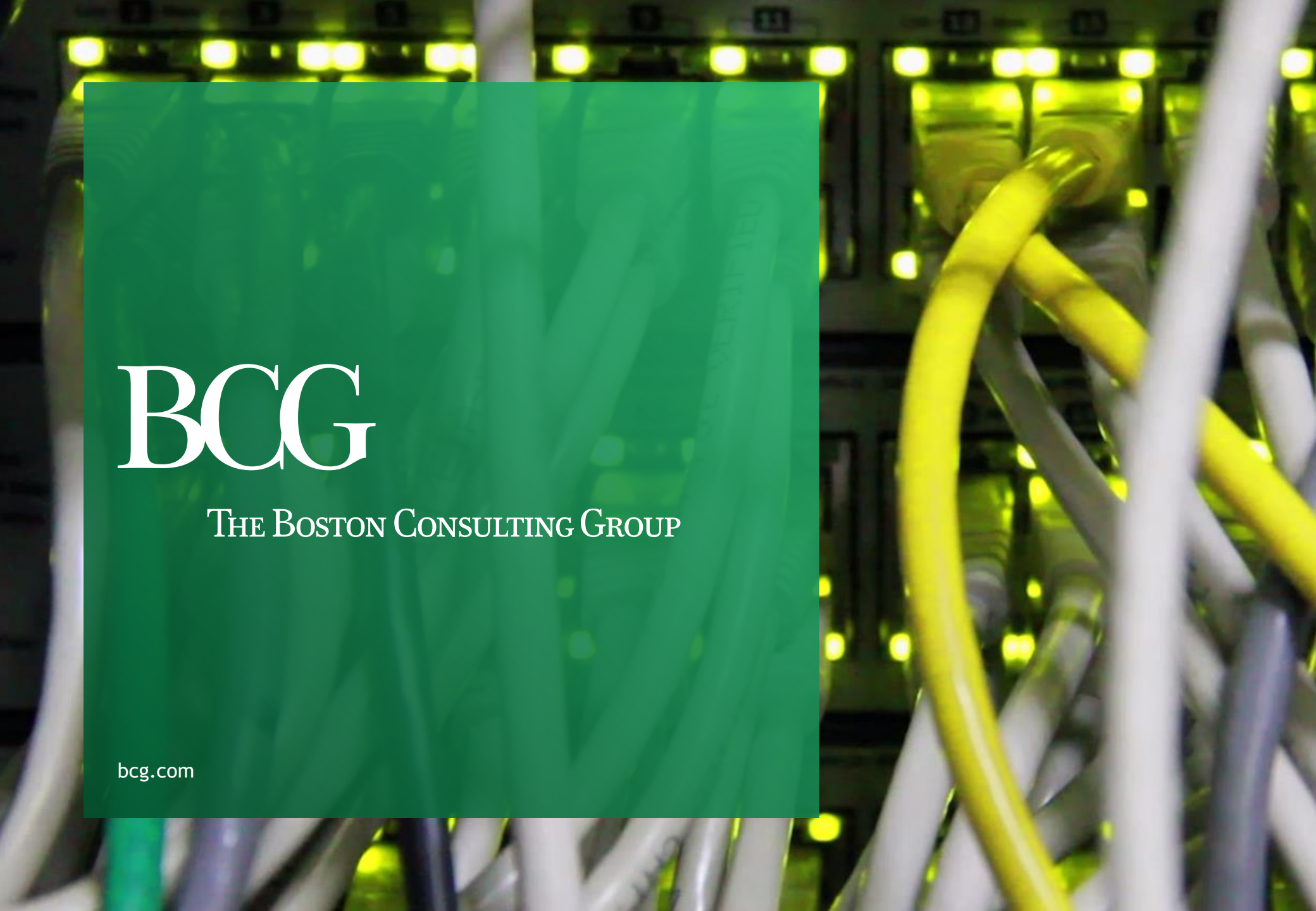
Key questions for our discussion today

What are the **biggest challenges** faced regarding Cybersecurity for Indian banks today?

How prepared are we for these threats? What **measures have already been taken**?

Is it enough? What are the **gaps that still remain**? How do we move to implementation beyond just compliance?

What should be the **action agenda going forward** – on technology, process, people..?


BCG
THE BOSTON CONSULTING GROUP
bcg.com