



SEGUROS
MONTERREY

THE FUTURE OF SMNYL IS TODAY

INNOVATION DAY





SEGUROS
MONTERREY

CYBER INSURANCE: DATA POWERED

Daniel Zavalza

INNOVATION DAY





SEGUROS
MONTERREY

CYBER INSURANCE



**CYBER
INSURANCE**



Harness growth securely and protect profits through greater data insights and risk led intervention in cybersecurity.



Why Cyber Insurance?

- Revenue or profit protection in the event of an attack
- Provides potential assurance to third parties that an organisation may deal with
- Good practice by governments to have some form of insurance in place

Why the SME Cyber Insurance risk profile is growing fast

- 43% of total cyber attacks target **small business**
- 74% of attacks on SMEs originated **outside the organization** while 34% of attacks had **insider support**
- 43% of SMEs have no understanding of **how to protect** themselves against cyber attacks & lack a defense plan
- 22% of SMBs switched to remote work without a cybersecurity threat prevention plan
- 64% of SMEs **don't have Cyber Insurance**
- 154 countries enacted **cyber-crime legislation**, many citing the need for Cyber Insurance

Last Year Alone:

- **43%** of SMEs reported at least one cyber attack
- **€ 184K to € 2.4M** was an average cost of an attack for a SME
- **40%** of SMEs suffered downtime of 8 or more hours due to an attack, costing **€ 1.4M** on average
- **€ 13.5K** SME cost for determining how a cyber-attack happened
- **60%** of SMEs go out of business after a cyber breach
- **63%** of breaches occurred due to Weak or stolen password

Sources:

*1 Source: Verizon 2019 Data Breach Investigations Report

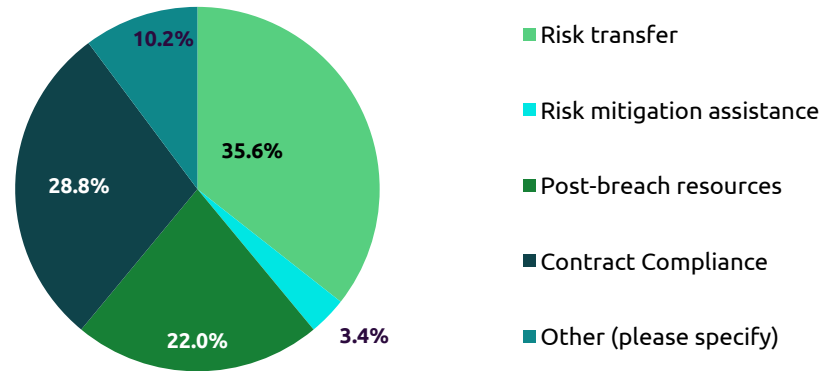
*2 Source: Hiscox Cyber Readiness Report

*3 Source: Fundera

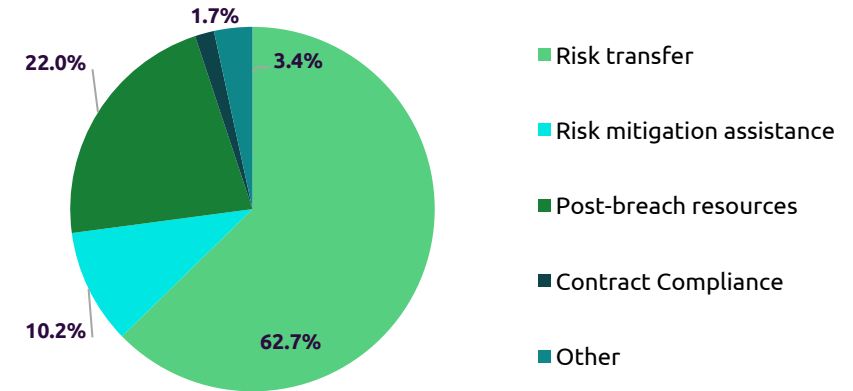
*4 Source: UNITED NATIONS Conference on Trade and Development

SME CYBER INSURANCE MARKET - OPPORTUNITIES

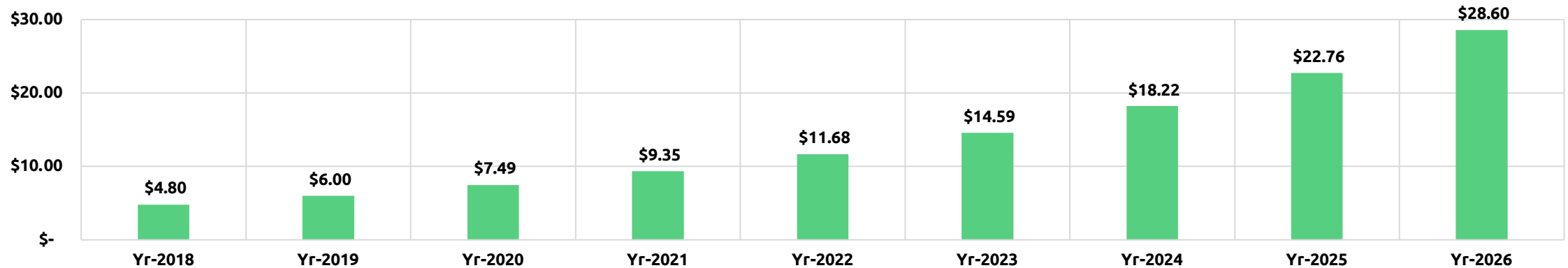
Drivers for SME Cyber Insurance



Drivers for Large Enterprises Cyber Insurance



Spending on Cyber Insurance in Billion US Dollars

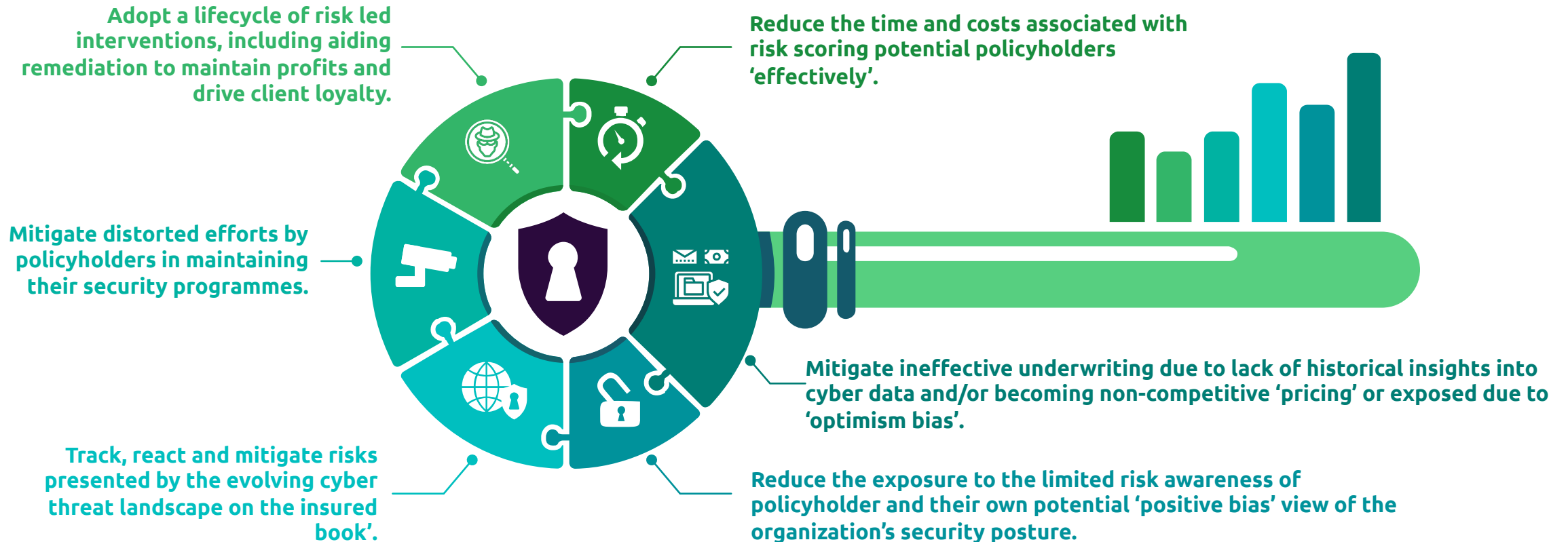


Source: CIAB

CHALLENGES FOR CYBER INSURANCE PROVIDERS

OPTIMISM HAS NO PLACE IN CYBER INSURANCE UNDERWRITING

Independent studies, market analysis, and surveys concur that a successful Cyber Insurance offering could ONLY flourish if the insurer is able to address a wide range of dynamic challenges.



CYBER INSURANCE OFFERING – A PLATFORM FOR INFORMED DECISIONS & INCREASED RESILIENCY



Policyholder Acquisition Services

Cyber Insurance Platform

Outside-In Assessment

Inside-Out Assessment



Policyholder Risk Management Services

Policyholder Education

At-Signing Assessment

Threat Intelligence and Alerting Service

Monthly Monitoring

Service Insight Reports



Post Breach Services

24/7 Cyber Insurance Bureau

Identification & Triage

Post Breach Risk Report

Incident Management

Incident Response

Forensic Investigation



Cyber Catalogue of Services

For Insurers

Security Audits of Corporates

Health Check for Policy Renewals

Forensic Investigation

Claims Investigation

For Policyholders

Remediation Consulting

Post Incident Security Assessment

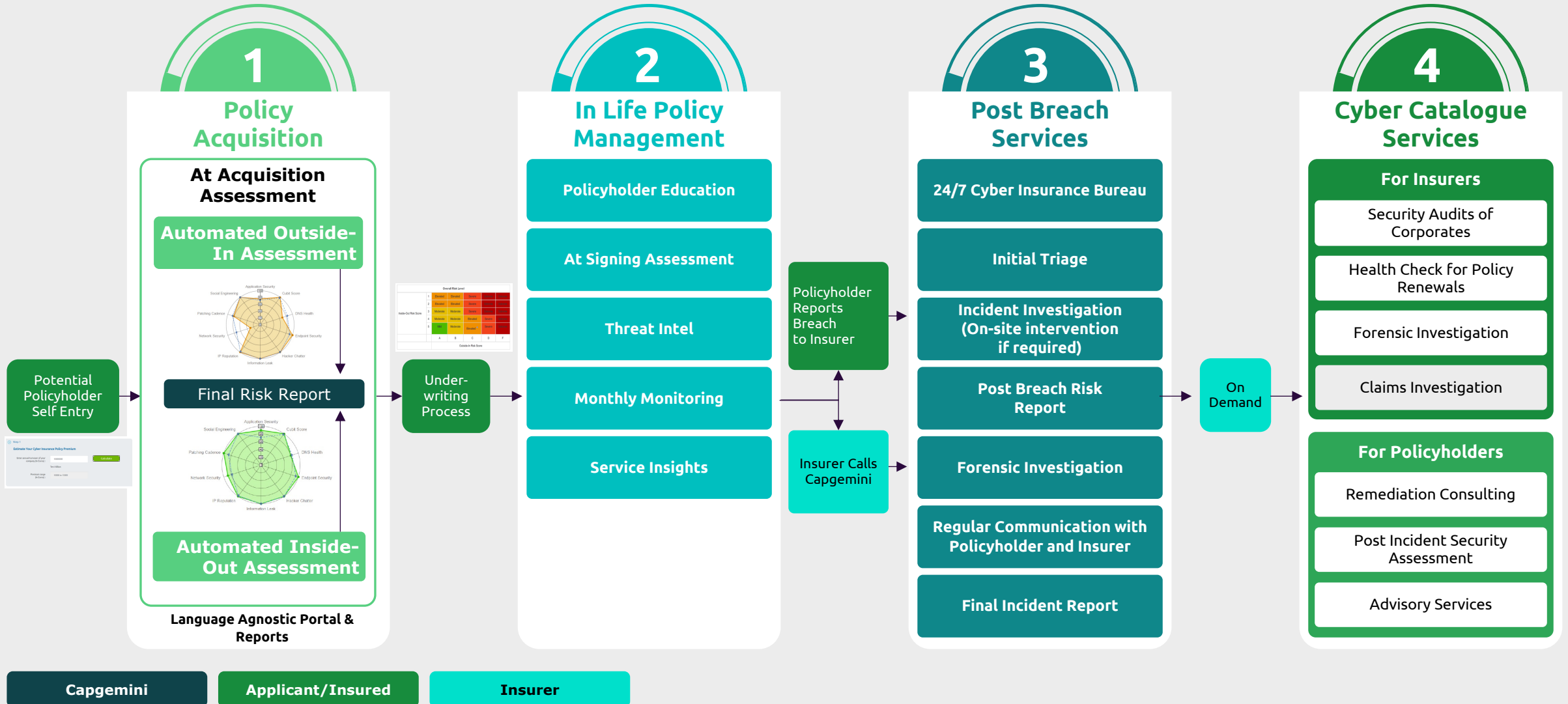
Advisory Services

“Informed Decisions” enable insurers to:

- Determine whether an applicant is a “Go” or “No Go” accurately
- Estimate the premium
- Avert future breaches
- Have lesser pay-outs

Language agnostic portal and reports.

CYBER INSURANCE OPERATING MODEL/WORKFLOW



OUTSIDE IN & INSIDE OUT RISK SCORING: MITIGATE THE LACK OF HISTORICAL DATA FOR UNDERWRITING AND COMPETITIVE PRICING

Automated Fast Score Capabilities (<10 Minutes) & Continuous Risk Score Monitoring.

1

Data Collection

- **Global sensor network** crawling the Internet from over 45 locations
- **27B + vulnerabilities** gathered per week and **700M + hits** to sinkhole daily

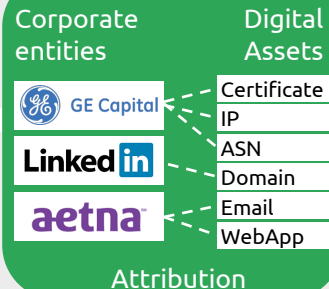
Over 45 locations



2

Attack Surface Discovery

- **Patented capabilities** discover an organization's attack surface
- Attribution of attack surface to **any organization worldwide**



3

ML-Powered Data Processing

- Data processing engine aggregates signals to **enhance accuracy**
- **Hundreds of risk factors** over 10 security categories
- **ML based risk severity** model that learns from user feedback



4

Fare accurate and predictive model

- A-F rating for **2.5M + companies**
- Low scores **7.7 X more likely to breach**
- **7 years** of historical data+ user contributed data

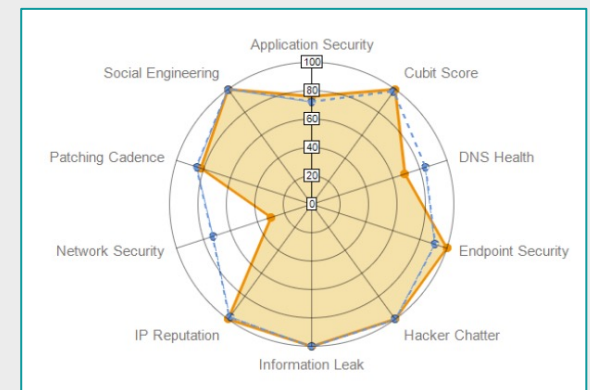
A-F rating for 1.5M + companies



7.7 X more likely to breach

Outside In:

1. Approach 'Attribute & Collect'
 - Id Digital Public Assets (e. domains, IP, SSL certificates etc.).
 - Measuring the feedback from these assets.
2. Scoring 0-100/A to F
3. Aggregated 'factor grades' >90/10 Categories.



OUTSIDE IN & INSIDE OUT RISK SCORING: MITIGATE THE LACK OF HISTORICAL DATA FOR UNDERWRITING AND COMPETITIVE PRICING

Request for Insurance Self-Assessment Questionnaire (Automatically Initiates Outside In Process). Aligned to Industry Security Standards; NIST, ISO27001 and CMMI Maturity Modeling Approach

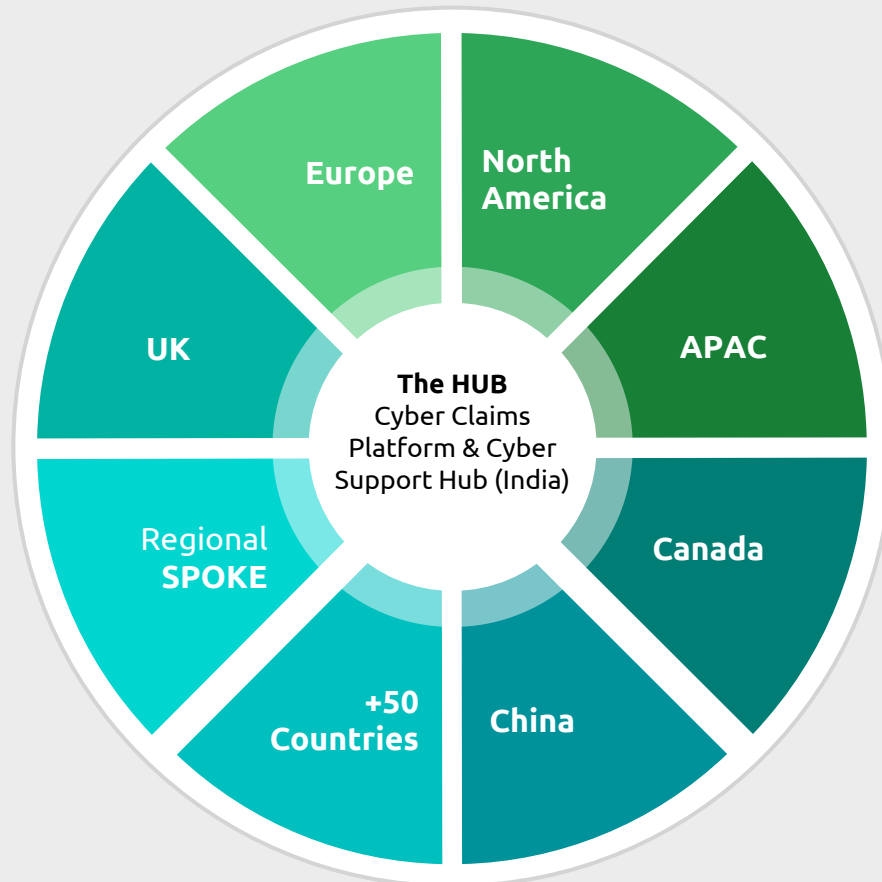
Inside Out Questionnaire:

1. 10 Categories, maximum of 41 questions designed to assess the security controls adopted by organization.
2. Align to industry standard security frameworks & CMMI i.e. Yes/No and Choice of 5 Options. Informs commercial weights.

| | | Overall Risk Level | | | | |
|-----------------------|---|-----------------------|----------|----------|---------|---------|
| | | A | B | C | D | F |
| Inside-Out Risk Score | 1 | Elevated | Elevated | Severe | Extreme | Extreme |
| | 2 | Elevated | Elevated | Severe | Extreme | Extreme |
| | 3 | Moderate | Moderate | Severe | Extreme | Extreme |
| | 4 | Moderate | Moderate | Elevated | Severe | Extreme |
| | 5 | Mid | Moderate | Elevated | Severe | Extreme |
| | | A | B | C | D | F |
| | | Outside-In Risk Score | | | | |

CYBER INSURANCE - GLOBAL DELIVERY MODEL (HUB & SPOKE) PLATFORM FOR SERVICING EXISTING REGIONS AND GTM VEHICLE FOR NEW MARKETS.

The challenges for delivery can be summarized as: ability to scale, multi-language, cost, balance of remote & onsite assistance, including investigation and specialist forensic support for high value claims.



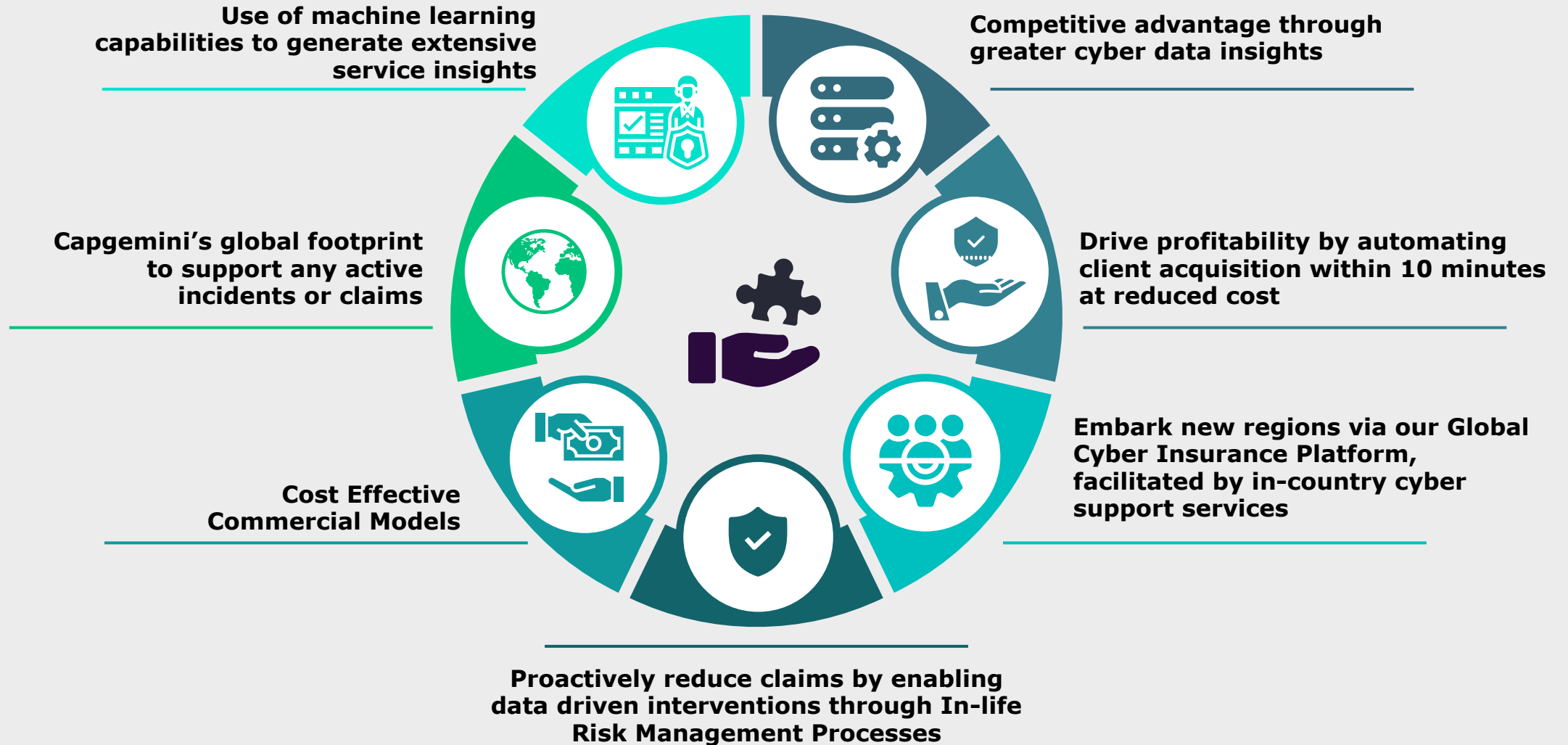
One Global Team:

- Capgemini employs 270,000 technologists, >4,500 are security specialists. Apart for the global network of delivery centres, we operate a network of 15 Cyber Defence Centres that support our clients and local security practices/CoEs in each country.

Cyber Insurance:

- Operates in HUB & SPOKE Delivery Model.
- HUB operates from India: Receive, review and categorise the attack types, incident Management & Remote Remediation (where possible).
- SPOKE provides Local Language and Onsite Cyber Support through regional experts: Act as the client relationship manager, conduct audits/interviews & acts as the intelligent onsite resolution lead by working with global support teams who will provide remediation recommendations and advice.

CAPGEMINI VALUE PROPOSITION: INFORMED INTERVENTIONS, RISK MITIGATION



WHY CAPGEMINI FOR CYBERSECURITY?

Industry Thought Leader



- Philosophy to **“Think like an Attacker”** to protect our Clients
- Leveraging service orchestration and **Machine Learning** to stay ahead
- Actionable Threat Intelligence** from commercial sources, National CERTs, and Security Agencies
- Security Labs to **Test Security Products**, and **Malware Analysis**

Industry Recognition & Global Coverage



- Recognized by Gartner** as a Niche Player in Gartner, Magic Quadrant for Managed Security Services, Worldwide(*)
- Leaders in MSS by **Hfs Research Blueprint** and **Nelson Hall NEAT**
- True Global presence and **Network of 15 connected Security Operations Centers & Labs**
- Shared** and **Dedicated Service Delivery** model to address our Clients’ Security Compliance Requirements and Risk

Proven Track Record



- 650+ Customers**, Cross-industry Experience
- Service Delivery Excellence - **70% Customers Highly Satisfied**
- Delivered **End-to-End Cyber Security Services** from Policy Definition/Strategic consulting to Deployment, Management & Monitoring
- Integrated MSS Portal** for Real-time Service Status & Client Interaction

Proven Processes & Methodologies



- We have our own way of working, the **Collaborative Business Experience™**, and draw on our **Right shore®** model
- Low Cost of Ownership** – doing more with less, while staying competitive
- Streamlined Processes** to improve Productivity and Compliance
- Security not bolted-on – **Security and Privacy by Design**

People Centric



- Strong **ONE Global Team of 4500+ Skilled Cyber Security** Experts
- Dedicated **Skills Development and Training** function for Cross-skilling and Up-skilling
- Team members hold **Industry Standard Certifications**, such as CISSP, CISM, CISA, CCSP, including ITIL, CEH, CCIE and other **Technology Certifications**

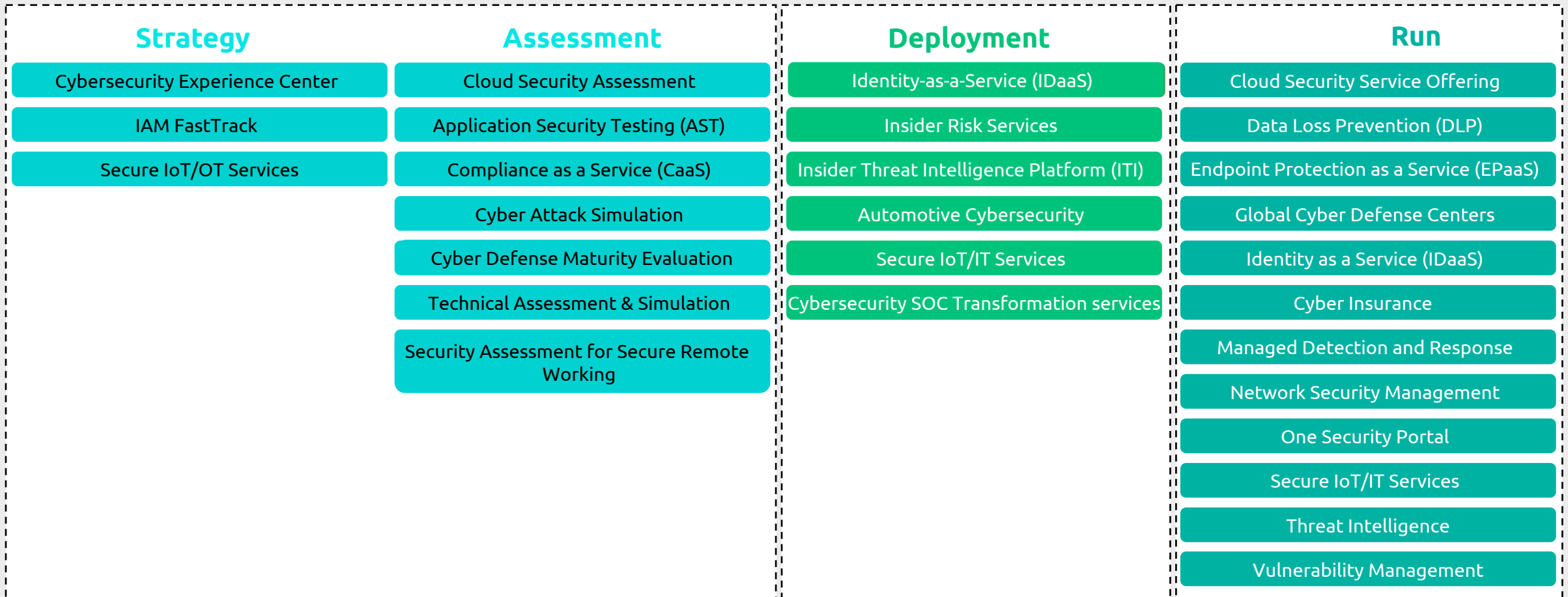
PORTFOLIO OVERVIEW

Pricing for these services are provided on demand

Cybersecurity **Define** Services

Cybersecurity **Protect** Services

Cybersecurity **Defend** Services



CYBERSECURITY CREDENTIALS: IMPROVING MARKET & ANALYST RECOGNITION





**GET THE
FUTURE
YOU WANT**

[capgemini.com](https://www.capgemini.com)



About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 360,000 team members more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2022 global revenues of €22 billion.

Get The Future You Want | www.capgemini.com



This presentation contains information that may be privileged or confidential and is the property of the Capgemini Group.

Copyright © 2023 Capgemini. All rights reserved.