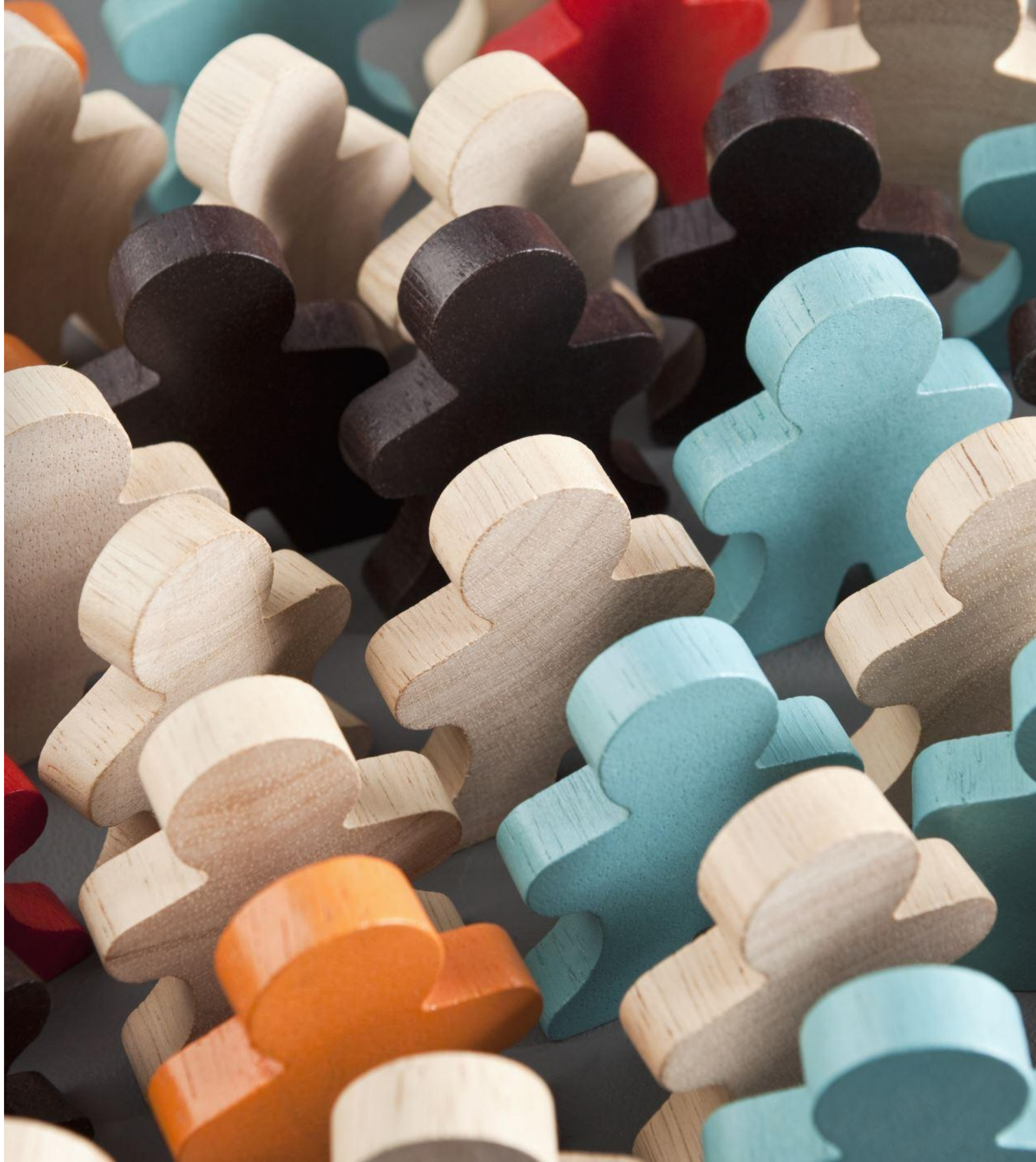
Securing What Matters, Strategies for Aligning Cybersecurity Operations with Business Priorities

Jigar Shah, CISO

Alignment Challenge

- Business leaders speak in terms of Revenue, Growth, and Customer Trust
- Cyber teams speak in terms of threats, vulnerabilities and controls
- Business thinking in terms of Strategy & Profit and Cyber focuses on Risk & Compliance
- The disconnect = missed opportunities + unclear ROI



Cybersecurity perception gap – Executives and Practitioners see risk differently

- Confidence at the top, Caution on the ground
- Executives using strategic lens □Governance Framework, Compliance certifications, Annual metrics
- Practitioners using tactical lens □Incident Response, Patch backlogs, alert fatigue etc.
- Two different views □Under prioritized risk areas, Blind spots becoming crisis, False assurance
- Technology doesn’t fix culture, Compliance =! Readiness, Measurement without meaning, Siloed view
- Culture+ Collaboration+ Communication+ Confidence □ Competence

Strategy 1: Translate Cyber Risk into Business Risk

- Express Risk in terms of business impact. (downtime, revenue loss, brand damage)
- Use Financial Model – e.g. Expected loss per incident
- Link every top Cyber risk to an Operational process or Business Goal.

KPIs:

- % of risks quantified in business terms
- YOY reduction in uninsured Cyber exposure

Strategy 2: Embed Security in Digital Transformation

- Security as a built-in part of innovation – DevSecOps to more of Product and Strategy Security
- Collaborate and Partner early in the game
- Secure your crown jewels

KPIs

- % of digital projects with security at design phase
- Mean time to remediate vulnerabilities
- # of secure code reviews per release

Strategy 3:Use Cyber metrics that matter to Executives

- Move from technical metrics (patch rate, # of alerts)
- Create Business Outcome metrics – (risk reduction, uptime, cost avoidance etc.)
- Create an executive level Cyber Health Index

KPIs:

- % reduction in high impacts incidents
- Average Financial impact per incident
- Cyber health score trendline

Strategy 4: Build cross functional cyber governance

- Involve Legal, Finance, HR, Operations and Business into Cyber Strategy
- Make Cybersecurity part of Enterprise Risk Governance
- Co-own Cyber decisions with Business

KPIs

- % of Business units with defined cyber risk owners
- Mitigation initiatives co-funded by the business

Strategy 5: Measure ROI on Cyber Investments

- Quantify Cost Avoidance and Operational Savings
- Present Cyber projects in ROI and pay back period terms
- Tie Security spends to measurable Business outcomes

KPIs

- ROI on security initiatives
- Reduction in annualized loss expectancy
- Mean time to triage and mean time to contain to avoid downtime