One National Investments – Risk Assessment

CYBR 658 Risk Analysis and Compliance

Shrutika Joshi

HA72777

Overview

- One National Investment is an investment management and wealth advisory service which is established in 2002.
- Its headquarters are located in Syracuse, NY, with locations in NY, NJ and CT having.
- Company’s budget is of almost $18 million and having 104 geographically dispersed employees with 30% staff working remotely. Company's mission is to delivering a safe, secure, and optimal work environment.
- Company ensures fair treatment for employees
- Staff receives IT security policies and training. Also receives handbook during onboarding containing bullet points on importance of security and data protection.
- The company develops and implements physical, operational, administrative, and technical security policies, procedures, and processes to mitigate both current and emerging threats. However, it is often the target of threats such as social engineering, malware and internal users.
- Challenges in keeping policies up to date and ensuring user awareness. So company need automated training system to address growing threats.

Risk Analysis Scope and Methodology

- **Risk Analysis Scope :**
  - Conduct risk analysis based on assessing the compliance of One National Investments with the security requirements outlined in Part 500 (500.0-500.17) of the NY DFS NYCRR.
  - Identify at least 12 requirements that One National has failed to meet and describe the findings Identified
  - Assess One National's security practices like access control mechanism, vulnerability management, physical security, security trainings and users acknowledgement to it, incident response plan and policy and procedure review, data encryption, asset management and provide risk mitigations

- **Methodology:**
  - Review One National's provided case study and analyze requirements mention in Part 500.0-500.17 to identify areas where One National's failed to comply
  - Identify deficiencies based on analyzing company's existing policies and procedures, examining contract with third party MSP vendor, and assess risks
  - Assign risk level (High, Moderate, Low) to each findings considering it's impact and likelihood
  - Provide vendor agnostic recommended approach on all risks identified and provide clear steps for remediation

Likelihood, Impact and Risk Level Criteria

- **Likelihood Criteria –** The probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities (High, Moderate, Low)
- **Impact Criteria –** The operational, reputational, or financial effect of the risk on your organization on a scale of (High, Moderate, Low)
- **Risk Level Criteria –** A measure of the extent to which an entity is threatened by a potential circumstance or event. Typically a function of:
  - (i) the adverse impacts that would arise if the circumstance or event occurs
  - (ii) the likelihood of occurrence.

- **References –**https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Criteria for Assessing Likelihood, Impact, and Risk Levels

References- NIST SP 800-30 Appendix G

Qualitative Values	Likelihood	Impact	Risk Levels
High	There is a high probability of the event or risk occurrence based on historical data, industry trends, or known vulnerabilities.	The event or risk occurrence would have significant consequences, resulting in severe financial loss, reputational damage, legal/regulatory non-compliance, or disruption of critical business operations	Risks with a high likelihood and high impact require immediate attention and mitigation due to their potential severe consequences.
Medium	There is a moderate probability of the event or risk occurrence based on some historical data, limited industry trends, or potential vulnerabilities.	The event or risk occurrence would have noticeable consequences, resulting in moderate financial loss, reputational impact, legal/regulatory challenges, or disruption of important business operations.	Risks with either a moderate likelihood and high impact or high likelihood and moderate impact should be addressed to minimize potential negative outcomes.
Low	There is a low probability of the event or risk occurrence based on minimal or no historical data, industry trends, or vulnerabilities.	The event or risk occurrence would have minimal consequences, resulting in negligible financial loss, limited reputational impact, minimal legal/regulatory implications, or minor disruption to non-critical business operations.	Risks with a low likelihood and low impact may still require some attention, but they can be managed with lower priority compared to higher-risk areas.

Risk Register

ID	Finding	Requirement	Likelihood	Impact	Risk Level	Recommendation (including cost)
1	Lack of recent Risk Assessment	- To identify all vulnerabilities, lack of security measures and configuration management risk assessment is necessary to perform - To Comply with Part 500.0	High	High	High	Conduct comprehensive risk assessment to identify and priorities security risks **Cost-** Small enterprise deployment: $75k to $150k Medium enterprise deployment: $250k to $500k Large enterprise deployment: $750k to $1 million **Reference-** https://www.scmagazine.com/product-test/content/metricstream-risk-management-solution-v6-0-2
2	Non-compliance with NY DFS NYCRR Part 500	As One Nationals is a financial institution from New York it should be in compliance with NY DFS NYCRR Part 500- Part 500.1	High	High	High	Financial institutions should follow laws and regulations of state **Cost –** NYDFS penalties start - $2,500 a day for each day of noncompliance. If noncompliance is determined to be a pattern by the NYDFS superintendent, the fine may increase to $15,000 a day. **Reference -** https://www.cyberpopup.com/articles/what-you-need-to-know-about-23-nycrr-part-500-nydfs-500#:~:

Risk Register

ID	Finding	Requirement	Likelihood	Impact	Risk Level	Recommendation (including cost)
3	Poor Vulnerability Management Process- High vulnerabilities are taking 60 days to resolve and there is no mechanism to resolve moderate and low vulnerabilities. Patch Management - patches are not getting tested before deploying	In order to resolve severe vulnerabilities in timely manner and reducing the possibility of attacker exploiting those vulnerabilities Avoiding data beach and harm to organization - Part 500.12	High	Moderate	High	Vulnerability Management process should be well define and priorities as per severity and timely remediation. Ensure patches are tested before deployment **Cost –** $999 to $4500 **Reference -** https://www.getastra.com/blog/security-audit/vulnerability-assessment-cost
4	Lack of security and privacy provisions in contract with vendor. Lack of third party oversight	Company should check third party service provider's policies and procedures for access controls, including its use of multi-factor authentication to limit access to relevant information systems and nonpublic information – Part	Moderate	Moderate	Moderate	Implement policies and procedures for third party MSSP **Cost –** This will be included in MOU cost

Risk Register

ID	Finding	Requirement	Likelihood	Impact	Risk Level	Recommendation (including cost)
5	Lack of encryption for non public or sensitive information	Encryption for data at rest - Part 500.15	Moderate	High	High	Ensure file level encryption of non public and sensitive data **Cost –** $65 per windows device with one year support **Reference -** https://www.esecurityplanet.com/products/top-full-disk-software-products/
6	Poor Asset Management	Each covered entity shall limit user access privileges to information systems that provide access to nonpublic information and shall periodically review such access privileges – Part 500.08	Moderate	Moderate	Moderate	Implement an automated asset management system to track and manage company-issued devices, including equipment retrieval upon employee departure **Cost –** startup cost - $2525 to $23259 **Reference -** https://www.starterstory.com/ideas/asset-management-business/startup-costs

Risk Register

ID	Finding	Requirement	Likelihood	Impact	Risk Level	Recommendation (including cost)
7	Poor Access Control Mechanism -	Employees access should be Role and location centric – Part 500.03	High	High	High	Strengthen access controls by implementing multifactor authentication (MFA) for all user accounts. **Cost –** $2525 to $23259 **Reference -**
8	Lack of Incident Response Plan	business continuity – Part 500.16	High	Moderate	High	Develop and document incident response procedures and that cover identification, containment, eradication, and recovery process **Cost -**500$ -50,000$ depending on how much it will cost if data breach happen

Risk Register

ID	Finding	Requirement	Likelihood	Impact	Risk Level	Recommendation (including cost)
9	Users not aware of security procedures	Employees are first point of contact for attackers in case of phishing, social engineering and any kind of attack requiring human interaction – Part 500.14	Moderate	Moderate	Moderate	Implement a regular and mandatory security awareness training program for all employees. **Cost –** 50 employees - $1000 **Reference -** https://www.trustnetinc.com/security-awareness-training/
10	Incomplete termination and departure procedures	Exit process should be well define– Part 500.03	Moderate	Moderate	Moderate	Update internal procedures to ensure timely removal of access privileges for users who are no longer employed. **Cost –** 500$ -50,000$ depending on how much it will cost if data breach happen

Risk Register

ID	Finding	Requirement	Likelihood	Impact	Risk Level	Recommendation (including cost)
11	Lack of incident reporting mechanism to report incidents or data breaches does not exist	Incident reporting mechanism should be in place so that employees can refer the process and timely should report the incident. As per the regulations data breach incidents should be reported within 72 hours - Part 500.17	High	Moderate	High	Implement an incident reporting mechanism to enable timely reporting and response to security incidents or data breaches. **Cost –** Minimal cost and team effort in building incident reporting mechanism
12	Weak physical access control	To secure the company, its asset and data and avoiding anyone breaching into company - Part 500.04	Moderate	Moderate	Moderate	Enhance physical access controls by implementing a badge management system and enforcing stricter visitor access policies **Cost –** $500 to $8,000+ per door **Reference -** https://www.ackermansecurity.com/blog/business-security/average-cost-access-control

Additional Considerations

1. We utilize vendors and businesses as third parties to support our efforts. Every relationship that we have established has a contractual relationship. Security and privacy concerns are not addressed in the contract. Should we be overseeing third party relationships?

- Yes. Ensuring security and privacy concerns addressed in the contract should be mandatory.
- Also company should sign NDA and MOU with vendors and should oversee how vendors are managing all security related requirements and whether they have proper process in place in case of any incident
- Also should assess the security practices of vendor

Additional Considerations

2. Often, in the past, we have allowed staff to keep company equipment after they are no longer employed with us. Managing a surplus of equipment is time consuming and resource intensive. How should we address this in the future?

- Yes. Developing a structured process for managing surplus equipment, particularly after employees leave the organization.
- Considering options such as equipment retrieval, data wiping, and secure disposal to prevent unauthorized access to sensitive information.
- Exploring cost-effective solutions, such as partnering with certified e-waste disposal services or implementing equipment reuse/recycling programs.

Additional Considerations

3. The CFO also acts in a CISO capacity. We have not had time to post and source for a CISO. Should be concerned that she serves in both roles?

- Yes it is definitely should be a concern. Regulatory bodies like the NYDFS recognize the importance of information security in financial institutions and require the separation of roles to ensure compliance with cybersecurity regulations.
- The roles of a CFO and a CISO have distinct responsibilities and require different areas of expertise. As the CFO, their primary focus is on financial management and strategic decision-making related to the organization's financial health. On the other hand, the CISO is responsible for overseeing the organization's information security strategy, implementing security controls, managing risks, and ensuring compliance with regulations. Combining these roles can lead to conflicts of interest, as the CFO may prioritize financial considerations over information security concerns.
- Overall, the separation of roles between the CFO and CISO in financial institutions aligns with best practices in governance, risk management, and compliance.

Additional Considerations

4. Firmwire does not timely remove access for users that are no longer with the organization. Our internal procedures describing terminations and departures via exit procedures have not been updated in a few years. How should we approach making sure the MSP has timely information to remove access?

- Updating the exit process to match with current industry standard
- Establishing a streamline communication between One National and Firmwire MSP to promptly inform them about user terminations and departure
- Regularly updating and reviewing access control policies and procedures to align with industry best practices.

Additional Considerations

5. As we expand and grow, should we consider other compliance standards, laws, or regulations to help us be secure?

- Yes. Since One National Investment is an investment management and wealth advisory service, it should considered standards relating to financial data like Payment Card Industry Data Security Standard (PCI DSS), GDPR standard
- Also since company is New York base, it should check whether company is in compliance with New York laws and standards
- Conducting gap analysis to identify areas where One National can align with additional compliance

Conclusion

- Based on the risk analysis conducted on One National Investments' compliance with Part 500 requirements, several deficiencies and risks have been identified. The organization has not met certain security measures, posing potential threats to the confidentiality, integrity, and availability of its data and systems. These findings highlight the need for immediate action to enhance security practices and achieve compliance.
- The risk analysis has demonstrated the importance of addressing vulnerabilities such as outdated policies and procedures, lack of incident response procedures and incident reporting mechanism, insufficient access control measures, and inadequate user training.
- Failure to address these deficiencies may lead to unauthorized access, data breaches, and reputational damage.

Conclusion

- To mitigate the identified risks, recommendations have been provided, focusing on implementing robust security measures, updating policies and procedures, enhancing user training and awareness programs, establishing incident response mechanisms and updating incident response plan, and improving access control processes. Each recommendation includes cost considerations to facilitate informed decision-making.
- In addition to addressing the Part 500 requirements, the case study raises additional considerations, including the oversight of third-party relationships, management of surplus equipment, the role of the CFO as a dual CISO, ensuring timely removal of user access, and exploring other compliance standards and regulations for securing financial data and for enhanced security.
- By implementing the recommended measures and addressing the identified deficiencies, One National Investments can strengthen its security posture, mitigate risks, and ensure compliance with Part 500. These actions will contribute to safeguarding sensitive data, maintaining client trust, and protecting the organization from potential cyber threats.

References

- [1]Cobb, M. (2022, Nov). How to perform a cybersecurity risk assessment in 5 steps. TechTarget.
  - https://www.techtarget.com/searchsecurity/tip/How-to-perform-a-cybersecurity-risk-assessment-step-by-step
- [2]Kelley Dempsey, Paul Eavy, George Moore (2017, June) Automation Support for Security Control Assessments
  - https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8011-1.pdf
- [3]Cherilyn Pascoe (2023, April 24) Cybersecurity Framework (CSF) by the National Institute of Standards and Technology (NIST)

  Link - https://www.nist.gov/cyberframework
- [4](2022, OCT) ISO/IEC 27001 - Information Security Management Systems (ISMS)

  Link: https://www.iso.org/standard/54534.html
- [5]Force, J. T. (2017). Security and privacy controls for information systems and organizations (No. NIST Special Publication (SP) 800-53 Rev. 5 (Draft)). National Institute of Standards and Technology.
  - Link : https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft
- [6] https://www.scmagazine.com/product-test/content/metricstream-risk-management-solution-v6-0-2
- [7] https://www.esecurityplanet.com/products/top-full-disk-software-products/
- [8]https://www.starterstory.com/ideas/asset-management-business/startup-costs
- [9] NIST Part 500
  - Link - https://www.dfs.ny.gov/industry_guidance/cybersecurity_requirements_financial_services_companies