RICHEY MAY
MORTGAGE TREND SERIES

2021 Q4 Mortgage Trend Series

Richey May's quarterly webinar series where our mortgage industry experts come together to give you insight into market trends that we're seeing as we serve clients across our various mortgage banking practices.

RICHEY MAY
MORTGAGE TREND SERIES

Housekeeping

- This webinar is being recorded today
- All questions will be addressed at the end if time allows (and via email if we run out of time)
- Presentation slide deck and recording will be distributed within 1-2 business days
- There will be a quick survey after the webinar

RICHEY MAY | Advisory

Today's Presenters

Mignonne Davis,
Internal Audit Manager

Olivia Nicholson
Director, Business Intelligence & Analytics

Jason Hamilton, CISSP
Director, Cybersecurity Services

RICHEY MAY
MORTGAGE TREND SERIES

Today's Agenda

- Compliance and Internal Audit trends impacting the mortgage industry
- Benchmarking trends in operations and finance
- State of Cyber Update: trends, recent case studies, and attack prevention ideas

Regulatory Emphasis on Compliance Increases

- CFPB emphasis on Mortgage Servicing
- Regulation F (FDCPA) Final Rule – Effective date of November 30, 2021
- State Regulators
- Fannie Mae requirements for Compliance Management Systems and Internal Audit

Regulatory Emphasis on Compliance Increases

- CFPB scrutinizing mortgage servicers:
  - Nearly 750,000 active forbearance plans were set to expire in September and October, according to figures from Black Knight, which means servicers processed up to 18,000 plans per business day during those two months.
  - According to the CFPB's acting director, David Uejio, there could be serious consequences for those servicers that don't comply with the regulations
- CFPB Report issued 8/10/2021 Mortgage Servicer's Pandemic Response varies significantly
  - Call Metrics
  - Forbearance exit metrics
  - Delinquency metrics
  - Borrower profile and limited English proficiency
  - Nearly half of the servicers in the report stated they do not collect or maintain language preferences which may lead to borrowers not receiving needed language assistance. Some servicers also stated they do not maintain borrower race which could lead to fair lending violations.
  - Pandemic assistance enrollment metrics

Regulatory Emphasis on Compliance Increases

- April 1, 2021 bulletin 2021-02—CFPB expects servicers to resource these activities appropriately and urged servicers to dedicate sufficient resources and staff.
  - Providing clear information to borrowers about options for payment assistance
  - Adherence to Regulation X for proactive borrower outreach
  - Adherence to ECOA (discrimination against applicants)
    - Fair servicing for limited English proficiency
    - Fair servicing for income derived from part-time employment, alimony, child support, public assistance etc.
  - Customer Service/telephone hold times
  - Continuity of Contact/Single Point of Contact
  - Timely and consistent Loss Mitigation evaluations
  - Adherence to Regulation X foreclosure protections and other Federal or State protections/restrictions
  - Fair Credit Reporting Act

Regulatory Emphasis on Compliance Increases

- Regulation F Final Rule – Effective date of November 30, 2021
  - Call Frequency Restrictions
  - Limited Content Messages / voice mail
  - Time and Place Requirements
  - Reasonable procedures for Email and Text Communication
  - Requirements for Providing Legally-Required Disclosures Electronically
  - Translated Disclosures / Limited English Proficiency Requirements for Disclosures
    - The Bureau is adopting a requirement that debt collectors make the disclosures required by §1006.18(e)(1) and (2) in the same language or languages used for the rest of the communication in which the disclosures are conveyed.
  - Validation Notices
  - Mortgage specific Validation Notice option that replaces itemization information with attached periodic statement

Regulatory Emphasis on Compliance Increases

- State regulators are increasing the number of companies they are auditing. With more states opening up, and auditors returning to offices, Richey May has heard of a number of companies being notified that they've been selected for audit.
- CA continues to scrutinize lenders' processes and compliance with strict escrow requirements.
  - Placement of Escrow Funds
  - Escrow Cash Accounts
  - No debit balances are allowed in the loan level liability accounts
  - California disclosures – Fair Lending notice must have correct name and address for the Department of Financial Protection and Innovation (DFPI)
  - Per diem interest on California loans-- ensure calculations are not in excess of the amount permitted by Financial Code section 50204, subdivision (o), and Civil Code section 2948.5.

Regulatory Emphasis on Compliance Increases

- Margin calls last March created chaos in the industry and lenders applied for Fannie Mae approvals in record numbers. Now, lenders are working to maintain robust compliance management systems and internal audit functions, whether staffed internally or outsourced to a 3rd party.
- An effective Compliance Management System has two interdependent control components:
  - Board and Management Oversight
  - Compliance Program which includes:
  - Policies and Procedures
  - Change Management Controls
  - Training designed to be borrower focused and to mitigate borrower harm
  - Compliance and Control Monitoring and Testing
  - Issue Resolution / Corrective action
  - Consumer Complaints
  - Service Provider Oversight

Regulatory Emphasis on Compliance Increases

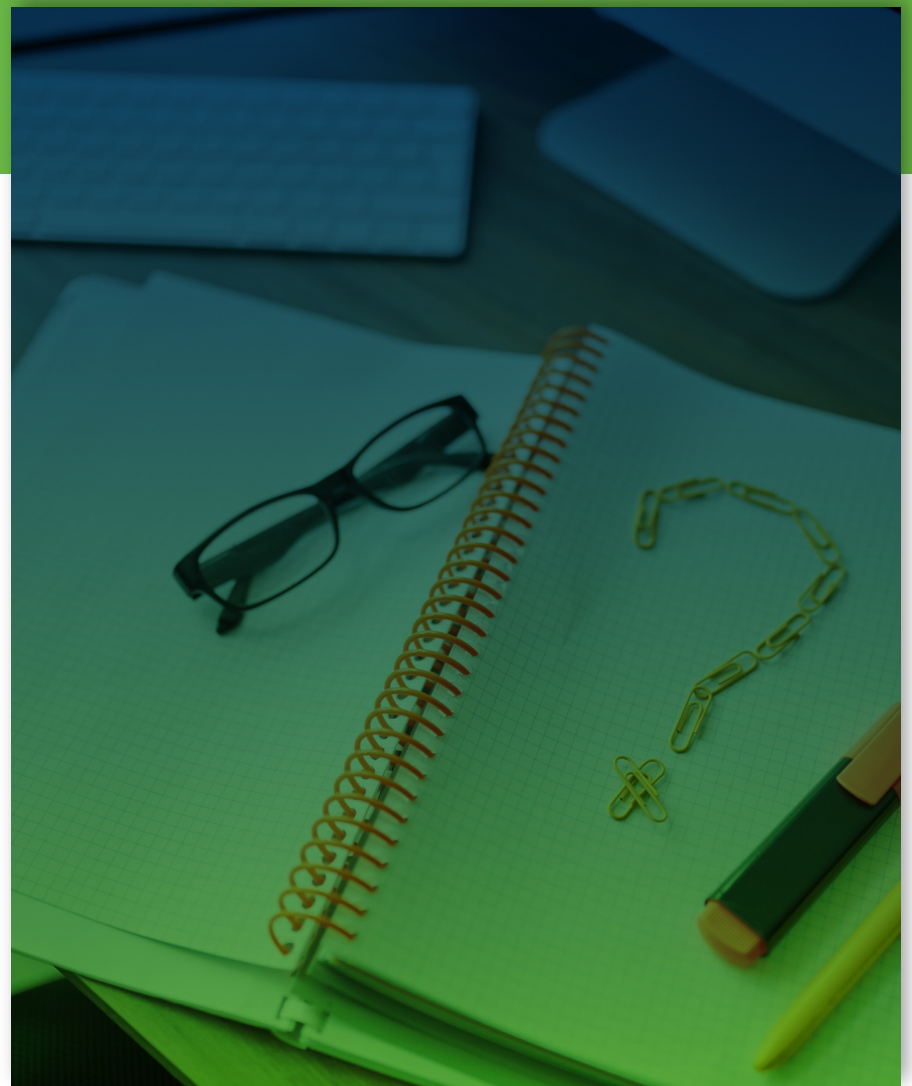
- Building a strong Internal Audit Function
  - Conduct a Risk Assessment
  - Develop an Audit Schedule/Plan
  - Develop a process to review the audit schedule periodically and adjust to incorporate emerging risks
  - Conduct audits and review findings with senior management and/or the audit committee
  - Establish a framework for communication and collaboration between internal audit function and the business units to assist the business units as they build the control environment
- What can lenders and servicers do to develop a Compliance Management System and an Internal Audit Function?
  - Decide if you have the resources and skill set internally to develop the internal audit function inhouse or whether you need to outsource the function.
  - Identify your lines of defense; how strong are they?
  - Documenting policies and procedures to prepare for the risk assessment
  - Have each business unit take inventory of the automated and manual controls in their department such as system hard stops, second level review processes and exception reports
  - Gather policies and procedures into a central location
  - If you have already done this, review the P&Ps and update as necessary

Tax Law Changes

- There have been a number of proposed tax provisions included in the recent infrastructure bills, and broader tax reform continues to be discussed – and expected.
  - Early end to the COVID-related Employee Retention Tax Credit (ERTC), now set to expire on 9/30/21
  - 1099 reporting requirements for digital asset brokers
- We are closely following additional tax law discussions and proposals and will schedule a separate webinar as soon as we have more clarity on the changes we can expect.

RICHEY MAY
MORTGAGE TREND SERIES

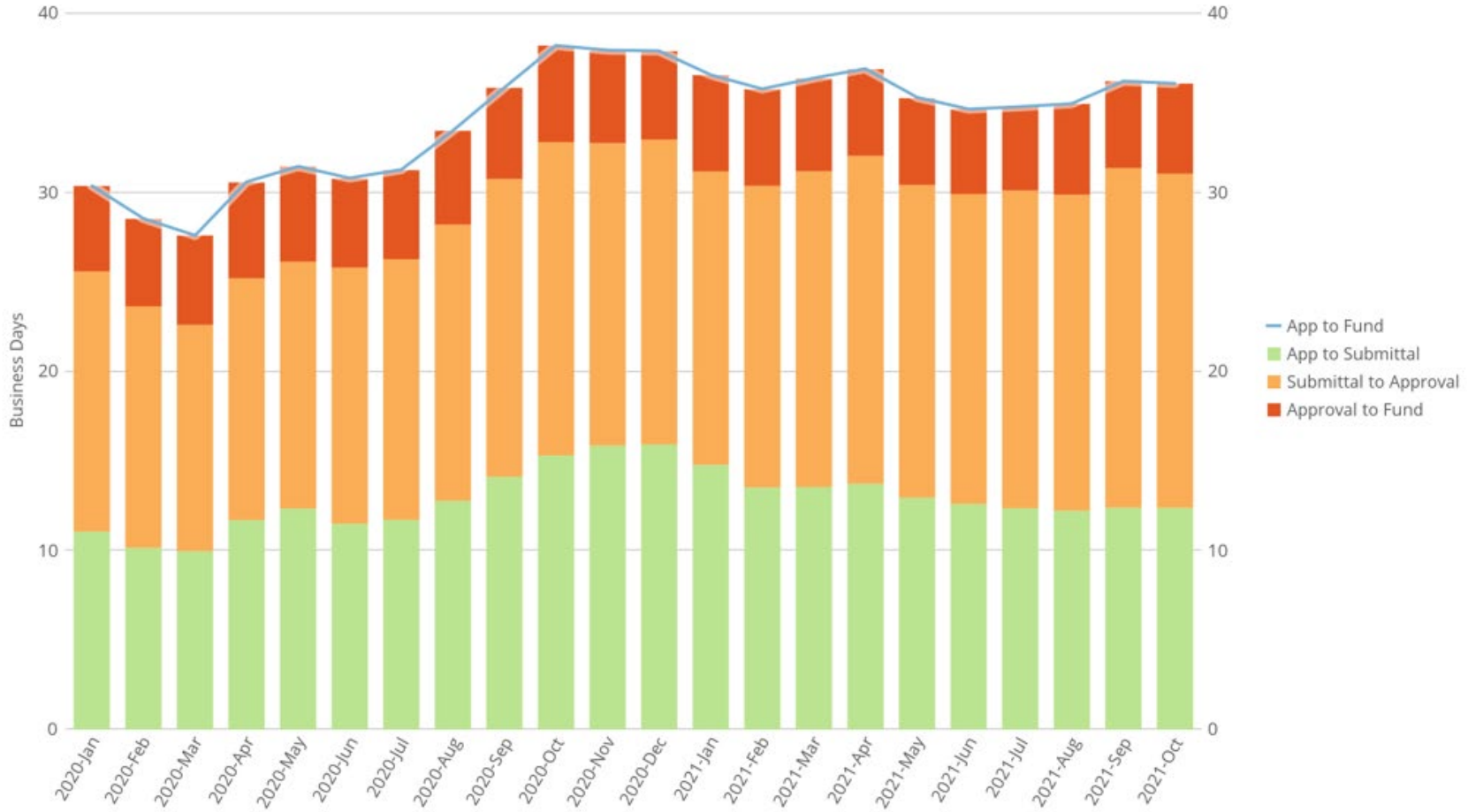
RICHEY MAY
ANALYZE



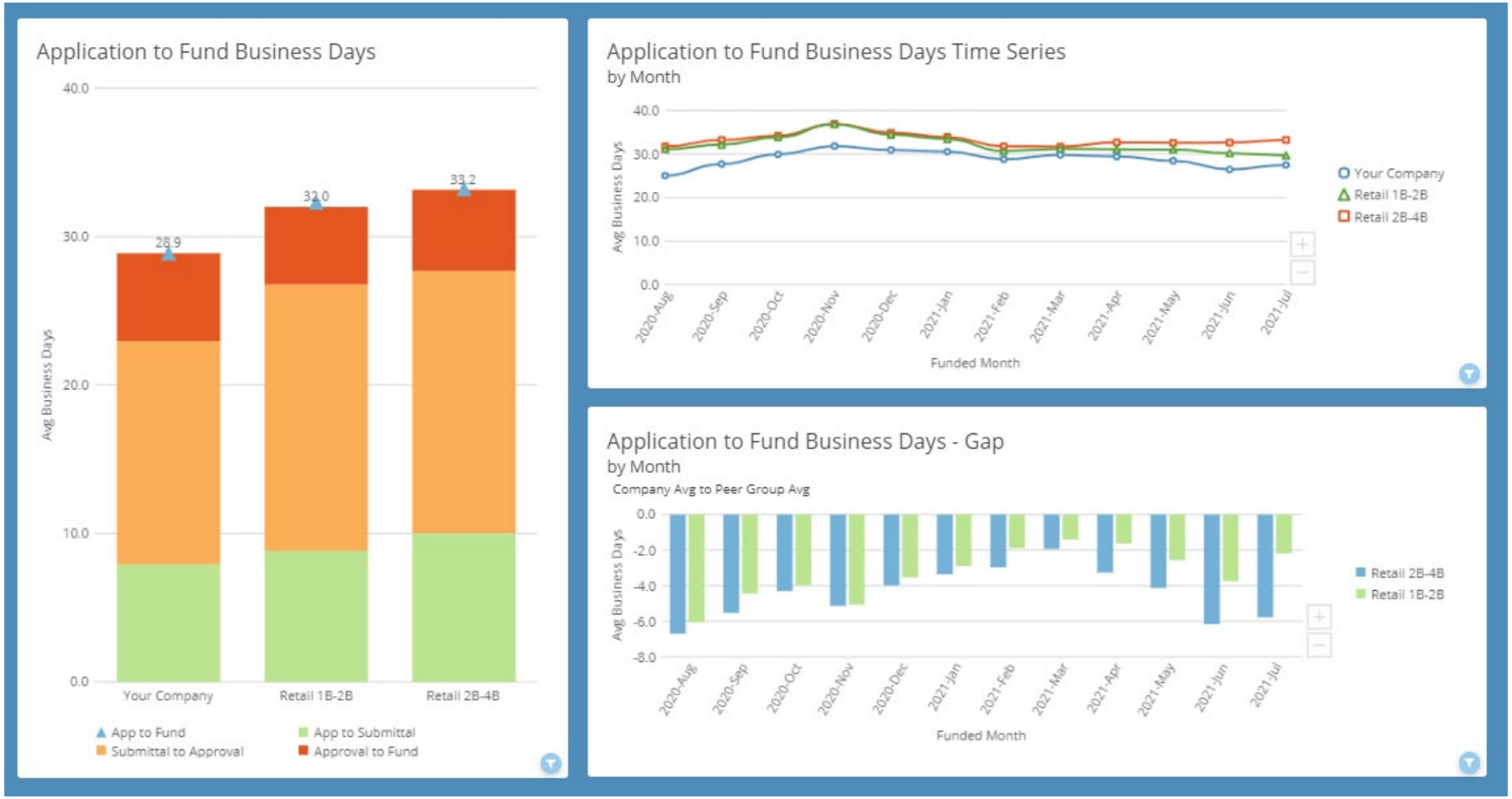
Business Intelligence for Mortgage

- Operations turn times
- Peer View Ops benchmark reporting

Operations – Turn Times



Peer View Ops – Turn Times



RICHEY MAY
MORTGAGE TREND SERIES

RICHEY·MAY SELECT

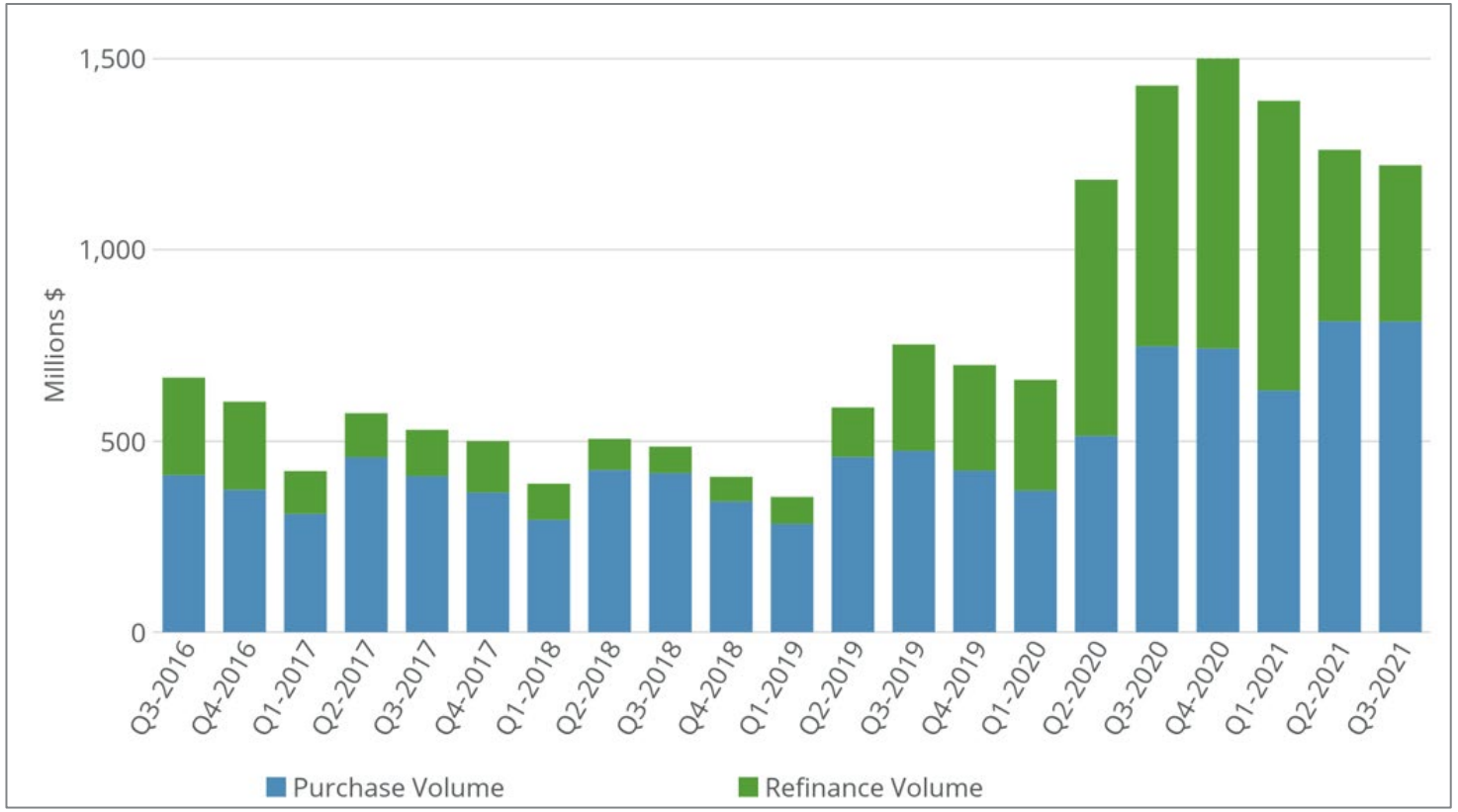
Financial Benchmarking for IMBs

- Q3 was relatively flat across all production & financial metrics
- Increased costs to originate
- Productivity metrics continue to decline

Originations

- Q3-2021 volume down only 3%, still historically high
- 1.6x previous quarter high before 2020 (Q3-2019)
- Q3-2021 refi share dropped only slightly to 34% (from 36%)

Origination Volume (millions)

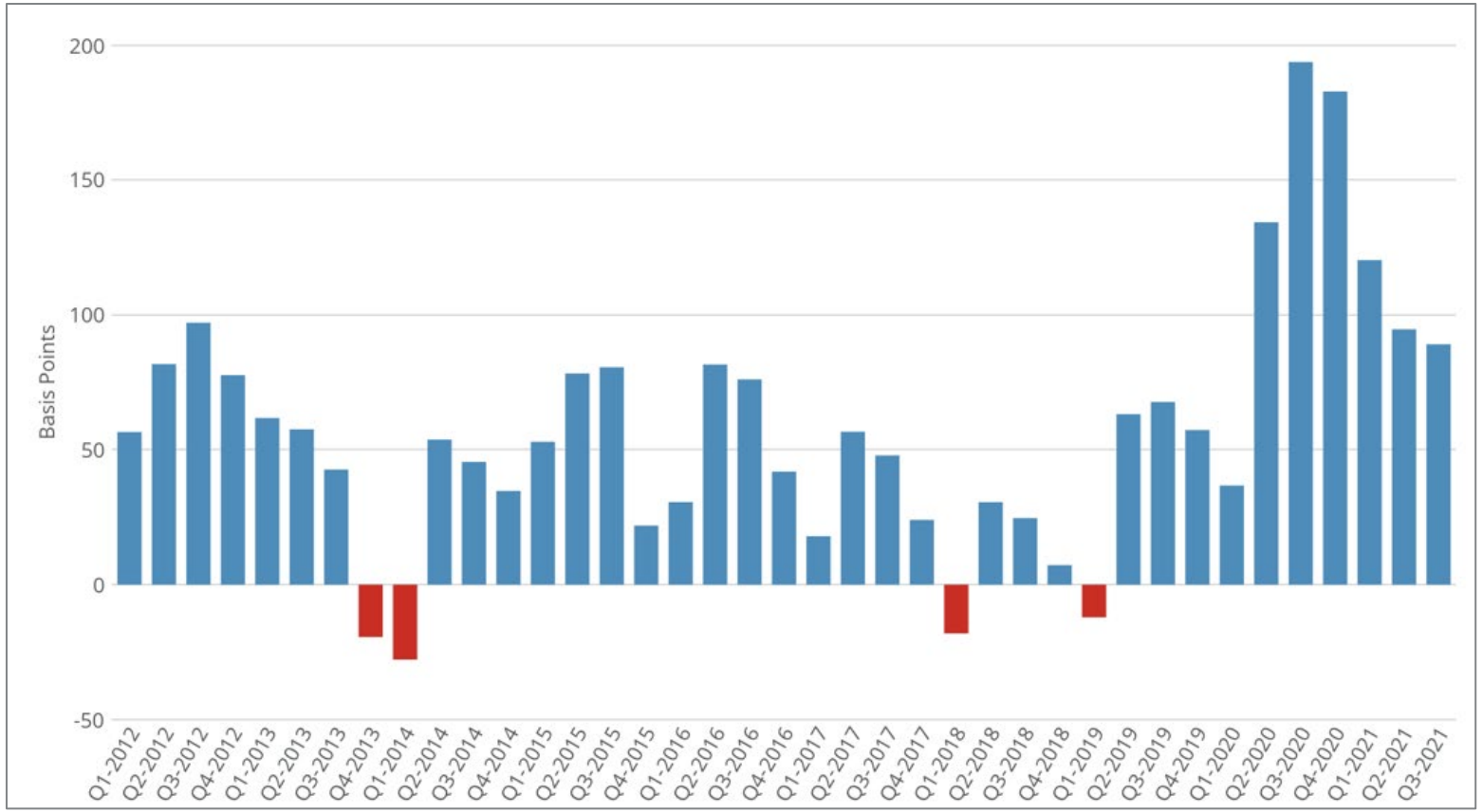


Source: RM Select, Financial Peer Group Benchmarking for IMBs

Net Production Income

- Q3-2021 NPI down 6bps (5.9%)
- Still higher than any pre-2020 quarter since 2012

Net Production Income Bps

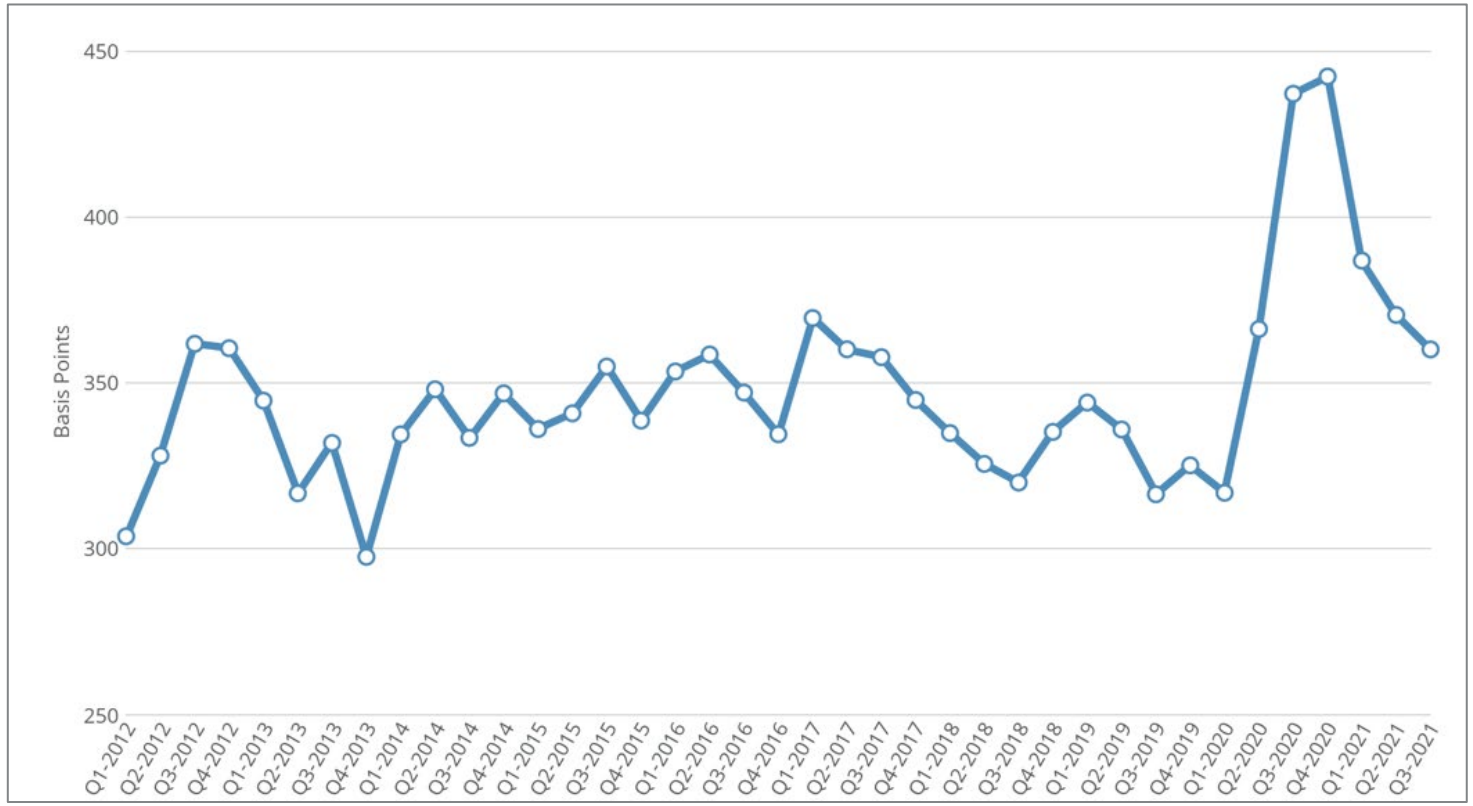


Source: RM Select, Financial Peer Group Benchmarking for IMBs

Secondary GOS

- Q3-2021 gain on sale down 10bps
- Still historically high

Secondary Gain On Sale Bps

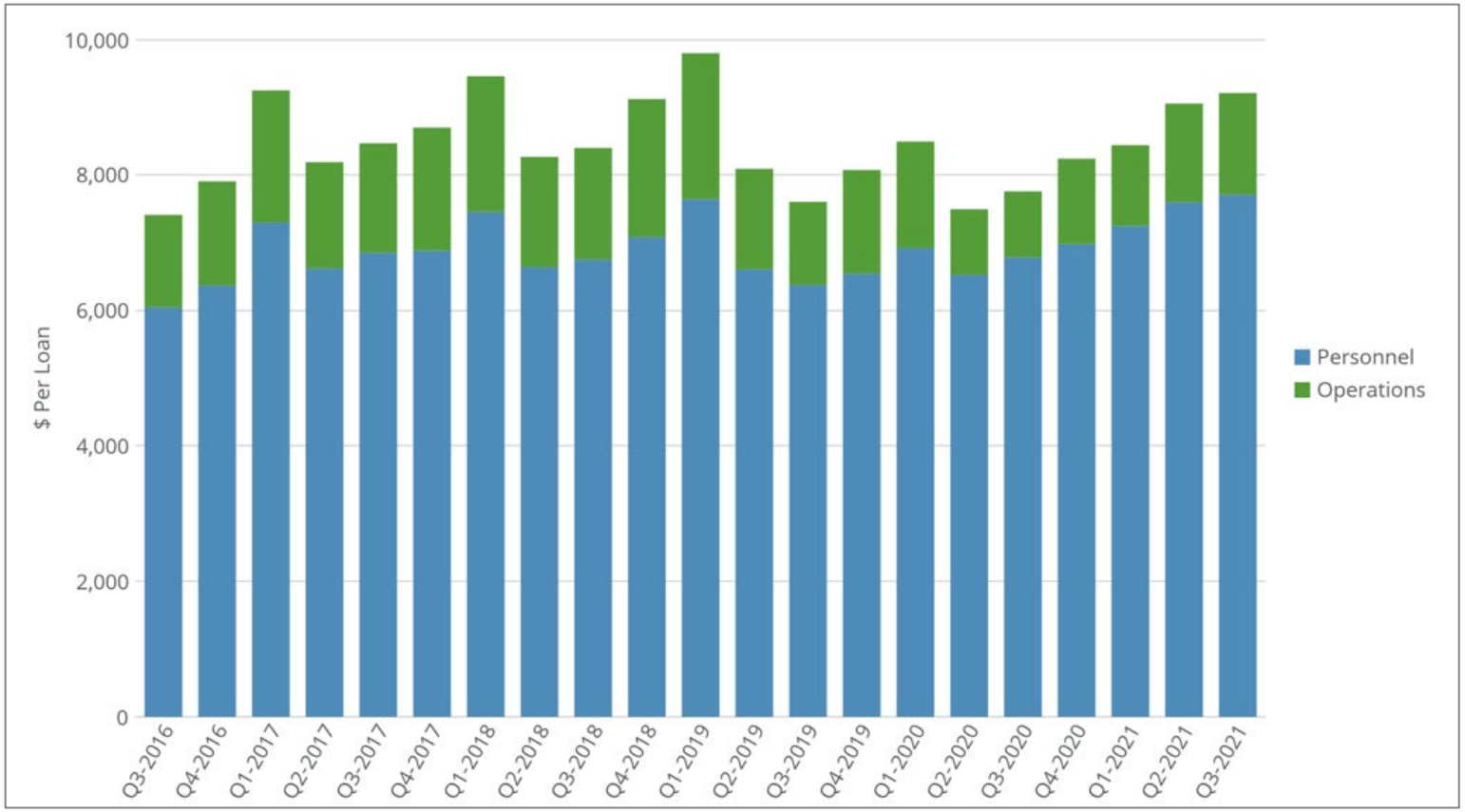


Source: RM Select, Financial Peer Group Benchmarking for IMBs

Costs to Originate

- Q3-2021 cost to originate up $157 per loan
- Sales CTOs for LOs, AEs & sales management up $117 per loan, while fulfillment and back office CTOs were flat or slightly down
- Operating costs up $45

Total CTO ($ per Funded Loan)



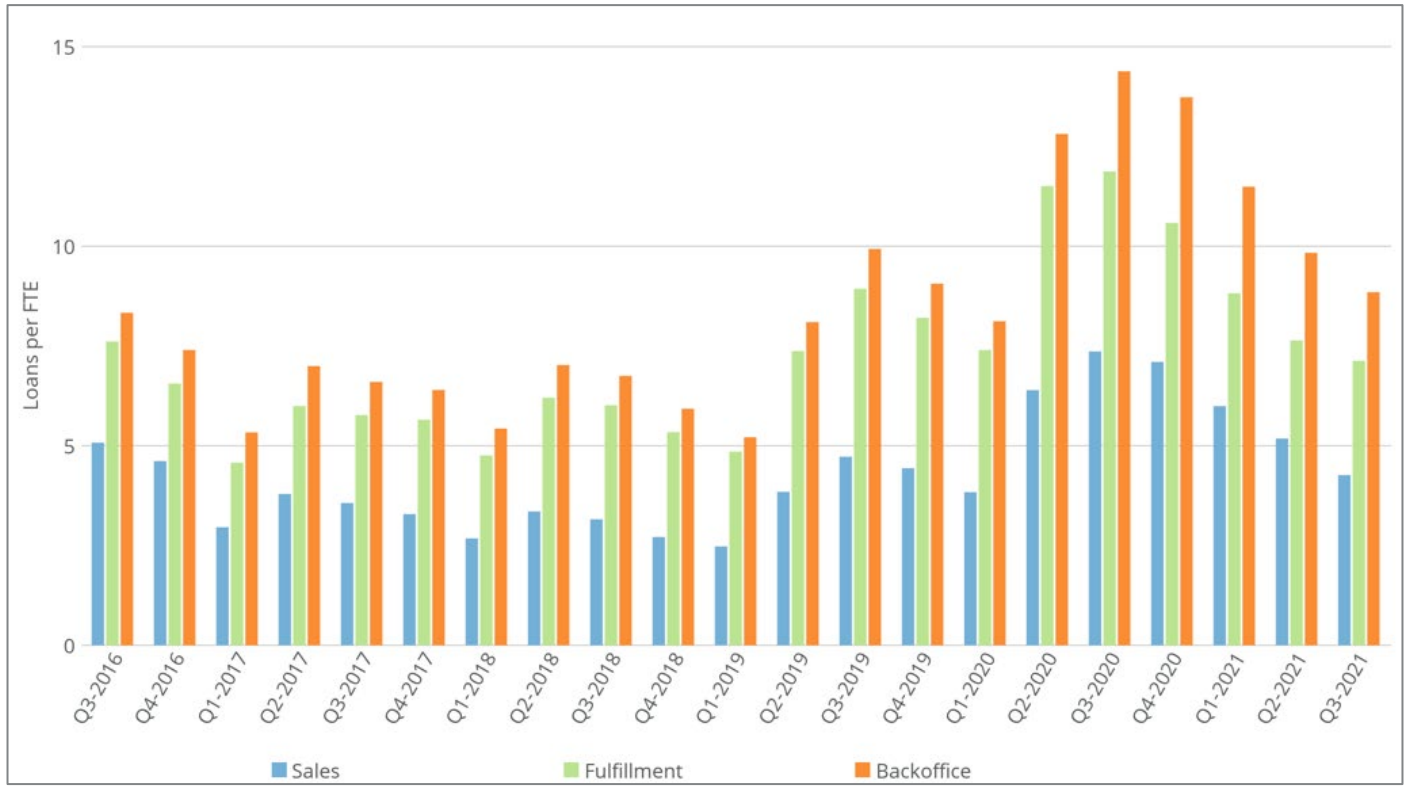
Source: RM Select, Financial Peer Group Benchmarking for IMBs

Servicing

- Q3-2021 closed loans per total FTE decreased to 1.95 from 2.17

- Declines in all headcount categories since Q3-2020

Closed Loans Per FTE

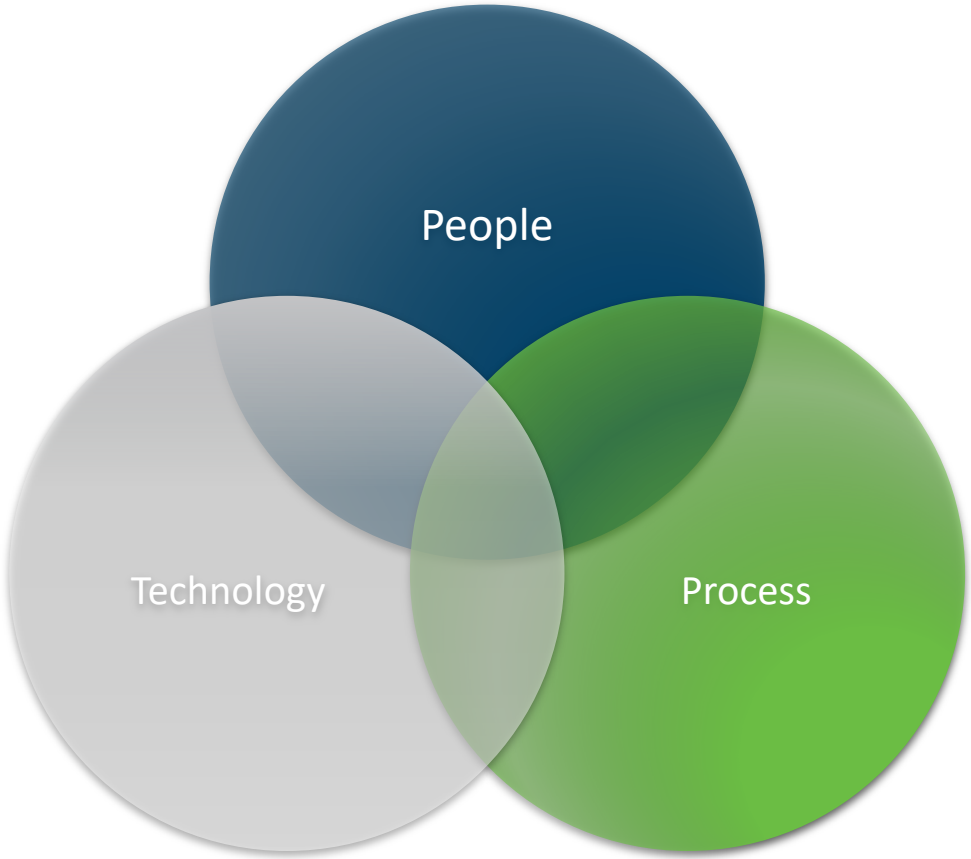


Source: RM Select, Financial Peer Group Benchmarking for IMBs

What is Cybersecurity?

- Cybersecurity is the combination of People, Process, and Technology working together to protect the Confidentiality, Integrity, and Availability of information assets that allow your business to function.

- The reason it seems so challenging is that for attackers to be successful, they **only need to compromise a single one of those elements, one time.**

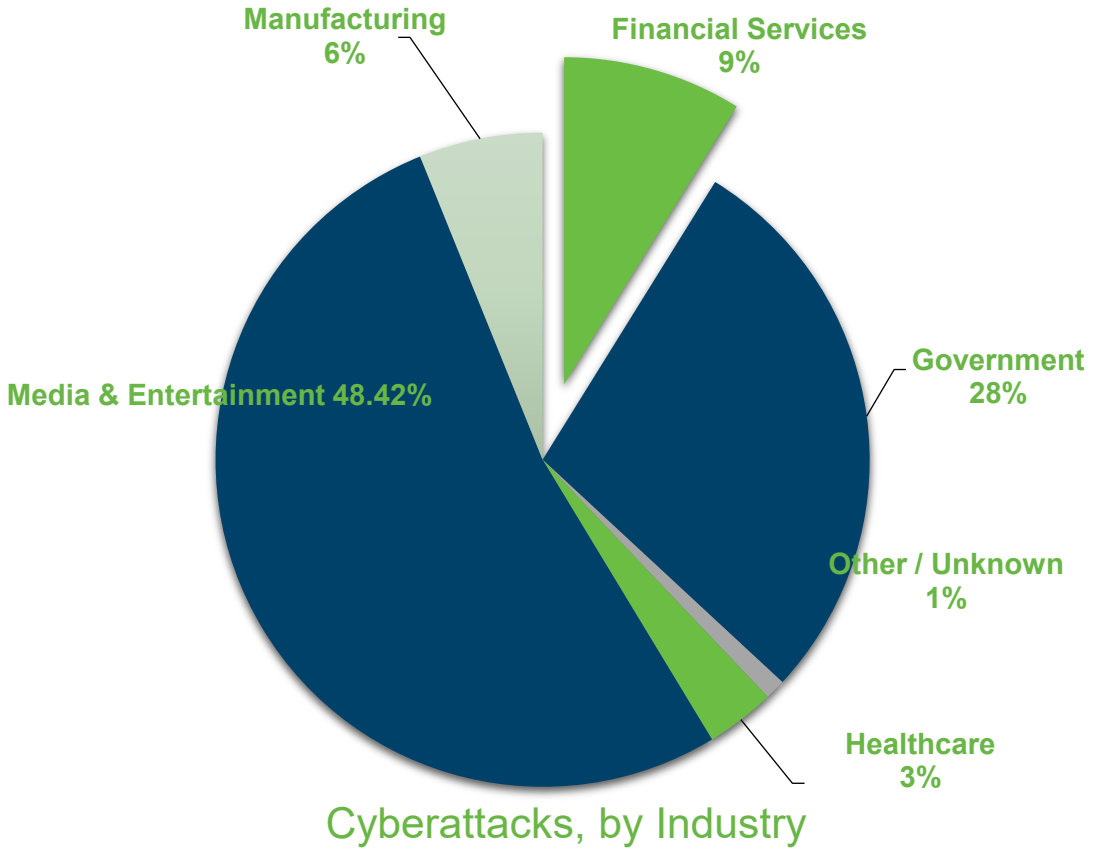


State of Cybersecurity

Today, the primary business for the majority of organizations is **INFORMATION.**

The Ponemon Institute reported Personally Identifiable Information (PII) is the costliest type of record to lose in a breach, at **$180** per record.*

The FBI IC3 identified **2,474** organizations in the United States impacted by Ransomware in 2020, with adjust losses of over **$29.1MM**.**



Cyberattacks, by Industry

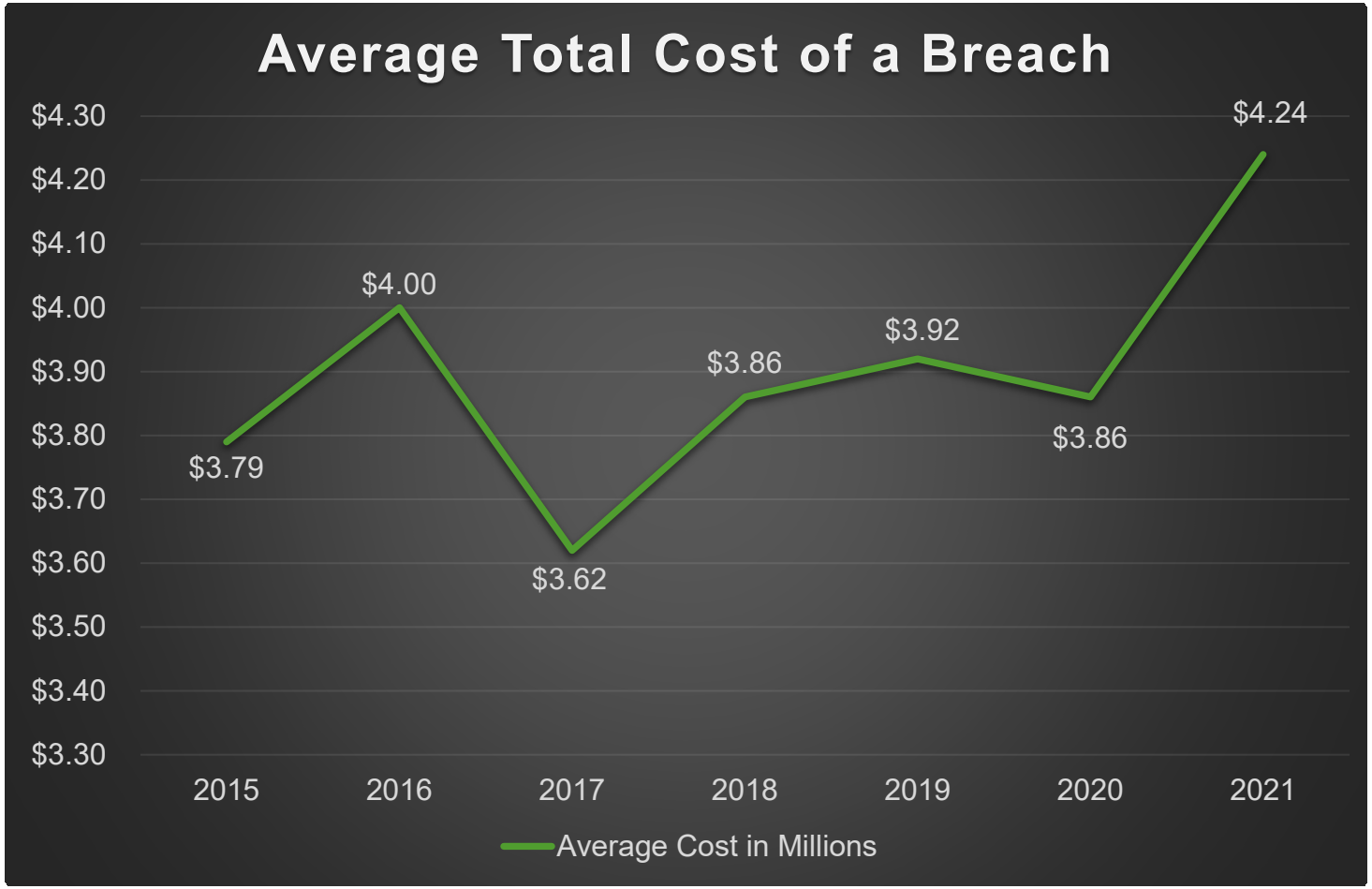
*IBM Cost of a Data Breach Report 2021 **2020 FBI IC3 Report

RICHEY MAY
MORTGAGE TREND SERIES

State of Cybersecurity

The 2021 Verizon Data Breach Report found that costs associated with remediation of cyber incidents are also on the rise.

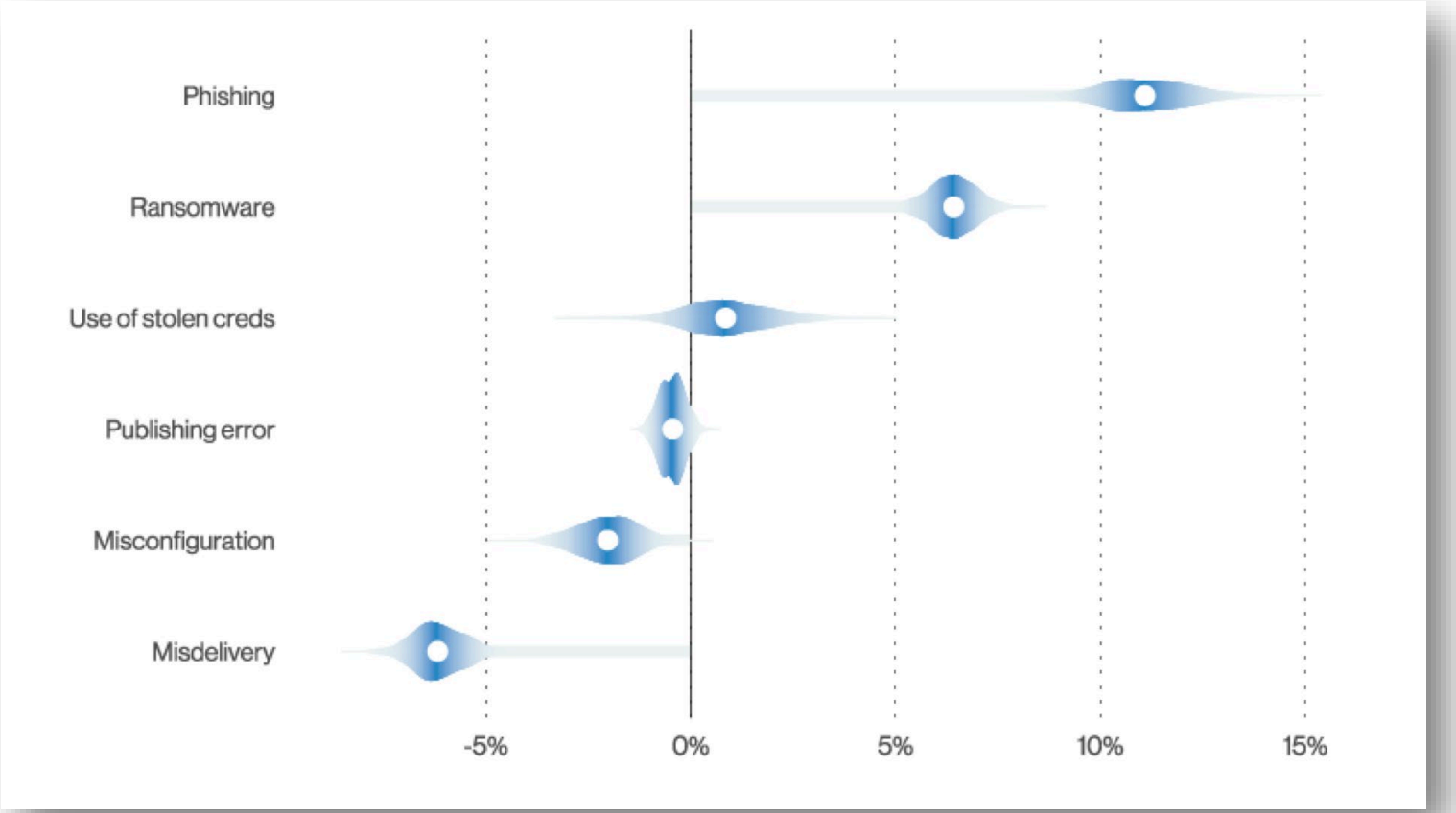
The Ponemon Institute finds the cost of a data breach has increased by **11.9%** since 2015, rising **$380,000** from 2020 to 2021.



Remote Work Challenges

The average cost was **$1.07 million** higher in breaches where remote work was a factor in causing the breach.*

Phishing continues to be most prevalent attack vector, as it has for the last two years.



*IBM Cost of a Data Breach report 2021

Current Threat Landscape

The **Window of Exposure (WoE)** metric represents the amount of time that an application has a serious vulnerability that can be exploited in a data breach.

Window of Exposure (WoE)

Roughly **40% of Finance applications** have vulnerabilities with a WoE of more than **365 days**.

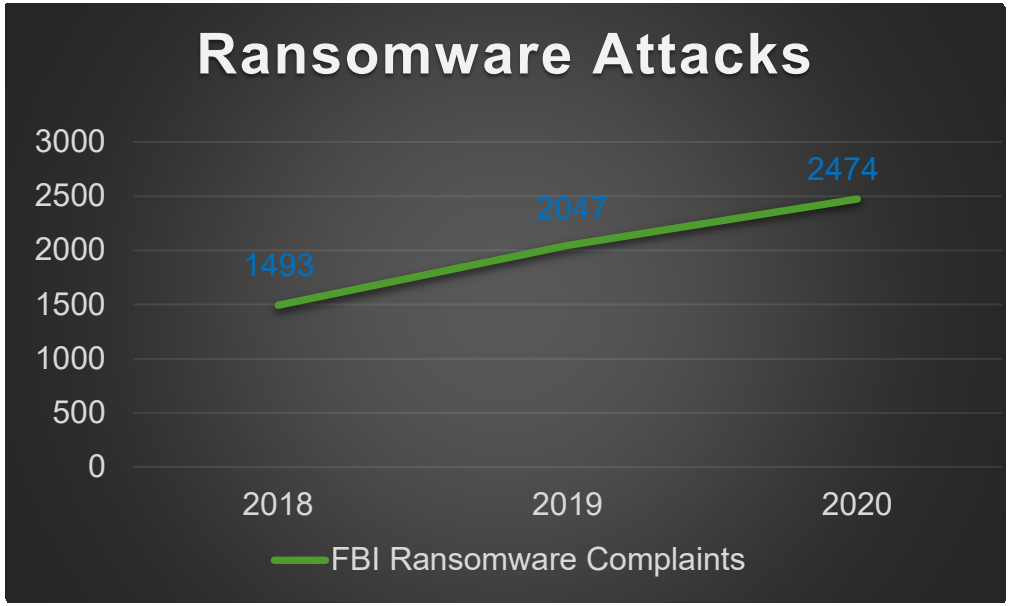
The Mean Time to Remediate (MTTR)

A report from WhiteHat Security found by the end of June 2021, all industries took an average of **246 days** to fix high-severity vulnerabilities.

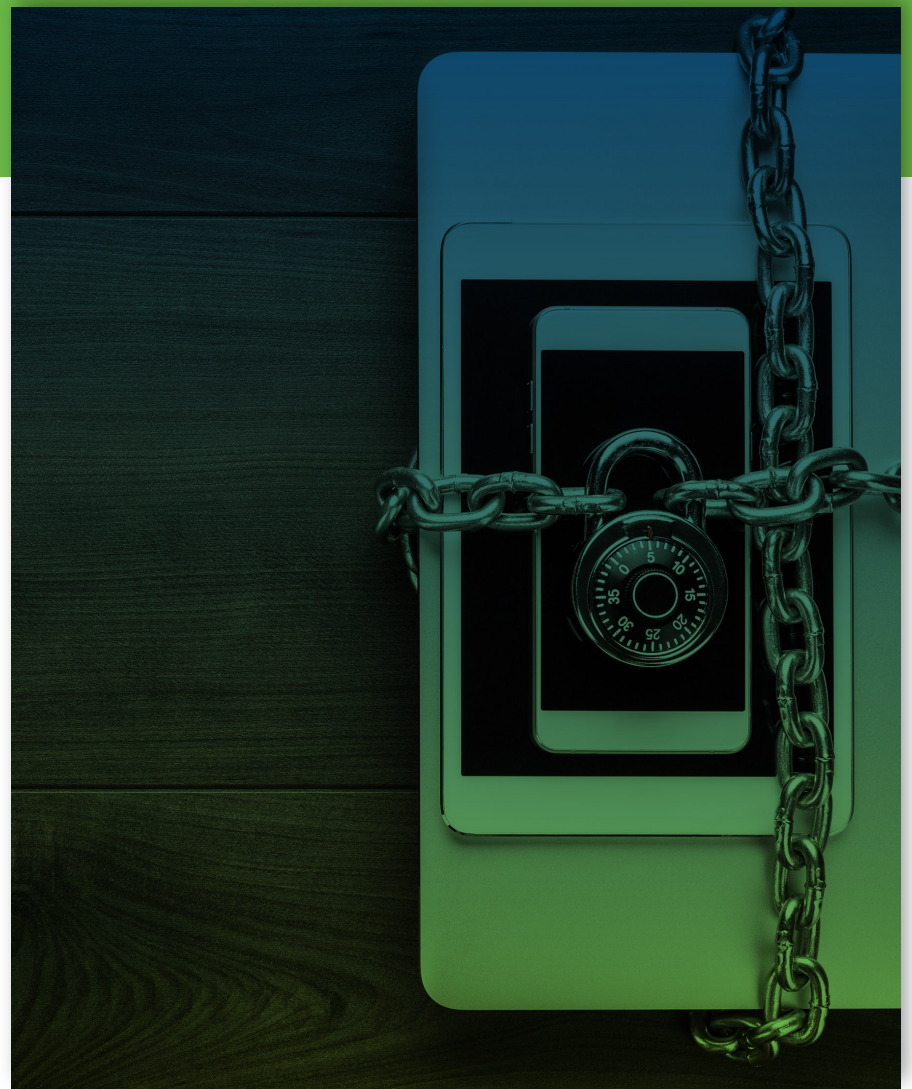
The Finance and Insurance industries average **286 days**.

Current Threat Landscape

Cyber attacks are more sophisticated than ever, and criminal organizations are leveraging the same technology delivery models we use in legitimate business. **Ransomware as a Service (RaaS)** has already become a standard attack method.



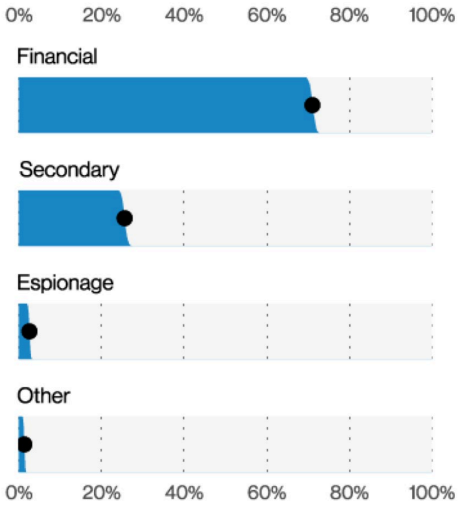
The ransomware attack on **Colonial Pipeline** in 2021 made national news when it resulted in a 6-day shutdown of fuel delivery to a large portion of the US. Although Colonial paid the ransom, they ultimately recovered normal operations by **restoring from their own data backups**.



State of Cybersecurity

THE VAST MAJORITY OF THESE ATTACKS ARE FINANCIALLY MOTIVATED.

As defined within the 2021 Verizon Data Breach Report, Organized Crime makes up nearly **80% of these attacks**, with less than 5% of them being Nation-state or State-affiliated attackers.



Compliance Requirements Continue

- Virginia has adopted a similar privacy law to California's CCPA.
- Illinois now has a cybersecurity law focusing on financial institutions very similar to New York NYDFS.NYCRR.500.
- Other states are adopting the FFIEC workbook as their cybersecurity framework for auditing and review.

Best Practices/Common Vulnerabilities

Multi-factor Authentication is For Everyone.

- Consider implementing Multi-Factor Authentication (MFA) for all remote access to your environment.
- MFA reduces the risk of users sharing passwords.
- MFA reduces the number of calls to your helpdesk for password resets.
- MFA reduces the ability of an attacker to compromise your platform remotely.

Best Practices/Common Vulnerabilities

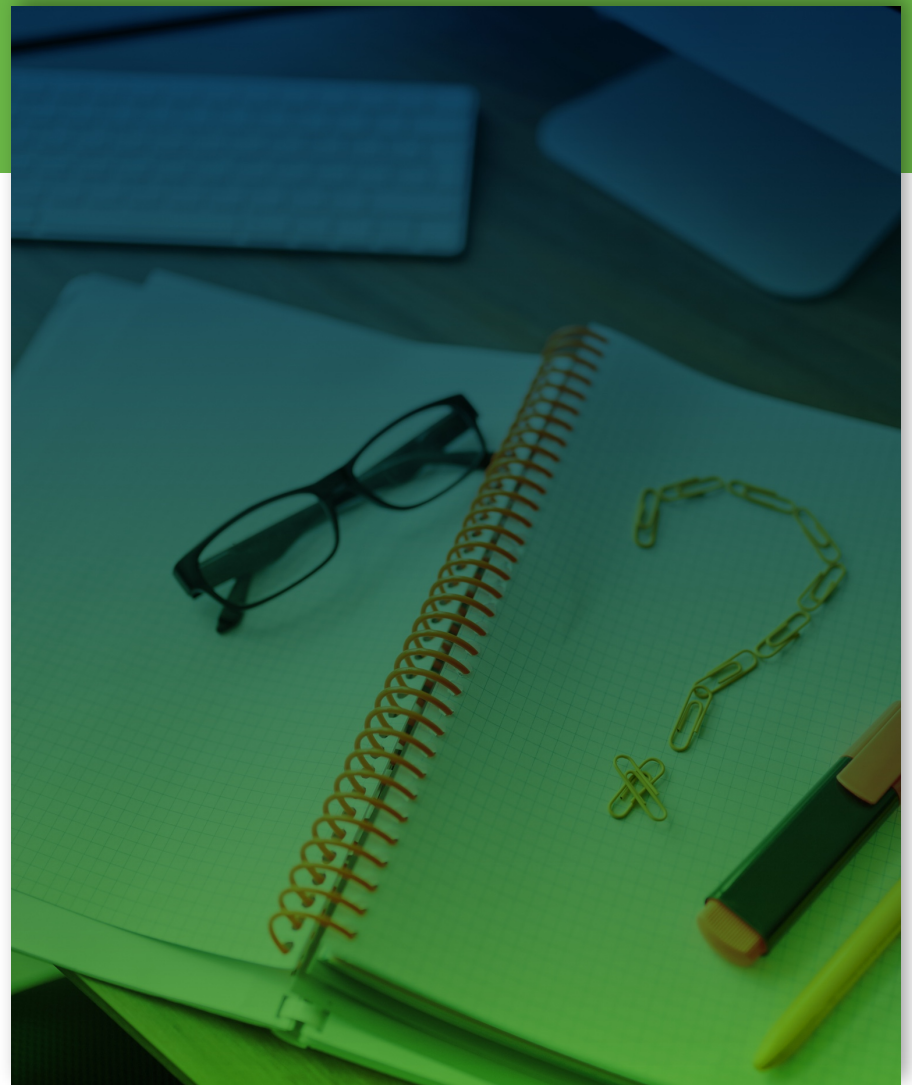
Develop, Update, and Test your Incident Response Plan:

- **76% of companies** surveyed by Cisco admitted to not having an updated IR/DR strategy.
- Having a comprehensive plan can reduce your downtime as well as help you respond to a cyberattack such as ransomware.
- Include contacting the FBI early in the response plan.
- Develop Technology Solutions that are resilient by design.
- Develop a Pandemic Plan (define a taskforce and communication strategy)
- **Test your plan.**

Best Practices/Common Vulnerabilities

Patch management is still one of the most important elements of security:

- Your customers' sensitive information is on endpoint devices, including smartphones, laptops, desktops, and servers.
- Patching reduces the threat of malicious software negatively impacting your daily business operation and compromising your customers' NPI data.
- Patching is not just for Microsoft products, but also 3rd party software from vendors such as Oracle and Adobe.
- Many of the major cybersecurity incidents that occurred in 2017, including Equifax, were the result of inadequate patch management practices.



Questions & Answers

Thank you!

For more questions and information regarding today's topics, please contact:

info@richeymay.com