Ransomware Assessment Facilitation

SUMMARY

Given the significant increase in ransomware attacks, financial institutions are encouraged to perform a ransomware assessment to identify and mitigate associated risks. Of note, the Bankers Electronic Crimes Taskforce (BECTF), state bank regulators, and the United States Secret Service have developed the Ransomware Self-Assessment Tool (RSAT) to help financial institutions periodically assess their efforts to mitigate risks associated with ransomware and identify gaps for increasing security. In addition to being an industry best practice and safeguard, we have observed that completing a ransomware assessment is becoming a regulatory expectation and/or requirement.

Ransomware is a type of malicious software (malware) that encrypts data on a computer, making it difficult or impossible to recover. Attackers usually offer to provide a decryption key after a ransom is paid; however, these keys may not work (if they are provided at all), which could make the financial institution's critical records unavailable. In addition, attackers may utilize extortion tactics to threaten the institution with public disclosure of exfiltrated customer or company information if the ransom is not paid. However, financial institutions choosing to pay ransoms, as well as companies that facilitate ransom payments to cyber actors on behalf of victims, including cyber insurance firms and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but may also violate OFAC regulations.

OBJECTIVE, METHODOLOGY, & SCOPE

In an internal audit liaison capacity, NETBankAudit will provide executive management and the board of directors with an overview of the institution's preparedness towards identifying, protecting, detecting, responding, and recovering from a ransomware attack. The methodology is derived from the BECTF's Best Practices for Banks: Reducing the Risk of Ransomware. The scope encompasses the following four ransomware phases and respective functions:

1. **Identify and Protect**
    - Risk Management
    - Insurance
    - Vendor management
    - Employee Controls
    - Audit & Testing
    - Backup Controls
    - Multi-Factor Authentication
    - Patch Management

- Configuration Controls

2. **Detect**
   - Data Loss Prevention
   - Alerting
   - Monitoring
3. **Respond**
   - Incident Response Plan
   - Ransomware Response Procedures
4. **Recover**
   - Restoration
   - Lessons Learned
   - Training
   - Communication

NETBankAudit's AFFIRMATION OF INDEPENDENCE

The engagement will adhere to the Institute of Internal Auditors (IIA) 2120 Risk Management standard that states, "*internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.*" The engagement also complies with the IIA definition of Internal Auditing that states, "*Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.*"

The FFIEC Interagency Policy Statement on the Internal Audit Function and Its Outsourcing **states that Internal Audit has a necessary and important** role within institutions to consult on new products and services and on mergers, acquisitions, risk analysis, and other corporate reorganizations. The guidance further states, "*This role typically includes helping assess and design controls and participating in the implementation of changes to the institution's control activities.*" The prohibited delineation of independence is Internal Audit assuming a business-line management role over control activities. NETBankAudit supports and abides by the FFIEC policy statement and does not perform business-line management activities.