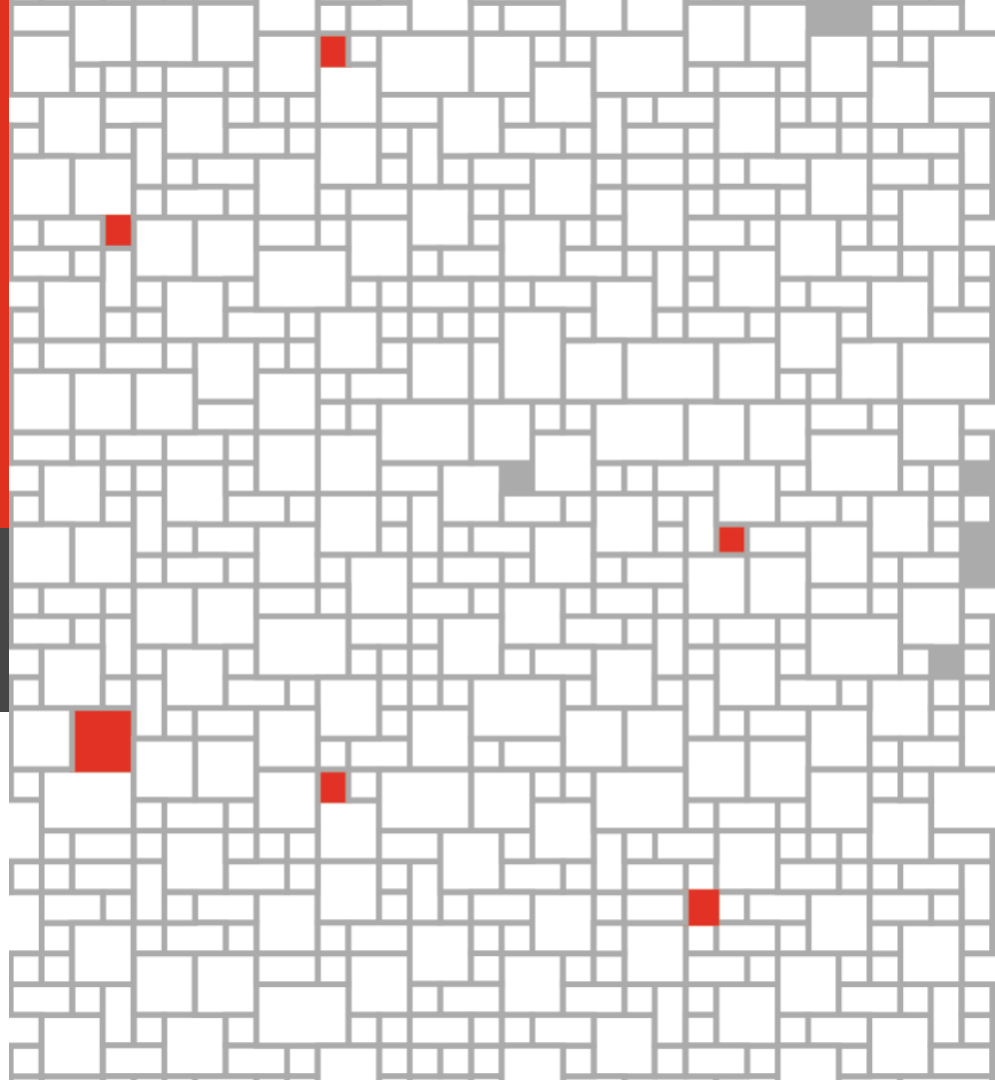


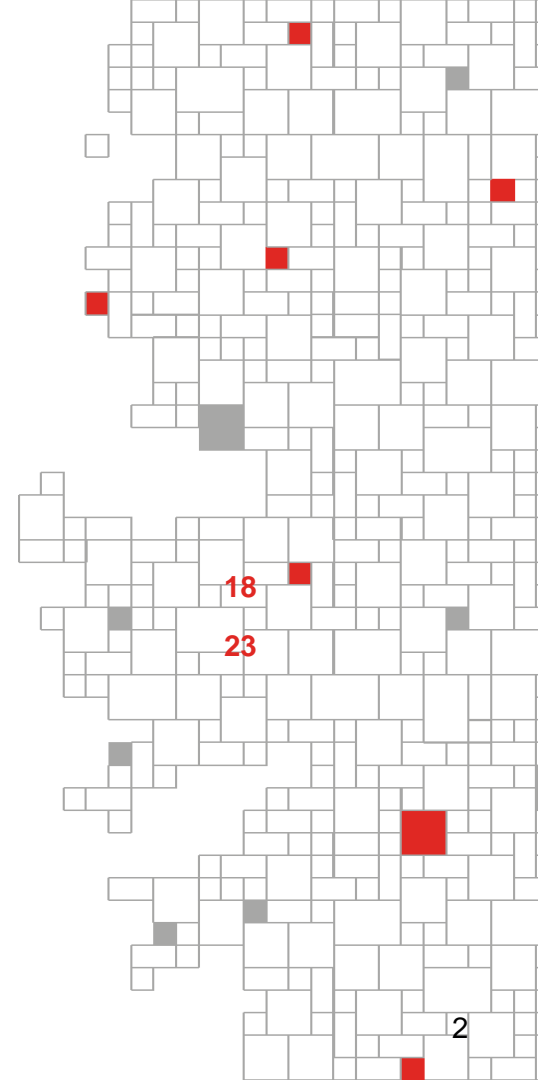
Raising the Resilience Quotient

Digital Trust Insights September 2019



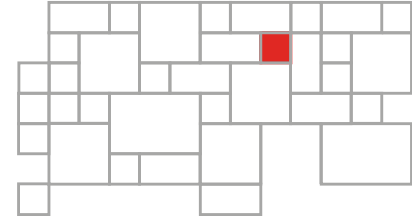
Contents

Digital Trust Insights September 2019	03
Setting the high resilience-quotient bar	04
What does it take to build digital resilience	09
Who are the high resilience-quotient respondents?	14
Methodology	18
Appendix	23



Digital Trust Insights September 2019

What it takes to build resilience in an organization is expanding well beyond enterprise IT.

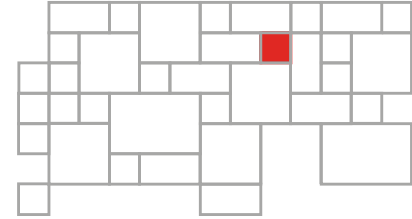


Keeping data and operations running smoothly and securely while digital connections multiply is changing the face of resiliency, according to [PwC's new Digital Trust Insights](#).

How are leaders revamping strategies to better position for resilience? Our global Digital Trust study of more than 3,500 business and IT leaders uncovered the attributes that are shared by a **high resilience-quotient (high-RQ) group** (top 25% of respondents).

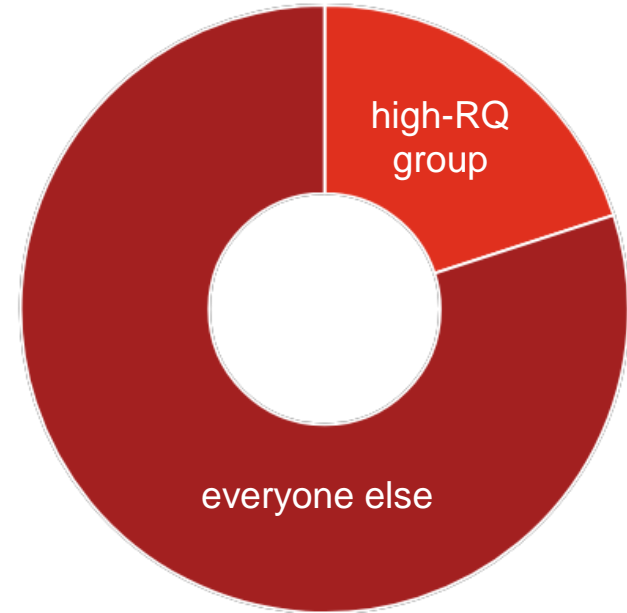
Setting the high resilience-quotient bar

High resilience-quotient (high-RQ) group

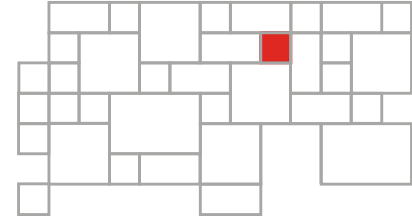


The top 25% lead across these areas

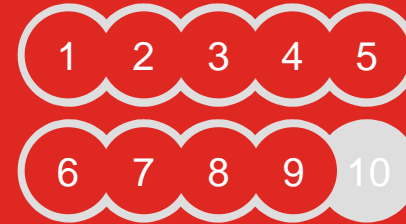
1. Visibility into core processes, assets and dependencies
2. Defining and testing impact tolerances
3. Building digital resilience by design



What it takes to build digital resilience



Without understanding how data assets and processes are connected to core business services and their interdependencies, an enterprise can't know which systems or assets to isolate if a disruption occurs.

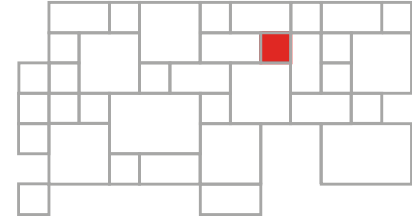


More than
9 in 10
high-RQ
companies

maintain an accurate inventory of assets
and refresh the list as needed
(vs. half of the rest)

PwC Digital Trust Insights survey, September 2019
Overall base size 3,532

In the face of new threats



The high-RQ group is aware that

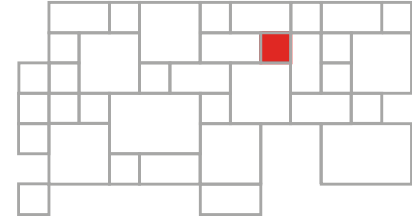
Data assets and processes are moving beyond the reach of enterprise IT. Common practices like cloud migrations and rollouts of IoT raise vulnerabilities.

59%

say that they have revamped strategies in the face of new, “very significant” threats (vs. 31%)

PwC Digital Trust Insights survey, September 2019
Overall base size 3,532

Managing emerging risks



The high-RQ group has

Gaining confidence in managing emerging risks that test cyber resilience

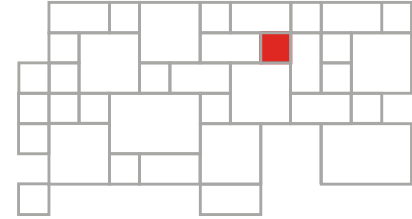
73%

more confident that they can manage emerging risks that test cyber resilience (vs. 24% of the rest)

PwC Digital Trust Insights survey, September 2019
Overall base size 3,532

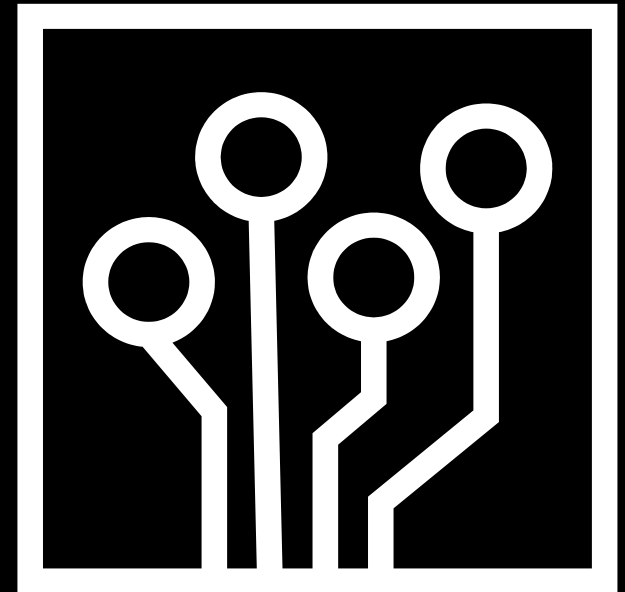
What it take to build digital resilience

Business resiliency: Shift beyond enterprise IT

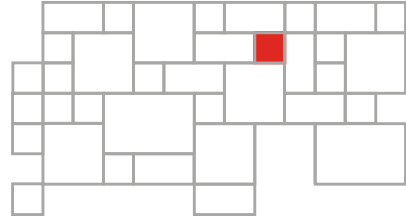


Companies aim for these standards

- Real-time view into critical assets and processes
- An enterprise-wide plan and response
- Continuous discovery and redesign of business services and processes



The 1-2-3 of building resilience



1 Visibility into core processes, assets and dependencies

- Create an extensive inventory
- Ensure inventory encompasses third-party relationships
- Use technologies to map critical assets and processes in-depth

91%

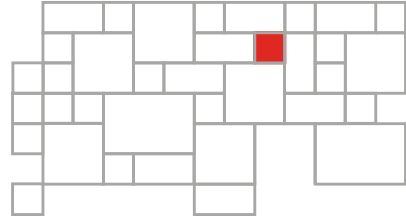
of high-RQ companies maintain an accurate inventory of assets and refresh the list as needed
(vs. only 47% of the rest)

PwC Digital Trust Insights survey, September 2019
Overall base size 3,532

The 1-2-3 of building resilience

2 Defining and testing how much disruption your organization can tolerate

- Set impact tolerances for critical business services and translate them into specific metrics
- Conduct tests of ability to stay within the impact tolerances
- Map impact tolerances to business services, not just critical ones

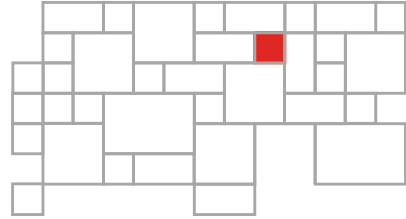


73%

of the high-RQ group have identified their most important business services (vs. only 27% of the rest have done so)

PwC Digital Trust Insights survey, September 2019
Overall base size 3,532

The 1-2-3 of building resilience



3 Building digital resilience by design: the next frontier

- Create an always-on, enterprise-wide perspective
- Build a team that monitors the stream of information, makes sense of it, and then responds together
- Use the platform and learn from disruptions to continuously redesign

34%

of high-RQ organizations have implemented “digital resilience by design” across the enterprise (vs. 14% of the rest)

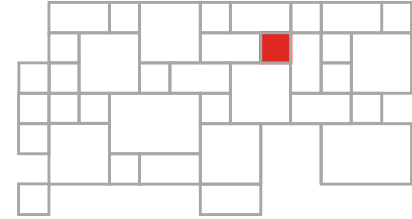
PwC Digital Trust Insights survey, September 2019
Overall base size 3,532

Who are the high-RQ respondents?

Methodology

Methodology

Digital Trust Insights September 2019

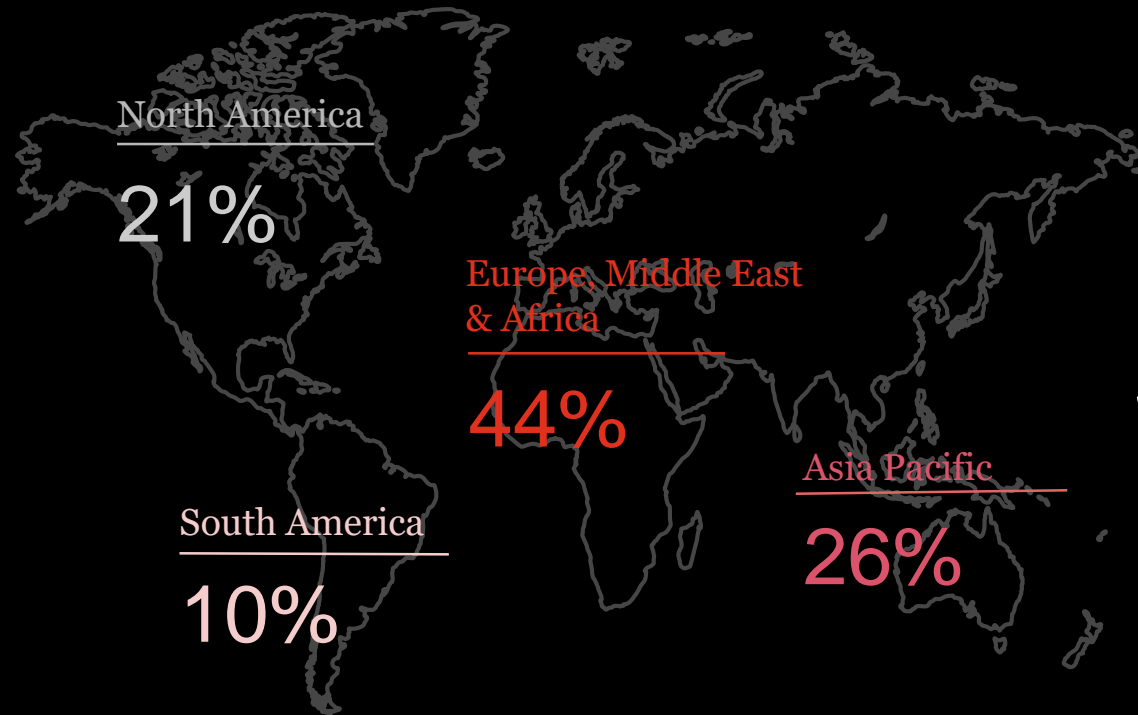
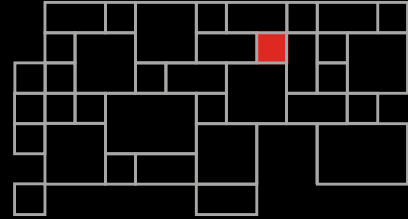


Digital Trust Insights September 2019, a worldwide study by PwC, was conducted online in July 2019

- Responses of 3,539 respondents from 61 countries who primarily hold titles CEOs, CFOs, CIOs, CISOs, CPOs, CSOs, General Counsel, VPs and directors of IT and security
- Fifty three percent (53%) of respondents from organizations with revenue of \$500 million+
- 21% of the respondents are from North America, 44% from Europe, Middle East & Africa, 26% from Asia Pacific and 10% from Latin America
- The margin of error is less than 1%; numbers may not add to 100% due to rounding

61 countries | 4 regions

Digital Trust Insights September 2019

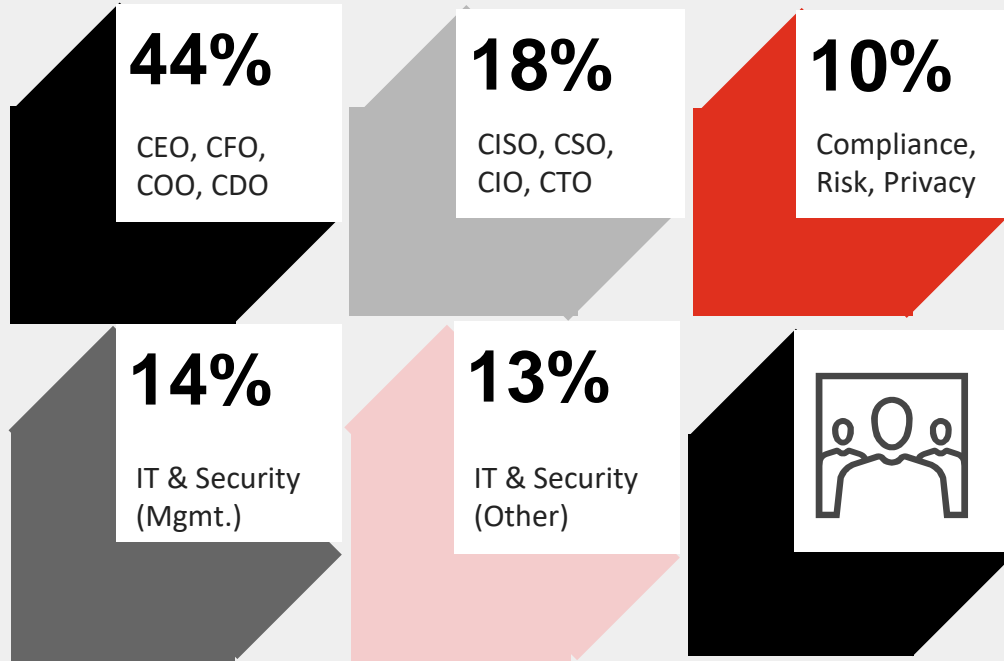
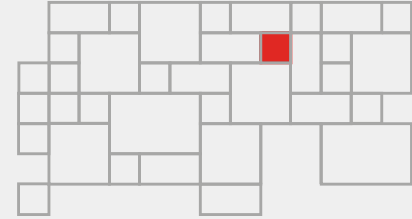


3500+

respondents

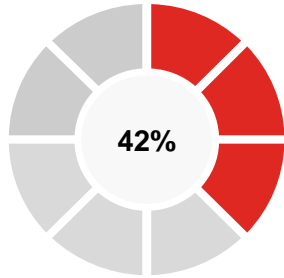
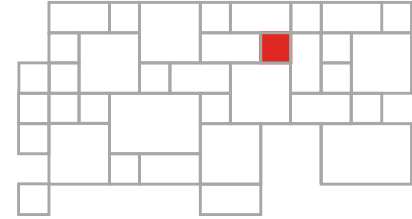
Respondents by title

Digital Trust Insights September 2019

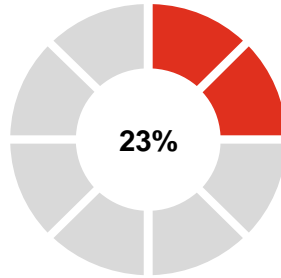


Respondents by business revenue size

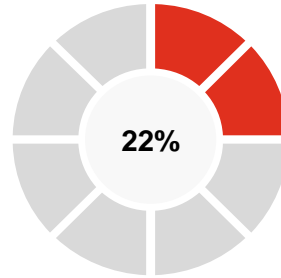
Digital Trust Insights September 2019



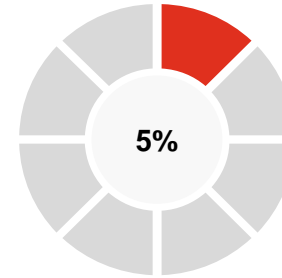
Large
>\$1B USD



Medium \$100M-
\$999M USD



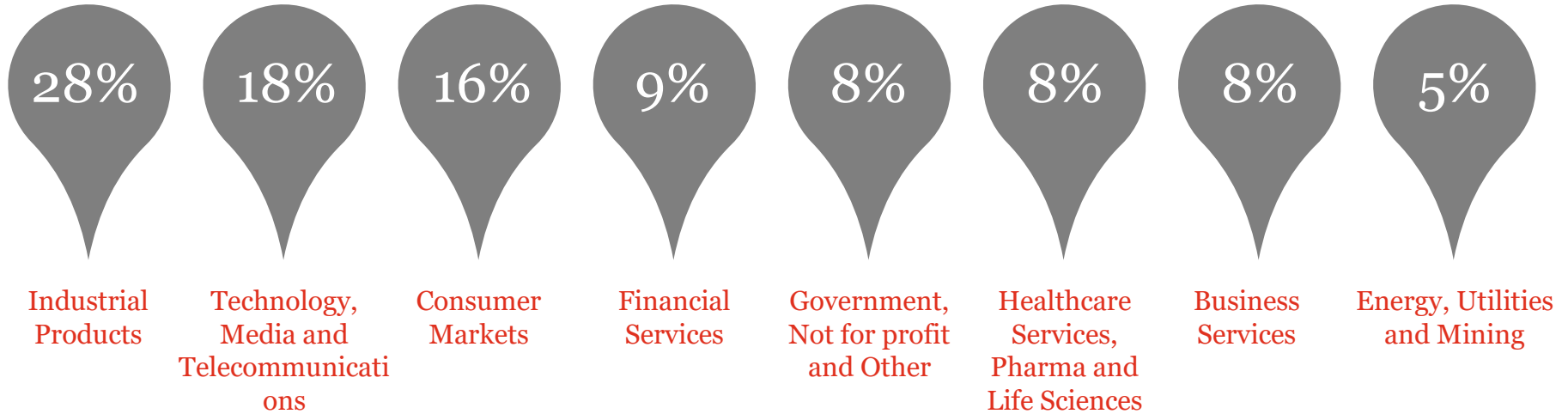
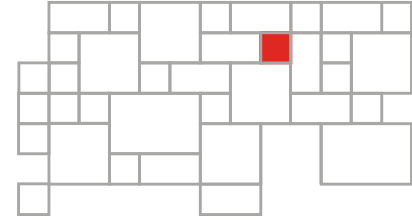
Small
<\$100M USD



Unsure/
Prefer not to answer

Respondents by key industries

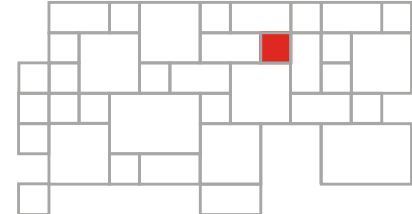
Digital Trust Insights September 2019



Appendix

Looking at the leaders

Digital Trust Insights September 2019

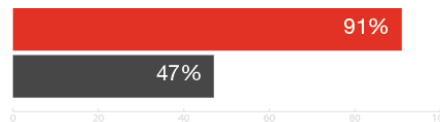


Across business and IT, leaders should excel in

- Alignment of cybersecurity function to the business objectives
- Coordination among functions to monitor and manage risks
- Risk-based approach to securing and protecting the business

■ High RQ Top 25% ■ Others

Have a full inventory of assets and refresh as needed



Applied automation to inventory core processes and assets



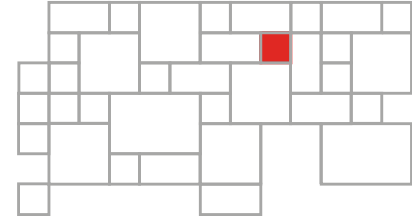
Applied automation to map dependencies



Q: To what extent has your organization done the following?
Base: 886 high-RQ; 2,646 others
Source: PwC, Digital Trust Insights, September 2019.

Looking at the leaders

Digital Trust Insights September 2019



Across IT, leaders should excel in

- Alignment of cybersecurity function to the business objectives
- Coordination among functions to monitor and manage risks
- Risk-based approach to securing and protecting the business
- NIST CSF maturity (self rating)

Contacts



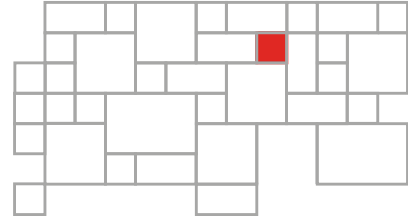
Georg Beham

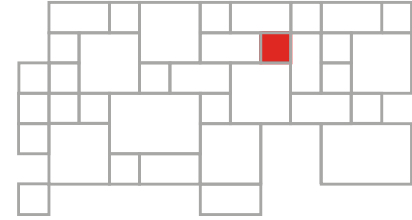
Partner, Cybersecurity & Privacy Leader

PwC Österreich

+43 732 611750

[E-Mail](#)





Thank you

For more information visit:

pwc.com/dti

pwc.com

© 2019 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.