5 Technology Advances

Creating a More Secure Work-at-Home Business Model

By Jim Farnsworth, *Executive Vice President & General Manager*
Sykes Enterprises, Incorporated

I've described in past articles how working from home is transforming American industry and jobs. This is no idle claim. The single largest demographic in the US labor force is millennials, who have very different expectations regarding the flexibility an employer should offer to their employees.

In addition to changing employee expectations, there are several business and social drivers that make incorporating a work-at-home (WAH) strategy more attractive to employers:

- Most work-at-home employees report higher productivity and reduced stress levels
- Employers can access a much larger labor force with a deeper pool of talent and highly specialized skills
- Studies have shown work-at-home employees are more engaged with their job and employer

With 45 percent of the American workforce now spending much, or all, of their time working from home, c-suite executives are beginning to recognize the benefits of a home-based workforce. However, one of the primary concerns for every business contemplating a work-at-home employment strategy is always security.

Over the past 20 years, technological advances have literally transformed our ability to not only recruit, hire and train remote employees, but also to keep those employees and the business environment safe and secure. When properly integrated, the following five tactics can help ensure your remote workers are as secure as their brick-and-mortar counterparts. These strategies focus on creating a secure work-at-home environment for customer-engagement agents, and can also be applied to other industries or types of remote-work models.

Ensure you are PCI compliant.

The Payment Card Industry Data Security Standard applies to companies of any size that accept credit card payments. You need to plan how your IT system securely stores customer information, how you will protect that data from any security breach and how your firewall can allow secure remote access. The industry best-practice security standards fall into 12 major areas, providing a comprehensive security framework that should be your baseline.

Use multi-factor authentication or biometrics for access.

Multi-factor authentication (MFA) is commonly used to ensure that only authorized users can access a controlled system. The simple way to think about it is "something they know and something they have." Users already "know" the something as — a username and password for most systems. A system with MFA will then prompt for information that needs to be retrieved from an additional device — "something they have" — such as a numeric key fob or other client device.

The user can only login by correctly passing through both levels of authentication. Given the low cost today of biometric-scanning devices for fingerprints, palm prints or eyes (retina scans), it is also feasible to consider biometric tests in addition to passwords. Remote workers should never be able to access your system just because they know a username and password.

Insulate personal or financial information with automation.

You can protect both your customer and your employees by using automated systems to handle personal financial information, for example, when taking payment from a customer. The human agent can pass the customer over to an automated Interactive Voice Response (IVR) system at the time payment card details are required. Once the card has been processed, the customer will then be returned to the agent. Automating the capture of financial or personal information ensures that the agent never hears or has access to this information.

Lockdown the PC desktop.

Your remote workers will be using standard PC equipment connected to the Internet, but certain minimum standards such as an antivirus firewall will be required in addition to basic protection. All non-business functionality will need to be locked down and unavailable when the system is being used for your business. This means that functionality such as printing the screen or saving data to the hard drive must be disabled. Virtual Desktop Interface (VDI) applications are sophisticated tools that allow a secure environment to be created — by harnessing these tools and only allowing remote employees to access from a locked and controlled cloud system, you will ensure a more secure environment.

Encrypt those calls.

In everyday life, most people are already using end-to-end encryption when they send messages using apps such as WhatsApp or Skype. Any communication undertaken by your remote workers needs to utilize similar levels of encryption, so if their connection is hacked it will be impossible to make sense of the data transfer — only the sender and receiver will have the key to the encrypted communication stream.

Creating a culture of security by offering training to your remote team is also extremely important, because the team may spot attempted security breaches even before your security team does. This security-first culture, combined with the approach I have outlined in these simple measures, addresses the three most significant security challenges that any work-at-home model has to contend with:

- **The desktop:** Controlling the desktop so that the agent has no opportunity to record any personal customer information
- **The network:** Eliminating the chance of access to the system via a hacked network
- **Personal data:** Payment shielding so detailed personal information is never shared — even if a rogue agent takes a job with the intention of stealing data, they will not have access to any personal payment information

Jim Farnsworth

Executive Vice President and General Manager

Jim Farnsworth serves as EVP & GM, Virtual Operations, Education, Travel & Consumer Products at Sykes Enterprises, Incorporated. He leads SYKES' Work At Home business group, internal shared services and a portfolio of industry solutions. Mr. Farnsworth has a demonstrated history of innovation, service and leadership for large-scale businesses and their customers over the past 20+ years. Mr. Farnsworth has successful experience leading outsourced and contracting arrangements with clients ranging from small businesses to Fortune 2000® companies around the world and has developed complex customer solutions for some of the world's leading brands.

ABOUT SYKES

Sykes Enterprises, Incorporated is a leading provider of multichannel demand generation and customer engagement services for Global 2000 companies and their end customers. SYKES' differentiated full lifecycle solutions and services — digital marketing, sales expertise, customer service, technical support and more through multichannel delivery platforms — effectively engage customers at every touchpoint of the customer journey. Our complete service offering helps clients acquire, retain and increase the lifetime value of their customer relationships through cost-effective solutions that enhance the customer service experience, promote stronger brand loyalty, and foster high levels of performance and profitability.

SYKESinquiries@sykes.com
www.sykes.com

SYKES®