The 2017 RedSeal Resilience Report

Cyber's "Perfect Storm" Looms as Four Security Fundamentals Face Crisis

Summary

The second annual RedSeal Resilience Report analyzed candid input from 600 UK and US CISOs and senior IT decision makers on the biggest cybersecurity challenges they face today. It uncovered four converging areas that put cybersecurity teams - and their organizations - at a distinct disadvantage.

1. *The threat landscape is growing faster than teams can respond*
2. *Lack of preparation is pervasive*
3. *Huge gap between perceived and true detection times*
4. *Compliance– not company strategy – drives cyber planning*

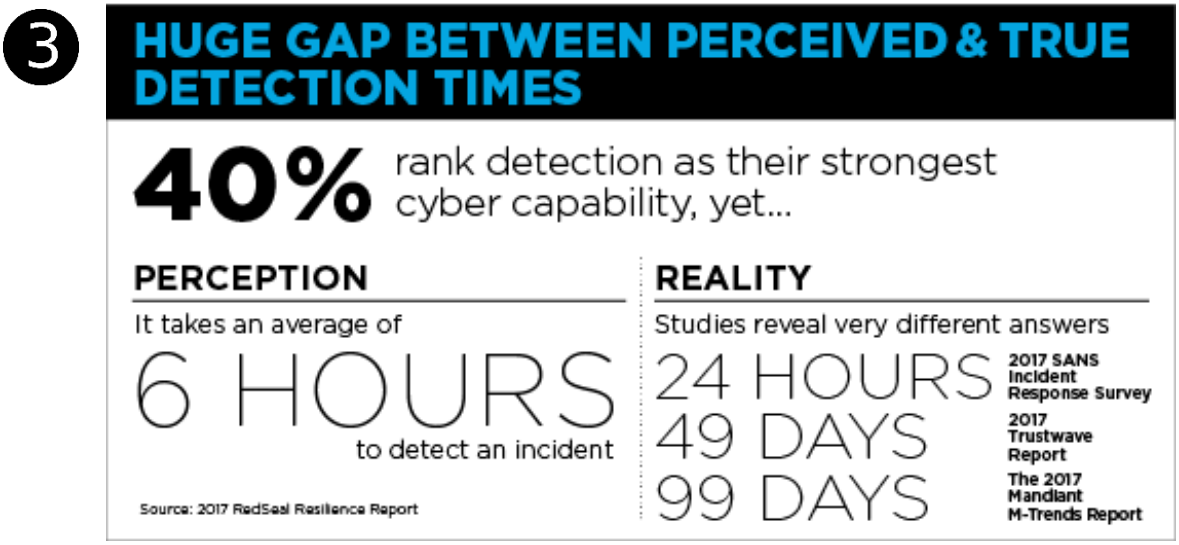
Key Findings

The burgeoning threat volume and complexity is outpacing security teams' capabilities. More than half (54 percent) of senior cybersecurity professionals think the threat landscape is evolving far faster than their organization can respond. Specifically:

- 54 percent report they don't have the tools and resources they need
- 55 percent can't react quickly enough to limit damage in the event of a major security incident
- 79 percent say their organization can't access insights to prioritize their response to an incident
- Only one in five (20 percent) are extremely confident their organization will continue running as usual upon discovery of a cyberattack or breach

Only 25 percent of respondents' organizations test their cybersecurity response to a major incident annually, if at all. It also found a strong correlation: as time since the last test increases, executives' confidence in the plan decreases.

- On average, it has been nine months since organizations created a complete blueprint, model or map of their entire network. This means pathways through their constantly changing network - and access to their most valuable assets – are neither confirmed to be secure nor clearly known at all.
- 55 percent concede they don't test their strategies frequently enough because it's resource intensive (29 percent), outside their budget (27 percent), or takes too much time (26 percent)



Once a network is compromised, a cyberattack festers until it's detected and resolved. Alarmingly, the RedSeal Resilience report reveals an industry-wide discrepancy between how long it takes from when an organization's network is compromised to when they become aware of the event.

- Perception: When ranking their capabilities, cyber pros voted "detection" as their strongest area (40 percent), with respondents reporting it takes an average of six hours to discover an incident

- Reality: Other studies of the same "time to detect" report drastically different times:
  - 24 hours (2017 SANS Incident Response Survey)
  - 49 days (2017 Trustwave Global Security Report)
  - 99 days (Mandiant's M-Trends 2017 Report)

This infers that – despite detection being considered the security teams' greatest strength – companies are struggling and not fully informed. Take for example, Sonic, which didn't know they were hacked until their credit card processor informed them of unusual activity. They acknowledged the breach – which compromised more than five million credit cards – 11 days after the first batch of cards were uploaded for sale.

Given the massive financial impact of breaches, cyber strategy should be the C-Suite's priority. However, 97 percent of respondents report that external regulations play a major role in their cybersecurity and resilience planning and implementation.

- 92 percent of organizations have had to adapt the way that they meet regulatory requirements due to the use of public cloud platforms such as AWS and Microsoft Azure
  - 12 percent of respondents' organizations had to do a total rethink
  - 49 percent had to make significant changes
- Only 27 percent are completely confident their IT systems can support these regulations
  - Therefore, 73 percent of companies which might not meet the requirements for using public clouds – such as AWS, where Deloitte faltered, and Azure, the source of hacks for Dow Jones, Verizon, and RNC to name a few –may be more exposed to attacks and breaches.

###

The RedSeal Resilience Report 2017 Methodology

The RedSeal Resilience Report 2017, an inside view into the state of the IT security industry, provides insights into strategies and challenges across the complex cybersecurity landscape. Each of the 600 CISOs, CIOs and senior IT decision makers (400 US and 200 UK) who participated had sole or majority responsibility for network cybersecurity within their organizations, 25 percent of which have more than 5,000 employees. They bring perspective from across a number of industry sectors including: retail and distribution; healthcare; technology; financial services; energy - oil and gas; manufacturing and production. Global market research firm, Vanson Bourne, conducted the research in the summer of 2017. The 2016 RedSeal Resilience Report explored the "Rise of Cyber-Overconfidence in the C-Suite," and found more than 80 percent of CEOs display "cyber naiveté," making their global organizations exposed to massive cyber-attacks.