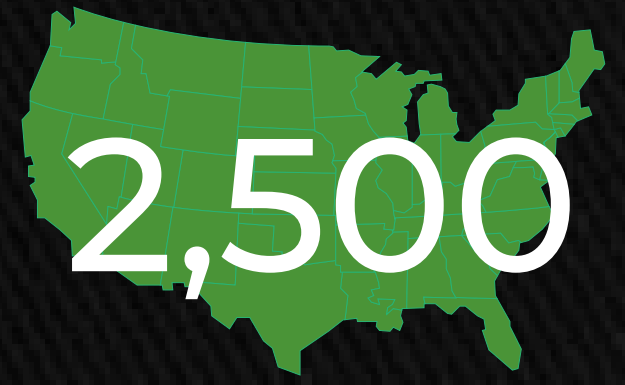# △ TeamLogic IT®
Your Technology Advisor

INFORMATION
SECURITY RISKS

52% of organizations that suffered successful cyber attacks in 2016 aren't making any changes to their security in 2017.
(Blog.barkly.com/cyber-attack-statistics)

97% of malware is unique to a specific endpoint, rendering signature-based security virtually useless.
(Webroot)

2,500 cases of ransomware costing victims **$24 million** in the US alone were reported to the Internet Crime Complaint Center.
(Turkel)

## ⚠ 7 WARNING SIGNS ⚠

1 Desktops, laptops, servers and other computing devices begin to slow, freeze or shut down on their own.

2 Co-workers, business contacts or friends report receiving spam messages from someone using a company email address.

3 Computer systems make processing sounds continually, even when not being used.

4 Web browsers switch automatically to other sites or search engines.

5 Unusual pop-up windows appear (even when not connected to a wired or wireless network).

6 Error messages multiply and cannot be resolved.

7 Data backup processes fail, improperly save files or generate error messages.

Q2 2016 malware traffic expanded for the fourth straight quarter. **5.7 billion messages** contained malware, mostly from ransomware. Botnet distribution of malware remained a popular conduit.
(Appriver Global Security Report)

5.7 BILLION

On average, **4,000 ransomware attacks occurred per day** in 2016, according to a report from the FBI in June 2016.

4,000 RANSOMWARE ATTACKS / DAY
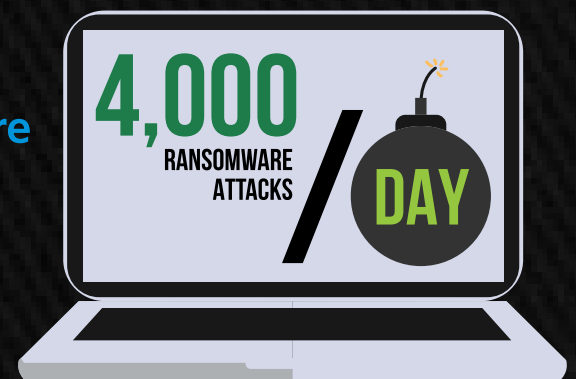
The amount of phishing emails containing a form of ransomware grew to 97.25% during Q3 2016, up from 92% in Q1 2016.

97.25%
92%
(PhishMe Malware Review)

390,000 malicious programs are registered every day by AV-Test Institute
(AV-TEST)

In Q3 alone, **18 MILLION** new malware samples were captured.
(Panda Labs)

500+ malware evasion behaviors used to bypass detection are being tracked by researchers.
(Kruegel)

15% of new files are malicious executables
(Webroot)

98% of Microsoft Office-targeted threats use macros
(Microsoft)

50% increase in email attacks where macros are the method of infection
(Tim Gurganus)