What to Say Instead

Cyber Babble	CEO	CIO	COO	CFO
"We need to implement Zero Trust."	"We're modernizing how our data moves across the company to **cut exposure** and **speed up decision-making**."	"We're reducing unnecessary trust paths in our systems … fewer single points of failure, **smoother operations**."	"We're tightening how systems talk to each other to **minimize operational disruption**."	"We're reducing fraud exposure and audit risk **without adding overhead**."
"Our attack surface is expanding."	"Growth has expanded our digital footprint … I'm quantifying that exposure, so you **know where the real financial risk sits**."	"Every new app or cloud service widens the IT footprint. I'm mapping that growth to **keep performance and risk balanced**."	"We're aligning security with **how our teams actually operate**, not slowing them down."	"This is about understanding where **uncontrolled cost and liability** can enter the system."
"We need stronger IAM controls."	"We're protecting customer and employee data by ensuring **access aligns to business need**."	"We'll streamline identity management so users get faster access, and we can **prove compliance with less manual work**."	"We're automating provisioning and off-boarding to **reduce human error and time loss**."	"It's a **cost-avoidance** play: fewer access-related incidents, less downtime, and cleaner audits."
"We must address shadow IT."	"We're eliminating ungoverned tech spend and **improving accountability for data usage**."	"We'll inventory unsanctioned apps and bring them under secure management, so they don't create **hidden dependencies**."	"We'll keep tools teams love… just make sure they don't expose sensitive data or **cause outages**."	"This **improves budget accuracy** … fewer duplicate subscriptions, **fewer unplanned vendor costs**."
"We need to improve incident response."	"We're **protecting brand trust and limiting business disruption** during inevitable incidents."	"We're tightening coordination between IT, ops, and security so **issues get resolved faster** with clearer ownership."	"We're **reducing downtime risk** … and making sure recovery playbooks actually work under pressure."	"It's about **preserving revenue** and **controlling loss** when something goes wrong."
"We need more funding for security tools."	"We can **show ROI** by tying investments to avoided losses and faster delivery."	"Let's align tool spend with what **delivers measurable uptime**, automation, or user efficiency."	"We'll prioritize spend where it accelerates **business continuity**."	"We'll present a **cost-to-risk ratio** … every dollar should have a quantifiable reduction in exposure."
"We have to manage third-party risk."	"We're protecting our supply chain and reducing dependency risk … critical for **investor confidence**."	"We'll assess vendors based on their ability to protect our shared data **without slowing delivery**."	"We're verifying vendor resilience, so **operations stay continuous** even if one provider fails."	"We're **reducing financial exposure** from vendor-driven breaches or penalties."
"We need to strengthen compliance posture."	"We're avoiding fines and ensuring the company can **scale safely into new markets**."	"We're mapping regulatory requirements directly to our workflows to **minimize audit friction**."	"Compliance tasks will feel more like **good business hygiene**, not extra work."	"This **reduces audit costs** and **improves our insurability profile**."
"We have to improve security awareness."	"We're building a culture of risk ownership across every function."	"We'll target training where **human error costs us most** … fewer clicks, faster reporting."	"We'll make **training relevant to actual workflows**, so teams don't tune it out."	"Fewer incidents mean **lower operational and insurance costs**."
"Our risk score is high."	"Here's the quantified exposure in dollars … and what it takes to move the needle."	"We're using real data to **prioritize** which issues block **business performance**."	"I'll show which risks **affect uptime** and which are just noise."	"Think of this as our **financial risk heatmap** … actionable, not theoretical."

CYBERPATH COACHING
TAKE CHARGE OF YOUR CYBER CAREER