Summary
High profile breaches have recently called the security of cloud-based applications into question. For businesses, collecting and storing employees’ confidential data is particularly sensitive. To protect this data, organizations must do their best to ensure their systems guard against both internal and external security threats. This white paper examines the security risk that Human Capital Management (HCM) applications like payroll, time and attendance, and human resource systems should address and the configurable characteristics a time and attendance system should have to guard against security breaches.
Security Breaches in the Cloud

Although the benefits of cloud-based applications outweigh traditional desktop software in terms of safety, overhead, accessibility, updates and compatibility, recent headline-making security breaches left many companies wondering just how safe their data is in the cloud.

Stolen: 40 Million Target Customers’ Payment Information

In 2013, starting the day after Thanksgiving, popularly known as “Black Friday,” through December 15, Target faced a massive hack that compromised more than 40 million customers’ payment cards. Experts now believe the hackers launched the attack by stealing authentication credentials to the Target corporate network from an HVAC subcontractor doing work for the large retailer, then uploaded malware to Target cash registers designed to capture customers’ card information. Bad press and consumer concern dogged the retailer through the holiday shopping season, and Target may be held liable for not complying with the payment card industry’s security standards.¹

Hacked: Facebook, Google, Twitter, Yahoo, ADP

Simultaneously, a computer virus originating from the Netherlands hacked 2 million Internet accounts in early December, stealing more than 1.5 million website login credentials (such as user IDs and passwords) and 320,000 email credentials for high-profile sites such as Facebook, Twitter, Yahoo, Google, LinkedIn and payroll service provider ADP.² The virus targeted commonly-used “dumb passwords,” including “123456,” “111111,” “admin,” and “password.” Affected companies notified owners of compromised accounts and changed account passwords, but Trustwave, a cybersecurity group based in Chicago noted with interest the inclusion of ADP among the social networking and email domains:

“It is only natural to have such domains [as the affected companies] in the mix, but it is surprising to see [ADP] ranked #9 on the list. Facebook accounts are a nice catch for cyber criminals, but payroll service accounts could actually have direct financial repercussions.”³

News of these hacks left consumers—and businesses—understandably shaken. Even as the Target investigation continues, many businesses are carefully reviewing the security of their cloud-based applications to ensure data safety and confidentiality.

The Drive for Data Security in Time and Attendance

Time and attendance data has the potential to be an Achilles heel for many businesses since it can include employees’ personal information. From Social Security numbers and birthdates to medical leave and payroll information, HCM systems are designed to deal in confidential data, making it important that these systems feature critical security measures that can be configured to protect both employers and employees from potential threats.

So what security features should businesses look for in a time and attendance system?
Guarding Against External—and Internal—Threats

To minimize the possibility of data hacking, the best time and attendance system can be configured to limit access to confidential data and help protect it from both external and internal threats. While the Internet hacking of Google, Facebook, Twitter, Yahoo and ADP was purely an external attack, the Target breach investigation suggests the hackers infiltrated the retailer’s internal network to collect customers’ payment information. Therefore, a time and attendance system must have configurable security features to help protect data both outside and inside the organization, including:

• **Protection of Sensitive Information**
  Best practices for storing employees’ confidential information (such as Social Security number, birthdate, pay rate or medical information) include storing it in one place—where it is needed for calculations or identification—rather than in multiple locations. For example, the employee’s Social Security Number and birthdate are not needed in a time and attendance system. Instead, employees can be identified by an assigned badge or ID number and can be sorted or stored by employment characteristics (such as job, department, team or group).

• **Restricted User Access**
  The system’s functionality and reporting capabilities are restricted according to users. This ensures that employees at different levels can only access information pertaining to themselves or their job responsibilities. The system should allow restriction rights for at least three levels: employees with no reports, supervisors, and payroll/HR administrators. Typically, employees will only have access to their individual information. Supervisors need access to both their individual information and the information of their direct reports for department scheduling and reporting. Finally, payroll and HR managers need broad access to both high-level and individual information and reporting to assist in administrative tasks and organization oversight.

• **Prompted Password Changing**
  The time and attendance system prompts users to change their password regularly (and encourages responsible password creation) to reduce the risk of password hacking. Ideally, passwords will be changed every 30–60 days. In addition, it includes a system in case a password is lost or forgotten.

• **Device Security**
  Physically-located system access points (such as kiosks or time clocks) and mobile devices require additional security features to protect users. Time-out values can be set to automatically log out users after a specified period of time. The system can “register” mobile devices so that users cannot log in on a device the system does not recognize. Also, time and attendance system administrators can configure mobile device access to limit users to basic features and functionality to protect the user in the event the device is stolen.

• **Off-Site Data Centers**
  The benefit of cloud-based applications is that organizations can avoid the overhead associated with storing their data locally. Instead, the cost of storing the data is handled by the vendor as part of the organization’s usage subscription. However, it’s important to realize that data must be physically stored
somewhere, and the storage facility must have security measures in place to protect it. These include automated data backups and disaster recovery plans in the event of prolonged power outages, flooding, fire or other natural disasters.

With these security features, organizations can feel confident their data is protected from internal and external security threats.

**Conclusion: Time and Attendance Data Security**

With the right safety features configured, cloud-based time and attendance systems can be more convenient and secure than traditional software. Protecting data from internal and external threats is critical to ensuring it is secure. This gives organizations the access and flexibility needed in a time and attendance system without compromising confidential data.

**About Attendance on Demand, Inc.**

Attendance on Demand supports the labor management needs of thousands of companies and more than a half million employees across North America. Launched in 2006, Attendance on Demand is a rapidly deployed, cloud-based solution that minimizes a company’s risk and technology investment while providing advanced features for securely managing labor data—calculating pay rules, scheduling employees, budgeting labor, and automating recordkeeping for labor law compliance. With standard uptime over the industry average of 99.995% and above average customer retention rates, Attendance on Demand removes the worry of maintaining expensive infrastructure. An extensive North American distribution network helps organizations use Attendance on Demand to reduce labor expenses and improve decision-making.

**References**

