CASE STUDY

mather lifeways®
Ways to Age Well

Contributor:

Charles Sankovich

Assistant Vice-President, Information Technology

LeadingAge® CAST
center for aging services technologies

The LeadingAge Center for Aging Services Technologies (CAST) is focused on accelerating the development, evaluation and adoption of emerging technologies that will transform the aging experience. As an international coalition of more than 400 technology companies, aging-services organizations, businesses, research universities and government representatives, CAST works under the auspices of LeadingAge, an association of 6,000 not-for-profit organizations dedicated to expanding the world of possibilities for aging.

For more information contact:

Zohra Sirat, Project Manager, CAST
zsirat@LeadingAge.org
(202) 508-9438
LeadingAge.org/CAST

BLUE ORANGE® COMPLIANCE

Conducting Table-Top Cybersecurity Exercises Improves Awareness, Preparedness, and Response

Categories

Improved Compliance
Improved Staff Education about Data Security and Privacy
Response to Cybersecurity Incident (breach, ransom, loss of mobile device(s), phishing, etc.)

Organization Name

Mather LifeWays

Organization Type

Life Plan Community

Other Partners

BlueOrange Compliance

Organization Description

Mather LifeWays is a non-denominational not-for-profit organization dedicated to serving older adults. Founded in 1941 by humanitarian Alonzo Mather, we have a long history of creating Ways to Age Well℠. Today, our efforts are transforming the lives of thousands of older adults through award-winning programs, gathering places, and residences.

Project Description

For the past three years Mather LifeWays has been working with BlueOrange Compliance to improve our HIPAA Security Compliance. Although we have strong technical infrastructure and an Incident Response Policy, Mather LifeWays had not tested the process within information technology (IT) or other business units. BlueOrange Compliance established an action plan following a recent assessment to strengthen our Formal Incident Response process. Mather LifeWays decided to conduct a cybersecurity data breach table-top exercise before the end of 2017.

Implementation/Response Approach

Mather LifeWays cybersecurity insurer makes available on their web portal cybersecurity templates that we used to modify for Mather LifeWays exercise. This was a significant time saver that allowed us to focus more on our objectives for the project, rather than drafting the scenario of the data breach. Our primary objectives for the initial table-top data breach exercise were to:

- Assess our knowledge of the Security Incident Response Process and Data Breach Notification Policy.
- Evaluate our response preparedness to a major breach incident from a recovery, operations, and communications standpoint.
- Educate and bring about awareness that data breach and cybersecurity is an organizational responsibility not just the IT department.

After the initial review of the cybersecurity table-top exercise template, we decided to break the exercises into two separate sessions, one for the IT staff and then a second one for the business leaders. This approach allowed us to focus on the IT and business needs in separate sessions without straying too far off track with either group.

The IT cybersecurity table-top exercise included the Chief Financial Officer (CFO), Assistant Vice President (AVP) of IT, IT Manager and helpdesk. The exercise presented increasingly more severe alerts regarding the potential threats. We were interested in what action was taken, for example, was a security ticket created, at what point does the helpdesk escalate the ticket to a manager, does IT know the requirements of the Security Incident Response Policy, are steps taken to mitigate the spread of the malware, do we have a disaster recovery plan, what is the recovery time objective, and what is the recovery point objective?

The business leaders' cybersecurity table-top exercise included the Vice President (VP) of Human Resources (HR)/Privacy Officer, CFO, Senior Living Vice Presidents (VPs), VP of Marketing, AVP of Risk Management, Director of Senior Living Operations, and AVP of IT. This session started where the IT department had just notified the Privacy Officer of the breach and had gathered the team. The business leaders were asked if they had enough information to declare a breach and who should be notified or if they would like to call in additional resources, for example open a claim with the cyber insurer and access forensic resources. Business leaders also had to discuss several communication scenarios, internal with residents and staff, external with media and government agencies. Operational concerns were discussed and what existing disaster planning would aid in the preparation for a scenario that would result in systems being offline for an unknown period.

Advantages to the Approach

By hosting two sessions, each session was just under two hours and both session's employees were engaged throughout the session. If the sessions were combined, employee engagement could be at risk due to the broader topics and number of employees in the meeting room.

Outcomes

IT Department Exercise

- Value was gained from putting the helpdesk through this exercise since the helpdesk has not experienced a breach or large-scale virus outbreak.
- The helpdesk gained knowledge and experience through the exercise.
- Development of a checklist was identified as a desired aid for the helpdesk to prevent staff from missing key decision points.
- Timely notification process was well understood at the helpdesk.

Business Leaders Exercise

- The team agreed to contact the cybersecurity insurer for legal advice, communications and forensics. It was determined that establishing contact now prior to an event and making vendor selection within the coverage would provide clear advantages.
- Operations leveraged existing disaster preparedness procedures and ensured that although additional support would be required, services and safety for residences would continue.
- Follow-up meetings will be scheduled to include input from operations for Business Impact Analysis and Data Criticality Analysis as part of the Contingency Planning process.

Challenges and Pitfalls to Avoid

Buy-in for table-top IT exercises can be challenging, so avoid making the session too long or too technical. Some departments might not have realized they are part of a team to respond to cybersecurity data breaches, so if this is your first exercise be careful not to be critical of anyone as this is a learning and awareness experience for everyone.

Being mindful of the time and managing the direction of the conversation to allow for concerns to unfold but keeping on track can be a challenge for the moderator of the exercise. We experienced this with the discussion around bitcoins and the varying knowledge levels within the group.

Lessons Learned

Your coworkers have invested their time in your initiative and they want to see you follow up with action. If you are unable to meet your commitments, then communicate with your coworkers and set new expectations.

Advice to Share with Others

It's a lot of work to lead the session and take notes, so we recommend that you designate these roles separately. The primary purpose is to get your coworkers talking about the data breach – make sure that everyone on the team is engaged, if they are not, bring them into the conversation.