The second annual State of Cybersecurity study by ISACA and RSA Conference shows that enterprises continue to view cybersecurity as a technology issue, not a business imperative. While cybersecurity professionals are seeing increased budgets and better alignment with strategic goals in 2016, few CISOs report directly to the CEO. The cybersecurity skills gap identified in previous years is actually widening, creating waning confidence that most teams can handle anything beyond the most basic attacks. These factors point to a critical need to educate CEOs and boards of directors on the strategic, cross-enterprise value of cyber defense and the importance of moving to a skills-based training approach to develop their cyber workforce.

**WANING CONFIDENCE**
- Security professionals are confident in their team’s ability to detect and respond to simple incidents. 82% agree.
- This has dropped 12 points from last year’s 87%.
- 75% expect a cyberattack in 2016.
- 27% say that it takes them half a year to fill a cybersecurity position.
- 59% say that fewer than half of cybersecurity job candidates were considered “qualified upon hire.”
- 30% experience phishing attacks every day.

**NEW TECH, NEW RISK**
- The State of Cybersecurity study also looked at perceived connections between risk and two emerging industry trends: artificial intelligence (AI) and the Internet of Things. Both can add significant value—if risk is effectively managed.
- Artificial Intelligence will increase risk in both the short and long term. 62% say yes.
- Internet of Things will expand attack surfaces further and exacerbate cyber risk. 53% agree.

**SITUATIONAL UNAWARENESS**
- 24% did not know if any user credentials were stolen in 2015.
- 24% did not know which threat actors exploited their organization.
- 23% did not know whether their organization had experienced an advanced persistent threat (APT) attack.
- 20% did not know whether any corporate assets were hijacked for botnet use.