Business Continuity
Tips & Lessons Learned in the Time of COVID

For the May edition of the AmeriHome Angle, in the spirit of providing meaningful and timely content for our clients, partners and prospects, we spoke with key members of the AmeriHome Business Continuity Team to learn more about the deployment of the AmeriHome Business Continuity Plan (BCP) during the current pandemic. While a BCP is likely to be part of every business's policy playbook, plans can never fully contemplate every scenario, and never comprehensively predict the effects the incident will have on physical locations, financial markets, federal, state, or local governments and laws. In this article, we will share AmeriHome's successes, as well as the lessons we've learned, since the decision was made to send employees to work from home on March 16, 2020.

AmeriHome's response to the Safer-At-Home Order issued by the state of California on March 19, 2020, was decisive, swift and by most measures, fairly seamless. Founded in 2014, AmeriHome had always been diligent about ensuring its data was secure and accessible from remote locations through establishing redundant data sites, as well as ensuring business could continue throughout a disruptive event by having a sound, tested BCP in place.

Shortly after AmeriHome Headquarters moved to Westlake Village, California, the Woolsey Fire ignited approximately 10 miles northeast of the new location. Within hours, its headquarters was squarely in the path of the fire, and the facility was under a mandatory evacuation which remained in place for three business days. Because much of the surrounding areas were also under evacuation orders, many employees could not even go home. Ultimately, AmeriHome was able to mitigate disruption to operations by mobilizing the workforce virtually and transitioning work where needed to the Dallas facility. The lessons learned from that event set the stage for our future response to the Coronavirus Pandemic.

Chase Wixom, SVP Business Operations, spoke to the formation of our Business Continuity Plan structure:

"Building on the lessons learned from the Woolsey fire, throughout much of 2019 and into early 2020, we conducted Business Continuity and Disaster Recovery tabletop exercises at all sites, and as a result, AmeriHome:

- Built a multi-level communications structure to address frontline, escalated, and executive-level communication and decision making;
- Updated its company-wide business continuity policies;

- Developed documented processes, defined roles, and established routines; and
- Formed various layers of support: Department BCP representatives, Crisis Management Team, Incident Management Team, and Executive Steering Group.

"Without this structure, we would not have been able to mobilize and communicate as effectively as we did in the current event with very little, if any, loss in productivity, while maintaining alignment with our control framework."

Ron Luker, FVP Information Security Officer, shared a few reasons AmeriHome's transition to work-from-home was smooth, as well as a few unexpected challenges:

"The first challenge we faced was the lack of system hardware inventory in the market, so we were forced to have many employees take home their desktop computers. This required manual whole-disk encryption of each desktop computer. We didn't need to add any new security measures since remote network access (VPN and AWS Workspaces) was already locked down. In addition, we had several key security controls in place well before the pandemic, including:

- Multi-factor user authentication;
- Machine authentication (only company owned assets allowed on VPN);
- Event logs (Event logs collected from AWS and our VPN Firewalls are sent to our Security Event and Incident Management (SIEM) system for analysis and correlation); and
- Antivirus, data loss prevention, and firewalls installed on all machines connecting to our internal network.

"One other contributing factor to our success in switching to remote work was having a mature single-sign-on (SSO) system, OKTA, in place:

- SSO is a centralized session and user authentication service in which one set of login credentials can be used to access multiple applications.
- It is great for productivity, IT monitoring and management, and security control.
- With one security token (a username and password pair), user access to multiple systems, platforms, apps and other resources can be enabled or disabled.
- An SSO also reduces the risk of lost, forgotten or weak passwords.

"Having OKTA in place helped reduce the Help Desk workload, freeing up technology support resources to focus on ramping up remote resource availability, rather than having to constantly reset user passwords and provision user access to systems and applications.

"The main challenge that we faced as a team was establishing a new baseline for what normal user behavior looks like. To better understand this, we have been using an application known as User and Entity Behavior Analytics (UEBA).

- UEBA is a type of cyber security process that first takes note of the normal conduct of users.

- It can then detect any anomalous behavior or instances when there are deviations from "normal" patterns.

"Shifting nearly all of our entire workforce to remote work in such a short period of time put this system into overdrive, as employee working hours and patterns changed. Until a new baseline was established, this led to the Information Security (InfoSec) team's investigating many alerts that turned out to be false positives. Prior to the remote work environment we were averaging about 300 investigations per month, and in the first 30 days after, that number increased to over 1,100."

Shelley Tam, EVP Human Resources, provided these keys for success:

"Having all Human Resources (HR) processes automated through an integrated Human Resources Information System (HRIS), and having previously documented the appropriate desktop procedures enabled us to work-from-home much faster and to facilitate responses to employee questions. Additionally, HR:

- Took an active role in convening players, contributed to overall discussion and plan, and drafted communications to the employees at large;
- Actively addressed individual issues/concerns, specifically employee health and safety;
- Remained a voice of reason, focusing on the employees and making sure they knew that we cared about them personally;
- Provided health and wellness resources;
- Communicated and over-communicated; and
- Modified recruiting and training strategies to go virtual such that we could continue to recruit, onboard, and retain remotely."

Shelley emphasized that over-communicating across multiple platforms is critical, noting that no one will look back and complain about having had too much information. Communications channels HR continues to utilize include:

- Corporate announcements
- Site-specific communications
- Internal webpages and social media platforms.

These notes from Chase, Ron, and Shelley represent just a fraction of the coordinated efforts by AmeriHome associates that have made our adaptation to a new working environment a smooth and thus far successful transition.

At an appropriate time in the coming months we will review our actions, interview associates, and further evaluate gaps to determine how effective our overall response was to this unprecedented event. With that being said, we have already identified and begun to learn from some gaps:

- Vendor assessments - Obviously this event was unprecedented, however, gaps were identified in our key vendors' recovery plans, for which AmeriHome had to quickly develop solutions.
- Hindsight - While we did form our Coronavirus Incident Management team in early February to track the progression and impact of the virus, there were proactive measures we could have taken to better support and streamline our work-from-home efforts, including preemptively encrypting desktops and creating additional hardware inventory.
- Varied maturity of departments - Through our 2019 and 2020 recovery testing exercises it became clear that there were departments that had not yet developed clear and concise recovery playbooks. Unfortunately, due to timing, we were unable to upskill those departments prior to this event to the optimal, desired degree. While the existing playbooks did greatly assist us in resource allocation, assigning more resources to the support of those departments with limited recovery plans, it still caused a more staggered response and some associate unease.

In summary, in a world with natural disasters and pandemics, it's more important than ever to have a thorough, well-tested, and secure business continuity plan. We hope to convey here that, while we have so far been fortunate in this transition due, in part, to our previous disaster recovery experience, plenty more lessons have been learned; things that we will plan for and do differently should there be a need in the future. AmeriHome associates have been truly amazing, like many impacted, in their resilience and ability to adapt to a new reality, and for that we are truly grateful.

We hope that you and your teams are staying healthy and productive, and we hope to see you in person or on a video call sometime soon!

This article is solely intended to provide an overview of AmeriHome's implementation of their business continuity plans. Readers should not rely solely on this information to create their own business continuity plans.