THINK HACKERS CAN'T GET INTO YOUR HRIS SYSTEM? THINK AGAIN.

8 Tips to Help Protect Your Employee Data

77%

of IT leaders say that they expect their companies to suffer a data breach over the next 3 years

SOCIAL SECURITY NUMBERS. NAMES. ADDRESSES. SALARIES. BANK ACCOUNT INFORMATION.

Your human resources information system (HRIS) holds a treasure trove of private information about employees that hackers would just love to get their hands on. And that makes the struggle to keep them away from it even more critical. Just last month, malicious actors gained access to employee data at Activision, a worldwide distributor of interactive entertainment products, and stole email addresses, phone numbers, and salary data of employees. While the situation was disturbing and unfortunate, it's not surprising.

So, with threats (and expectations) high for security issues down the road, business leaders are wise to ask their teams now: "How can we increase security measures to protect the employee data stored in our HRIS?"

Here are just a few best practices organizations of all sizes can consider to help ensure their private HRIS data remains, well, private.

ADOPT A ZERO-TRUST POLICY

Zero trust policies mean "never trust, always verify" both internal and external users who look for access to your systems. These days, you've simply got to assume that your systems are ALWAYS at risk for a cyberattack. So, make it a rule: Unless users can be verified, they don't gain access to private data.

USE MULTI-FACTOR AUTHENTICATION

Think of this as a "belt-and-suspenders" approach to security - especially if you're still relying on single-factor authentication to confirm identities. As cyber criminals grow more sophisticated in gaining unauthorized access to data and systems, so too must your verification process. Practices like multi-factor authentication (MFA) confirm user identities through at least two different ways to prevent unauthorized access. This way if someone steals login credentials and happens to make it through your first level of security, there' still another layer that can deny access.

In the last year:

large organizations increased their use of MFA by **20%**

55% of small organizations said they used MFA for HR applications

AHT INSURANCE
A BALDWIN RISK PARTNER

ENCRYPT DATA

One of the most important ways to decrease risk and increase safety is to use encryption technology to garble private data whether it's sitting in the cloud, hosted on your server, or being emailed to employees. So even if despite all your safety precautions, malicious actors happen to access it, they won't be able to read it or use it for their own nefarious purposes.

LIMIT ACCESS

Another practical way to protect private HR data is to limit who in your organization needs access to it. Establish processes for approving user access. As a general rule, only those with a direct business reason should have access to confidential information about employees or job applicants. Everyone else? Just say no.

DELETE OLD OR UNWANTED INFORMATION

Another practical way to protect private HR data is to limit who in your organization needs access to it. Establish processes for approving user access. As a general rule, only those with a direct business reason should have access to confidential information about employees or job applicants. Everyone else? Just say no.

BUILD A CULTURE OF TRAINING

Together with a written cyber security agreement that all employees can sign, ongoing training programs that reinforce important security practices are key. For instance, if you run a training session about email scams, follow-up up with a "test" phishing email to all who attended to make sure they understand what to do. If they don't act within the guidelines you set, then have them repeat the training until they get it right. By creating a loop of training, you can ensure that the people who need it most, get it. And further close gaps of vulnerability in your organization.

CONSIDER AI TRENDS

Hackers already exploit AI for social engineering purposes, mimicking emails from CEOs, for example, to gain access to systems or transfer funds to different accounts. To combat these latest tricks, organizations can engage IT teams to explore how AI, in turn, may help protect sensitive HRIS data. **In many cases, AI can boost security by:**

- flagging possible incidences of fraud
- blocking suspicious activity before it has a chance to do damage
- denying access to information for unapproved individuals

These are just a few ways to enhance the security of your HRIS data. Of course, cyber insurance, can also offer important financial protection against the effects of cyberattacks.

Contact us for help finding the right coverage for your organization and get connected to other resources that can help you shore up protection.

CONTACT US

AHT INSURANCE
A BALDWIN RISK PARTNER