Trusted capability in information technology and cybersecurity ecosystem visibility

Introducing:
Leader Insights Knowledge Hub

This platform provides leaders a cross line of service view of the estate articulating the IT Operations and Cybersecurity current state in one single pane of glass.

Common Operating Picture

The Leader Insights Heads Up Display showcases ecosystem behavior, including:

- **Synthesized View:** A clear and consistent IT OPS and Cyber storyline distilled into key themes for quick understanding
- **Solution:** A platform that allows organizational leaders, managers and staff to have a common view of the behavior of the IT OPS and Cyber landscape in order to take action

Value to our clients

Maintain Visibility	Continuous Monitoring & Testing	"At the Ready" Executive Level	Tool Capability to Leaders
The dashboard platform provides leaders with an updated aggregated view across both the IT OPS and Cyber organizational landscape	Provides a platform to automate controls and requirements testing for continuous monitoring in order to drive organizational maturity and adherence	The Leader Insights Heads Up Display frames IT OPS and Cyber knowledge vignettes in executive level presentation ready format that is continuously updated	The platform brings to life data from tools already employed by the organization bringing knowledge insights and leaders together reducing mean time to awareness and understanding

Results from the PwC's Global Digital Trust Insights survey indicate:

71%
of CIO / CISOs stated improved visibility to the organization's landscape is critical

52%
say Cloud transformation is a central business focus area

62%
say that their organizations are expanding their digital growth

Our strategy: Leader Insights Heads Up Display

Business benefits

- Provides a risk based aggregated view of key IT OPS and Cyber indicators
- Ongoing – continuous monitoring capability that is executive ready
- Understanding of adherence to compliance requirements
- Platform offers the ability to share the current state of security and IT operations with leaders outside IT

Target audience

- > CIO
- > CISO
- > Business Leaders
- > Risk Leaders
- > Compliance Leaders
- > Internal Audit Leaders
- > IT Operations Leaders
- > Governance Leaders

Deployment

- The platform leverages the power of Tanium and other technologies in order to harness data to create leader insights
- PwC provides the Leader Insights Heads Up Display as a service

Risk Fundamentals

➔ The platform harnesses the power of tools deployed within the environment in order to analyze the current **IT OPS and Cyber hygiene practices**

➔ The **platform details vulnerability, asset management, patching and compliance attributes** in order to provide actionable insights

Key Insights

➔ The key insights section of the dashboard articulates the **breadth of the estate**

➔ The platform **showcases how assets are being leveraged** within the organization (servers, Cloud and on-prem devices)

➔ The platform **highlights key areas of focus** from patching, abandoned assets, over leveraged application licenses, etc.

Compliance

➔ **Out of compliance endpoints** introduce a variety of risk to the environment, from allowing attackers to more easily move throughout an environment

➔ The platform **pulls forward key adherence and compliance elements** enabling staff to take action

Contact

Jon Mackey
Director
jonathan.e.mackey@pwc.com
843-446-3100

Bryon Blohm
Director
bryon.c.blohm@pwc.com
317-450-1523

Tim Stoner
Principal
timothy.stoner@pwc.com
317-418-8740

Updated as of 2/3/21

PwC's 2022 Global Digital Trust Insights Survey

About the findings

Our findings from the 2022 Global Digital Trust Insights survey of 3,602 business and technology executives around the world tell us what's changing and what's next in cybersecurity.

Key takeaways include:

- CEOs believe they give "significant" cyber support, but only 3 in 10 non-CEOs agree
- More than 50% expect a surge in reportable incidents next year
- 69% expect their cyber budget to increase in 2022
- 75% of executives report too much complexity in their organization leading to "concerning" levels of cyber and privacy risks
- 60% said that they have taken no actions that promise a more lasting impact on their third-party risk management

Target audience:

Security and IT Leaders: CISO, CIO, CTO, CSO, CPO, COO, CRO, Heads of IT
Business Leaders: CEO, CFO, President, Board of Directors

[Read our full report here](#)

5 key takeaways for all C-suite to guide you on your cyber journey:

1. **The CEO:** Frame cybersecurity as important to business growth and customer trust — not just defense and controls — to create a security mindset organisation-wide.
2. **The CISO:** Equip yourself with the skills you need to thrive in the evolving, expanding role for cyber in business. And reorient your teams, if you haven't already, towards business value and customer trust.
3. **The CFO:** Work with the CISO in taking a risk-based approach to cyber budgeting that ties to business objectives.
4. **The COO:** Map your system, especially your most critical relationships, and use a third-party tracker to find the weakest links in your supply chain.
5. **The CRO:** Strengthen your data trust processes. Data is the target for most attacks on the supply chain. Data trust and good third-party risk management go hand in hand.

Contact

Sean Joyce
US Cybersecurity, Risk and Regulatory Leader
sean.joyce@pwc.com

Joe Nocera
Cyber and Privacy Innovation Institute Leader
joseph.nocera@pwc.com