Introduction

These comments are being submitted by Rocio Baeza. Rocio is the CEO & Founder of CyberSecurityBase, a Chicago-based data security consultancy. The team specializes in the FinTech space, with deep experience in the online payday lending industry[1].

- Previous Work Experience: GE, Enova, Cash America
- Past Certifications: Certified Information Systems Auditor (ISACA); Certified Information Privacy Professional/US (IAPP)
- Past Collaboration with Federal Regulators:
    - SEC: Proposed Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (May 2022)
    - FDIC, OCC, Board: Proposed Interagency Guidance on Third-Party Relationships: Risk Management (Oct 2021)
    - Various Federal Bank Regulators: Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, including Machine Learning (July 2021)
    - CFPB: Section 1033 - Consumer Access to Financial Records Proposed Rule (Feb 2021)
    - FTC: Comments to Safeguards Rule, 16 CFR part 314, Project No. P145407 (Aug 2020)
    - FTC: Information Security & Financial Institutions: An FTC Workshop on GLB Safeguards (July 2020)
- Other:
    - Attends the California Consumer Privacy Act Board Meetings
    - Collaborated with City of Chicago Clerk Office in assessing data security controls for the Chicago CityKey ID Program (a government-issued ID card for Chicagoans)
    - Host of the GDPR Stand Up podcast (a weekly podcast; 2018 - 2019)

My perspective includes over a decade of working experience working with Chief Compliance Officers at FinTechs needing help demonstrating compliance to their information security requirements. This work includes providing virtual Chief Information Security Officer (vCISO) services, performing security audits, gap assessments, and developing and implementing customized cybersecurity policies.

Online Lender Background

These comments are based on years of work in developing cybersecurity programs for US FinTechs that operate exclusively online and are starting on their data security journey. Our ideal clients are US-based FinTechs that are “small-dollar lenders”, lend directly to consumers, have up to 50 employees, have secured over $250mil in funding, collect high volumes of consumer personal information, partner with numerous data vendors for underwriting, have an in-house data analytics team, and a growing team of in-house and offshore developers. These FinTechs are subject to the GLBA, state-specific data security and data privacy laws and regulations, and oftentimes subject to the PCI-DSS. These FinTechs do not have an in-house CISO, but have tremendous pressure from bank partners, investors, and stakeholders to develop a cybersecurity strategy, develop and implement a cybersecurity program, and manage cybersecurity risks in the same manner that the company is managing other business risks.

[1] Also known as “small-dollar lending”

Throughout my career, I have supported numerous FinTechs in building cybersecurity programs. Through this journey, I have developed a framework that we use at CyberSecurityBase to support our clients. Our support is unique, as it allows us to engage with FinTechs in a way that is cost-effective (over hiring a full-time CISO), provides faster results (because we have executed similar projects in the past), and educates busy executive leaders (that need to manage security risks but don't have time to learn how to do it on their own).

I believe that I am uniquely positioned to provide valuable perspective that may help the NIST finalize Cybersecurity Framework 2.0. As an experienced data security professional, supporter of regulation aimed to protect consumers, and a young mom, my desire is to help NIST update the framework in a way that clearly guides organizations on how to reduce cybersecurity risks.

It is important to note that I support the proposed changes. NIST has done an excellent job in developing resources around cybersecurity. In submitting these comments, my goal is to provide recommendations that advance NIST goals.

Line 150 reads: "The primary audience for the Framework consists of those responsible for developing and leading a cybersecurity program. The Framework can also be used by others involved in managing risk-including executives, boards of directors, acquisition professionals, technology professionals, risk managers, lawyers, human resources specialists…to guide their cybersecurity-related decisions…"

In response to the request for "concrete suggestions for improvements to the draft…", I urge that an implementation checklist be added to the Informative References that are expected to be available online on the NIST Cybersecurity Framework website.

The Implementation Checklist

The recommended checklist would benefit professionals that are tasked with managing cybersecurity risk for their organization, and do not have experience in the cybersecurity or cybersecurity governance space. Ideally, this checklist provides step-by-step directions for using the NIST Cybersecurity Framework 2.0 and adopting it as an internal tool.

The recommended checklist would also benefit professionals managing cybersecurity risk. This checklist can serve as a catalyst for moving the cybersecurity industry to a standardized and accepted methodology in managing cybersecurity risks.

As a professional with 15 years of experience in data analytics, product management, IT security, audit, 3rd party risk management, and cybersecurity consulting in financial services, it is concerning to see that the cybersecurity industry has not standardized its methodology like other industries have (i.e. accounting, legal, medicine). Unfortunately, the current state is leading to a growing pool of professionals supporting organizations with components of their cybersecurity program, in a manner that is illogical, highly disconnected, and sometimes handled at the detriment of the organization.

This is a critical gap, as we are facing a shortage of cybersecurity professionals.

An example may help illustrate the gravity of the situation.

Let's take an online lender ("lender") that originates loans in the United States. The lender launches in 1-2 states, stands up operations, and focuses on servicing customers and optimizing underwriting processes. Oftentimes the lender needs to incrementally adopt cybersecurity controls, as it starts to increase loan originations, generate revenue, and acquire venture capital funding to further expand operations.

The lender will oftentimes operate for some time, before it is in a position to bring on an in-house Chief Compliance Officer or a Chief Information Security Officer. This is perfectly reasonable, especially in the early stages of the business. If the lender is successful in increasing customer acquisition, converting leads, and optimizing underwriting processes to keep default rates at bay, the lender will seek partnerships with banks and others to scale operations. It is at this point, where the lender will be required to demonstrate that it has the capabilities to develop, implement, and manage a cybersecurity program. This bank requirement helps manage their 3rd party risk, satisfy federal consumer protection requirements, and requirements from bank regulators.

In following, serving, and discussing with leadership at various lenders, it is not uncommon for the lender to approach the need for developing a cybersecurity program as follows, and in this order:

- Publish a Privacy Policy on the website
- Download a set of policies and procedures that include expected topics (i.e. passwords, anti-virus, encryption, building security, etc.)
- Search for free online security awareness training modules for the staff to watch
- Search for a service provider to perform a penetration test on the "network"
- Search for an auditor to perform a cybersecurity audit and/or risk assessment
- Remediate issues reported by the auditor
- Repurpose a 3rd party due diligence questionnaire obtained from a past employer and adopt as the lender's due diligence questionnaire
- Create new policies, based on incoming due diligence requests from investors, insurance carrier, 3rd party vendors, bank partners, and auditors

The approach described above is usually the result of the cybersecurity function being handled by a team composed of IT administrators, software developers, Legal, Compliance, Operations and/or HR team members, that is "advanced" as members of the team have capacity to handle.

To a professional that is not experienced in cybersecurity risk management, it may be difficult to understand why the approach described above is a recipe for disaster. I will try my best to articulate the top-line concern with this approach.

An effective cybersecurity risk management program requires that the following activities be carried out, in this specific order:

- Assemble foundational inventories (i.e. data flow diagram(s), network diagram(s), IT asset inventory, 3rd party vendor inventory, data security requirements from governing laws/regs/contractual obligations)
- Obtain confirmation from various stakeholders, that the foundational inventories are complete and accurate
- Document processes/procedures that employees and contractor are currently performing
- Analyze how governing laws/regs apply to the lender, given the data processing environment set up and current procedures
- Establish the lender's cybersecurity vision and risk thresholds levels
- Develop a customized cybersecurity policy set based on the lender's data processing environment, underwriting, and other business processes
- Develop a customized cybersecurity awareness training program, that is structured with:
    - Baseline material
    - Team-specific expectations
- Calibrate the documented processes to align to the documented cybersecurity policy set
- Execute a warm-handoff of the changes needed for teams to implement
- Set up audit training wheels, to ensure that process owners are aware of process triggers and proficient in executing the necessary procedures
- Perform an audit 45-60 days from training delivery, to measure compliance with agreed policy requirements and procedures
- Establish the cybersecurity risk register

The above activities are the exact ones that we now execute with each and every online lender that we support.

There are more activities, but we will limit to the ones above, to keep this as focused as possible.

In reviewing the NIST Cybersecurity Framework 2.0, it is clear that framework concepts overlap with our approach in developing our client's cybersecurity programs.

However, for the inexperienced professional that is looking to leverage the NIST Cybersecurity Framework, it is likely that they will approach as follows:

- Download the NIST Cybersecurity Framework
- Read the NIST Cybersecurity Framework
- Perform Google searches to digest the information and how to "implement" the NIST Cybersecurity Framework
- Refer to the Appendix and download Templates for Profiles and Action Plans
- Create a Google Sheet and set up with
    - Table 1: Notional organizational profile template
    - Table 2: Notional action plan template
- Start to fill in the tables with information, based on their interpretation on "what to capture"

- Solicit input from others at the organization
- Email a copy of the “completed” tables to senior leadership
- Wonder where to go from here…

No Implementation Checklist - A Missed Opportunity

An implementation checklist must be developed and added to the Informative References documentation set, if we want the NIST Cybersecurity Framework 2.0 to accomplish the following goals:

- help organizations reduce cybersecurity risks
- provide actionable steps to professionals with no hands-on-experience in leading a cybersecurity program, including executives, boards of directors, acquisition acquisition professionals, technology professionals, risk managers, lawyers, human resources specialists

As a practitioner and service provider to the small-dollar lenders for the last 15 years, I assure you that in its current form, the NIST Cybersecurity Framework is not usable to the small-dollar lending industry. This includes

- lenders
- LMS providers
- lead providers
- bank data providers
- data, aggregators
- call center software providers
- Bank partners
- ACH processors
- Card processors payment processors, and
- IBV providers

Closing Remarks

I thank you for reviewing these comments and recommendations and possibly taking them into consideration as you finalize the NIST Cybersecurity Framework and next steps for Informational References and Implementation Examples.

The CyberSecurityBase team is available in contributing to the development of Informational References. It will be an honor to join the many contributors to the NIST Cybersecurity Framework 2.0, for the advancement of the cybersecurity industry.

Should you or any member of the team have any follow-up questions or clarification requests for any items covered in this document, please feel free to reach out directly.

Sincerely,
Rocio Baeza
CEO and Founder of CyberSecurityBase
[redacted]