

# 5 Enlightening Statistics about Third-Party Cyber Risk

## ISLAND HOPPING

# 50%

Carbon Black reports that half of today's attacks leverage "island hopping", a method which attackers use third-party providers to infiltrate the target company

## NOT ME, HIM!

Bomgar reports that two third of security professionals believe that they have been possibly or definitely breached through a third party.



## THIRD-PARTY ACCESS

# ↑ 75%

Increase in third-party providers that have access to IT systems according to Bumgar.

Despite the increase on third-party access, only about

# 50%

 of the organizations

take necessary measures for data-governance, PwC report says.

## Tip: Continuously Monitor Your Third-Party Cyber Risk

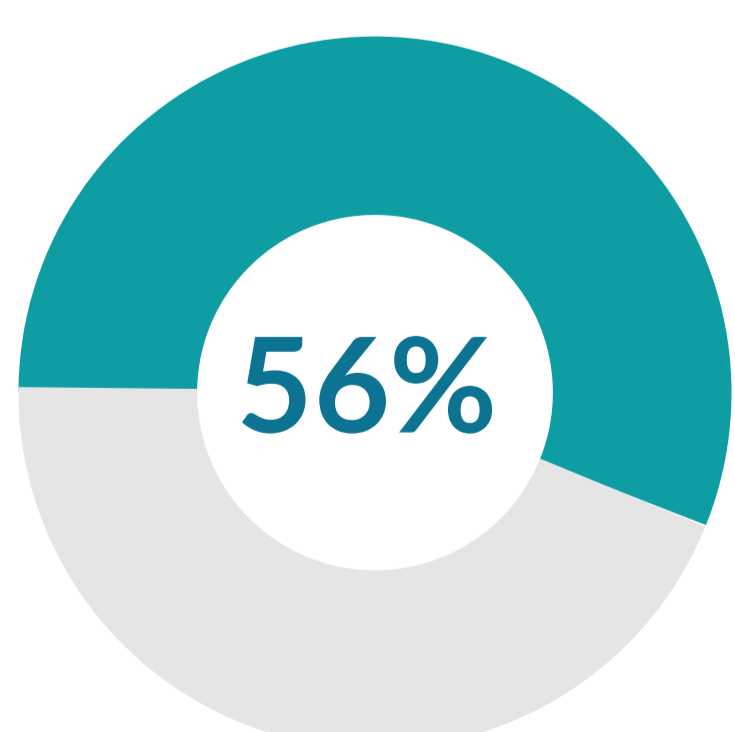


Your ecosystem multiplies your cyber risk and it is important to know how secure your vendors are. We can help.

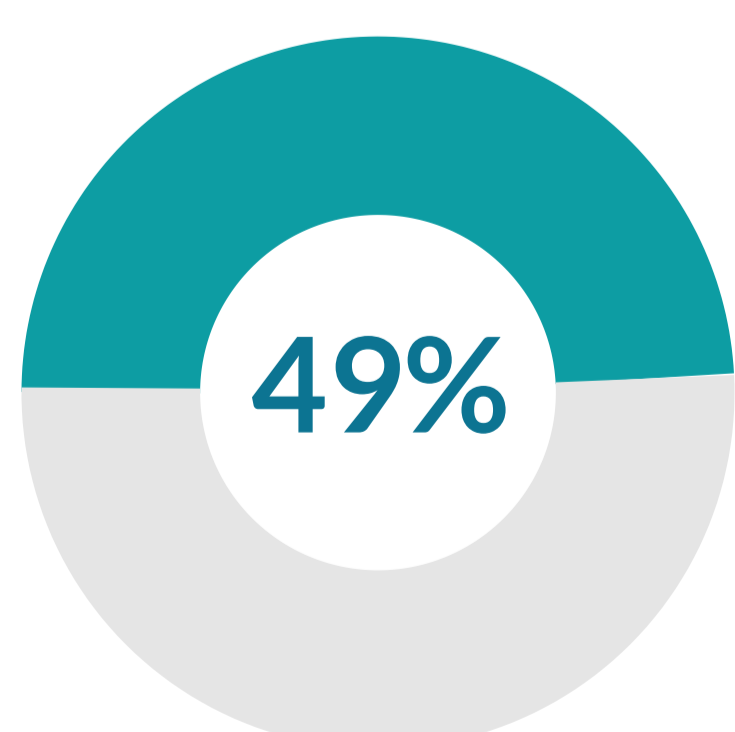
[info@normshield.com](mailto:info@normshield.com)

## LACK OF MEASURES ON DATA GOVERNANCE

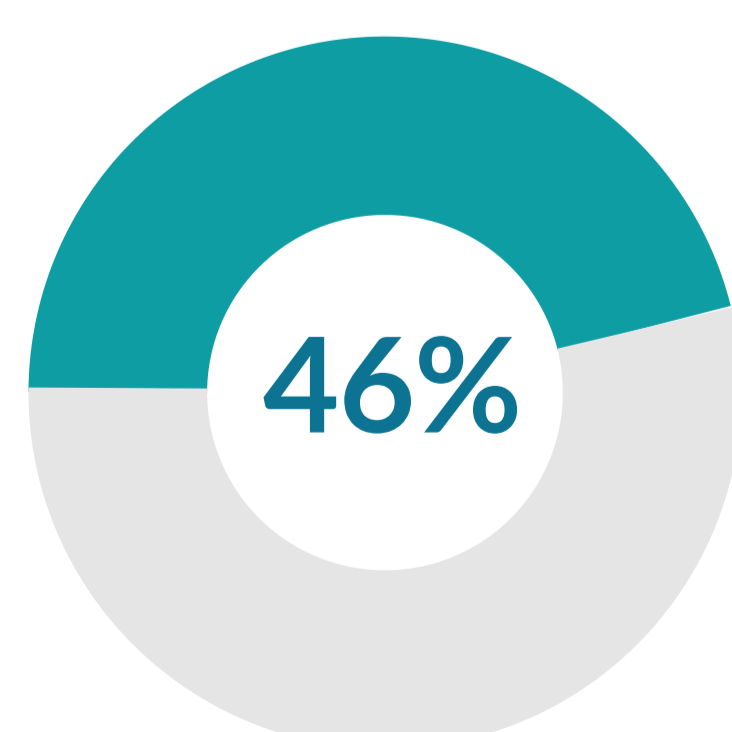
PwC report shows that many organizations are at the beginner level on data governance and do not take key measures to prevent third-party data breaches.



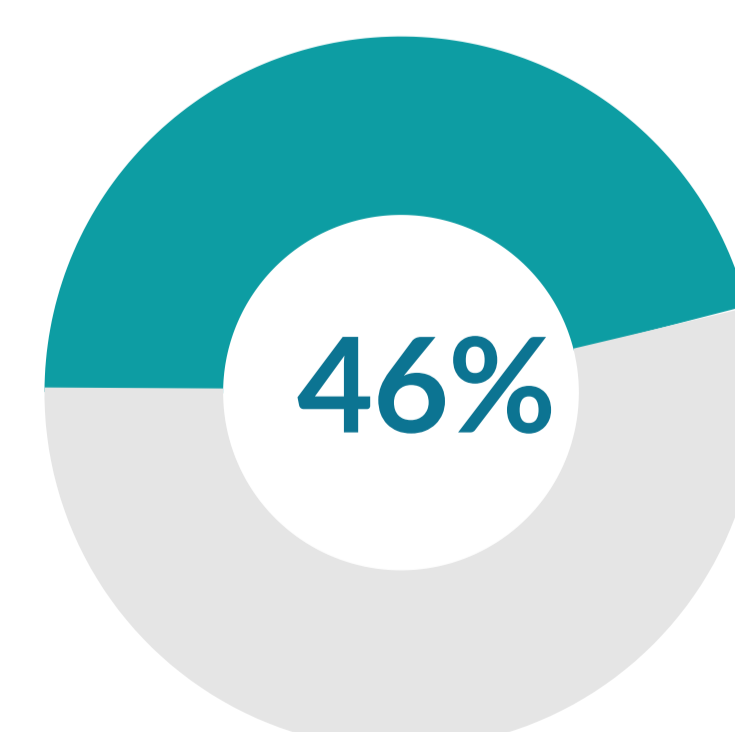
Have an overall information security strategy



Limit personal data collection, retention and access to the minimum necessary



Conduct compliance audits of third parties that handle personal data



Require third parties to comply with their privacy policies