Subject: MAC Committee – Security & Compliance
When: April 10, 2019

Committee Chair: Denise Pappu (Wells Fargo)

Attendees:

McCracken
- Kim Cooper (kim.cooper@mccrackenfs.com)
- Shari Hartwell-Cook (Shari.Hartwell-Cook@McCrackenFS.com)
- Karla Ferguson Karla.Ferguson@McCrackenFS.com
- Karen P
- Denise Ross
- VJ Bernier

VHDA
AMPF
Wells Fargo
Sterling Bank
Berkadia
Columbia
HomeStreet
Trimont
Red Capital
Key Bank
CBRE
Fannie Mae
Graystone
CapOne
Chase

Discussion Items / Meeting Minutes

- Denise R & VJ to join the call
    - Denise R & VJ want to understand topics
        - Infrastructure vs Application
    - Outline the different asks so they can pull right resources for topics
    - Topics from last calls
        - **Configuration Changes**
            - Failed login messages (Steve Armstrong – Chase)
                - Security policies are asking for generic messages vs showing login information
                - Coming from internal and external audits – needs to be generic
                - Will be in next release – there is a job/heat for this
                    - CS and Portal needs to have same changes
            - Connection Pool

    - Connection pool is not ending within x minutes which is presenting incorrect dates/times for File Maintenance date/timing (Denice Doce)
    - Existing job available
        - There is a temporary fix available. Long term fix underway. It is not going to pick up from connection pool id but pull from user. Next release should have fix.
    - Can be an audit issue for file maintenance
    - MFS needs to make a change to auto disconnect
        - Check with MFS on the job so all customers can take advantage
    - Is there a way to show the user id in pools who the user is when they are signed onto Portal? Need better way to see who is signed into the Portal.
        - If assistance needed call ASP when in shared environment.
- Web application firewall
    - TLS1.2
    - Questions around configuration and how MFS is ensuring protection per security analyst requirements
    - VJ –
        - TLS1.2 – nested under firewall
            - Encryption standard
            - Forces browsers to use that
        - Load Balancers do have encryption
        - Web application firewalls
            - Code level updates recently done – allow turning on application rules for encryption. Base Rules.
            - Due dates for each customer is underway
            - Process to update is underway for a customer currently.
- Multi-factor authentication – this is a need by many companies. How can this be obtained and when? It will need to be per customer request.
    - Greystone, Trimont, Columbia, Chase
    - High business entailments – like approval for cash disbursements (Steve – Chase). Can it be at module level?
    - MFS working on this on Portal side. Looking at product to implement. Customers outside of ASP may need other work/discussions. Steve to reach out VJ.
    - Wiring projects underway will have this ability
- Other Portal security concerns:
    - Invalidate cookies when user logs out?
        - Security concerns
    - Invalidate session id when user logs out?
    - Accessibility from home locations vs work

        - Firewall settings / IP restrictions
        - Work computer vs personal – multi-factor authentication plays into this
            - This can relate to how each customers internal network team identifies IP restrictions (white list)
    - Denice Doce has these questions on their annual survey that can provide more details to the ask.

- **Audit reporting**
    - SOC 2
        - Auditors are asking
            - Key/Columbia/Graystone, plus
        - Would like MFS to provide what the SOC2 will cost vs SOC1
        - MFS did a preliminary assessment
            - MFS would like to reduce number of vendor assessments if possible
            - SOC1 would still be needed
            - No timeline for SOC2
    - Report listing of disabled users (Disabled = Why, time, who, also ID status, who disabled the profile, the program that disabled the profile)
        - Custom report for Denice Doce now
        - Audit concern for all customers
        - Custom Report for users can be requested
    - Defined timeline for Medium Findings to be remediated from audits
        - Timeframes needed for findings
        - Companies are providing standards – would like to have better timeframes
        - Is there a way to "share" common items between companies that will not conflict with customer privacy?
        - Shared environments – penetration testing
            - Is that occurring? How/when can customers get results for auditors?
            - Penetration Testing – MFS had a meeting with customer. Results were loaded into MFS system to track. Summary report was sent out recently. MFS internal policy not to give it out detailed.

- **Vulnerabilities**
    - Information Security Red Team
        - Question to MFS – so how is MFS is managing for vulnerabilities for all customers? Do they have a database that houses the information for reporting?
        - MFS reporting/remediation tool. Reviewed monthly with Denise R for timing. Scanning managed by VJ monthly and reviewed with Denise R quarterly. Exception process followed. Policy available for customer to obtain.
        - Recommend Mirco join a roundtable discussion at conference to present the behind the scene process.

- Cyber Security / Cyber Resilience program
    - Proactive disciplines
    - Threat analytics
    - Advanced malware protection
    - DDoS protection
    - Reviewed annually and updated for emerging threats?
    - Integrated with Incident Response program?
    - Conduct cyber security exercise?
    - VJ – Team manages. More structure to be worked on with consultant. They (VJ and Mirco) are building a program and hope to be done later this year.
    - Move out as a separate topic
- **Other groupings**
    - GDPR –
        - General Data Protector Regulation – Is MFS prepared or able to manage this? Who manages actual data will need to remove that data from Strategy per customer request.
        - Auditors are started to review/ask about this
        - Denise R – MFS has started work with GDPR, working with MFS contractual – is MFS in alignment. No different security changes. Just contract write-up change is needed.

- Open Discussion
    - Any new items?
    - ADA compliant
        - What are the changes needed per customer?
        - In the past when asked by customers, MFS did not make changes since Strategy was not consumer facing
        - Borrower Inquiry is not ADA Compliant at this time
        - Employee needs are now being looked at for ADA compliant
            - MFS would need to implement many changes – Sub-committee to be started for discussion after results of survey
        - MFS noted a lot of changes
        - MFS to reach out to customer base to as who needs to be ADA compliant

Tasks:

- MFS conference
    - Roundtable on Security/Config for infrastructure (VJ/Micro/others)
        - Configuration
        - Vulnerabilties
        - Cyber Security / Cyber Resilience
        - Audit Needs
- Kim Cooper to send out survey to all customers asking about ADA compliance needs
        - Strategy needs – employee
        - Borrower Inquiry – customer facing
        - Who is interested in being on sub-committee to discuss needs/requirements?

Next Meeting – June 12th, 2019 @ 3pm ET --- Look out for new meeting planner!