# Regional Financial Corporation: Cybersecurity Discussion

David A. Wagle

School of Business, Northcentral University TIM-8301: Principles of Cybersecurity

Dr. Bill Souza May 16, 2021

# Regional Financial Corporation: Cybersecurity Discussion Introduction

Financial institutions are infamous as being highly targeted by cyber-crime. In 2019, financial services companies were the number one victims of cyber-crime with respect to the cost of the attacks on the US economy according to the US Congressional Research Service (Scott, [2021).](#_bookmark8) It is therefore incumbent upon Regions Financial Corporation (RFC) to ensure the cybersecurity of our corporate environment, including points of vendor integration and customer contact against the most dangerous cyber-threats.

# About Regions Financial Corporation

RFC is a full service financial institution headquartered in Birmingham, Alabama.

RFC operates in the South, Midwest, and Texas, covering 15 states with 1,369 branch locations. In addition to retail banking operations, RFC offers equipment finance, commercial finance, investment services, brokerage services, wealth management services, non-profit investment consulting, trust services, and low-income housing fund syndication. In fiscal 2020, RFC generated $1.094B USD in net income (Regions Financial Corp., [2021).](#_bookmark6)

# Governing Laws, Regulations, and Oversight Bodies

As a financial services company, RFC is covered by a multitude of laws, regulations, and regulatory bodies which impact cybersecurity requirements. The most important laws governing RFC as a US based financial institution are: the Gramm-Leach-Billey Act of 1999 (GLBA), the Sarbanes-Oxley Act of 2002 (SOA), the Fair and Accurate Credit Transaction Act (FACT), the Bank Protection Act (BPA), and the Bank Service Company Act of 1962 (BSCA) (Murphy & Scott, [2016;](#_bookmark3) Scott, [2021).](#_bookmark8)

Key implications of these laws are as follows:

* **GLBA:** Privacy standards, disclosure limitations, and security standards and practices to consumer data from unauthorized access, use and disclosure.
* **SOA:** Requirements to file reports identifying internal and external risks to the business and actions taken to protect against those risks.
* **FACT:** Require regulatory bodies to provide guidelines to protect against identity theft.
* **BPA:** Regulatory bodies must provide minimum security standards for banks and savings and loans protecting against “robberies, burglaries, and larcenies”. Cybersecurity has been assumed to be included by various bank regulators.
* **BSCA:** Provides for the regulatory authority to regulate and supervise financial institutions, including over partnerships with technology providers.

Additionally, the Federal Financial Institutions Examination Council (FFIEC) provides cybersecurity assessment tools for financial institutions; the Federal Trade Commission (FTC) publishes privacy and safeguard rules; the Federal Stability Oversight Council provides guidance on threat channels; the Security Exchange Commission (SEC) provides guidance on protecting security trading and brokerage activities; and the Commodity Futures Trading Commission (CFTC) provides similar information about commodity and futures trading (Murphy & Scott, [2016;](#_bookmark3) Scott, [2021).](#_bookmark8)

The US has eight “systematically important financial market utilities” (SIFM Us) which are designated by Financial Stability Oversight Council (FSOC). These

self-regulatory organizations (SROs) can and do propose rules that may be adopted as well. Additionally, financial institutions can be subject to Presidential Policy Directives, also known as Executive Orders, such as PPD-21 “Critical Infrastructure Security and Resilience” (Scott, [2021).](#_bookmark8)

# Risks

The risks associated with cybersecurity events effectively boil down to a few major categories. These are risks to investor relations and confidence; customer relations and

confidence; vendor relations and confidence; intellectual property; regulatory and legal costs; and, operational capability. All cybersecurity events have the potential to negatively impact RFC in one or more of these areas.

Cybersecurity events have been shown to have a significant impact on investor’s willingness to invest (Perols & Murthy, [2021).](#_bookmark5) This is unsurprising as weak cybersecurity for financial institutions represents a real threat to operational capabilities which would impact profitability. Fiserv, a payment enablement corporation that services 1.4B global accounts for roughly 10,000 financial institutions globally noted in a recent report that consumers are highly concerned about cybersecurity and change their behavior in response to cybersecurity events impacting their financial service providers (Davies, [2020).](#_bookmark0)

Vendor management risk may be the most serious area of impact. Currently, vendors are largely rewarded for innovative technologies that bring new services and capabilities to customers. The vendors receive these rewards regardless of the risk exposure their products induce to their direct customers (Vagle, [2020).](#_bookmark12) Security breaches at RFC will not likely be attributed to RFC’s vendors should RFC customer data be impacted.

And, RFC’s customers desire the kinds of innovative technology that vendors are producing often without adequate security testing.

Cyberattacks, of course, always present a threat to intellectual property. Whenever an unauthorized person has access to confidential, restricted, or secret data, there is a risk to intellectual property. As of 2015, only 16% of a corporation’s value is related to tangible assets. The various types of intellectual property provide the basis for a much larger percentage of corporate value. This property can take the form of trademarks, design rights, copyright, patents, trade secrets, customer data, and other confidential data (Wymer, [2018).](#_bookmark13) Because of the international nature of cybercrime, the ability to effectively protect intellectual property after an event is limited, as the jurisdiction to where the data is moved may not even be known or knowable.

Regulatory and legal costs of cyberattacks can be extensive. Victims of cybercrime

often face costs related to reporting requirements; forensic investigations to determine what data was accessed or stolen; costs associated with notifying customers; costs associated with protecting customers from further harm such as credit repair services, credit monitoring services, identity theft insurance, and so forth. Companies may also face potential fines from state and federal authorities if cybersecurity practices are deemed to have been inadequate or if notifications were delayed beyond required reporting timelines (Baer & Dodson, [2021).](#_bookmark1)

Finally, there is the potential threat upon operational capability. As the recent ransomware attack on Colonial Pipeline Co. showed, cyberattacks can completely cripple operational capacity given the right circumstances (Neuman, [2](#_bookmark4)021). Obviously, the potential impact on a financial institution being unable to meet operational demands would have a knock-on effect to customers as well as potentially generating enormous regulatory and legal costs related to such events.

The growth of electronic and connected financial services increases the risks that RFC faces from external threats. It has been pointed out that cybersecurity breaches are a systemic phenomenon for the financial services industry. This is in part because

cyber-technology is now considered “must have” features for financial consumers (Uddin

et al., [2020).](#_bookmark11) This creates a system risk to financial systems. Any one financial institution’s external risk is a function of the attack surface the institution presents. The greater the number of technology services offered to customers, the greater the external threats.

However, the fewer technology services offered to customers, the lower the financial institution’s appeal is to customers.

As Uddin et al. [(2020)](#_bookmark11) notes, this means that cybersecurity risk is unavoidable. But, more importantly, the costs associated with the necessary investment to address cyber-risks and losses is an operational expense and will almost never be adequately covered by insurance against cyberattacks (Low, [2017).](#_bookmark2)

# Guidance

Addressing cybersecurity risks requires a holistic approach to technology operations.

Security must be a component of all activities and thought of as a “built-in” rather than “bolted on” feature. The US Government has acknowledged that developing ways to scale security and to ensure security is retained when systems are combined is one of the “five hard problems” of security (Scala et al., [2019).](#_bookmark9) However, as a key issue facing RFC is the adoption of technology to retain or gain competitive advantage, it is a problem that must be tackled head-on.

To this end, security operations must address the overall integrity of the environment, and not be focused on system-level security. A new way of addressing this problem is to employ Chaos Engineering (Rosenthal & Jones, [2](#_bookmark7)020). This approach, developed at Netflix explores the complexities of a highly interconnected system by forcing component and sub-component failures randomly and unpredictably as part of integration testing. By varying different failure modes and combinations of modes, weaknesses in the system can be discovered more readily and resiliency increased.

While RFC has strong security practices at the component level, those practices should be augmented to include chaos engineering as a requirement. This is in no small part because most cyberattacks and data breaches start with human error providing

mis-configured vulnerabilities (Torkura et al., [2020).](#_bookmark10) By analyzing risks of various attacks, and injecting faults into the system which could expose those risks, By adding a strong chaos engineering practice, similar to that employed by web-cloud services such as Amazon and Google, RFC will drastically improve the overall security of their environment.

This technique can be applied for every internal and external connection point both between systems and components and within systems that rely upon web-api functions for data access. This will address the overall attack surface of RFC with a robust testing methodology that is focused on discovering areas of heightened risk based on potentially realizable faults and accounting for the realities of both human and system error. While

this method, as with any method, can not guarantee a secure environment, it actively seeks to address the “hard problems” in cybersecurity and provides a truly robust, holistic, and realistic testing framework for cybersecurity in a low-cost, repeatable, and highly automated way.

# References

Baer, A., & Dodson, C. (2021). Victims of solarwinds cyberattack face investigation costs, liability issues [newspaper]. *Bloomberg Law*. Retrieved May 14, 2021, from [https://news.bloomberglaw.com/privacy-and-data-security/victims-of-solarwinds-](https://news.bloomberglaw.com/privacy-and-data-security/victims-of-solarwinds-cyberattack-face-investigation-costs-liability-issues) [cyberattack-face-investigation-costs-liability-issues](https://news.bloomberglaw.com/privacy-and-data-security/victims-of-solarwinds-cyberattack-face-investigation-costs-liability-issues)

Davies, A. (2020, January 15). *2020 trends in fraud and financial crime risk management*. Fiserv. Retrieved May 13, 2021, from [https://www.fiserv.com/en/about-fiserv/the-](https://www.fiserv.com/en/about-fiserv/the-point/2020-trends-in-fraud-and-financial-crime-risk-management.html) [point/2020-trends-in-fraud-and-financial-crime-risk-management.html](https://www.fiserv.com/en/about-fiserv/the-point/2020-trends-in-fraud-and-financial-crime-risk-management.html)

Low, P. (2017). Insuring against cyber-attacks. *Computer Fraud & Security*, *2017* (4), 18–20. <https://doi.org/10.1016/S1361-3723(17)30034-9>

Murphy, M. M., & Scott, A. P. (2016, March 23). *Financial services and cybersecurity: The* *federal role*. Congressional Research Servcie.

Neuman, S. (2021). What we know about the ransomware attack on a critical u.s. pipeline [newspaper]. *NPR.org*. Retrieved May 14, 2021, from [https://www.npr.org/2021/05/10/995405459/what-we-know-about-the-](https://www.npr.org/2021/05/10/995405459/what-we-know-about-the-ransomware-attack-on-a-critical-u-s-pipeline) [ransomware-attack-on-a-critical-u-s-pipeline](https://www.npr.org/2021/05/10/995405459/what-we-know-about-the-ransomware-attack-on-a-critical-u-s-pipeline)

Perols, R. R., & Murthy, U. S. (2021). The impact of cybersecurity risk management examinations and cybersecurity incidents on investor perceptions and decisions. *Auditing: A Journal of Practice & Theory*, *40* (1), 73–89. <https://doi.org/10.2308/AJPT-18-010>

Regions Financial Corp. (2021, February 24). *2020 10-k final*. Retrieved May 13, 2021, from [https://ir.regions.com/~/media/Files/R/Regions-IR/documents/2020%2010-](https://ir.regions.com/~/media/Files/R/Regions-IR/documents/2020%2010-K%20Final%20Draft%20for%20Website.pdf) [K%20Final%20Draft%20for%20Website.pdf](https://ir.regions.com/~/media/Files/R/Regions-IR/documents/2020%2010-K%20Final%20Draft%20for%20Website.pdf)

Rosenthal, C., & Jones, N. (2020). *Chaos engineering : System resiliency in practice*.

Sebastopol, O’Reilly Media. Retrieved May 14, 2021, from http://proxy1.ncu.edu/login?url=https://search.ebscohost.com/login.aspx?direct= true&db=edsebk&AN=2430575&site=eds-live

Scala, N. M., Reilly, A. C., Goethals, P. L., & Cukier, M. (2019). Risk and the five hard problems of cybersecurity. *Risk Analysis*, *39* (10), 2119–2126. <https://doi.org/10.1111/risa.13309>

Scott, A. P. (2021). Introduction to financial services: Financial cybersecurity.

*Congressional Research Service: Report*, 1–3. Retrieved May 13, 2021, from http://proxy1.ncu.edu/login?url=https://search.ebscohost.com/login.aspx?direct= true&db=tsh&AN=150117923&site=eds-live

Torkura, K. A., Sukmana, M. I. H., Cheng, F., & Meinel, C. (2020). Cloudstrike: Chaos engineering for security and resiliency in cloud infrastructure. *IEEE Access*, *8*, 123044–123060. <https://doi.org/10.1109/ACCESS.2020.3007338>

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: A synthesis of literature. *Risk Management*, *22* (4), 239–309. <https://doi.org/10.1057/s41283-020-00063-2>

Vagle, J. L. (2020). Cybersecurity and moral hazard. *Stanford Technology Law Review*, *23* (2), 71–113. Retrieved May 13, 2021, from http://proxy1.ncu.edu/login?url=https://search.ebscohost.com/login.aspx?direct= true&db=a9h&AN=146575576&site=eds-live

Wymer, K. V. (2018). Cybersecurity, shareholders, and the boardroom: An analysis of current and proposed measures for protecting corporate intellectual property. *Journal of Intellectual Property Law*, *25* (2), 227–240. Retrieved May 14, 2021, from http://proxy1.ncu.edu/login?url=https://search.ebscohost.com/login.aspx?direct= true&db=a9h&AN=133417615&site=ehost-live&scope=site