What you Need to Know about HR DATA SECURITY to Protect your Organization from Outside Threats

eBook

TABLE OF CONTENTS

Introduction

When it comes to data security, many businesses tend to think of things like firewalls and email spam blocking software to protect their sensitive data. But they often overlook their biggest vulnerability -- the human error of their own employees.

Pronounced as one of the worst publicly announced data breaches to ever impact the U.S., last spring hackers stole the sensitive data of more than 143 million U.S. consumers by exploiting a flaw in the commonly used Apache Struts framework. This flaw had been patched by Apache over two months prior to the Equifax incident. Equifax failed to deploy this patch, allowing hackers to remotely obtain the private data.

Introduction

While no organization deliberately sets out to become another data breach statistic, some organizations still may not understand the critical need for cyber security protection as it relates to employee data. HR data regularly contains sensitive Personally Identifiable Information (PII) that makes it a key target for criminals. In order to best protect an organization from attacks, and keep HR data secure, it's critical to understand the three essential questions around HR data security covered in this eBook.

What you Need to Know about
HR DATA SECURITY
to Protect your Organization from Outside Threats

Source of Breach: Greatest Threat

Source of Breach
Greatest Threat

The **greatest threat** to HR data security is not remote hackers but **social engineering**, an attack that relies heavily on human interaction and often involves deceiving individuals into breaking normal security procedures.

The greatest threat to HR data security is not remote hackers but social engineering, an attack that relies heavily on human interaction and often involves deceiving individuals into breaking normal security procedures. Whether it be via individuals falsely representing themselves as IT staff, or through finding a loophole in poorly maintained password hygiene. The first thing HR teams must do to ensure data security is to provide ongoing training for their organization around data security best practices – no matter if data is kept on premise, or offsite.

Source of Breach: Greatest Threat

"...training is the greatest possible weapon against cyber security threats"

Employee error is to blame for most data security breaches. According to Egress Software Technologies, human error accounted for nearly 67% of security compromises. Another study from information security company PhishMe exposed a 789% increase in email phishing attacks containing malicious code, including ransom-ware, in the first quarter of 2016 over the final quarter of 2015.

What you Need to Know about
HR DATA SECURITY
to Protect your Organization from Outside Threats

Source of Breach: Greatest Threat

The results of these and other studies should serve as a call-to-arms for businesses that training is the greatest possible weapon against cyber security threats. Businesses should regulate password updates, and establish policies surrounding email etiquette. HR can also establish a strategy to automate employee termination which would automatically shut off employee access to their network and business applications when the employee leaves an organization.

What you Need to Know about
HR DATA SECURITY
to Protect your Organization from Outside Threats

Data Storage: Forward-Thinking Trend

Recent years have seen a trend toward more advanced technological solutions for managing employee data. Although saving HR data on local servers was a successful business strategy in its time, it is no longer the most secure option.

Information Services Group (ISG), a global technology research and advisory firm, predicts that more than half of all enterprises will move all or some of their HR systems to the cloud by 2020. In their annual report, ISG advises that when "looking at specific factors that impact the selection of new HR technologies, data security ranks the highest."

Data Storage
Forward-thinking Trend

Recent years have seen a trend toward more **advanced technological solutions** for managing employee data. Although **saving HR data** on local servers was a successful business strategy in its time, it is no longer the most secure option.

Data Breach Protocol: Best Practices

In the event of a data breach, the first thing an organization should do is hire a third-party IT team that specializes in incident response and data forensics to analyze traffic and determine the root cause of a breach. Using an unbiased third-party specialist will allow you to learn exactly what has been accessed and compromised, detect what liabilities created the breach, and recommend best practices to ensure the breach doesn't occur again.

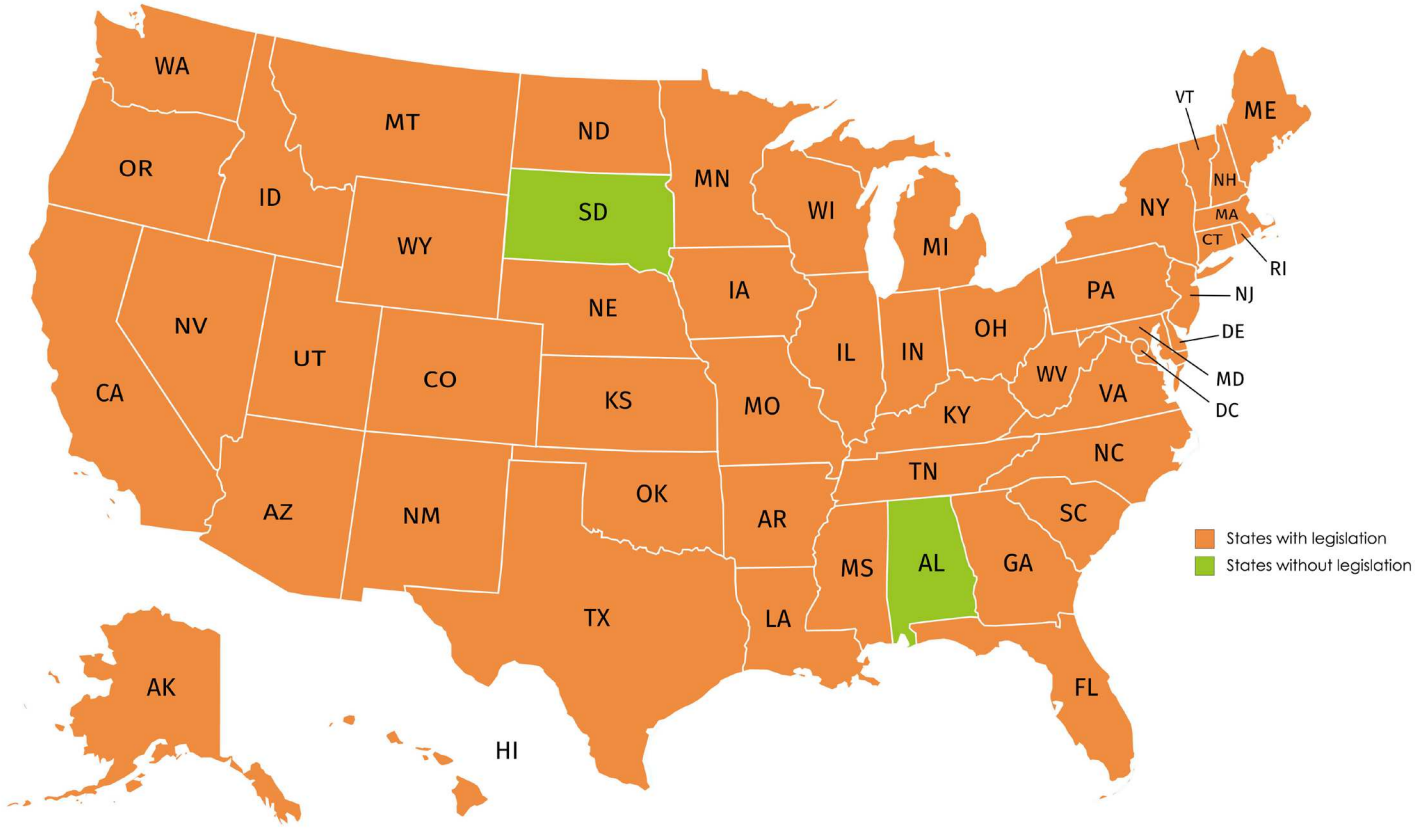
Data Breach Protocol
Best Practices

The first thing an organization should do is **hire a third-party IT team** to determine the root cause of a breach. Once you understand the forensics and have a solution in place you need to **communicate the facts to affected employees.** Lastly, **research state law regarding whom to notify** in case of a breach and determine whether your breach type is covered by legislation.

Once you understand the forensics and have a solution in place, you need to communicate the facts to affected employees. It is crucial that you communicate what happened, who is affected, what solution you are putting in place, and how you are helping those affected by the breach

Data Breach Protocol: Best Practices

Lastly, research your own state law regarding whom to notify in case of a breach and determine whether your breach type is covered by legislation. Forty-eight states, the District of Columbia, Guam and Puerto Rico have all enacted data breach notification statutes, with Massachusetts and California having the most rigorous standards; leaving only Alabama and South Dakota without legislation.



Conclusion

Whether it's employee's social security numbers, insurance information, or bank account information — at some point a hacker will see your businesses vulnerable data as their next big paycheck.

If your organization, or your HCM vendor, haven't suffered a data breach, you're either very fortunate or are already prepared.

Do you know which you are?

That's why everyone in your company — not just IT — needs to understand the threats and how to mitigate them.

Data Security: Ascentis HCM

Ascentis primarily hosts its products with RagingWire data center. RagingWire is audited annually for SOC1 Type II compliance. Ascentis also hosts certain clients from our own data center. That data center is also audited annually for SOC Type II compliance. Both data centers are consolidated into the Ascentis SSAE16 Type II report, which is available upon request.

Powerful Integrated HCM Solutions for the Mid-Market

Ascentis realizes that the number one asset in any organization is its people. Ascentis' comprehensive suite of HCM (human capital management) solutions helps organizations develop and elevate their workforce, supporting greater productivity and advanced performance. Total cost of ownership is reduced through our innovative fixed-pricing plans and low implementation fees.

Learn More

Copyright and Permissions