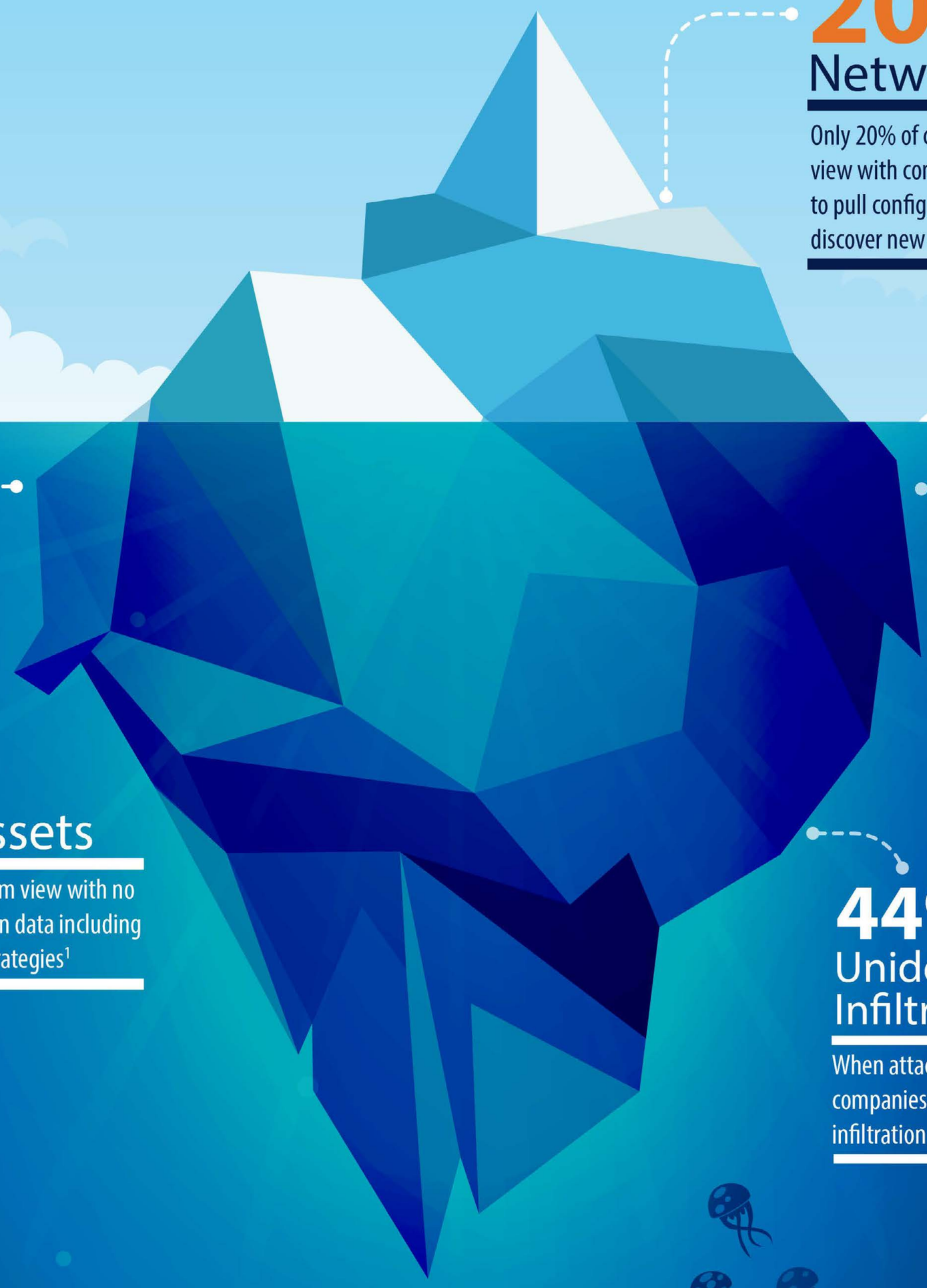
The ICS Cybersecurity Iceberg:

An incomplete inventory leaves you exposed to cyber risk



20%
Network Assets

Only 20% of cyber assets are in plain view with common protocols available to pull configuration information and discover new systems[1]

25% +
Cyber Breaches

Current employees or insiders were responsible for at least 25% of cyber breaches[2]

80%
Proprietary Assets

80% of cyber assets are hidden from view with no protocols to pull deep configuration data including I/O cards, firmware, and control strategies[1]

44%
Unidentified Infiltration

When attacked, nearly half of the companies never identified where the infiltration or infection took place[2]

Insider Threat
49%
Top Threat

Nearly 50% of power and process industry companies cite insiders as one of their top three threat vectors[2]

33% +
Successful Control Layer Attacks

Attacks that successfully breached the control system environment grew more than 33% between fiscal years 2014 and 2015[3]

50% +
OT Exploits

Exploits of OT systems soared more than 50% between 2014 and 2015[4]

© PAS Global, LLC 2017.

www.pas.com/ics-iceberg

1 *PAS, Inc.* 2014. PAS ICS Cybersecurity Case Study.
2 *The State of Security in Control Systems Today.* Tech. N.p.: SANS Institute, 2015. Print.
3 *ICS-CERT Fiscal Year 2015 Report.* Rep. N.p.: ICS-CERT, 2015. Print.
4 *Turnaround and Transformation in Cybersecurity.* Rep. N.p.: PricewaterhouseCoopers, 2016. Print.