CYBERSECURITY FOR SMALL FINANCIAL SERVICES FIRMS

SDDco Group

CORE CHECKLIST GOALS

The five core goals of the Checklist are to:

1. Identify and assess cybersecurity threats to small business
2. Protect the infrastructure from cyber intrusions
3. Detect a compromise or vulnerability
4. Respond via a risk-based plan
5. Recover or replace lost data

THE TWELVE CHECKLIST STEPS

If you store, use or electronically transmit *Personally Identifiable Information* (PII) which includes names, social security numbers, and dates of birth or sensitive information such as financial records, account information, tax filings, addresses and collectively private data, then institution of the following 12- step program should be considered:

1. Find the PII

Conduct an internal audit to:

- Locate the private data in your business (network drive, system folder, laptop or email) and complete separate entries for each location
- Rate each level of risk (low, medium, high) and project the impact of loss to the firm or customers

See: NIST: Guide to Protecting the Confidentiality of PII

2. Minimize the Eyes

Lessen access to private data:

- Decide if you can remove private data from your systems and networks and still properly conduct business (keep in mind any recordkeeping obligations)
- Identify and remove people or systems that do NOT need access
- Remove the private data or stop sharing

See: Minimizing Collection of PII, NISTS Guide...PII pages 3-4l

Powered by AdvisorArmor

3. Manage Third-Party Risks

Identify and lessen third-party access to private data. If you transmit private data to vendors, a clearing firm or your customers:

- List all third parties
- Assess their security protections:
    - Obtain at least the most recent SSAE 16 report
    - Assign to each a risk severity level
    - Limit third-party access to data required for business reasons

See: Vendor Management, Report on Cybersecurity Practices (see pp. 26-30) and AICPA's Reporting on Controls at a Service Organization

4. Protect Private Data

Assess and remedy your firm policies regarding:

- Password strength and change cycle
- Removable storage media restrictions
- Malware/anti-virus software programs
- Firewall use

See: Password Strength Tips, SANS Consensus Policy Resource Community – Password Protection Policy and NIST to Malware Incident Prevention and handling

5. Protect Systems

Assess and remedy protections for all systems holding private data:

- List all private data systems (e.g. holding trading orders or customer accounts)
- Identify risks that could result from system loss
- Assess and remedy system protections, including:
    - Password strength and change cycle
    - Malware/anti-virus programs
    - Firewall use
    - Backing up

See: Password Strength Tips, SANS Consensus Policy Resource Community – Password Protection Policy and NIST to Malware Incident Prevention and handling

6. Use Encryption

Assess where private data is encrypted (protected while traveling to external sources) and remedy practices:

- Consider risk severity levels and resources to decide on remedies to make, such as:
  - Encrypting all outgoing emails
  - Encrypting all PII and sensitive data at rest or in storage
  - Masking the data when displayed

7. Protect Employee Devices

Assess device permissions, restrict where indicated; isolate network access to approved and encrypted devices:

- Identify devices with access to private data and assign a risk severity level to such data identify risks that could result from system loss
- Decide whether to deny employee access to all or some private information
- Decide whether to incorporate heightened protection procedures for devices, e.g., device data encryption and/or the ability to remove erased devices that are lost or stolen

See: Securing Mobile Devices, SANS Institute on Cybersecurity The Critical Security Controls for Effective Cyber Defense Version 5.0 (see page 19)

8. Monitor Controls

Draft, implement and monitor firm policies and procedures governing private data. A few monitoring reminders:

- Access to private data must be stopped when relationships to vendors, contractors or employees are terminated
- Conduct periodic training on cybersecurity policies and procedures, addressing firm-specific risks, systems, and incident history
- Perform cybersecurity due diligence when engaging vendors

See: Vendor Management, FINRA's Report on Cybersecurity Practices (see pages 31-33)

9. Test Protections

Consider adding an annual IT penetration test to assess infrastructure protections:

- Hire a third-party vendor or use internal staff to conduct the "pen" test
- Determine the scope of systems to be tested:
  - Identify internal and external vulnerabilities to attempt to obtain sensitive info from the firm
  - Remedy policies as needed

See: Conducting Penetration Testing, NIST's Technical Guide to Information Security Testing and Assessment

10. Detect Intruders

Assess whether to invest in an Intrusion Detection System (IDS):

- Did firm receive any threat info from outside sources (e.g., FS-ISAC)?
- Are processes in place to act?
- Does firm use tools to regularly scan systems for vulnerabilities, secure configuration, and current patch levels?
- Does firm monitor scan results and address discrepancies?
- Do metrics track your firm's cybersecurity controls and report conditions to senior executives?
- Do firm members report suspicions of intrusion to the CCO or IT manger?

See: Intrusion Detection System, NIST's (draft) Guide to Intrusion Detection and Prevention Systems (IDPS)

11. Draft a Response Plan

Plan, communicate, respond, and govern as follows:

- Plan responses to these likely incidents:
  - Loss of customer PII, data corruption, denial of service (DoS) or distributed denial of service (DDoS) attack, network intrusion, customer account intrusion and malware infection
- Respond as appropriate for the risk and your business:
  - Fully or partially shutdown systems, disconnect system from network, delete and reinstall malware, or disable a user from system access
  - Inform clients and regulating bodies on remedy
- Consider these cybersecurity governance steps:
  - Entrust one individual to lead all cybersecurity compliance
  - Maintain a list of incidents
  - Create a dashboard to track remedies, programs, and staff training
  - Review customer complaints
  - Address cybersecurity status at management and compliance meetings
  - Share metrics with CEO and COO
  - Buy cyber-security insurance

- Recover Private Data

Assess where recovery steps are necessary to proceed with business and if subsequent vulnerabilities are addressed:

- Do regularly scheduled backups restore private data if lost in a cyber incident?
- Can you rebuild breached systems if necessary?
- Can compromised files be replaced with clean versions?
- Is a plan in place to:
  - Install patches, change passwords, and tighten network, should a cyber-incident take place?
  - Heighten network monitoring and protect resources after an incident?

See: Eradication of Cyber breach and Recovery, NIST's Computer Security Incident Handling Guide (see pages 35-37)

THE CHECKLIST AND THE LAW

Using a cybersecurity checklist "does not create a 'safe harbor' with respect to rules, federal or state securities laws, or other applicable federal or state regulatory requirements."

"Regulators review firms' approaches to cybersecurity risk management, including: technology governance, system change management, risk assessments, technical controls, incident response, vendor management, data loss prevention, and staff training."

Expect a review of a firm's ability to protect sensitive customer information and its compliance with SEC regulations, including:

- Regulation S-P (17 CFR §248.30): Firms must adopt written policies and procedures to protect customer information against cyber- attacks and other forms of unauthorized access
- Regulation S-ID (17 CFR §248.201-202): Firms have duties for detection, prevention, and mitigation of identity theft
- The Securities Exchange Act of 1934 (17 CFR §240.17a-4(f)): Firms must preserve electronically stored records in a non-rewriteable, non-erasable format

CHECKLIST TAKEAWAYS

Small financial services firms can use the Checklist to

1. Identify and inventory their specific digital assets;
2. Assess compromise impact to the firm and their customers;
3. Identify likely protections and processes that secure their assets;
4. Perform a risk-based assessment, considering firm resources, the impact of potential breaches, and available protections and safeguards;
5. Decide which risks to remediate.

Small financial services firms should develop a cybersecurity program to best suit their business model. They may use the Checklist as their resource (informed by NIST and FINRA's Report on Cybersecurity Practices) and/or SIFMA's small firm checklist, NIST guidance, or SEC guidance. Firms should also maintain internal policies and procedures to comply with current cybersecurity federal and state requirements.

CHECKLIST TAKEAWAYS

Small firms relying on clearing firms and vendors to maintain customer accounts and transact business should not assume that others would be responsible for cyber-incidents.

Some firms may need outside assistance in understanding the technology or terms of the Checklist and implementing a program. Consider working with an outside technology or regulatory compliance professional.