DATA MANAGEMENT
DM®
PAYROLL SERVICES

PAYROLL briefs

DELIVERING BUSINESS INSIGHTS

ISSUE 5 | 2019

Protecting Payroll Data from Cyber Threats

In the eyes of a hacker, intercepting payroll data like employees' bank account numbers, social security numbers, home addresses and wages would be like hitting the jackpot. A breach of this nature can cause irreparable damage to your employees' trust and confidence, not to mention costly reputation and financial damages. These consequences don't allow for error. Controls must be put in place to ensure employees' personal information and payroll data always remains confident and secure from cyberattacks.

Ways to Help

Most companies these days rely on a third-party provider to process their payroll. But, that doesn't relinquish an employer's responsibly to take strong measures to secure any computerized payroll information lingering on its employees' desktops, email servers and company networks, or even its third-party provider's payroll system, for that matter.

While you cannot stop criminals from attempting to steal this data, you can take steps to prevent their efforts from being successful. Check out these best practices for protecting payroll data from ending up in the hands of lurking cyber predators.

Polish payroll security procedures. Review your payroll procedures on an annual basis to ensure an appropriate level of security is in place. Train each employee handling payroll data to follow the outlined procedures. Make sure these take into consideration evolving cybersecurity concerns.

Plan regular software or system updates. Applying updates as they become available helps improve security by closing gaps in your system that may leave your information vulnerable. Communicate with your IT department to ensure each employee is aware of updates and knows how to install them.

Build a resistant firewall. Be sure your IT department has installed a good firewall to block unauthorized access. A proxy server should be established to control and limit Internet access and audit the network connections frequently.

Continued on back

Service Offerings

- Payroll Processing
- Payroll Tax Filing & Compliance
- Time and Attendance Solutions
- Direct Deposit of Pay
- Employee Self Service (/ 🤖)
- Wage Garnishment Compliance
- Report Writer (Payroll Control™)
- 401(k) 360 Data Interchange
- ACA / W-2 Compliance
- Applicant Tracking
- Onboarding
- Human Capital Management
- Benefit Administration Solutions
- General Ledger EDI
- Workers' Comp Audit Report
- Time Off Accruals

Don't Forget...

Daily payroll cut-off
time is 3:00pm EST

☎ (248) 244-3293
Customer Service
8:30am-5:00pm EST M-F

📠 (248) 244-3271

✉ cs3293@dmpayroll.com

Continued from front

Update login credentials. Hackers will exploit weak passwords to infiltrate systems with minimal effort. Select unique, long passwords containing a blend of numbers, symbols, and upper and lowercase letters. Update all passwords on a regular basis. It may be helpful to set automated reminders when it's time for a change. Also, be sure to block access to this data and any payroll systems when an employee responsible for handling payroll leaves the company.

Be wary of phishing emails. Many phishing emails ask for payroll information like a W-2 form or social security number. Appearing to be genuine, these emails may reflect the CEO's name and ask for payroll information for an employee. As a rule of thumb, do not give out any payroll information via email without verbally verifying the request directly with the sender before responding with any sensitive employee data. Ask your IT department or an outside expert to train staff to spot the signs of a scam with strategies like checking the email reply address.

Avoid unsecured networks. If you are working on submitting payroll from your mobile device or home computer, you will want to make sure you are working on a secured Wi-Fi network. Make sure these devices have all their updates ran as well. Cyber criminals prey on those using unsecured networks.

Work with a secure third-party payroll provider. It's crucial you select a trustworthy service provider, like DM Payroll Services, that employs proper security measures to keep your employees' data protected.

Get a cyber checkup. Even though precautionary steps are likely being taken to protect your organization's payroll and other sensitive data, the evolving cyber landscape can still leave unknown vulnerabilities lurking in the background. Wondering just how protected your data really is? Consider having an independent third-party assess your information systems environment and its integrity. DM Payroll Services recommends working with its affiliate firm Doeren Mayhew. Armed with a team of security experts, they offer a suite of CYBERCLAW ™ security solutions designed to fit every budget and set of needs.

Working with DM Payroll Services, you can rest assured that your payroll data is protected on our end. Want to double check to see how secure it and other data is on your end? Contact us today. We will put you in touch with Doeren Mayhew's cybersecurity advisors.

bank holiday to note

Memorial Day — Monday, May 27

Navigating EEO-1 Data Requirements

As you get ready to prepare your EEO-1 report this year, some events have occurred that may impact your filing. Following the government shutdown this year, the Equal Employment Opportunity Commission (EEOC), the agency responsible for collecting EEO-1 data, pushed the reporting deadline from March 31 to May 31, 2019.

However, in March a judge ruled Component 2 to the EEO-1 form – data on hours worked and pay information for employees by race, ethnicity and sex originally – put in place by former President Obama's administration and later yielded by the Trump administration, should be immediately reinstated. The decision led to a debate over when this additional required information should be submitted to the government.

Not equipped to begin collecting this pay data by May 31, the EEOC delayed the Component 2 data filing requirements until September 30, 2019. That didn't sit well with worker advocate groups. In early April, they asked a federal judge to uphold the original judgement, requiring Component 2 data to be collected by the same May 31 deadline for Component 1 data related to the number of employees who work for the business by job category, race, sex and ethnicity.

On April 25, the judge approved the delay, ordering that employers must submit their EEO-1 Component 2 data by September 30, 2019.

Start Preparing Now

With the decision now finalized, companies required to file are advised to start collecting EEO-1 data for Component 1 – this data is due on May 31. As for Component 2, your employees' pay data must be submitted to the EEOC before September 30. If you haven't already, start considering a strategy for compiling the Component 2 data so you are ready when the time comes.

DM Payroll Services' software includes an easy EEO reporting component you can use to compile your information with one click. If you are not leveraging this resource, contact us today to get started.

Through Payroll Briefs, Data Management Payroll Services provides its clients with general information on legal developments related to payroll administration. If such developments appear relevant to your specific situation, you should discuss them with your professional advisor before taking any action.