CyberSecurity Maturity Of Indian Industry - 2017

FIRECOMPASS

Content

- Background
- Methodology
- Scoring Model
- Data Set
- Key Findings
- Detailed Findings
- Conclusion

Background

Cyber security is now a persistent business risk, across organizations of all size, large or small. To secure businesses, you need to have in place a variety of security technologies along with skilled personnel and mature processes.

In this report we've researched the current cybersecurity maturity of Indian industry based on the kind of technical security controls they have in place against modern day attacks.

CyberSecurity Breaches & Impact

Zomato hacked: Security breach results in 17 million user data stolen
Source: ET

India based payment processing firms ElectraCard & enStage breached, Visa delists them.
Source: TOI

Data of about 3.2 million debit cards was lost in what is claimed to the India's biggest breaches. SBI, HDFC Bank, ICICI, YES Bank and Axis were worst hit by the breach of the debit cards.
Source: ET

Top Cyber Threats – Verizon DBIR 2017

- **Cyberespionage**: Cyberespionage is now the most common type of attack seen in manufacturing, the public sector and now education

- **Ransomware & Malware is big business:** Fifty-one (51) percent of data breaches analyzed involved malware. Ransomware rose to the fifth most common specific malware variety. Ransomware – using technology to extort money from victims - saw a 50 percent increase from last year's report

- **Phishing** is still a go-to technique: Forty-three percent of data breaches utilized phishing, and the method is used in both cyber-espionage and financially motivated attacks.

- **Pretexting** is on the rise: Pretexting is another tactic on the increase, and the 2017 DBIR showed that it is predominantly targeted at financial department employees – the ones who hold the keys to money transfers.

Source: [Verizon 2017 Data Breach Investigations Report (DBIR)]

India vs World (ITU : GCI Report 2017)

As per, International Telecommunication Union's (ITU) Global Cybersecurity Index (GCI) 2017 :

- **India** is **ranked 23rd out of 164** Nations, with a score of 0.683
- **Singapore & US** are ranked 1 & 2 respectively, with a score 0f 0.925 & 0.919 respectively
- Singapore, Malaysia & Australia are the top three countries in **Asia & Pacific Region**

The ITU report is based on the following aspects

1. **Legal**: Measured based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime.
2. **Technical**: Measured based on the existence of technical institutions and frameworks dealing with cybersecurity.
3. **Organizational**: Measured based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level.
4. **Capacity Building**: Measured based on the existence of research and development, education and training programmes; certified professionals and public sector agencies fostering capacity building.
5. **Cooperation**: Measured based on the existence of partnerships, cooperative frameworks and information sharing networks.

Source: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

Methodology

1. Online survey was conducted for which 200+ organizations in India responded, across verticals
2. Respondents were CISOs or equivalent (i.e. responsible for CyberSecurity)
3. Survey comprised questions around current technology controls in place and roadmap
4. Technologies were classified based on the NIST CyberSecurity Framework (CSF) functions (Next Slide)
5. The Scores were calculated based on the method outlined in Scoring Model slide

Methodology (continued)

NIST Cyber Security Framework (promoted by USA government) was leveraged to classify the technology controls capabilities across the following 5 dimensions

1. **Identify** - Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities
2. **Protect** - Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services
3. **Detect** - Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event
4. **Respond** - Develop and implement the appropriate activities to take action regarding a detected cybersecurity event
5. **Recover** - Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event

Source: https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework

Scoring Model

1. Each of the technology controls currently deployed have been classified based on Control Type, i.e. The kind of capabilities they provide (Identify, Prevent, Detect, Respond). “Recover” was not considered for this report

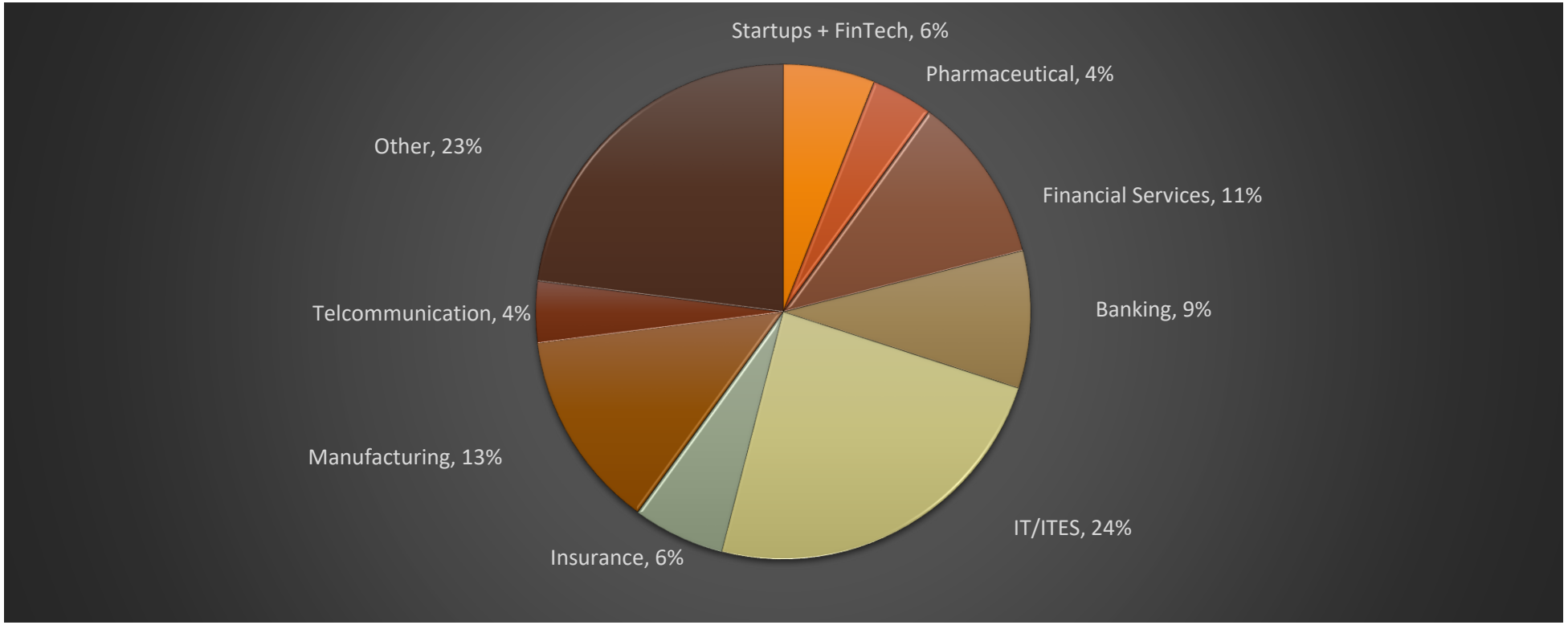
2. Data from 200+ Organizations was individually tagged based on above mentioned technology controls capabilities

3. Statistical Analysis was conducted to assign maturity score for each of the box mentioned above

4. Average across companies in an industry was taken to arrive at industry scores

Data Set: Participant Demographics

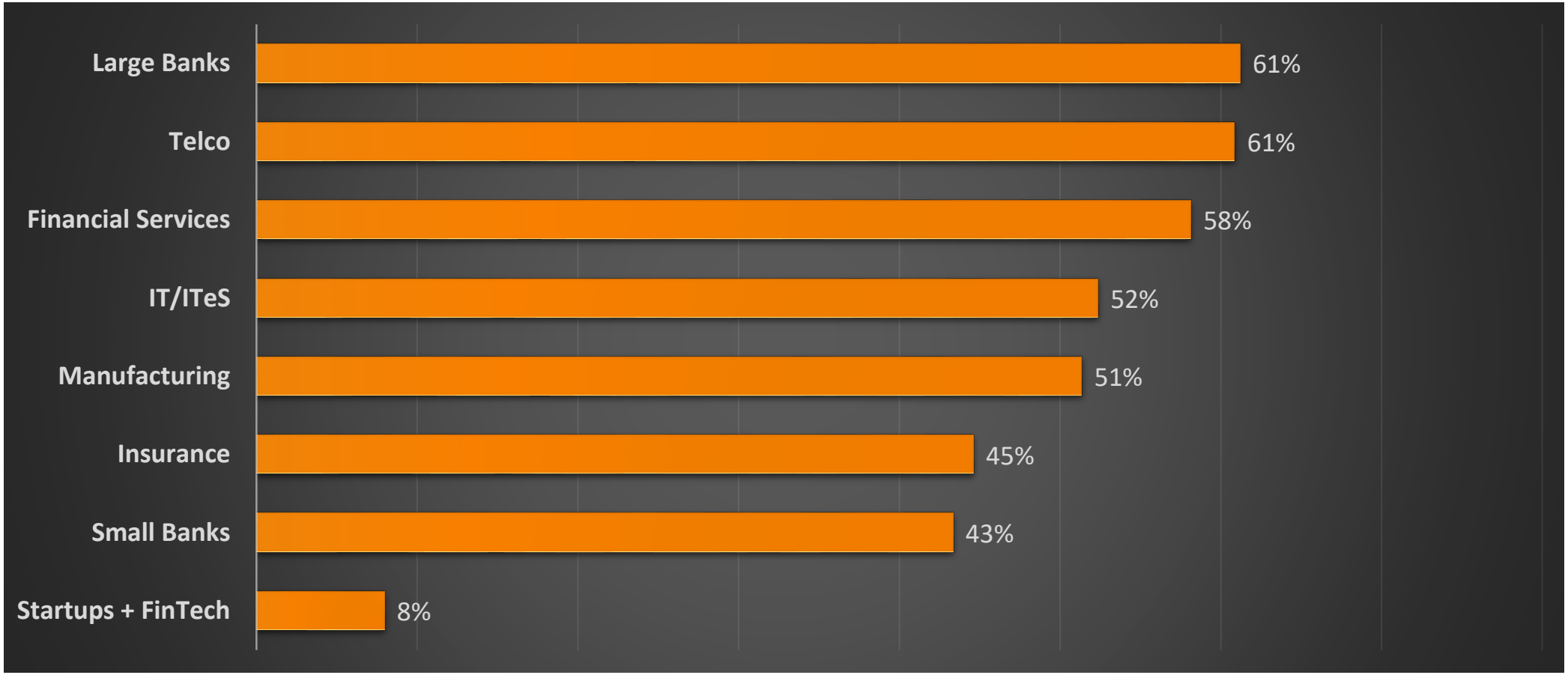
25+ Technology Controls related data for 200+ Organizations, across industries. Collected via online surveys. Respondents were primarily CISOs or Equivalent titles. Industry wise breakup below:



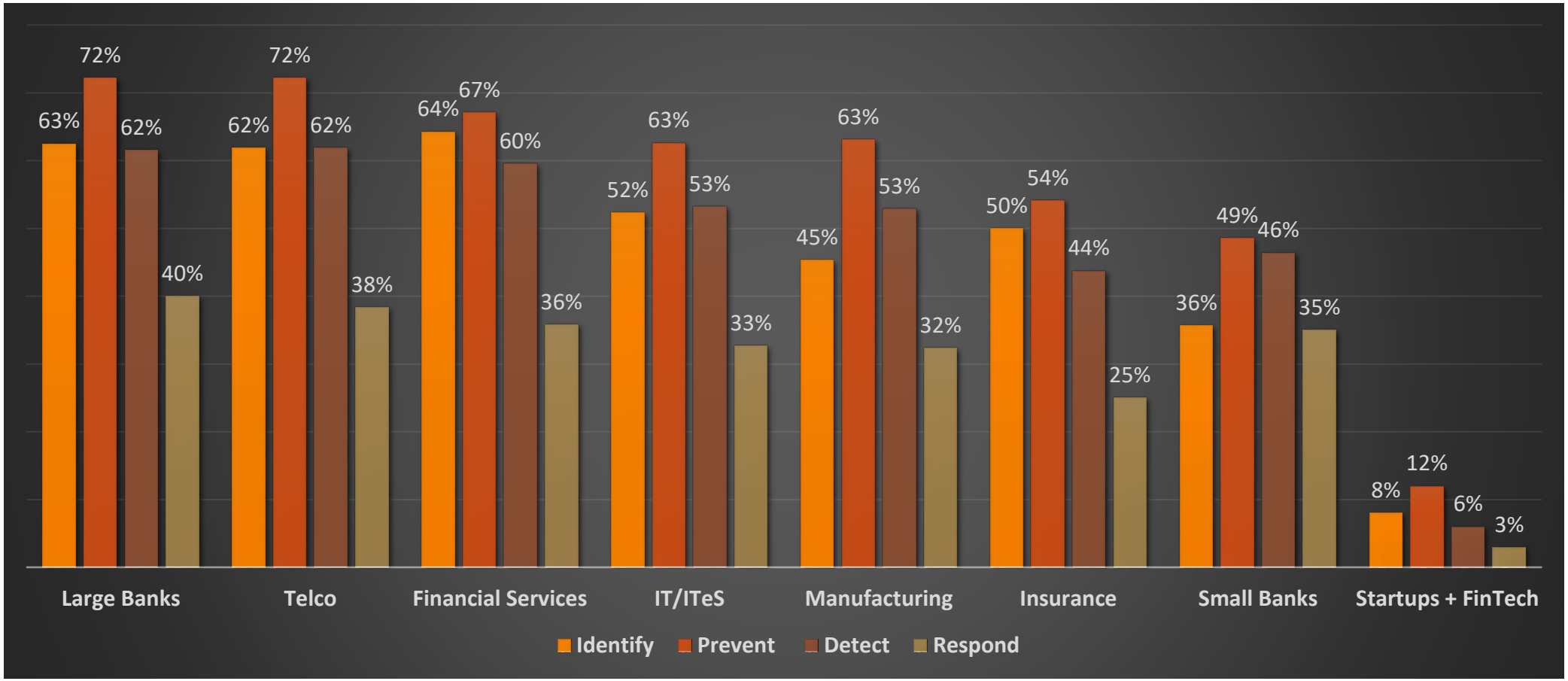
Key Findings

1. Large Indian Banks and Telcos are the most mature with average score of ~60% with Small Banks and Insurance are lagging far behind at ~45%
2. Internal Technology Controls are primarily around prevention, with not sufficient measure implemented around detection & response
3. Indian organizations are primarily compliance driven & reactive, with average security scores hovering around ~50/ 100
4. Response Capabilities across sectors is very poor, ranging between 25 to 40%
5. Preliminary data on startup shows that the security maturity is abysmally low at around 8%

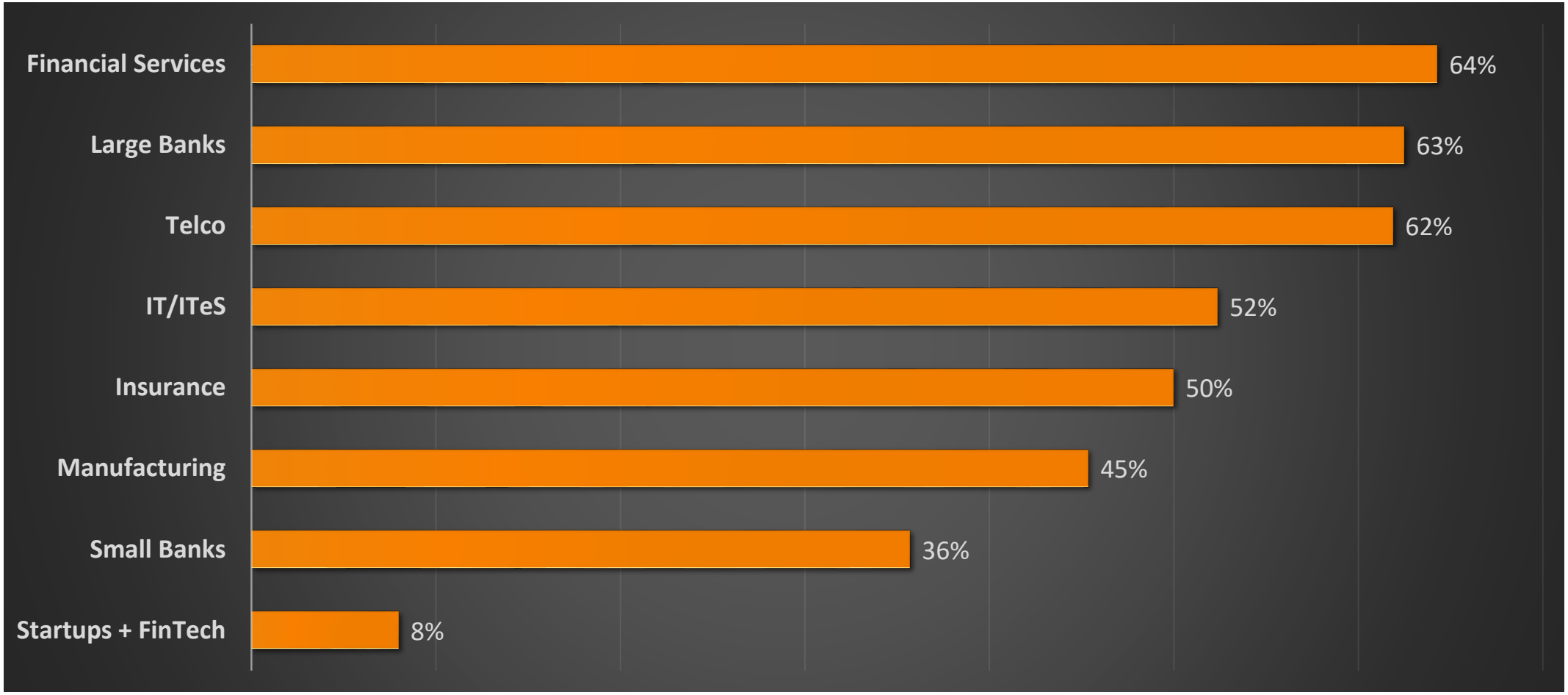
Scores by Industry (Overall)



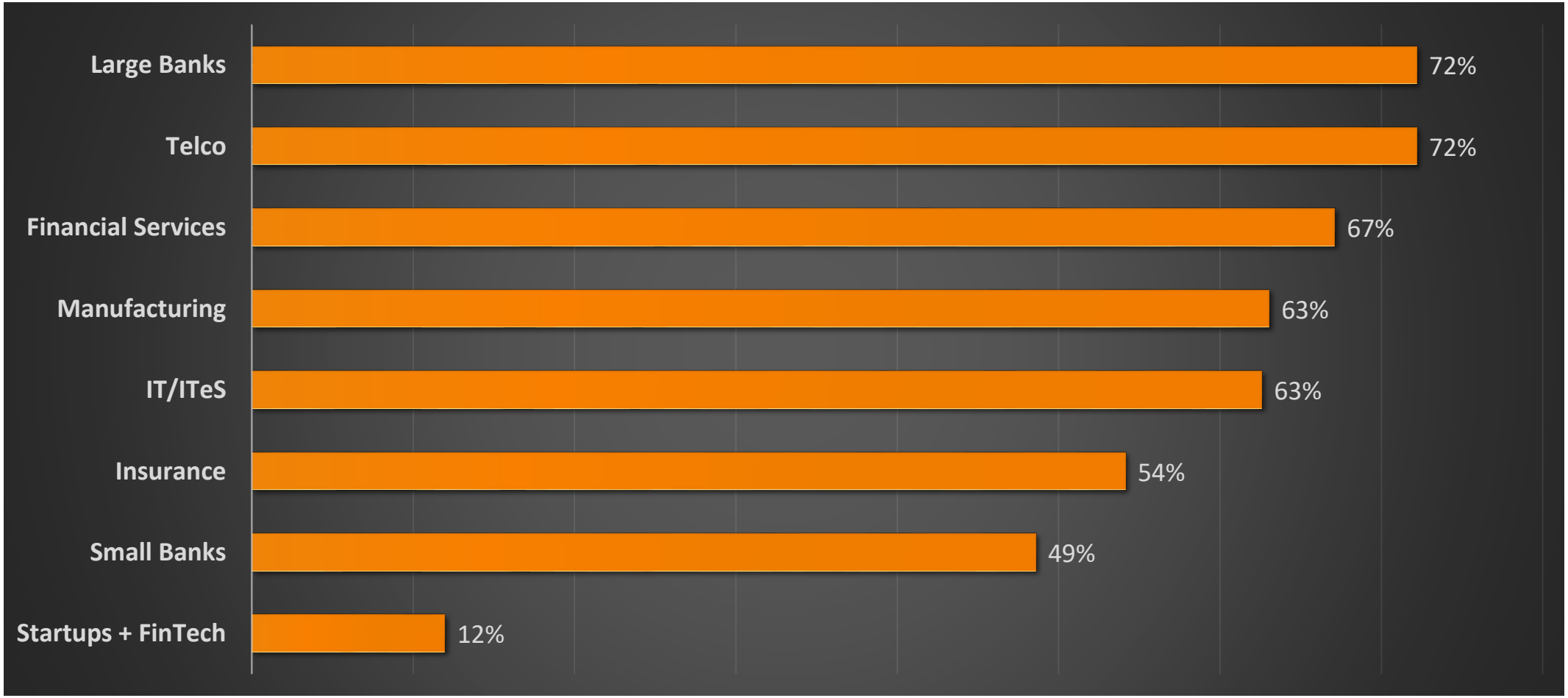
By Industry (by Capabilities)



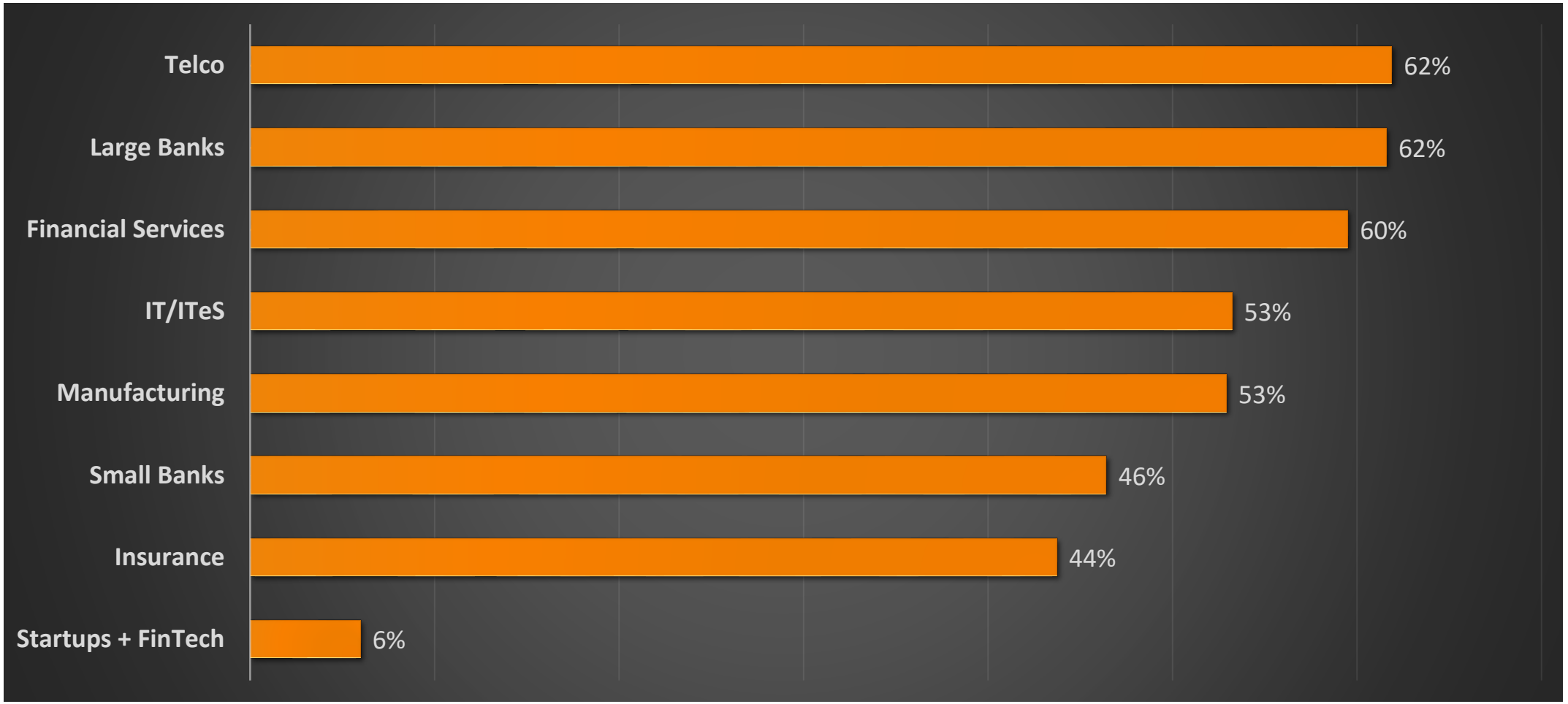
Identification Capabilities (by Industry)



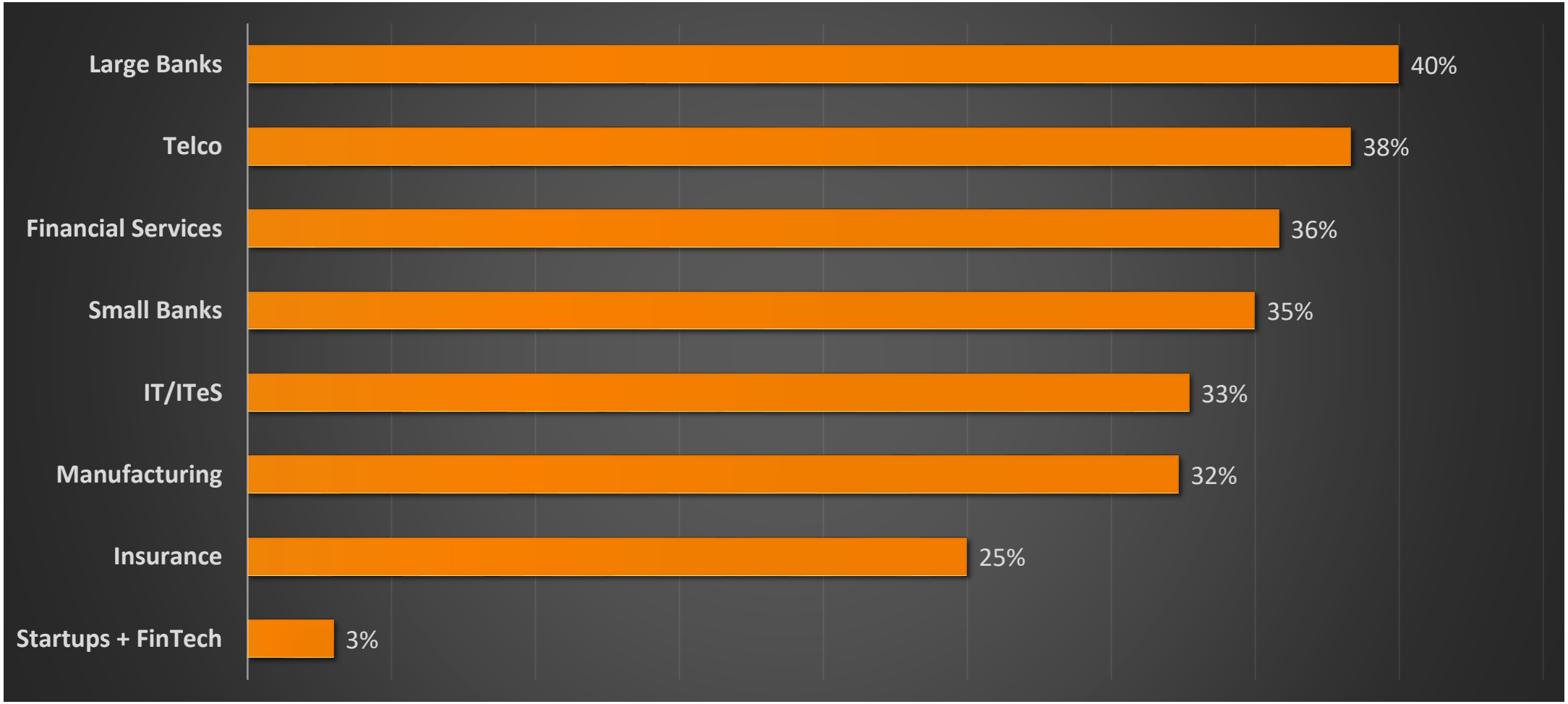
Prevention Capabilities (by Industry)



Detection Capabilities (by Industry)



Response Capabilities (by Industry)



Recommendations to Boost CyberSecurity

- CyberSecurity investment should be spread out across the spectrum, by taking a balanced approach to investments, like a financial portfolio
- Security Architecture should be well defined, taking into consideration that it's highly likely that you'll be hacked sooner or later, and impact should be minimal
- Ethical hacking is a small part of the overall security program, build CyberSecurity in, right from the design stage and NOT defer it towards the end
- Management should consider CyberSecurity as a major enterprise risk and have a strong focus towards managing it
- New regulations & frameworks like that from RBI are a welcome move, where they've made a board approved CyberSecurity Policy mandatory for banks

Recommendations for Startups (incl. FinTech)

- Management & Investors should put a strong emphasis on beefing up CyberSecurity, as a breach can have a catastrophic impact on business
- Do NOT assume that startups are not a target for hackers. Most of the startups are easy prey for opportunistic hackers and startup breaches are rapidly rising
- CyberSecurity is not always costly, and a strong posture can be achieved by a combination of right processes, low cost tools and a small but skilled team
- Security should be considered right from the design stage of the product and be continuously assessed throughout the lifecycle (incl. DevOps). Fixing issues later can be 30x higher than at design stage.

Thank You!

Website: www.firecompass.com
Email: contact@firecompass.com