TATA CONSULTANCY SERVICES

Building on belief

TCS Risk & Cybersecurity Study

Cyber confidence

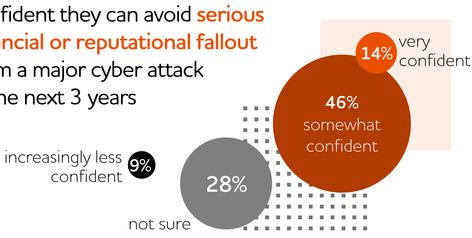
Companies and governments struggle today to keep up with the tactics and technology hackers and cyber criminals use to steal data, cause damage, and hold business activity ransom.

We surveyed more than 600 cyber executives—chief information security officers and chief risk officers—to find out which kinds of companies are succeeding in this arms race... and which are falling behind.

We focused our study on four industries in North America and Europe/the UK particularly beset by increasing levels of cyber attacks: banking & financial services, manufacturing, utilities, and media & information services.

The good news

A majority of CISOs and CROs feel confident they can avoid **serious financial or reputational fallout** from a major cyber attack in the next 3 years



Enterprise blindspot

Digital ecosystems were lowest on cyber executives' list of potential hacker targets to worry about...

#1	Finance
#2	Customer databases
#3	R&D
#4	Sales/ecommerce
#5	Marketing
#6	Manufacturing plants/production/procurement
#7	Human resources
#8	Legal
#9	Distribution/supply chain
#10	Ecosystem partners

...despite the **growing number of cyber threats** using these inter-connections between companies and industries as their attack vectors

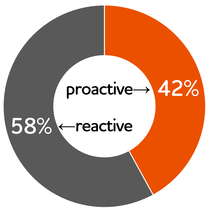
Insufficient focus

One in six **boards of directors** only discuss cyber risk & security issues "occasionally, as necessary" or even "never"...

...and only two in five boards do so at every meeting, or every meeting of a committee of the board

Needs attention

A majority of **C-suite executives & business unit heads** still only address risk & cybersecurity after it's brought to their attention, after an attack, or not at all



How confident are you feeling about your cyber strategy?

Get recommendations plus more insights & findings from the

TCS Risk & Cybersecurity Study
on.tcs.com/risk-cybersecurity