Navigating Cyber Breaches in the Receivables Management Industry

By Ken Dash and Daniel Palmer

This article is an excerpt from the Fall 2023 RMAI Insights *magazine (pages 22, 23 and 42), originally published October 3, 2023.*

The accounts receivable management (ARM) industry plays a crucial role in recovering debts and managing financial obligations. However, as technology advances, the industry faces growing cyber threats and an urgent need for robust cybersecurity measures. From the theft of sensitive personal information to the disruption of operations, the repercussions of cyber breach in this sector can be far-reaching. In this article, we delve into the world of cyber breaches within the ARM industry, exploring the unique challenges and offering insights into safeguarding sensitive data.

Breach Example

A collection agency became aware of an incident affecting systems within various data centers. The investigation showed that the threat actor gained unauthorized access to the data centers via an exploit of a publicly accessible server.

After establishing a foothold within the environment, the threat actor was able to move laterally to systems within the data centers. They conducted reconnaissance of the network usage, harvested credentials, escalated privileges to privileged accounts, identified and deleted onsite backups, and deployed ransomware.

As a result of the attack, more than $15,000,000 was paid for business interruption, forensics, data recovery, ransom payment, and legal costs. Further, numerous third-party consumer class action claims were made as a result of the release of consumers' personally identifiable information (PII) and personal health information (PHI).

Understanding the ARM Industry's Cyber Security Landscape

It is crucial for collection agencies, debt buyers, law firms, originating creditors, and vendors to handle and protect PII, PHI, and financial credit information in compliance with applicable laws and regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), to ensure data privacy and prevent unauthorized access or breaches.

Holding high volumes of valuable data, such as the following, can make businesses in the ARM industry he targets of cyber threat actors.

1. PII includes Social Security numbers, names and addresses, dates of birth, employment, and income details.
2. PHI includes any information in a medical record that can be used to identify an individual including PII, account numbers, and health plan beneficiary numbers.
3. Payment card industry (PCI) information includes cardholder name, card account number, expiration date, verification number, and security code.
4. Financial and credit information includes account numbers, credit scores and reports, payment histories, outstanding balances, and interest rates.

The GDPR and the CCPA are two essential regulations that significantly impact the ARM industry when it comes to cybersecurity and data breaches. Both GDPR and CCPA impose strict requirements for the collection, storage, and processing of personal data. In the event of a cyber breach, businesses must adhere to the GDPR's and state law stipulations for breach notification, which include specific timelines and communication obligations.

Targeted Cyber Threats in the ARM Industry

The ARM industry faces various targeted cyber threats that can compromise the security of sensitive data and disrupt operations. Some common cyber threats include:

1. **Phishing Attacks and Social Engineering** - Phishing is a prevalent threat where cybercriminals impersonate legitimate entities or individuals to trick recipients into revealing confidential information. Businesses may be targeted through deceptive emails, messages, or phone calls attempting to obtain login credentials, PII, PHI, or financial data. Social engineering techniques exploit human psychology to manipulate individuals into divulging sensitive information or granting unauthorized access. In the ARM industry, social engineering attacks may involve impersonating debtors, clients, or internal employees to gain unauthorized access to systems or extract confidential data.
2. **Ransomware** - Ransomware is a type of malicious software that encrypts files or restricts access to a system until a ransom is paid. Businesses are at risk of ransomware attacks, which can severely disrupt operations, compromise client data, and result in financial loss if critical information is held hostage.
3. **Insider Threats and Employee Misconduct** - Insiders, such as employees or contractors with authorized access, can pose a significant risk. Intentional or unintentional actions, such as data theft, unauthorized access, or data mishandling, can lead to data breaches.

The Consequences of a Cyber Breach in the ARM Industry

A cyber breach can have severe consequences that impact both the businesses, and the individuals whose data has been compromised.

Non-compliance with GDPR and CCPA can result in significant financial penalties. In the case of a cyber breach caused by inadequate security measures or failure to adhere to breach notification requirements, businesses may face substantial fines and legal consequences.

A cyber breach can disrupt normal operations. System downtime, compromised data, and the need to investigate and remediate the breach can impact business processes, hinder debt recovery efforts, and cause delays in client services. Demands can be made by clients for non-compliance with service level agreements. Businesses may need to allocate additional resources to recover and restore operations, leading to further financial and operational strain.

Any data breach can have severe reputational consequences. By complying with GDPR and CCPA and demonstrating a commitment to data protection and privacy, businesses can maintain trust with consumers, clients, and business partners, mitigating the reputational damage that can arise from a cyber breach. News of a data breach can spread quickly, eroding clients' trust and confidence in the business' ability to protect their sensitive information. This can lead to a loss of clients, decreased business opportunities, and a damaged brand image that may take time to recover.

> **“To combat targeted cyber threats, businesses must implement robust cybersecurity measures, including regular employee training on identifying and responding to cyber threats, deploying advanced threat detection and prevention systems, maintaining secure network architecture, implementing strict access controls, and conducting regular security assessments and audits.”**

Under GDPR and CCPA, individuals have enhanced rights regarding their personal data. In the event of a cyber breach, affected individuals have the right to be notified promptly, understand the impact of the breach, and potentially seek legal remedies if their rights are violated.

The aftermath of a significant cyber breach can expose the personal and financial information of thousands of individuals. Affected individuals may band together to file a class-action lawsuit seeking compensation for damages and harm caused by the breach.

Mitigating Cybersecurity Risks

To combat targeted cyber threats, businesses must implement robust cybersecurity measures, including regular employee training on identifying and responding to cyber threats, deploying advanced threat detection and prevention systems, maintaining secure network architecture, implementing strict access controls, and conducting regular security assessments and audits. Here are some best practices for mitigating cyber risk:

Risk Assessment and Management:

a. Conduct a comprehensive risk assessment to identify potential vulnerabilities, threats, and risks specific to your accounts receivables business.

b. Prioritize risks based on their potential impact and likelihood of occurrence.

c. Develop a risk management plan that includes mitigation strategies, risk transfer options (such as cyber insurance), and incident response protocols.

Network Security and Access Controls:

a. Implement robust firewalls, intrusion detection and prevention systems, and secure network configurations to protect against unauthorized access.

b. Apply strong access controls, including role-based access, least privilege principles, and multi-factor authentication (MFA) to ensure that only authorized personnel can access sensitive data and systems. These controls should be enforced for remote access, backup access, and privileged accounts.

c. Regularly update and patch all software and systems to address known vulnerabilities. Critical vulnerabilities should be patched within 24 hours.

Data Encryption and Anonymization:

a. Encrypt sensitive data both in transit and at rest to protect it from unauthorized access.

b. Anonymize or pseudonymize data where possible to minimize the potential impact of a data breach.

Employee Education and Training:

a. Conduct regular cybersecurity awareness training programs to educate employees about potential threats, such as phishing attacks and social engineering.

b. Promote strong password practices, including using complex and unique passwords and implementing password rotation policies.

c. Encourage employees to report suspicious activities, such as phishing emails or unauthorized access attempts, to the IT or security team.

Incident Response and Recovery Plans:

a. Develop and regularly test an incident response plan to ensure a swift and coordinated response in the event of a cyber breach.

b. Establish clear roles and responsibilities for incident response team members.

c. Regularly back up critical data and test the restoration process to ensure data can be recovered in case of a breach.

Vendor and Third-Party Risk Management:

a. Assess the security practices and protocols of third-party vendors and partners that handle sensitive data.

b. Include cybersecurity requirements in contracts and agreements with vendors, ensuring they meet the necessary security standards and comply with applicable data protection regulations.

Conclusion

In an era where data breaches can spell financial disaster and damaging reputational harm, the ARM industry must be at the forefront of cybersecurity. As businesses embrace digital transformation, the need for robust cybersecurity measures becomes paramount. By understanding the cybersecurity landscape and implementing comprehensive frameworks, , businesses can proactively safeguard sensitive data, protect their reputation, and maintain trust with clients and consumers alike. Prioritizing cybersecurity is not only a legal obligation but a necessary step towards a resilient and secure ARM industry in the digital age.

Ken Dash

Managing Director

Risk Strategies Company

Ken Dash is Managing Director of Risk Strategies, a national insurance brokerage and risk management company with more than 150 offices and 4,500 employees in the United States, Canada, and the Cayman Islands. As the National Consumer Financial Service Practice Leader, Ken oversees and services Risk Strategies ARM Industry clients. He has dedicated over 30 years to the receivables management industry as an advocate for debt buyers, collection agencies and collection law firms, creating specialized insurance products and reducing their total cost of risk.

Daniel Palmer

National Cyber Team

Risk Strategies Company

Daniel Palmer is Associate Director of the National Cyber Team of Risk Strategies. Daniel is responsible for providing coverage and program design advice regarding program improvements creating customized and comprehensive coverage for client's data security, privacy, and errors & omissions exposures. Daniel also develops and manages client relationships, account strategies, and insurance marketing activities.