II. Security Concerns

Solving Your Data Security Issues Across the Invoice-to-Cash Landscape

By Laura Whitt-Winyard and Adina Rubin of Billtrust

No matter what anyone tells you, fraud and data breaches are not the cost of doing business. Sure, there are unavoidable security risks for organizations today. Yes, your network may get hacked, or you may become the victim of malware. Sending electronic invoices and collecting payments online may increase your company's vulnerability to both fraud and security breaches. But if you fail to protect your business by preparing for the worst-case scenario, integrating security protocols and using secure, automated technology to handle your invoicing and payments, you're the only one to blame. The price you'll pay is a loss of revenue, and most importantly, a loss of trust.

Luckily, the internet, SaaS (Software as a Service) solutions, and security technology can be some of the most powerful tools in your arsenal to help you mitigate those security risks. But before we dive into the technology, let's explore the problem, and understand the risks involved.

Data breaches are defined as any event where sensitive, protected or confidential data has been viewed, stolen or used by an unauthorized party. It can include personal health information (PHI) and personally identifiable information (PII), as well as trade secrets and intellectual property. Fraud can take many forms, including fake payments, using both paper and electronic formats. Corporate data breaches can affect individuals and businesses alike, making private information public, which can lead to stolen money and products. Unfortunately, fraud permeates the world of business, causing extensive damage to organizations.

What the numbers tell us

When we look at the statistics around data breaches, there are three main causes, all of which can be prevented. According to the Ponemon Institute 2017 Cost of Data Breach Study, human error (24%), system glitches (24%) and criminal attacks (52%) account for the root causes of data breaches to organizations across industries. Human error includes employees and contractors who cause data breaches by careless actions, while criminal attacks are malicious and may include malware, criminal insiders, SQL injection code and phishing scams. The proliferation of mobile platforms creates new opportunities for fraud, along with the increase in compliance failures.

Don't forget that data breaches are expensive too. The average company spends over $1 million on forensic investigation, assessment and audit services alone. Add to that the cost of a damaged reputation and a loss of trust, both of which can be hard to quantify exactly, but studies have been done to show the consequences. When customers leave and lawsuits are filed, the loss of present and future business will hurt your bottom line for years to come. The Ponemon study identified the average cost of each stolen record at about $225 per record, and if it includes health data, that cost jumps to $380 per record. Multiply that by tens of thousands of records and it's easy to see how the average data breach will cost an organization about $7.35 million.

Assessing your organization's needs

So, what does this mean for your organization? It means that you need to make protecting your business, your customer data, and your cash flow a priority, using the most secure options available to you today. Security is not a one-time solution, but a never-ending process of protecting your business from new threats that pop up every day, reducing the mean time to detection and mean time to repair. Routine data backups and processes that help you recover quickly from a breach are necessary because the numbers show that your business is likely to suffer from a data breach or fraud at some point.

You need to implement several comprehensive plans. The first one is focused on the people in your organization by getting them to understand and uphold the security measures you will put in place. Next, you will need to create policies

which govern all internet use, devices, security and access to your network. Finally, you'll need a plan of attack to specifically cover the risks in the areas of purchasing and payments. This three-pronged approach will help you identify the most serious risks and protect your most sensitive data on all fronts. Let's focus on your invoice-to-cash process and evaluate your unseen potential risks.

Invoice delivery risks

What kind of security risks are involved in invoicing? You'd be surprised at how simple mistakes here can have a big impact. In August 2017, Aetna inadvertently revealed the HIV status of 12,000 customers by accidentally printing it near the mailing address so the data was visible through the envelope window. HIPAA violations carry a fine of $100 to $50,000 per incident, and the full extent of repercussions of this act have yet to be determined.

Conversely, if your organization has manual invoicing processes, your staff may accidentally send the wrong invoice to the wrong customer, revealing your customers' business data to their competitors. You have no way to prevent human error, and it's a mistake that happens more often than you think. If you outsource your printed invoices to a third-party vendor, you have abdicated control over the process, and you have no idea who may be accessing the data on the invoices before they are mailed.

Preventing payment fraud

Payment fraud is found in every payment method, across every payment channel, and the quantity and value of fraudulent payments are astonishing. Studies show that over 75% of organizations experiences paper check fraud, 46% are victims of wire-transfer fraud, and 30% suffer from ACH debit fraud, proving there's no way to avoid fraud. There are other important risks we need to address when it comes to payments. Your employees may use a variety of unsecured processes within your office, which not only opens your business to security breaches, but also to fines and penalties if your security is violated or word gets out to the public.

Let's start with credit cards. Untrained employees may write down a credit card number for use at another time, and then store that number in an unlocked drawer or filing cabinet, or worse - right on top of their desk. Emailed "virtual" or one-time-use credit card payments are the newest method of payments for businesses, but they also have gaping security holes. Emails are sent to unsecured email accounts, and AR team members are directed to create a login and password in order to securely access the number and process the payment. This results in the creation of thousands of logins and passwords which are not often locked down, but are instead scribbled on a piece of paper or saved in a spreadsheet.

Paper check payments are no more secure than credit cards. Often paper checks will sit in someone's desk for days until a bank run is made to deposit them. There is no method of ensuring that checks are legitimate until they are deposited. Few organizations lock up checks in a safe or handle them securely. Add up the number of unlocked offices, unsecured laptops and other security vulnerabilities at your organization, and you're looking at a situation where there are a lot of opportunities for breaches.

Securing your cash application process

The cash application process is where your AR team will match up payments with remittance data and reconcile paid invoices, freeing up cash for use within the organization. If your business still uses a manual cash app process, you have unsecured paper files and spreadsheets with invoice and statement data, along with photocopies of checks and other documentation, creating vulnerabilities across the entire department.

Some organizations use automated cash application software, but you still need to be careful. Some newer software companies have misrepresented their automation technology, and they outsource some processes to inexpensive overseas labor. Using one of these unsecured software solutions means you have no control over security of your customer payment data.

Adopting a security-first mindset

So how do you mitigate risks and remove these vulnerabilities? There is no single solution that a company can just buy and implement. Protecting your organization and your data requires adopting a philosophy in which security is a top priority and a daily effort. Each person within your organization can accidentally cause a data breach through careless actions, such as clicking on a link in a phishing email, connecting to an unsecured Wi-Fi signal, or leaving a laptop open and unlocked momentarily in a coffee shop. The damage caused by a careless decision can't always be mitigated by security technology.

Your company's employees, executives and contractors must be aware of security risks and protocols through frequent training and

informational updates when new risks are discovered. Once all stakeholders are on board, and your employees understand the value and necessity of security measures, you can begin a multi-channel approach to secure your data.

Protect your cash flow

All companies deal with financial transactions, and there are laws and regulations which define how to keep financial and sensitive data secure. The most stringent and prescriptive one is from the Payment Card Industry Security Standards Council called PCI-DSS. You may know this as PCI compliance, a series of 12 requirements with 250+ sub requirements that define how to handle credit card data securely and protect your network from malicious attacks.

Regardless of whether or not you accept credit cards, if you store any kind of financial information, your organization is required to be PCI compliant. Adhering to PCI compliance standards can be complicated and costly, requiring audits, new technology and designated resources to implement and maintain security standards. The costs of PCI non-compliance are extensive, including hundreds of thousands of dollars in fines and penalties from banks and credit card institutions, as well as the cost of civil litigation and lost business.

A better approach to data security

While you can do-it-yourself, there is an easier method available to organizations that want to avoid the rigors and hassle of maintaining compliance of security standards for PCI-DSS, NACHA, NY-DFS, SSAE16, and others.

Many businesses choose this option to skip the investment of time and money. Instead they choose to outsource the processing and storage of credit card numbers and financial data to a third-party vendor who excels in data security. By using a secure, cloud-hosted solution, there is never any sensitive data stored on your system, removing most of the burden of maintaining compliance from your team and their laptops.

Upgrading to the total package

There are several secure invoice-to-cash solutions on the market today, so you'll need to choose wisely. The best advice is to consider automated solutions which offer the most flexibility to both you and your customers, allowing you to accept a variety of payments securely, including paper checks, ACH and wire transfers. It should be able to process all types of payments automatically and verify that all payments are not fraudulent by communicating with banking institutions to confirm that funds have cleared.

Using secure payment methods will build trust with your customers and provide them with secure payment options, such as an online portal or IVR (Interactive Voice Response telephone payment system). Automated cloud-hosted solutions also remove the risk of human error from your business, providing a nearly touchless process.

If you're fully committed to protecting your data, you'll want to make sure that your secure invoicing and cash application solutions can interact seamlessly with your automated payment system, further decreasing the risk that unauthorized individuals can access your data.

You can get automated invoice delivery solutions which use SFTP to securely receive invoicing data from your ERP. That data can be used to send invoices to customers using a variety of methods including print, email, and for maximum security, an online presentment portal. You'll want to use a print facility in the US that offers mail tracking to ensure correct delivery and has measures in place to prevent glitches in the mailing process. Ask for a tour of the print facility before you hand over your data, and inquire about their acceptable failure rates (which should be zero percent).

To round out the invoice-to-cash process, you should have a secure automated cash application system in place. The cash application process involves matching payments with invoices and remittance data, exposing sensitive information if it's handled manually by a team of people. Choose an automated solution which removes virtually all human interaction, hosts payment data in the cloud and off your systems, and sends reconciled payment files to your ERP securely.

You can never have too many backups

The last piece of the data security puzzle is the backup protection you'll need when, not if, your business is breached. The numbers show us that it's going to happen eventually, so every business should be prepared for when that comes, and that means having a secure offsite backup of all your data.

The most frequently asked question is, "How often should I have my data backed up?" The answer is, "Always backup your data as often as you can afford to lose it." If you can recover from losing one day's data without too much effort, then a daily backup solution is perfect for your

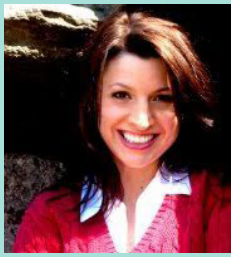
business. If, however, five minutes of data loss would cause irreparable damage, you'll need a 24/7 real-time data replication solution in place.

It all comes down to trust

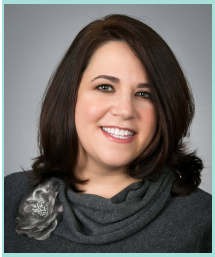
Professional and personal experiences have shown that every minute and every dollar spent on threat detection, prevention and remediation is time and money well spent. From sensitive customer data to credit card numbers, no one wants to lose the things most important to them. It's up to you to make every person within your organization feel invested in protecting the business and its most valuable information asset - data.

When you put time and effort into protecting your customers and your data, it shows. Each and every time there's a headline about the most recent company to have data compromised, your customers will gratefully pay your invoices, secure in the knowledge that they can still trust your organization to keep their data protected.

About the Authors:



***Laura Whitt-Winyard**, CISSP, CISA, CISM, CRISC, has over 16 years of Information Security experience. She serves as the Information Security Director at Billtrust and is responsible for definition and implementation of the company's global information security program and strategy.*



***Adina Rubin** is a writer at Billtrust where she educates finance executives and professionals about the benefits of optimizing AR efficiency. She has a bachelor's degree in journalism from Boston University, and a master's degree in education from Duquesne University. She would love to hear from you on Twitter and LinkedIn.*