RISE OF THE REMOTE WORKFORCE

PART 2: SOC CERTIFIED TECHNOLOGY PARTNERS ARE NO LONGER A RECOMMENDATION, BUT A NECESSITY

AN XAMIN WHITEPAPER

> “Two-thirds of consumers would no longer do business with a financial institution whose detection and response were deemed slow and inept.”

Community banks and credit unions continue to be a preferred target for cybercriminals because smaller organizations -- with limited IT budgets and lower profiles -- are an easier mark for bad actors. Now, as the remote workforce expands a financial institution’s security perimeter beyond the walls of its branches and into the homes of its employees, the threat of attack to small and midsize financial institutions is no longer a question of *if*, but *when*.

Organizations forced to integrate work-from-home (WFH) options into their plans have seen the risk-perimeter expand to include the devices of employees sitting in their living rooms, minivans and local coffee houses. On one hand, the tier-one organizations have always had the resources and budget to ensure accountability for end-to-end risk in this environment – positioned for optimal *detection* and *response.* However, on the other hand, small and mid-sized businesses (SMBs) are often caught flat-footed when faced with a cyber incident. The implications of this are devastating. In fact, according to a recent survey by Banking Dive, two-thirds of consumers would no longer do business with a financial institution whose detection and response times were deemed slow and inept.

To address these concerns, SMB financial institutions have been partnering with managed service providers (MSPs) for their technology needs. MSPs can assist by acting as either an alternative to in-house IT departments or as an extension of the IT department – an added layer of security and service. As more banks, credit unions and reputation-sensitive organizations turn to MSPs, it is imperative that they hold their IT providers to the highest standard of compliance and accountability. This is where the SOC 2 comes in.

WHO SETS THIS STANDARD? AND WHAT IS SOC 2?

We’re glad you asked...

In response to concerns by leaders in the financial services industry on oversight and dependability of third-party IT security service providers, the American Institute of CPAs (AICPA) created a system of audits and reports called Service Organization Control -- SOC. While the SOC is a full suite of oversight solutions, the SOC 2 framework focuses specifically on the security and protection of customer data. And, an MSP holding a SOC 2 certification demonstrates they are invested in providing the highest standard of security in caring for this critical information.

HOW DO TECHNOLOGY PROVIDERS OBTAIN THIS CERTIFICATION? AND HOW DOES THAT PROTECT MY FI?

To achieve the SOC 2 certification, an MSP must go through an external audit of their systems and controls, which is conducted by an independent AICPA-licensed third-party organization. During this audit, MSPs are required to prove that they have effective internal controls in place and an ability to follow strict information security policies. A successful audit means the MSP is accountable to the AICPA's five "Trust Principles" for working with financial institutions: *security, confidentiality, availability, integrity and privacy*, so executives can trust that a SOC 2 MSP is managing risks appropriately.

Just as hackers and other "bad actors" are always looking for vulnerabilities, so too are the regulators responsible for oversight of financial firms. Just last year, the FDIC released a letter, FIL-19-2019, encouraging financial institutions– as part of their due diligence – to ensure that business continuity and incident response risks be adequately addressed in service provider contracts. However, with this certification, the audit is conducted annually, guaranteeing that compliance is *ongoing*, which can work in the financial institution's favor in the eyes of examiners -- speeding up their own audit process as it pertains vendor due diligence and the IT infrastructure review.

Additionally, it is recommended that any organization hosting consumer records in the cloud should work to minimize risk and exposure by meeting the criteria of the SOC 2 report. The tier-one financial institutions have already embraced the SOC and are accountable to SOC standards for security compliance, and it is our belief that low and mid-market organizations will also soon be required by regulators to comply with these same standards. When working with technology providers, it's important to ensure they are also adhering to the SOC 2 standards – working to keep your institution and its data safe.

> "The financial services industry contributed 62% of exposed data in 2019, according to a Bitglass report."

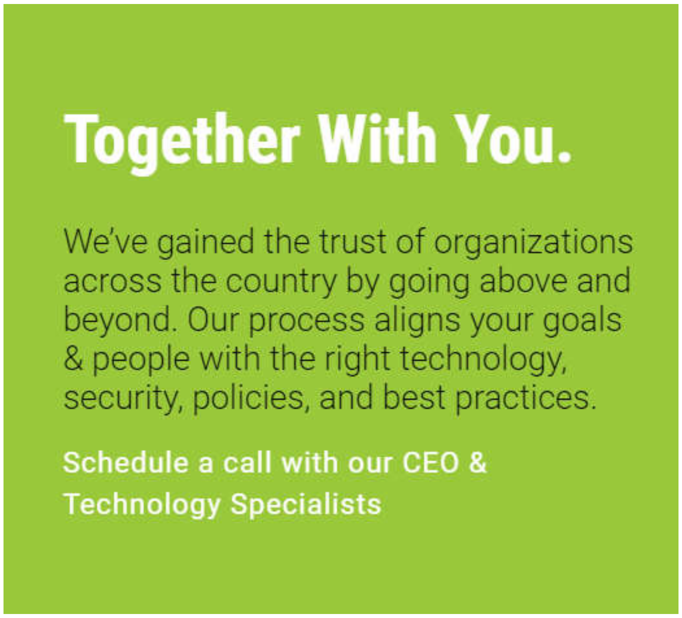
Cybercrime is a daily occurrence and is often unavoidable, and the rise of the remote workforce and move to a more distributed environment presents new challenges in accountability. Having a SOC 2 certified technology provider managing risk and protecting consumer data gives business leaders confidence, especially when entrusting critical data to an outside IT management provider.

Whether your employees are back in the office, working from home or some combination of the two, using a SOC certified technology provider is no longer just a recommendation – it is a necessity.

Xamin has helped financial institutions for over 20 years align goals & people with the right technology, security, policies, and best practices.

STAY TUNED FOR PART 3: FLEXIBLE WORKPLACE MEANS MORE THAN JUST 'REMOTE' WORKPLACE

ABOUT XAMIN



Together With You.

We've gained the trust of organizations across the country by going above and beyond. Our process aligns your goals & people with the right technology, security, policies, and best practices.

Schedule a call with our CEO & Technology Specialists

Infrastructure | Security | Data Protection
Cloud | Professional Services

1-844-44XAMIN
www.xamin.com