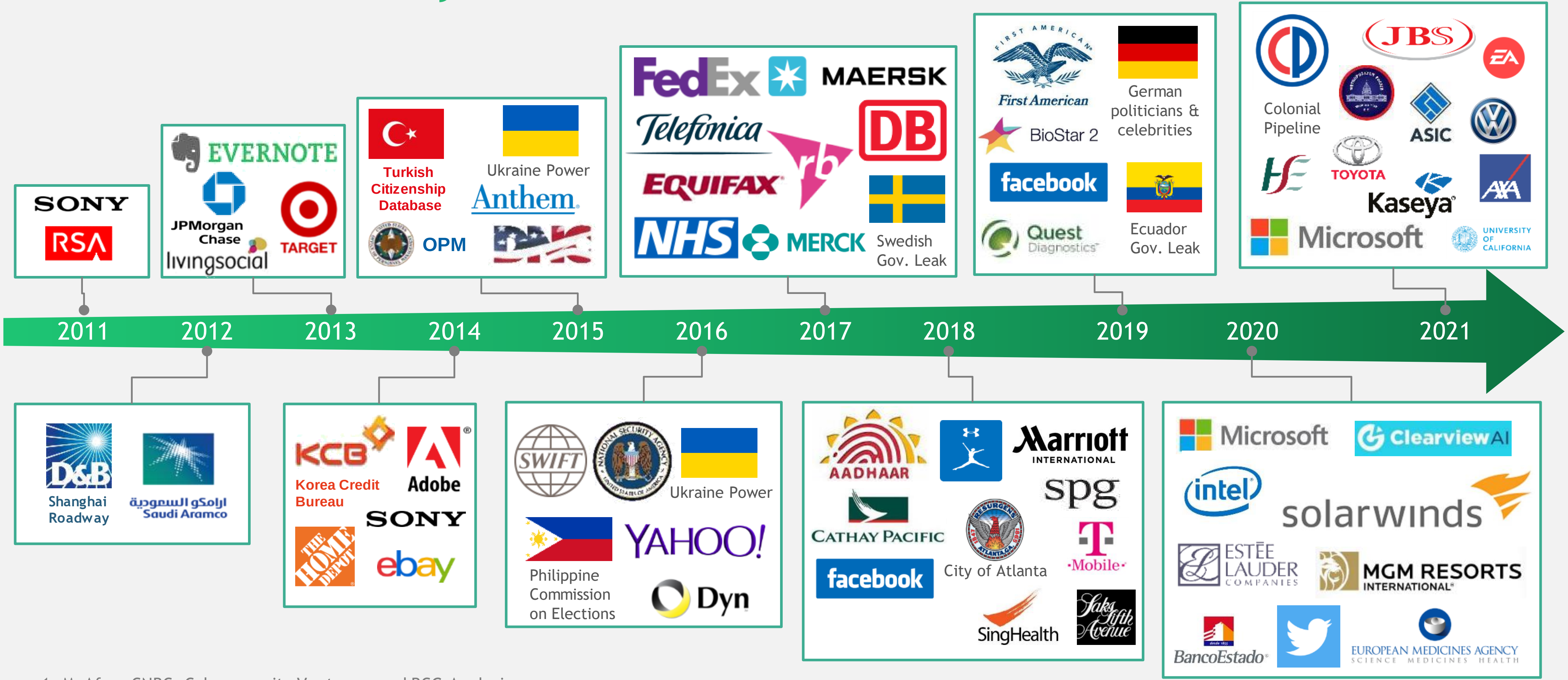
BOSTON CONSULTING GROUP

Cyber Fusion: *Preparing for digital attacks, frauds, and upcoming demands of personal data protection*

A FIBAC : Cyber Think Tank Panel

NOV 2022

The challenge is real: Global cost of cybercrime rose from $445B in 2015 to $2T+ today[1]



2011

2012

Shanghai Roadway

2013

2014

Korea Credit Bureau

2015

Turkish Citizenship Database

Ukraine Power

2016

Ukraine Power

Philippine Commission on Elections

2017

Swedish Gov. Leak

2018

City of Atlanta

2019

German politicians & celebrities

BioStar 2

Ecuador Gov. Leak

2020

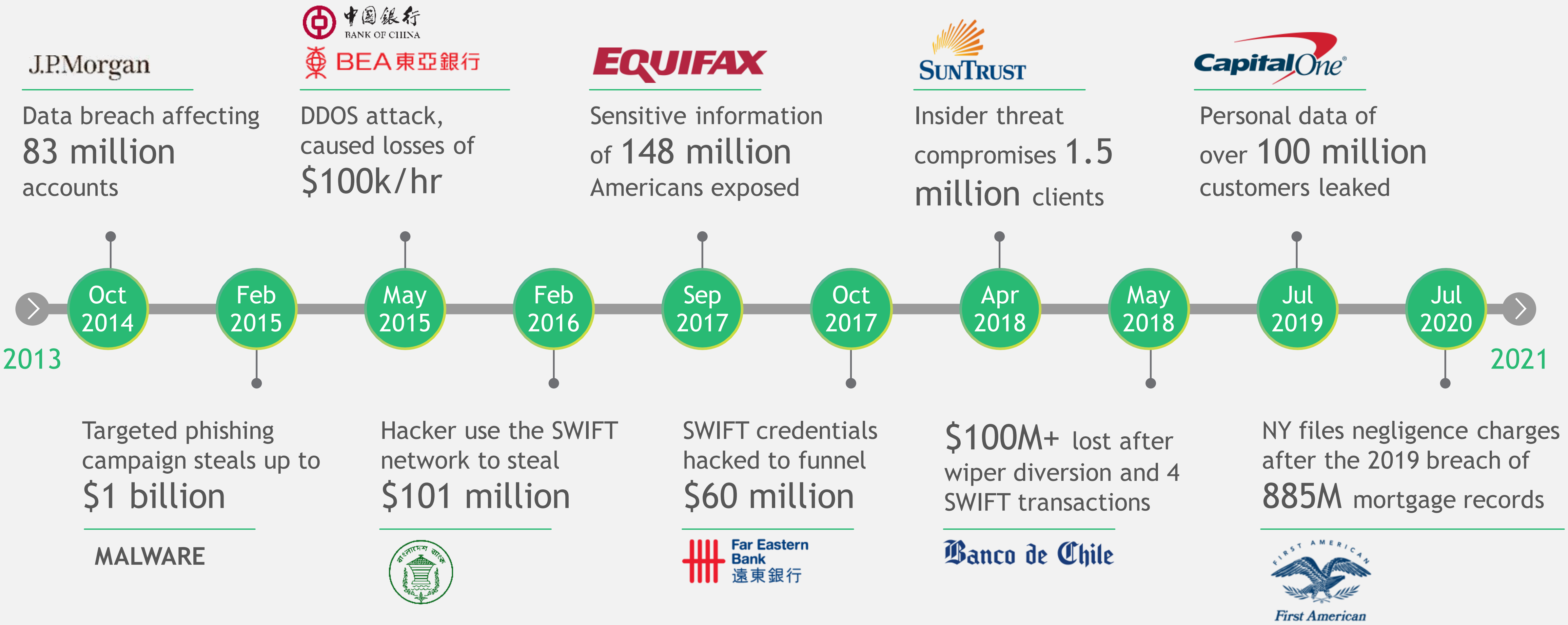
2021

Colonial Pipeline

[1] McAfee, CNBC, Cybersecurity Ventures, and BCG Analysis

Source: Press reports and BCG Analysis

The financial damage is real: Cybersecurity and IT risk Mgmt. issues are estimated to be costing FIs $50B+ per year[1]



2013

Oct 2014 — J.P.Morgan
Data breach affecting 83 million accounts

Feb 2015 — MALWARE
Targeted phishing campaign steals up to $1 billion

May 2015 — 中国银行 BANK OF CHINA / BEA 東亞銀行
DDOS attack, caused losses of $100k/hr

Feb 2016
Hacker use the SWIFT network to steal $101 million

Sep 2017 — EQUIFAX
Sensitive information of 148 million Americans exposed

Oct 2017 — Far Eastern Bank 遠東銀行
SWIFT credentials hacked to funnel $60 million

Apr 2018 — SunTrust
Insider threat compromises 1.5 million clients

May 2018 — Banco de Chile
$100M+ lost after wiper diversion and 4 SWIFT transactions

Jul 2019 — Capital One
Personal data of over 100 million customers leaked

Jul 2020 — First American
NY files negligence charges after the 2019 breach of 885M mortgage records

2021

[1] Ponemon Cost of Cyber Crime Study, The Banker, BCG research and analysis
Source: Press reports and BCG analysis

Cyber attacks are hitting hard – Industrial goods and manufacturing sector are also not spared

Auto parts maker Denso targeted in ransomware cyberattack

Meat giant JBS pays $11m in ransom to resolve cyber-attack

Chemical distributor pays $4.4 million to DarkSide ransomware

Ransomware Attack Shuts Down A Top U.S. Gasoline Pipeline

Aluminum maker Hydro battles to contain ransomware attack

Chinese intelligence officers charged in US aviation hacking

Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks

Cyber-attack that crippled NHS systems hits Nissan car factory in Sunderland and Renault in France

As of 4 February 2022

As IoT-enabled products become more common…

… impact of cyber security issues is expanding to physical and safety

- Integrated sensors/actuators in lab/LIMS and processing equipment allow collection/ adjustment of real-time operations data
- Edge and Fog computing technology addresses limitations of the cloud (e.g., latency etc.)
- Cloud technology enables remote control, and central storage of information
- Remote operation center does the controlling, monitoring and analytics

- Sabotaged operations by hacking and taking over the operations (e.g., process intervention) or performing a denial-of-service attack
- Reputational damage by deteriorating product quality/HSE implications

IoT-related risks need to be carefully managed

57%

of IoT devices are vulnerable to medium- or high-severity attacks

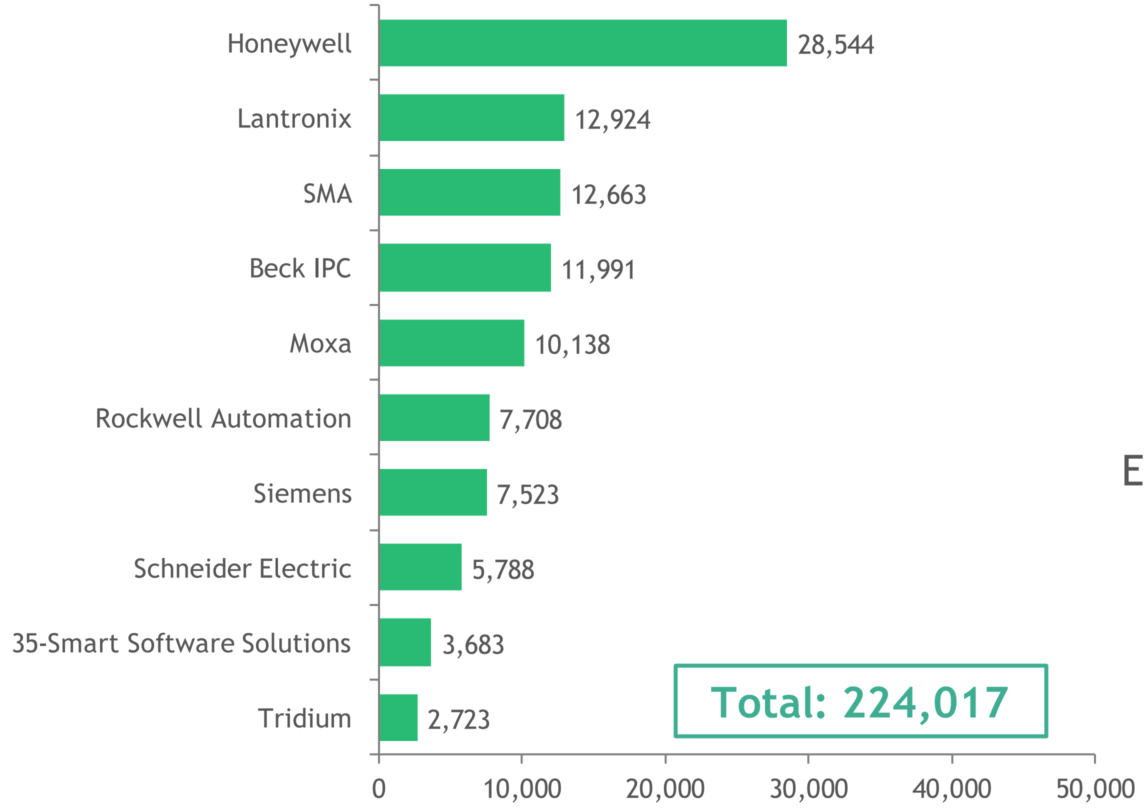
98%

of all IoT devices are unencrypted, exposing confidential data to the network

Source: Unit 42, 2020

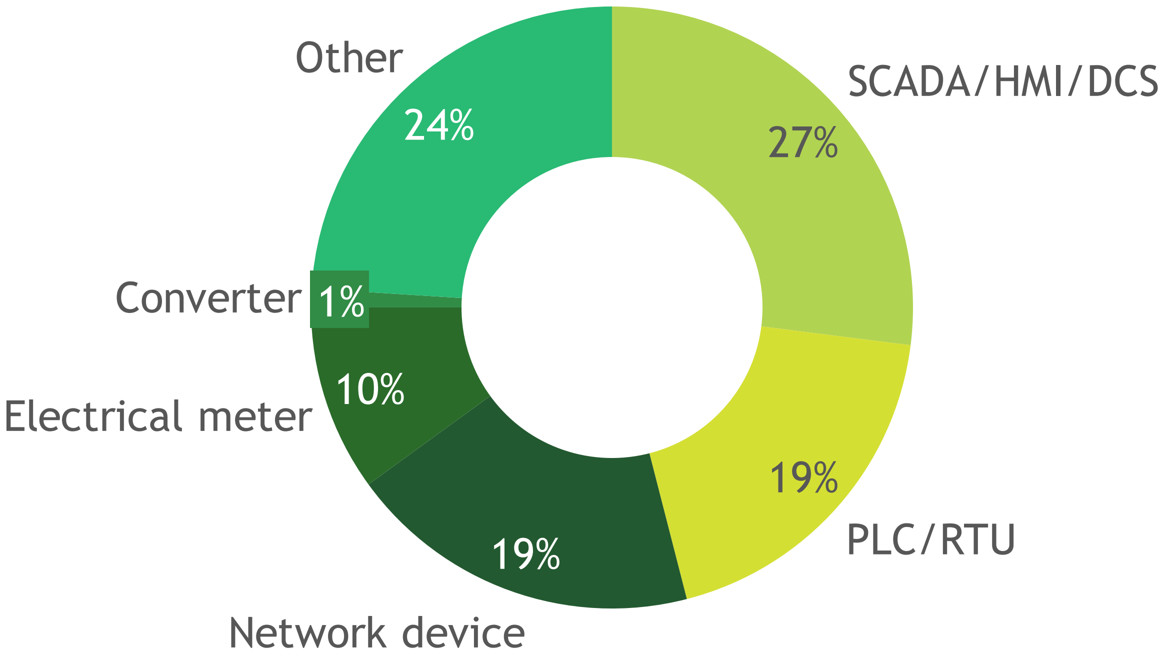
Over 220,000 internet accessible OT systems were visible to public search engines (60% CAGR 2011-18)

Internet accessible ICS components by vendor



Total: 224,017

Internet accessible ICS components by type



Search engines used: Shodan, Google, Censys
Source: Positive Technologies Security. ICS vulnerabilities: 2018 in review, April 11, 2019

Attacks can come from multiple types of actors with differing objectives

External attackers

Cyber criminals
(Black hat)

Criminal orgs that sabotage company operations & steal data for commercial gain

Looking for the easiest way to steal something of value

Hackers
(White or grey hat)

Individuals/orgs that uncover weaknesses in systems & products in the hopes that companies will deal with them

Good intentions

Hacktivists

Individuals/orgs that attack companies for political or ideological reasons

Attack areas that can disrupt or embarrass the target

Nation States

Developers of advanced "cyber weapons"

May include corporate espionage to gain an advantage for domestic companies

Terrorists

Organizations wanting to spread fear

Currently low sophistication, but may purchase services from professional hackers

Internal actors

Intentional

Disgruntled employees/ individuals seeking revenge, financial gains or blackmailed by criminal orgs by leaking sensitive information to the press or competitor

Involuntary

Employees accidentally leaking sensitive information, being susceptible to social engineering and phishing attempts

Source: IBM 2015 cyber security intelligence index

FI Institutes : Landscape for cyber has shifted – From Reactive to Proactive & pre-emptive using new gen technology

Cyber Fusion Concept

Prediction: Risk Analysis using AI/ML/NLP Enabled

New hyper-converged business models require advanced defense mechanisms using Cyber-tech :

- Fused multi-channel threat view
- Attacker-centric proactive approach (Behavioral analytics)
- Automated intelligence gathering and forensics
- Fraud Analytics & Threat Intelligence using AI / ML
- Automated Remediation
- Security by design (Shift left approach - DevSecOps)

Recovery & Response: The Build Approach

Automated & integrated preventive systems to be built for detection, prevention & Recovery

IP Entry Protocols
(OnPrem, Co-Lo, Cloud, 3rd Party)

Network, Firewall, Ports , Server Farm

Application log, access controls, events, tokens

Cyber Data Aggregation & Metadata Management

Analytics & MLP for fraud, Risk, threat

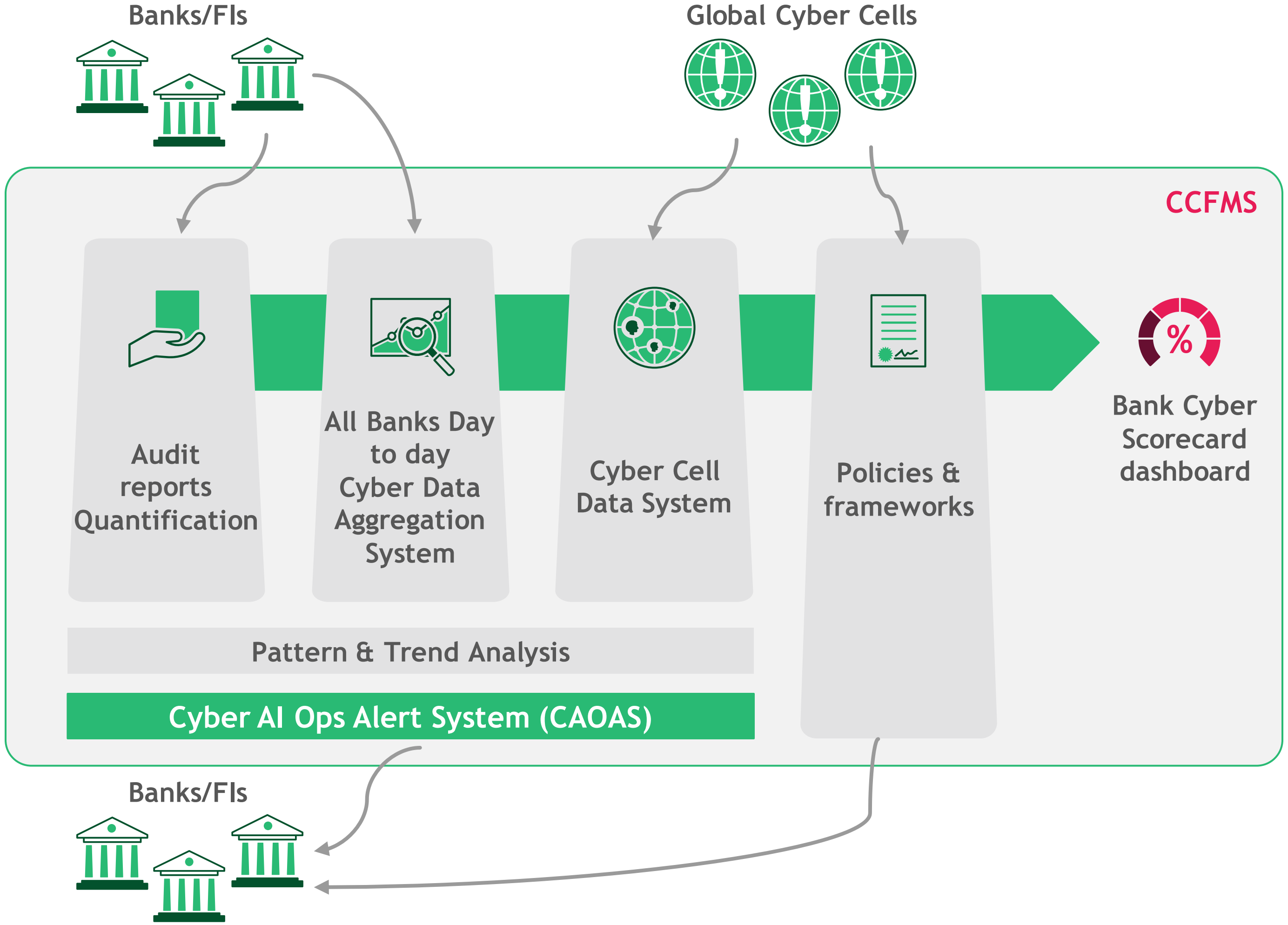
Proactive Alerts & Monitoring

Prevention & Detection: AI Enabled SOC Center

Preventive & pre-emptive alerts to be designed using AI Ops model

- Threat mapping
- Deception
- War Gaming & Game theory
- Smart False positive reduction intelligence
- X-tended detection & response
- Network detection & response
- Endpoint detection & response
- Fraud analytics

Country Level - Centralized Cyber Fusion Management System (CCFMS) – Envisioning Panopticon Model


Banks/FIs
Global Cyber Cells
CCFMS
Audit reports Quantification
All Banks Day to day Cyber Data Aggregation System
Cyber Cell Data System
Policies & frameworks
Bank Cyber Scorecard dashboard
%
Pattern & Trend Analysis
Cyber AI Ops Alert System (CAOAS)
Banks/FIs

How this works (A Cyber Panopticon Model) :

- Centralized system (CCFMS) at **country level** managed by **central authority**
- **All banks**, cyber data integrated at CCFMS
- CCFMS integrated with **adjoining countries central cyber cells** & aggregates data proactively
- Collected data used for **preventive analytics using MLP**
- CCFMS is **powered by AI / ML** capabilities for **predictive analysis & response** to all banks.
- CCFMS generates **proactive patterns** and sends to banks as **preventive measure & warning**
- CCFMS sends preventive & **recovery solutions** to adjoining banks
- CCFMS is powered by **Cyber, Data, MLP & domain experts**

BOSTON
CONSULTING
GROUP

Lets hear from our Industry Leaders & Experts…

Sankarson Banerjee
CIO
RBL Bank

Lalit Kumar
Head of Security
AWS

Vipin Surelia
Chief Risk Officer
- India and South
Asia, Visa

Sameer Ratolikar
CISO
HDFC Bank

Rajiv Mishra
CGM, DIT
Union Bank of
India

A FIBAC : Cyber Think Tank Panel

NOV 2022