Securing Your Remote Call Center Environment

Many businesses with call centers are implementing remote work environments or expanding their existing remote workforce. For some, this is a way to achieve social distancing in response to the coronavirus pandemic. Others are looking to realize remote work benefits such as reduced costs, improved employee retention, scalability to meet demand, follow-the-sun support, or ability to provide business continuity during extreme weather or natural disasters.

While remote call centers offer many benefits, they also come with unique security challenges. Fortunately, Tevora's team of security specialists has extensive experience securing these environments for some of the world's largest companies. We can be a trusted partner to help you protect your valuable systems and data as you expand your remote call center workforce.

Risk Assessment

We recommend starting with a risk assessment. This gives you a clear view of all risks associated with your remote call center environment and identifies security weaknesses that should be addressed to ensure your network, systems, and data are protected against cyberattacks. Tevora uses its proven HydraRisk method, which relies on quantitative and repeatable processes, to help you identify and prioritize risks.

Risk Mitigation Plan

Once your remote call center security risks have been identified, Tevora can help you develop a prioritized risk mitigation plan to address security gaps. Based on our extensive experience working with clients, some of the areas that frequently require security improvements are:

- **Policies and Procedures**—many companies have not updated their policies and procedures to address the unique security risks associated with remote call centers. For example:
    - Are personal devices allowed? If so, are there restrictions on functions that can be performed on these devices?
    - Are remote agents required to use VPN’s or data encryption technologies?
    - What methods will be used for authenticating remote agents (e.g., multifactor authentication)?
    - Are there specific functions that cannot or should not be performed by remote agents due to security constraints?
    - Should remote agents follow different procedures to protect personally identifiable information?

- **Systems and Technology**—Unique systems and technical solutions are often needed to secure remote call center environments. For example:
    - Systems to ensure remote users are assigned appropriate privileges and permissions for accessing corporate network systems and resources.
    - Data Loss Prevention (DLP) tools to ensure sensitive data is not being lost or accessed by unauthorized users.
    - Technologies and tools to meet the encryption, VPN, and authentication requirements for remote users.
    - Specialized systems to ensure remote call center agents can securely process credit card and other payment information.
- **Monitoring**—Special capabilities may be needed to monitor activity in your remote call center environment to ensure it stays secure on an ongoing basis. For example:
    - Monitoring tools to determine if remote call center agents are inappropriately sharing sensitive information with outside parties.
    - Routine data scans and manual inspections of devices used by remote agents to look for evidence of compromise or cases where agents are not following recommended security policies and procedures.

In addition to helping you develop a risk mitigation plan, Tevora's experienced team of security specialists can partner with you to implement the recommendations identified in the plan.

Compliance

If your industry is one in which you must demonstrate compliance with industry-specific standards, Tevora's expert compliance team can work with you to audit your remote call center and prepare the necessary reporting to demonstrate your compliance to the appropriate standards organization(s). We are fully qualified to assess compliance with the following industry standards:

- PCI DSS
- PA-DSS
- P2PE
- HIPAA
- NYS DFS
- ISO 27000
- CSA Star
- HITRUST
- FISMA
- FedRamp
- DFARS
- SOC
- NERC
- FERC

Remote Support in the Time of Coronavirus

While we love working with clients on-site, we are fully equipped to work with you remotely to help secure your remote call center environment. This allows you to get started on this important work now as we all wait for the coronavirus pandemic to subside.

If you'd like to speak to an expert to get more information on how Tevora can help you secure your remote call center environment, give us a call at (833) 292 1609 or email us at sales@tevora.com.