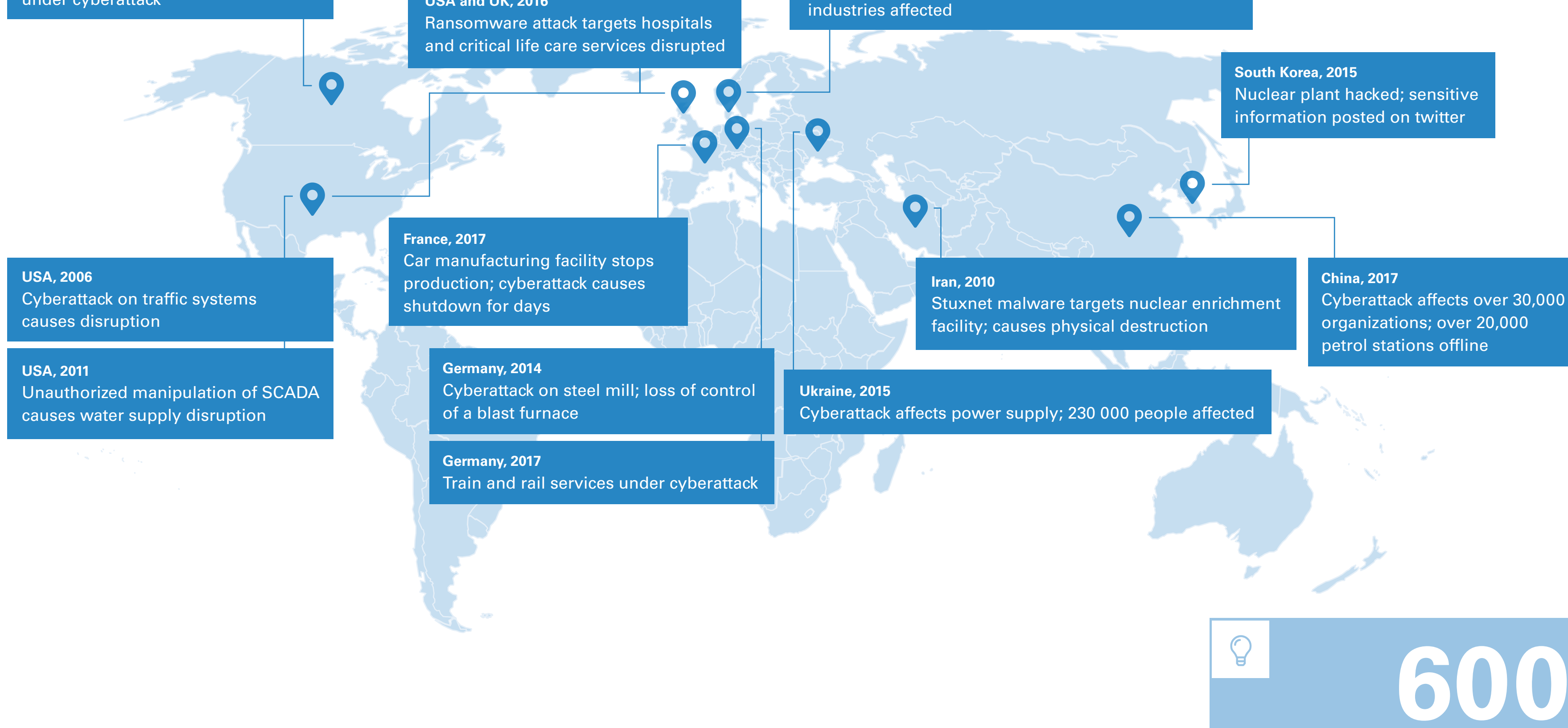


Operational Technology. Protected.



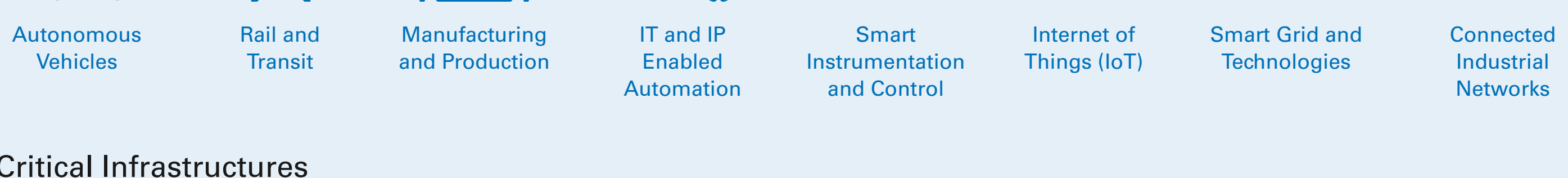
ATTACKS ON ICS AND OT SYSTEMS ARE INCREASING IN FREQUENCY AND SOPHISTICATION



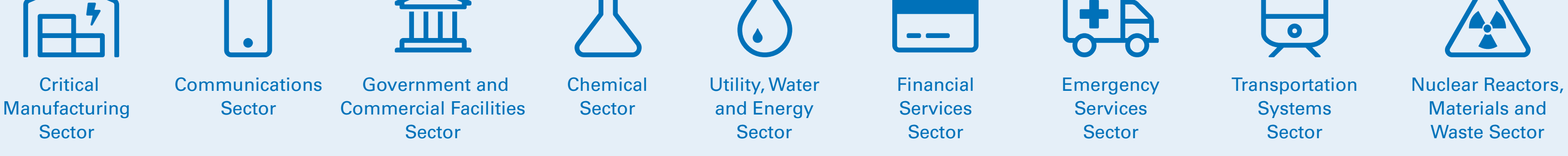
600
Billion US-Dollar
Cybercrime costs the world almost \$600 billion, or 0.8% of global GDP per year

WHO NEEDS INDUSTRIAL SECURITY?

Industries that use cyber physical systems such as



Critical Infrastructures

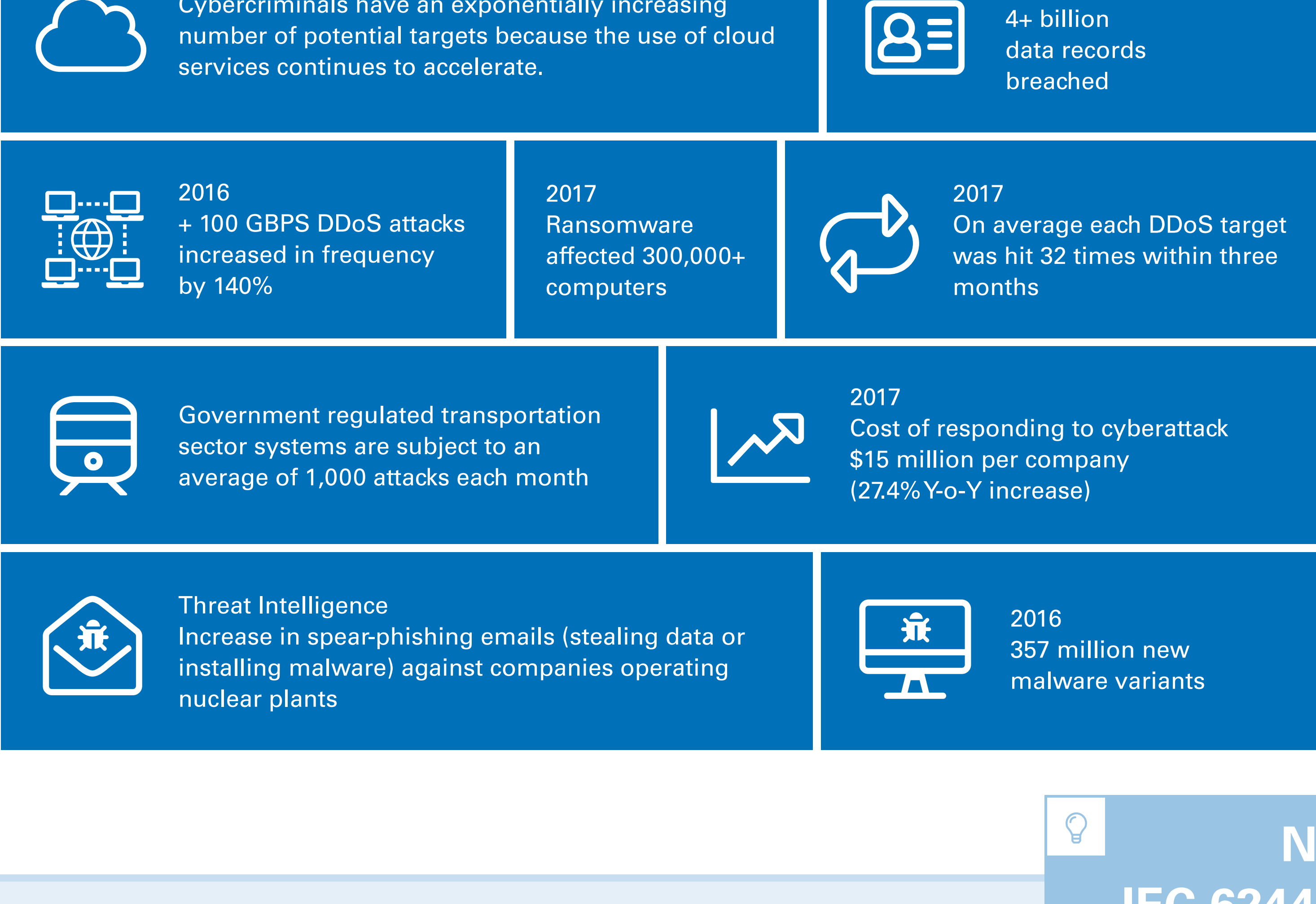


Industries which operate in a



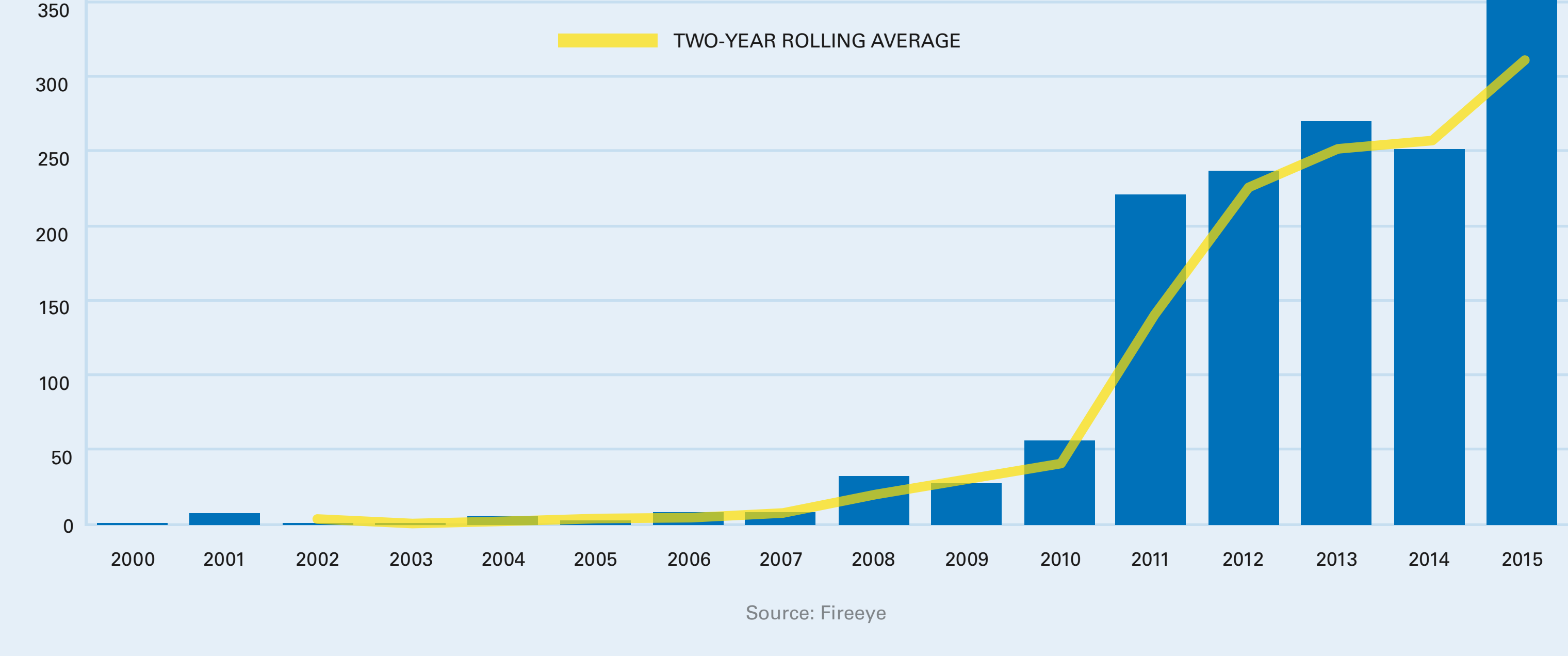
Nearly **1 Million**
new malware threats released every day

GLOBAL CYBER THREAT TRENDS

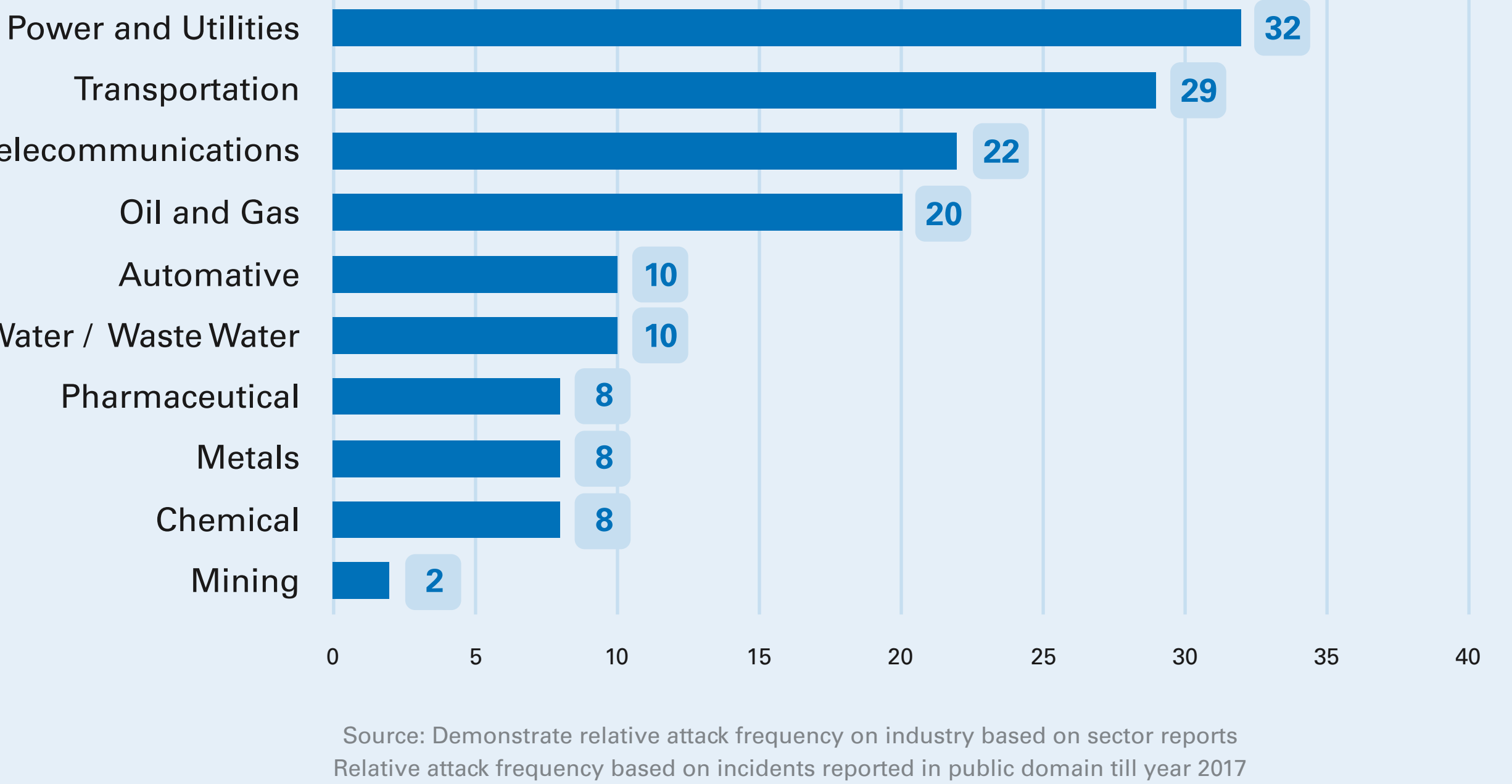


NIST CSF IEC 62443 Series
are two important standards used to help establish an effective industrial and OT cybersecurity program

EXPONENTIAL INCREASE IN INDUSTRIAL CONTROL SYSTEM AND OT SECURITY VULNERABILITIES



GLOBAL TREND OF TARGETED INDUSTRIES



4,000
daily ransomware attacks
were estimated by the FBI for 2016

2018 PREDICTIONS FOR OT AND INDUSTRIAL SECURITY

Threats

- Ransomware
- Denial of Service
- Insider (deliberate or accidental) Threat
- Intellectual Property Theft
- Cybersecurity Skills Shortage
- Lack of Understanding of the Cybersecurity Risk Domain by Functional Safety Teams

Impacts

- Failure of Functional Safety
- Disruption of Services
- Litigation and Financial Loss
- Reputation Damage
- Regulatory non-Compliance

Our Services

6 STEPS TO IMPROVE CYBERSECURITY WITHIN YOUR INDUSTRIAL AND OT ECOSYSTEM

- OT Cybersecurity Risk Assessments
- OT Architecture Review
- OT Systems Penetration Testing
- OT Policy, Process and Procedure Review
- OT Systems Incident Response and Recovery
- OT Systems Security Monitoring

MANAGING CYBERSECURITY RISKS IN OT ENVIRONMENTS HELPS TO AVOID



OUR HERITAGE: INDUSTRIAL SECURITY SERVICES FOR MORE THAN 145 YEARS

