Three Key Components of **Data Security**

Focusing Your Efforts to Safeguard Your Institution and Consumers

ConServe
Accounts Receivable Management

Introduction: Three Key Components of **Data Security**

In today's interconnected world, data security is paramount. Unfortunately, as technology advances, so to do the methods employed by cybercriminals, with an increasing number of sophisticated attacks targeting financial institutions, including credit unions and banks.

From January 2018 to June 2022, financial companies suffered nearly a thousand data breaches, affecting over 153.3 million records.[1]

As the threat landscape (and corresponding regulations) continue to evolve, financial institutions need to be more diligent than ever when it comes to ensuring their consumers' data is secure.

We've identified three vital areas that can have a major impact on the effectiveness of your data security efforts – and on your ability to safeguard your instutition's reputation and consumer trust.

[1] www.comparitech.com/blog/vpn-privacy/financial-data-breaches

ConServe
Accounts Receivable Management

1 Proactively React to Changing Consumer Behaviors

The recent surge in data breaches has led to well-founded concerns about security among consumers. Likewise, consumer expectations regarding data privacy have reached new heights. As a result, financial institutions must address these evolving expectations and behaviors, prioritizing transparency in data handling and protection practices to build and maintain their consumer's trust.

At the same time, digital transformation has brought convenience and new services to consumers. For example, millennials and Gen Z seek (and expect) digital payment options for convenience, but this shift also introduces new vulnerabilities.

To strike a balance, financial institutions should invest in secure digital consumer experiences, including robust authentication methods, secure mobile banking apps, and regular security updates. Additionally, the National Association of Federally-Insured Credit Unions (NAFCU) recommends minimizing points of data collection to further reduce potential issues.

When vetting third-party partners, such as outsourced collections agencies, be sure to look at the consumer experience, as well as the ensuing security issues and how they are addressed.

Millennials & Gen Z seek (and expect) digital payment options for convenience, but this shift also introduces new vulnerabilities.

2 Prioritize Employee **Training & Process Compliance**

While technology plays a vital role in data security, human error remains a significant risk factor. In many instances, the line between secure and data breach can be only a click away. For this reason, preparation is key. A recent research study concluded that security awareness training is effective in changing employee behavior and measurably reduces security-related risks by between 45 and 70 percent.[2]

To reinforce the importance of data protection and risk mitigation, financial institutions should prioritize comprehensive training programs that cover cybersecurity awareness, safe browsing practices, phishing threats, and the importance of strong passwords. Regularly updating and reinforcing security policies and procedures will help foster a security-conscious culture within your institution.

Preparing for a data breach or cybersecurity incident is as important as preventing one. Develop a robust incident response plan that outlines the steps to be taken in case of an incident, assigns responsibilities, and establishes communication protocols. Integrating business continuity planning into your overall data security strategy will help minimize disruptions and ensure your institution can quickly recover from any incidents.

Note that this focus on employee training and business continuity planning should extend to third-party partners, including outsourced collection services.

Financial institutions should prioritize comprehensive training programs that cover cybersecurity awareness, safe browsing practices, phishing threats, and the importance of strong passwords.

[2] https://blog.knowbe4.com/train-employees-and-cut-cyber-risks-up-to-70-percent

3 Establish Systems to **Keep Up with the Ever-Changing Environment**

Data security is a complex and dynamic process, requiring financial institutions to adopt comprehensive systems that cover administrative, technical, and physical contingencies.

At the same time, financial institutions operate in a regulatory environment that demands accountability, documentation, and adherence to evolving regulatory standards. The rise of AI and cloud computing add yet another layer of complexity.

To help keep pace, financial institutions should establish robust, multi-layered data security frameworks that encompass encryption, access controls, network segmentation, regular audits, and vulnerability assessments. Implementing strong authentication mechanisms such as multi-factor authentication (MFA) can significantly enhance security by adding an extra layer of protection.

Likewise, financial institutions who outsource collection services need to align with agencies who demonstrate compliance with industry regulations and possess reputable accreditations such as ACA International Blueprint Quality Management System®, FISMA, PCI and SSAE 18/SOC 1 Type II.

> Financial institutions should establish robust, multi-layered data security frameworks that encompass encryption, access controls, network segmentation, regular audits, and vulnerability assessments.

Conclusion

Remember, data security is an ongoing process, requiring constant vigilance, adaptation, and investment. By adjusting to changing consumer expectations, prioritizing employee training, and implementing robust data security measures, financial institutions can help mitigate the risks associated with data breaches, cyberattacks, and fraud.

This in turn protects your reputation and helps ensure the long-term success of your institution. Ultimately, by prioritizing consumer security and privacy, financial institutions can enhance trust and differentiate themselves in the competitive landscape.

Let us help your institution's collection services become secure and compliant. Contact us today to learn about The ConServe Advantage®.

Let's **Get Started!**

Call **(866) 761-0700**, email **salesinfo@conserve-arm.com**, or visit **conserve-arm.com/meet-conserve**

The information provided in this E-Book is strictly for the convenience of our customers and is for general informational purposes only. This information is not intended as legal advice may not be used as legal advice. Legal advice must be tailored to the specific circumstances of each case. Every effort has been made to assure this information is up to date as of the date of the publication.

ConServe
Accounts Receivable Management