The Data Dilemma

Safeguarding employee privacy is a key concern in today's digital economy.

By Marta Chmielowicz

With the digital economy in full swing, HR leaders are embracing technologies that capture employee data and deliver insights that can be interpreted to better attract, retain, and grow talent. But the flood of numbers pouring in from talent management platforms across the organization carries risk as well as reward.

"One major pain point that companies face is the vast amount of information there is to protect," says Mike Couvillion, chief technology officer at Kazoo. "Even for smaller organizations, each employee has quite a bit of sensitive information held by the company—meaning it's a pretty big task to securely manage and safeguard it all, especially as organizations grow. Add to that the prevalence of internet-connected devices and the ability to work remotely from any location, there are more access points than ever before for intruders to try to breach employee data."

And the consequences of a data breach can be severe. For example, when a 2014 data leak at Sony Pictures Entertainment exposed over 100 terabytes of private employee information—including social security numbers, emails, salary data, medical histories, birthdates, and home addresses—Reuters reports that the company was forced to pay $8 million in settlements.

How can companies prevent these data breaches and better protect themselves and their employees? Kon Leong, CEO and co-founder of ZL Technologies, recommends a personalized approach.

"Every HR department needs to get a read on the company's privacy comfort zone," he explains. "Different companies under various regulations and cultures will have different answers, so policies will also vary. For example, a European company's approach will invariably depart from a U.S. company due to differing notions of privacy."

He suggests that all organizations establish an information governance committee from various areas of the business that can work together to evaluate the company's specific needs and implement a unified privacy policy.

Protecting Employee Data

Employee data is incredibly useful for measuring performance, identifying skill gaps, and recruiting new talent, but balancing access and analysis with data security can be a major challenge—especially when information is dispersed across numerous HR systems.

To keep a firm grasp on sensitive information, employers need to look inwards and address any internal processes that could increase risk. "The best methods to help maintain privacy of employee information will not come from protecting the perimeter, but rather from protecting it from the inside. In other words, although building a wall around your data is important, make sure you know what is actually within those walls as well," Leong says.

HR professionals should take into consideration these three best practices:

- **Create a culture of safety awareness.** Upon hearing the words "data breach," many automatically assume that threats can only come from an external source: A hacker finds a crack in the firewall or distributes an email containing malware. But in fact, McAfee's *Grand Theft Data* study reports that 43 percent of serious data breaches are caused by internal employees and contractors—and half of those are accidental.

Common Sense Privacy Policies

Data security is a complex issue when dealing with numerous HR systems, but with these simple steps from Kim Lessley, director of solution management at SAP SuccessFactors, organizations can better protect their employees.

- Ensure that HR systems housing personal data automatically sign out after a period of inactivity.
- Set up printers so that employees cannot leave print jobs sitting unattended.
- Adopt a good spam filter to catch phishing and scam emails.
- Implement multi-factor authentication to access the corporate network.

HR has a responsibility to educate employees in order to protect data from the inside out. “An integral part of safeguarding employee privacy is to create a culture focused on security and privacy awareness by educating your people on how to safely handle sensitive information,” says Couvillion. “When employees know how to maintain their own security, they’re in a better position to keep company and employee data safe, help secure the network, and protect their own personal data.”

Leong recommends that HR professionals offer interactive training sessions and gamified cybersecurity lessons to build accountability and teach employees skills that they can apply at work and at home. Educating employees about simple safeguarding tactics like password security, social engineering hacks, and general file security best practices can make a big difference, Couvillion says.

- **Know where data is stored.** From candidate relationship management and applicant tracking systems to learning platforms, payroll management systems, and recognition software, employee data is often scattered across the organization.

“One of the major pain points when it comes to data security is knowing where your employee data is stored and who has access to it,” says Kim Lessley, director of solution management at SAP SuccessFactors. “Even if an organization has the good fortune of managing all of these processes out of a single HR system, chances are they will still have integrations to third-party systems, such as external vendors for background checks, employment verification, and benefits management. Understanding where this data is and how it flows from one system to another is a major challenge for most organizations.”

Often, lack of integration across systems requires HR staff to manually gather data from multiple sources and compile it into spreadsheets for analysis, placing the information in an unsecure format and increasing the odds that it will be seen by an unauthorized employee.

To combat this risk, Lessley suggests that HR professionals limit the amount of data that their organizations store. “A good rule of thumb is to practice data minimization—only collect and store the information you absolutely need, purge it when you no longer have a business need for it, and limit access to employee data to only those who really need it for their positions,” she says.

Additionally, Lessley says that employers should map out the data that resides in each system, as well as the ways that data flows between platforms. Only then can they maintain oversight of the information and establish processes for granting permissions to access that data.

“Ensuring employee privacy requires an iron grip on data. To achieve this, organizations need to be able to search the data ‘universe’ to locate, manage, and remediate information across various data silos,” Leong agrees.

- **Maintain proper authorization practices.** Another challenge of data security is managing authorizations and keeping them up-to-date as systems change and employees move around the organization. Lessley recommends that organizations establish a clear process for granting data authorizations and review it on a regular basis.

“An organization may start out with an HR department of two people who perform all HR tasks and therefore need to be able to access all employee data,” she explains. “Over time, the company grows and the department expands to six people specializing in different areas of HR. Do all HR employees need to have access to all employee data, or can you segment and limit what sensitive data certain roles can access?”

Couvillion says that employers can add an extra level of security by storing their private and confidential data on secure, protected networks. “Firewalls, two-step or biometric authentication methods, encrypted data, and other new technologies should be leveraged to protect and maintain the privacy of employees,” he says.

Data Breach Procedures

No matter how diligent an organization is about its privacy protection policies, data breaches can happen—and HR leaders need to know how to respond. “The most important thing an HR professional can do is to act quickly in the event of a data breach,” says Couvillion. “Knowing what sensitive employee data and information the organization holds—and where it's being kept—is key to this quick response, as is working closely with IT, compliance, finance, and other departments throughout the organization to get to a solution quickly."

Lessley suggests that organizations set up a breach response team beforehand that is trained to respond quickly in the event of a hack. This team should include a member of the senior leadership team, an HR professional, a legal representative, and a marketing or public relations professional to demonstrate that the company is taking the threat seriously and ensure that it is prepared to answer employee questions and keep messaging consistent.

She also recommends that organizations take the following preemptive steps to prepare for the worst:

- Create a plan documenting how HR will work with IT to identify impacted data, notify employees of a breach, and correct any issues.
- Determine what information HR will need to collect and communicate in the event of a breach. This can include the time and length of the data breach, the cause, the type of data that was compromised, impacted employees, and next steps.
- Prepare messaging templates, FAQs, and plans for live Q&A sessions that the breach response team can consult in the event of a breach.

POSTED AUGUST 15, 2019 IN RISK AND COMPLIANCE

Leave a comment

Related Posts

Under Fire
Mitigating Harassment
The Conundrum of Cannabis
CEO's Letter: Protecting Our Own
Preventive Measures
A Clean Slate
Ensuring Fair Hiring Practices
Complications in Crossing Borders
Ready or Not, Here it Comes
Creating a Culture of Compliance

SharedXpertise Media, LLC, 123 South Broad Street, Philadelphia, PA 19123

BY BEAVAN