CalTech

The Top 10

IT Health Gaps of 2019

Every year, CalTech monitors, tracks and records the most common gaps we see with new clients as a part of our IT Operations Assessment These are the top 10 IT gaps we're seeing in 2019, from 10 to 1. Curious? See how you stack up.

10 ***Disaster Recovery solution*** does not match up with the recovery needs of the organization. Also, DR solution is not thoroughly and regularly tested. The organization only learns of its inadequacy during a disaster.

9 ***Lack of proactive/strategic planning***. As a result, IT departments end up in a constant state of playing catch up.

8 ***Inadequate patch management solutions,*** resulting in many devices not receiving the latest updates and leaving the organization at greater risk of compromise.

7 ***Large amounts of Windows 7 and Server 2008 devices*** on the network. Note: such devices must be upgraded/replaced by January 2020 (end of life date).

6 ***Inadequate IT support staff.*** As a result, end users are often left waiting for IT issues to be resolved, negatively impacting productivity.

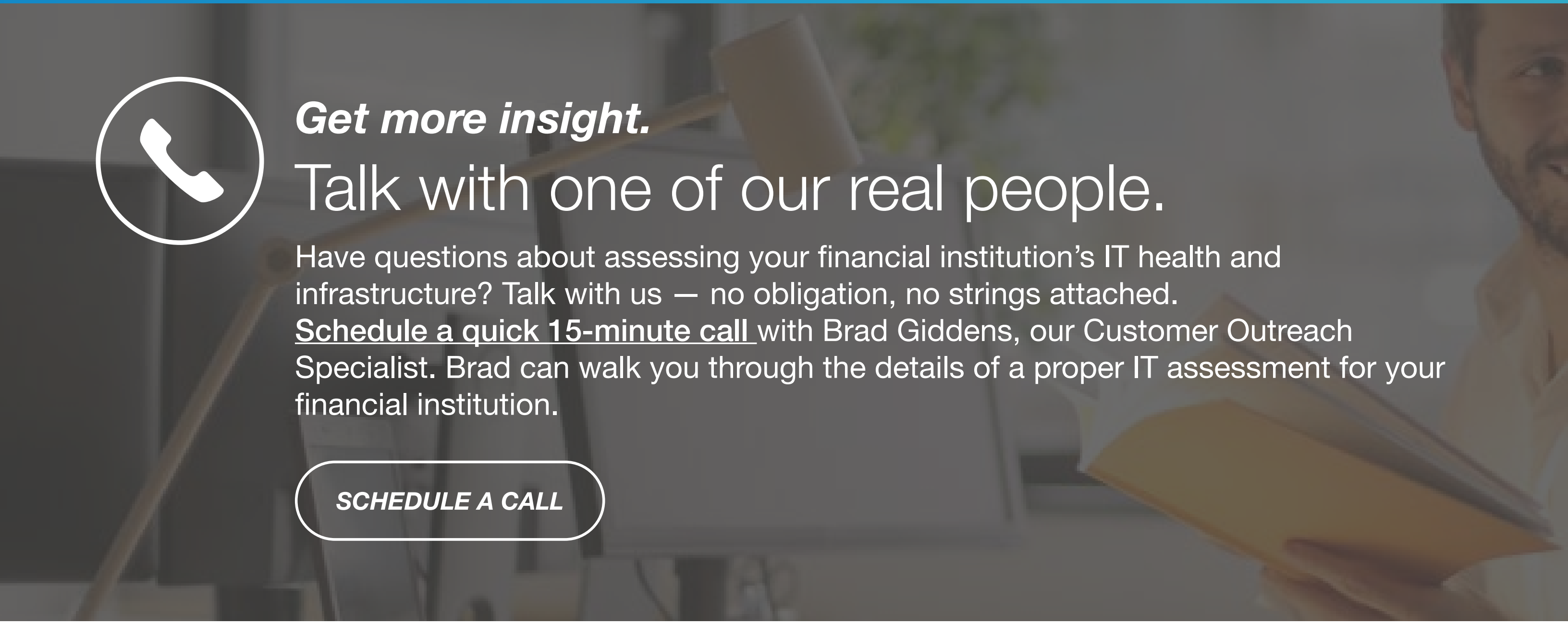
5 ***Customer not taking advantage of*** the benefits of secure cloud-based offerings (e.g. Organization has large amount of physical/virtual servers to manage and maintain, versus moving to a secure offsite 24x7-monitored facility).

4 ***WAN/Internet connectivity contracts*** have been in place for years without review. Prices on these services typically drop every year. Many organizations are overpaying by thousands every month.

3 ***Lack of employee cybersecurity training.*** Note: employees are an organization's most important line of defense against cybersecurity threats. Industry data shows that upwards of 90% of security compromises are caused by an employee clicking a malicious link.

2 ***Lack of Multifactor Authentication*** on all external services: email, VPN, etc. This is an integral part of hindering or stopping common cybersecurity threats.

1 ***Email compromise*** due to employee giving up credentials as a result of a phishing email. Note: This is one we very commonly see — with compromised credentials, attackers download complete copies of a user's mailbox, often compromising further personal information of employees and/or customers, and then email all of the user's contacts to continue the attack. Many institutions have been forced to notify all customers that their personal information may have been compromised.



Get more insight.

Talk with one of our real people.

Have questions about assessing your financial institution's IT health and infrastructure? Talk with us — no obligation, no strings attached. Schedule a quick 15-minute call with Brad Giddens, our Customer Outreach Specialist. Brad can walk you through the details of a proper IT assessment for your financial institution.

SCHEDULE A CALL