DATA CUSTODY, SECURITY AND PRIVACY

The Era of Digital Adoption

M&G SOLUTIONS & kredit

EXECUTIVE SUMMARY

What is Data Custody, Security & Privacy?

Data Privacy is an individual's right to control their data. *Data Security* is the process of protecting data from unauthorized access and data corruption. *Data Custody* is the process of having the legal right and authentic control over a particular set(s) of data elements, which are then authorized for storage and use by any particular custodian(s) of that data.

Why Should You Prioritize Codifying Your Data Practices?

Data custody, security and privacy are the three foundational elements of building trust between a company and consumers. Appropriate data security protocols will be a significant differentiating factor for many consumers and potential clients.

What Regulatory Bodies Govern Compliance?

In 2016, the CFPB brought its first enforcement action against an Iowa-based online payment platform. Prior to that, data security had been a safety and soundness issue for financial institutions, not a consumer financial protection issue. The FTC has brought multiple legal actions against organizations that have violated consumers' privacy rights or misled them by failing to maintain security for sensitive consumer information or caused substantial consumer injury. Even the states are ramping up their efforts to enforce privacy - the California Consumer Privacy Act went into effect on January 1, 2020 and Virginia enacted the Consumer Data Privacy Act that goes into effect on January 1, 2023. Data privacy is likely to be a key area of legislative and enforcement focus under the Biden administration.

How Can My Organization Ensure Mastery?

Leveraging technology & 3rd party expertise that augments your digital strategy and aids in your efforts to comply with the numerous regulations that the ARM industry must abide by can reduce manual processes by enabling true automation. Your investment in technology should reduce your overall risk, minimize costs, increase efficiencies and help you gain a competitive advantage.

WHO SHOULD OWN DATA SECURITY, PRIVACY & CUSTODY?

Board & Management Oversight

In a depository or non-depository consumer financial services company, the board of directors is ultimately responsible for developing and administering a compliance management system that ensures compliance with consumer financial law. Because the effectiveness of a compliance management system is grounded in the actions taken by the board of directors and senior management, it is important that the board demonstrate clear expectations about compliance within the entity, and its service providers, and adopt a clear policy statement regarding consumer compliance.

Day-to-Day Accountability

Data Custodians are responsible for the safe custody, transport and storage of the data and implementation of business rules.

A *Data Steward* is an oversight or data governance role within an organization and is responsible for ensuring the quality and fitness for purpose of the organization's data assets, including the metadata for those data assets. A *Data Steward* may share some responsibilities with a *Data Custodian*, such as the awareness, accessibility, release, appropriate use, security and management of data.

Whether it's a dedicated *Information Security Officer*, *Privacy Officer*, *Data Custodian* or *Data Steward*, creating accountability for the planning, implementation and maintenance of data assets is a critical component to a successful *Data Security and Privacy Plan*.

Do Your Vendors Embrace Digital Innovation?

Your expectations of regulatory compliance for your vendor network should mirror the expectations of your own company. They should be clearly defined in any Contract, Schedule and/or Statement of Work that is entered into with a vendor.

KEY PERFORMANCE INDICATORS

The best IT security professionals use metrics to tell a story, especially when giving a report to non-technical colleagues. Some examples of clear metrics that you can track and present to stakeholders include *Intrusion Attempts, Mean Time to Detect Security Threats (MTTD), Mean Time to Resolve Security Attacks (MTTR) and Mean Time to Contain Attacks (MTTC).*

Escalation

Incident Response is the methodology an organization uses to respond to and manage a cyberattack. As the number of cyberattacks increases in scale and frequency, incident response plans become more vital to a company's cyber defenses. Equifax's decision not to share information with the public following its 2017 hack significantly hurt its brand. A successful Incident Response Plan contains appropriate and timely methods of escalating issues to stakeholders and is regularly reviewed with employees to ensure they understand their role in escalating issues.

Training

Education is essential to maintaining an effective compliance program and keeps your employees abreast of the requirements created by consumer financial law. Compliance training should be directed to individuals based on their roles, and commensurate to the nature and risks to consumers presented by the organization's activities. Training content should be reviewed regularly by a compliance professional to ensure the content is current and reflects things like new regulatory requirements, changes in business practices, or product offerings. As a best practice, training should be delivered at hire, prior to an employee having access to consumer data or speaking with consumers, and annually thereafter.

Privacy, Security & Custody Reporting

Understanding the types of reporting that is available on the platforms and systems that you use today and leveraging those reports to determine breaks in policy and procedure is a key component of compliance monitoring. The CFPB defines "monitoring" as, "a compliance program element that seeks, in an organized and risk-focused way, to identify procedural or training weaknesses to provide for a high level of compliance by promptly identifying and correcting weaknesses." If your reporting functions do not provide you with the insight into your privacy, security and data custody practices that you need to properly identify issues, consider leveraging outside expertise to help you develop a strong compliance monitoring program.

REGULATORY OVERSIGHT

Regulatory Requirements

There are a multitude of US regulations that address data custody, security and privacy that you should be evaluating. To name a few: Gramm Leach Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Fair Credit Reporting Act (FCRA), California Consumer Privacy Act (CCPA) and Virginia's Consumer Data Protection Act (CDPA). If you are transacting in the EU, then you should also consider the General Data Protection Regulation (GDPR) legislation.

Feedback Reviews

In the CFPB's 2016-02 Compliance Bulletin and Policy Guidance on Service Providers, they stated, "To limit the potential for statutory or regulatory violations and related consumer harm, supervised banks and nonbanks should take steps to ensure that their business arrangements with service providers do not present unwarranted risks to consumers." As such, it is imperative that your vendor oversight program include a regularly scheduled review of your vendor's internal policies and procedures, controls and training. The results of the review should lead to timely feedback and/or corrective action to address deficiencies.

Required Resources

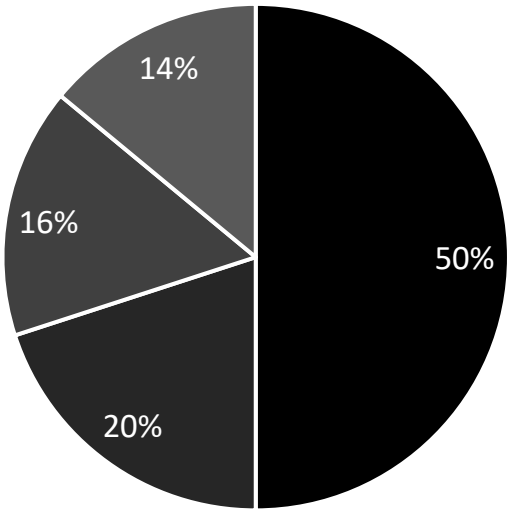
Conducting a SWOT (strengths, weaknesses, opportunities, and threats) analysis will facilitate a realistic, fact-based, data-driven look at the strengths and weaknesses of your organization and initiatives. Awareness and understanding of regulatory requirements is critical in today's regulator-heavy environment. If regulatory expertise is not one of your strengths, then engage with a professional that can help!

Review Cadence

The cadence of your security reviews should be commensurate with the size and complexity of your operations and practices. At a minimum, policies and procedures should be reviewed annually to ensure they reflect the organization's current practices. Based on compliance requirements such as PCI-DSS and ISO 27001, the frequency of vulnerability scans is generally quarterly. Penetration testing and certified security audits are typically performed annually. Ultimately, developing a schedule that both complies with regulatory or compliance requirements will greatly reduce the risk of a cyberattack against your organization.

RESOURCE ALLOCATION & INVESTMENT PLANNING

Average Cybersecurity Spend Allocation by Category



- Operational Infrastructure Security (50%)
- Vulnerability Management & Security Monitoring (20%)
- Governance, Risk and Compliance (16%)
- Application Security (14%)

Source: Gartner “IT Key Metrics Data 2019: Key IT Security Measures: by Industry”

Companies with large troves of sensitive data in their systems, and especially ones in the sensitive data business, should expect to be targets for attackers in search of data that can be used for identity theft, credit card fraud, or insurance fraud. A proactive approach to cybersecurity can be the best strategy for safeguarding against these inevitable attackers.

Security spending best practices are an exercise in risk management. Businesses need to determine if they want low risk at a high cost or high risk at a lower cost, and if they are making the best use of the available budget.

Cost Benchmarking by Industry Vertical

Banks & Financial Services	*Software & Internet Services*
7.3% IT Spend Allocated to Cybersecurity	**8.7%** IT Spend Allocated to Cybersecurity
$5.60 Cybersecurity Spend per $1,000 of Revenue	**$7.14** Cybersecurity Spend per $1,000 of Revenue

TECHNICAL CONSIDERATIONS

Technical Capabilities as Strategic Advantage

Leveraging technology that augments your current strategy and aids in your efforts to comply with the numerous regulations that the ARM industry must abide by can reduce manual processes by embracing true automation. Your investment in technology should reduce your overall risk, minimize costs, increase efficiencies and help you gain a competitive advantage.

There are quantitative and qualitative factors that an enterprise must consider when deciding whether to "build" its own platform(s) or "buy" platform services from a vendor. In the "build" decision, overall costs are associated with the technology and labor needed to design, develop and operate a platform. In the "buy" decision, overall costs are generally embedded in the pricing offered by the platform vendor, although there are sometimes relatively small, up-front, design-related labor costs. Often, the ability to meet regulatory compliance and security requirements can impact the decision to use an in-house or a vendor-provided platform.

Infrastructure

IT infrastructure consists of hardware, software, network resources and services that are required to run the organization successfully. Latency, zero downtime and high performance are all factors that must be considered. Infrastructure needs to be maintained, upgraded and even replaced over time to ensure it meets evolving standards. If your organization does not have a plan to manage these upgrades and enhancements, leveraging outside technology can help alleviate this pain point.

Privacy

Privacy can become a way to engage with your customers and show them you respect their data. Build in consent models whenever you collect or use data. A privacy-respectful company will reap the benefits of their data diligence through improved customer relations and a trusted brand image.

TECHNICAL CONSIDERATIONS (CONT'D)

Risk Assessments

Conducting regular risk assessments and partnering with a vendor that can independently review your data and security practices make up the foundation of successful IT operations. Security and privacy policies MUST reach out to the extended data and vendor ecosystem.

Data Custody

Data custody specifies the holding and management of enterprise data in the eyes of the law. In a time where identity fraud and data theft is increasing, individuals and businesses both are coming together to tackle the issue of data custody by increasing the buy-in of all stakeholders in the process: companies, individuals and public institutions.

CONCLUSIONS & TAKEAWAYS

Due in part to the COVID-19 pandemic, a large majority of customer journeys now begin digitally. Therefore, to remain competitive in today's digital age, every organization must embrace the use of technology. Using digital technologies can help you transform existing business models into entirely new engagement strategies. The use of technology should also reduce your overall risk, minimize costs, increase efficiencies and help you gain competitive advantage. Conversely, if developing and deploying your own platform is not part of your organization's core strength, then technology can become a distraction and risk. Aligning your organization with trusted partners that can meet your core business needs and provide a solution that is cost effective and low risk will help make your digital journey successful!

Kredit's mission is to provide every collection agency, debt buyer, legal firm, and creditor with a welcoming digital interface they can leverage to flexibly interact with consumers and enable those individuals' financial health.

Schedule a demo to learn more about how Kredit's platform and dedicated team of technologists can enable your digital transformation efforts.

Book a Demo

or reach out directly to dave@trykredit.com

M&G SOLUTIONS

NOW IS THE TIME

Make M&G your strategic business partner and together we can move your business in the right direction. We assist our partners with a thorough assessment, design, and execution of critical strategies to drive performance by providing:

- Reporting and analytics
- Operational contact strategy (voice, digital, work from home, etc.)
- Regulatory and compliance guidance and CMS framework design
- Debt sale, recovery, and legal strategy

Book a Call

or reach out directly to colene.mcninch@maxgraves.com