THE BIG DATA PROBLEM IN CYBERSECURITY

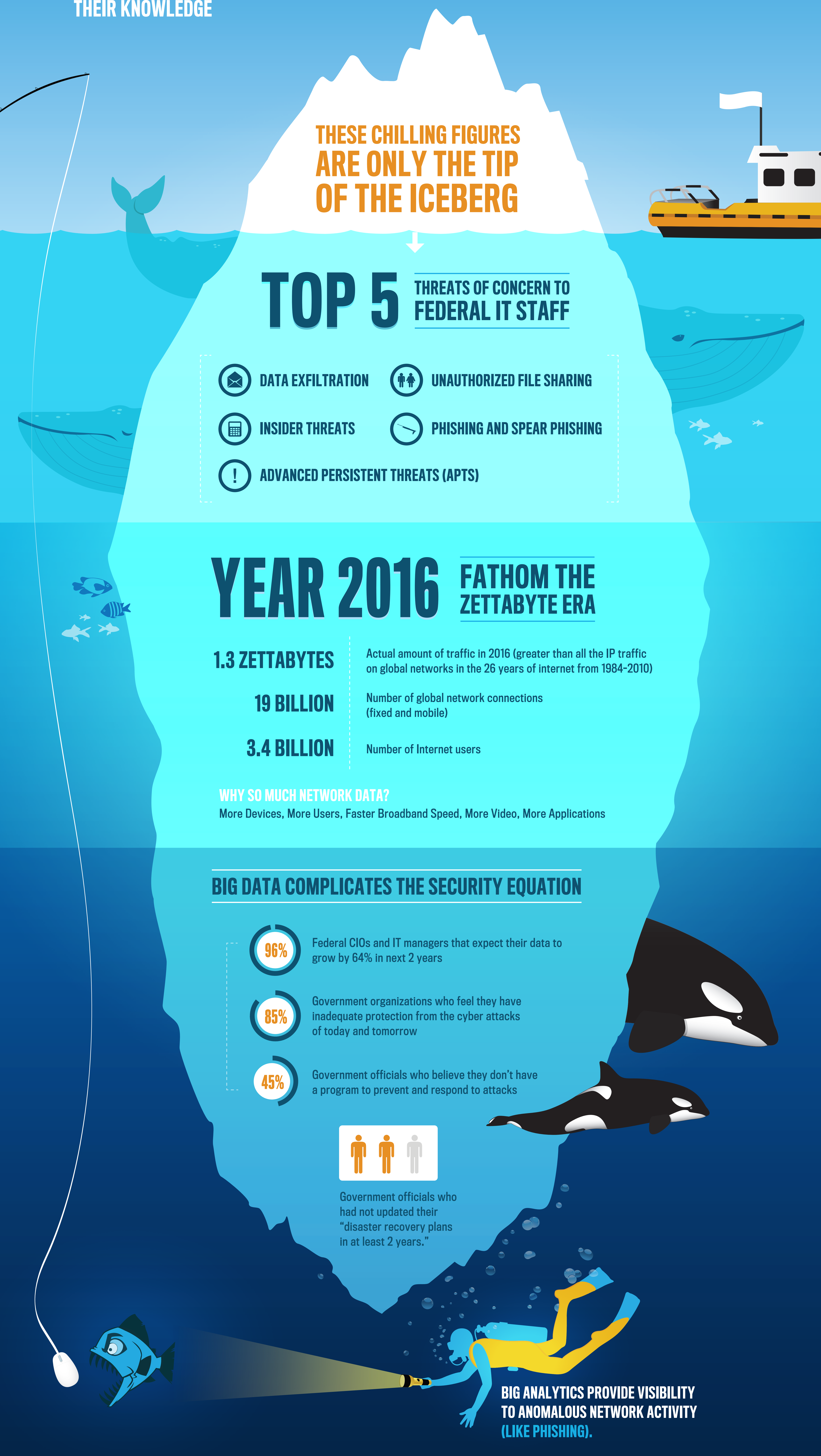
The Threat Beneath the Surface

40%
BELIEVE THEIR ORGANIZATION HAS BEEN COMPROMISED BY AN APT WITHOUT THEIR KNOWLEDGE

90%
BELIEVE CYBER ATTACKS ARE INCREASING IN SOPHISTICATION

6 Mil
DAILY CYBER ATTACKS ON THE PENTAGON

680%↑
CYBER ATTACKS ON U.S. FEDERAL AGENCIES BETWEEN FY'06 AND FY'11.



THESE CHILLING FIGURES ARE ONLY THE TIP OF THE ICEBERG

TOP 5 THREATS OF CONCERN TO FEDERAL IT STAFF

- DATA EXFILTRATION
- UNAUTHORIZED FILE SHARING
- INSIDER THREATS
- PHISHING AND SPEAR PHISHING
- ADVANCED PERSISTENT THREATS (APTS)

YEAR 2016 FATHOM THE ZETTABYTE ERA

1.3 ZETTABYTES	Actual amount of traffic in 2016 (greater than all the IP traffic on global networks in the 26 years of internet from 1984-2010)
19 BILLION	Number of global network connections (fixed and mobile)
3.4 BILLION	Number of Internet users

WHY SO MUCH NETWORK DATA?
More Devices, More Users, Faster Broadband Speed, More Video, More Applications

BIG DATA COMPLICATES THE SECURITY EQUATION

96%	Federal CIOs and IT managers that expect their data to grow by 64% in next 2 years
85%	Government organizations who feel they have inadequate protection from the cyber attacks of today and tomorrow
45%	Government officials who believe they don't have a program to prevent and respond to attacks

Government officials who had not updated their "disaster recovery plans in at least 2 years."

BIG ANALYTICS PROVIDE VISIBILITY TO ANOMALOUS NETWORK ACTIVITY (LIKE PHISHING).

TO DEAL WITH BIG DATA, BIG ANALYTICS TOOLS AND TECHNIQUES ARE NEEDED FOR REAL-TIME RESPONSE TO CYBER ATTACKS.

SECONDS OR MINUTES
Time required to capture, analyze and correlate massive amounts of network activity data from multiple sources.

100%
Amount of network data to discover patterns that discern the 99.9 % of benign traffic from the 0.1% of data that indicates suspicious activity.

FEDERAL AGENCIES MUST INTEGRATE TWO CURRENTLY SEPARATE IT SECURITY ANALYSIS SYSTEMS:

- Real-time systems for applying static rules, dynamic analysis, and filters to network traffic
- Forensic analysis systems for deep analysis, trending and discovery

BIG ANALYTICS TOOLS APPLY ADVANCED ANALYTICS TO MASSIVE DATA SETS TO

- **Extract** insights and deliver the right ones to the right people for quick action
- **Handle** the avalanche of structured and unstructured data
- **Maximize** resource efficiency, collaboration and productivity
- **Avoid** data redundancy and improve data quality and re-use
- **Improve** end results for both users and those who rely upon them
- **Reduce** data analysis time from weeks to minutes

www.Teradata.com #TDGOV

InformationWeek's 2012 Federal Government Cybersecurity Survey, TechAmerica's 22nd Annual Survey of Federal Chief Information Officers | http://www.gao.gov/assets/600/590367.pdf | 2011 Cost of a Data Breach Study: United States
http://www.informationweek.com/news/security/attacks/240001271 | http://www.meritalk.com/pdfs/big-data/MeriTalk_Big_Data_Gap_Press_Release.pdf | Symantec 2011 Internet Security Threat Report (ISTR)

EB 6657 10.12

TERADATA