COMING TO GRIPS WITH DATA SECURITY

This critical investment will help your company prevent data loss, comply with industry regulations and win clients.

By Anne Rosso May
Once thought of as a special service offered by only the largest companies, today data security is essential for companies of all sizes. Over the last several years, credit and collection industry members have had to come to grips with data security—what it means, what clients expect them to have, what regulators require them to do, and how they can manage all these expectations while still turning a profit.

In addition to establishing internal data security systems to secure confidential information and guard against data loss, collection agencies and their clients are also required to validate the data security of their vendors.

Today you must consider: What sensitive data does your company have, where does it live, who accesses it and how are you protecting it?

“It’s the number one thing today from a client’s point of view,” said Don Taylor, president of Automated Collection Services in Nashville, Tenn. “It used to be: ‘How is your recovery?’ and ‘What type of performance can you give?’ But now it’s: ‘What’s your data security and compliance?’ We can’t get serious about contracting with a new client if I don’t have extensive data security and compliance in place.”

Effective data security can make or break your business, but it’s an incredibly complicated obligation. Unfortunately, there’s no definitive checklist to help you determine how to structure your data security plan. The answer depends on a variety of factors—and may take a fair amount of resources to discover. The best approach is to assess both the current landscape and the nuances of your business, and dive in as soon as possible.

“In my view, this single topic is going to have more impact on our industry than anything we’ve seen in the recent past,” Taylor said. “Collection agencies must take vendor validation, data security and compliance seriously. If you ignore these requirements, you may wake up one day and realize you are no longer in business.”

IDENTIFYING RELEVANT STANDARDS AND REGULATIONS

The first step in establishing a data security plan is identifying which standards, regulations and laws apply to your company.

There are a number of federal regulatory bodies that have something to say about data security, including the Federal Trade Commission, the Consumer Financial Protection Bureau and the Department of Health and Human Services.

An agency’s clients’ needs will also drive its data security needs; these can vary according to the type of market you serve.

William “Chris” Dunkum, president of First Collection Services in Mabelvale, Ark., said that figuring out which standards his company is expected to meet has been the most challenging part of putting together a data security program.

“There are so many different standards out there that we’re under in the collection industry,” he said. “It’s difficult figuring out which one or which group of them we need to meet, and to what level.”

Depending on their business model, collection agencies and their clients may need to develop data security practices in accordance with:

- The Gramm-Leach-Bliley Act (GLBA).
- The Health Information Technology for Economic and Clinical Health Act (HITECH).

“Collection agencies must take vendor validation, data security and compliance seriously. If you ignore these requirements, you may wake up one day and realize you are no longer in business.”
• The Health Insurance Portability and Accountability Act (HIPAA) rules, such as the Omnibus Rule.
• The Red Flags Rule.

In addition, individual states may impose requirements over the safeguarding of sensitive consumer information, including obligations that require collectors to inform consumers in the event of a security breach of consumer information.

To date, 47 states, as well as Washington, D.C., Guam, Puerto Rico and the U.S. Virgin Islands, have enacted legislation requiring some form of consumer notification following a data breach. Only Alabama, New Mexico and South Dakota have remained silent on the issue.

Clients also expect collection agencies to earn quality assurance certifications and meet various standards. These may include:
• Health Information Trust Alliance (HITRUST) Common Security Framework — A certifiable framework of security controls for healthcare organizations that scales according to the type, size and complexity of the organization and its systems. It is specifically devoted to the protection of PHI.
• ISO 27000 series — A best practice framework for information security.
• National Institute of Standards and Technology (NIST) — Drafted by the Commerce Department in 2013, NIST provides a voluntary cyber security risk framework that helps organizations choose information system controls.
• PCI DSS — A security standard with 12 high-level requirements designed to protect payment card data and related consumer information. Any company that handles consumer payment card data must demonstrate PCI DSS compliance.
• SSAE 16 — Replacing SAS 70, SSAE 16 reviews a company’s internal controls over financial reporting. Within the SSAE framework, there are three service organization control reports. There is no one-size-fits-all standard that will ensure your company has secured all of its confidential data. Companies operating in the credit and collection industry will likely need to meet several standards in order to keep every aspect of their business secure and continue to attract and retain clients.

VENDOR RISK MANAGEMENT

In the past, the consequences of any data security missteps made by a company’s third-party partners generally stayed with that vendor—the risk did not transfer to the collection agency.

Today entities can be held accountable for their service providers’ actions. Companies must prove their vendor’s data security is sufficient through comprehensive due diligence assessments, and must continually

Minimize Your Liability with Monthly State Collection Law Updates

“ACA’s State Guide is our Bible—we use it every single day.”

— Recent ACA Convention attendee

If you’re not already subscribing, you’re potentially missing dozens of state collection law updates.

Subscribe today!
acainternational.org/store
work to ensure vendors are maintaining that compliance.

The CFPB requires collection agencies to take steps to ensure their business arrangements with service providers don’t “present unwarranted risks to consumers.” Companies must guarantee all vendors are keeping consumer data secure, taking steps that include:

- Reviewing the service provider's policies, procedures, internal controls and training materials to ensure it conducts appropriate training and employee oversight with consumer contact or compliance responsibilities.
- Ensuring service provider contracts spell out clear expectations about compliance, as well as consequences for violating any compliance-related responsibilities, including engaging in unfair, deceptive or abusive acts or practices.
- Establishing internal controls and ongoing monitoring to determine whether the service provider is complying with federal consumer financial law, and taking prompt action to address any issues.

These expectations present a big challenge to collection companies, which may have dozens or even hundreds of vendors to verify. These could include scrub providers, consumer reporting agencies, letter companies, skiptracing providers, accounting firms and data providers—any company that receives confidential data from you.

“I don’t care who it is,” Taylor said. “Equifax, Experian, Lexis-Nexis—those are big, reputable companies, but I still have to ask data security and compliance questions, including requests for documentation. This validation is essential to use their services.”

Cloud vendors in particular can pose unique risks. If another client in your cloud infrastructure has a breach, is your data still secure? If any of your data is in the cloud, you must find out where it is being stored, who touches it and what controls are in place to protect it.

Earlier this year, the CFPB took Sprint and Verizon to task for failing to properly monitor their vendors, levying a hefty fine against the companies. Still, many collection agencies and their creditor

Overview of the Data Security Process

Data security is not a one-and-done project—it is a continuous process, notes Joshua Schreiner, chief compliance officer and general counsel for Columbia Ultimate. He provided the following general overview of a sound data security plan:

- Conduct a periodic risk assessment of your entire operation.
- Analyze that assessment and implement security measures (such as through technology or policies and procedures) to reduce risks.
- Train your employees on your policies and procedures.
- Audit for inconsistencies and correct nonconformities.
- **Repeat.**

**CLIENT RISK MANAGEMENT**

Gone are the days when clients “verified” your data security system by having you check a box on a form. Today clients are—or should be—asking for detailed information on agency policies, security and audits. Personal site visits are often necessary before clients sign a contract with your agency. They need to know where you use their information and how you are protecting it.

This validation can be extensive, and asking and responding to questions can take time. Taylor noted that when his company was recently vetted by a large organization, he had to answer hundreds of questions about all facets of his organization, including data security, policies and compliance. “It was the most comprehensive vendor security assessment I’ve ever been through,” he said.

In spite of all the attention lavished on third-party compliance, some of your clients may not be aware of what they should be doing. For example, Taylor estimated that 90 percent of universities, credit unions and hospitals do not validate their collection agency partners, likely because they are simply unaware of what is required.

Even if clients do know that they should be verifying collection agencies’ data security programs, they may not know exactly what they should be looking for. Dunkum noted that a few years ago, a utility company asked about his company’s HIPAA compliance—a security standard totally unrelated to the client’s market niche.

“That’s how far everyone was reaching for guidance,” he said. “We are all trying to figure out what standards are out there and what we have to meet.”

Not only are clients often failing to properly vet their third-party partners, but they may overlook their own data security program. Scott Brownlee, vice president and chief compliance officer for Grimley Financial in Haddonfield, N.J., noted that in his experience, client attention to data security “varies wildly across the landscape.”
“The most important piece of any data security puzzle is your employees. You can invest thousands of dollars in security technology, but one click on a malicious email by an untrained employee can unleash a virus and essentially flush that money down the drain.”

“I am very concerned for a couple of our clients,” Brownlee said. “When it comes to keeping current on their data security, it almost seems as though they are burying their heads in the sand. On the flip side, I have clients that have made data security one of the top priorities and it shows.”

Clients that don’t pay attention to data security may not be in business for very long. If you have clients that aren’t carefully validating their vendors and taking steps to enhance their own data security beyond a simple firewall, it’s to your advantage to sit down with them and review the rules and regulations that may apply to their business.

Brownlee helps keep clients apprised of relevant data security obligations and industry regulations by posting articles on LinkedIn as well as emailing his clients regular industry-relevant articles, including some on data security.

He also pays close attention to any changes in his clients’ third-party vendor pool. For instance, when a client’s vendor wanted to implement a new technology that Brownlee thought exposed both his company and the client to risk, he requested his client insert a paragraph into a revised business associate agreement to exempt his company from any culpability with that program if it went through with the change. Ultimately, the client chose to not to move forward with the technology.

“That vendor wasn’t concerned about security and regulations at all,” Brownlee said. “We all want big checks—who doesn’t?—but not at the expense of your client’s well-being.”

STOP, COLLABORATE AND LISTEN
A risk assessment can help you determine where you are most vulnerable and point out any obvious first steps you should take to enhance data security. While small and medium-size companies may be able to handle some corporate risk assessments and data security themselves, it is often cost-effective in the long run to find an auditor who can do a holistic information security audit for your company.

Dunkum’s first data security steps involved listening to others in the collection industry as well as his clients. Once he had a general idea of what was expected of him and how other companies were approaching the issue, he hired a data security company to help audit his information system.

Confidential consumer information, health information, payroll information, call recordings, company data, even old RFP responses—you must lock down and account for every piece of sensitive information in your company.

A security expert can help you harden your network and recommend threat detection tools and data loss prevention software that can map to your corporate polices. It can also conduct regular tests of your data security system—which is essential as creative cybercriminals dream up new ways to attack companies’ systems.

Grimley Financial’s security company conducts monthly tests to ensure the system is strong. Last year, for the first time, the security company was able to penetrate Grimley Financial’s email server and launch a denial of service attack—flooding the server with tens of thousands of spam emails per minute for 15 minutes.

“It didn’t compromise anything, it just shut our email system down,” Brownlee said.

Cyber Insurance
Is your data insured? Cyber insurance is a relatively new but increasingly valuable addition to a collection agency’s risk management toolbox.

Cyber insurance can help mitigate losses from a data breach or hacker attack. Most insurance carriers provide some form of cyber risk coverage. Derek Tessmer, sales manager for Collectors Insurance Agency, suggested that collection agencies review this coverage, as it is often somewhat basic and may not address all exposures or comply with client contract requirements.

For example, most cyber security offered through an E&O policy won’t cover consumer notification or credit monitoring costs, which could be significant expenses in the event of a security breach. Often companies will need to obtain a separate stand-alone policy for notification and credit monitoring coverage.

For more information on cyber insurance, ACA International members can contact Collectors Insurance Agency, a subsidiary of ACA International, at collectorsinsurance@acainternational.org.
“And now we’ve adapted and changed to prevent that from happening again.”

The most important piece of any data security puzzle is your employees. You can invest thousands of dollars in seemingly bulletproof security technology, but one click of a mouse on a malicious email by an untrained employee can unleash a virus and essentially flush that money down the drain.

Collection companies must write and enforce data security polices that apply to all levels of the company. Data security should also be part of your overall employee training program—no different than how you would train staff on the Fair Debt Collection Practices Act or Fair Credit Reporting Act.

“Collectors need to have a mindset of protecting consumers’ information,” Dunkum said.

TACKLING THE COSTS

There’s no way to sugarcoat it: data security is expensive and requires a large initial investment, followed by ongoing maintenance costs. Taylor estimated that large companies spend tens of thousands of dollars to implement and maintain a data security system.

First there are proactive costs, such as new hardware and software, third-party security consultants, data loss prevention tools, regular audits and changes to internal policies and procedures.

But these costs pale in comparison to any reactive costs your agency may incur if you suffer a data breach. These can include legal fees, regulatory fines, consumer notification fees and remediation costs—not to mention the significant blow to your company’s reputation and potential loss of clients.

According to a 2014 survey from the Ponemon Institute, the average cost of a data breach was $3.5 million—15 percent more than what it cost in 2013.

Brownlee estimates that while his company has spent more than $100,000 in the last three years on hardware alone to upgrade its security, that expense was not one lump sum.

“It’s built into our monthly budgets now,” he noted. “You have to spend the money and find a way [to afford data security]. Once you bite off on it and commit to doing it, you get used to the budget change pretty quick.”

Data security costs increase operational expenses at a time when shrinking margins are already hurting agency profits. Collection companies have to look at all areas of their business to determine how data security expenses will impact the rest of the organization.

“Many of our clients are seeking ways to reduce other operational expenses, such as data, letters, infrastructure and unit costs,” said Joshua Schreiner, chief compliance officer and general counsel for Columbia Ultimate. “These changes push agencies to adopt more technology that can automate manual processes and improve the collection operation to reduce expense.”

STAY ON YOUR FEET

Data security affects all businesses, regardless of size. Unfortunately, smaller business may be slower to adopt necessary security requirements because those expenses don’t directly generate revenue. But sound data security processes can help you retain and attract clients—and they become more important with each passing day.

“It’s guaranteed you’re going to get hit at some point,” Brownlee said. “It’s a matter of if you can defend against [a security attack] and stay on your feet, or if you will get knocked down and out.”

Anne Rosso May is editor of Collector.