

SPONSORED TOPICAL WEBINAR

An Educational Resource for APA members
from Compliancy Group.

Compliance and Security: Why You Need Both to be HIPAA Compliant

February 28, 2024

PAID FOR BY



DISCLAIMERS

Liam Degnan has a working relationship with Compliancy Group. As such, he has both a financial and intellectual interest in the webinar content. The purpose of this presentation is to provide a balanced view on HIPAA Compliance.

The content was created by Compliancy Group and does not reflect the views of APA or its editorial staff. Email advertising@apa.org to learn more.

ATTENDANCE

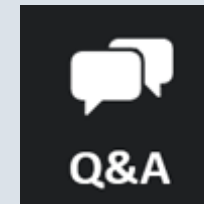
- No CE credit will be offered for this webinar.
- A “Certificate of Attendance” will be emailed to live attendees only.
- You must attend for 45 minutes to receive the certificate.

RECORDING

- A recording of this presentation will be emailed to everyone in 2 weeks' time.
- The recording will include the presentation slides.

HAVE A QUESTION?

- You are on mute. Communicate using the **Q&A box** in the webinar screen. Submit your questions for our speakers using the Q&A box.
- Presentation slides will be posted in the **chat box** of your webinar screen.





Liam Degnan, Senior Sales Engineer

PRESENTER

Liam Degnan has an 8+ year history of experience combining risk management, SaaS sales, and regulatory compliance in the healthcare space. Liam speaks on a variety of platforms and topics, with an emphasis on simplifying HIPAA, OSHA, SOC 2 and other general healthcare compliance regulations.

Introduction to HIPAA Compliance

Who Needs to be HIPAA Compliant?

Covered Entity

- Any organization that collects, creates, or transmits PHI electronically
- Organizations that are considered Covered Entities include: healthcare providers, healthcare clearinghouses, health insurance companies etc

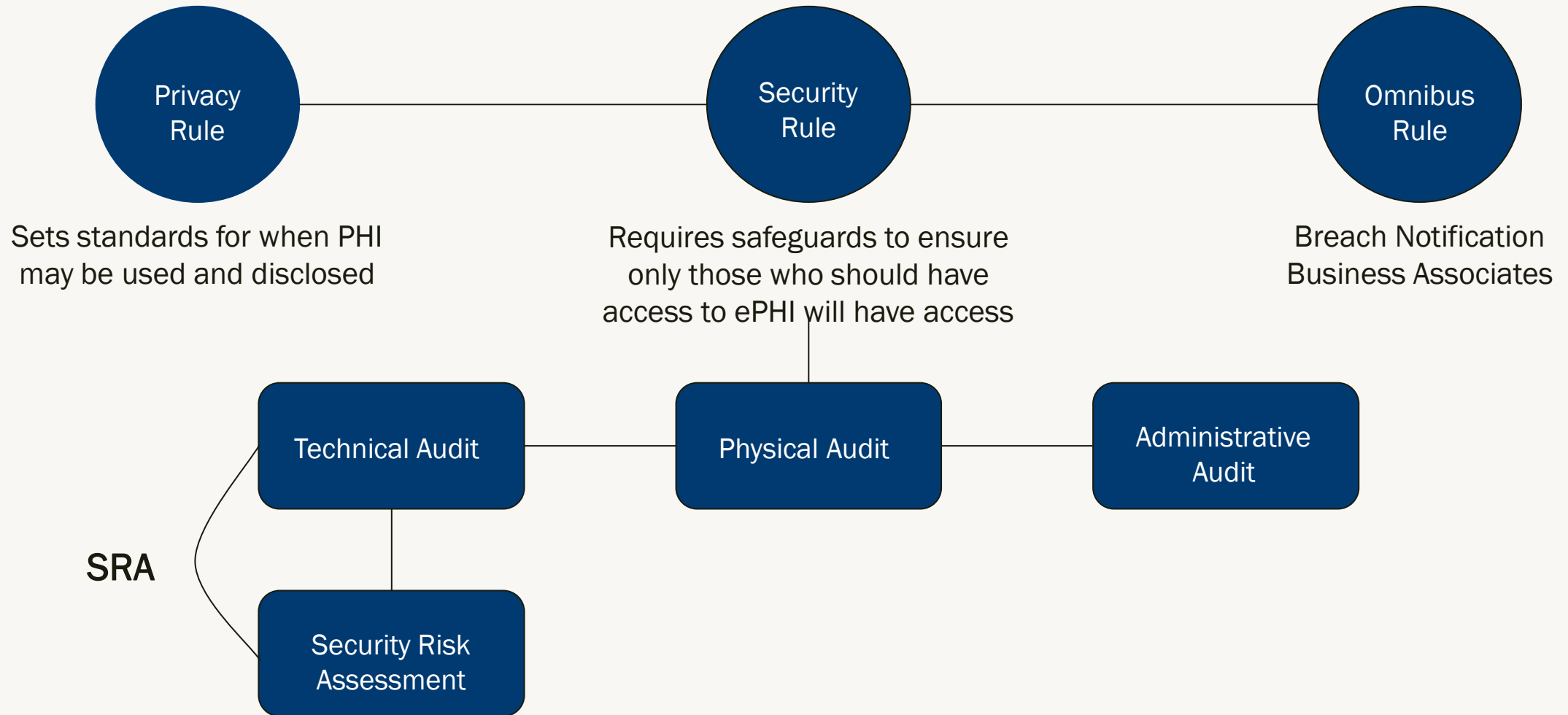
Business Associates

- Any organization that encounters PHI in any way over the course of work that it's been contracted to perform on behalf of a covered entity
- Examples of Business Associates include: MSPs, IT Providers, faxing companies, cloud storage providers, etc.

7 Fundamentals of an Effective Compliance Program

1. Implement written policies, procedures, and standards of conduct
2. Designate a person to ensure they are followed
3. Conduct effective training and education
4. Develop effective lines of communication
5. Conduct internal monitoring and auditing
6. Enforce standards through well-publicized disciplinary guidelines
7. Responding promptly to detected offenses and undertaking corrective action

HIPAA



Patient Engagement: HIPAA is Good for Business

HIPAA Compliance is **legally required**, but also represents a unique growth opportunity

Patients are often concerned about their privacy and confidentiality. Implementing an **Effective Compliance Program** can help ensure your patients feel safe and secure

68%

of patients are not confident
that their healthcare provider
protects their medical records

53%

of patients believe that their
provider's negligence
caused/contributed to identity
theft

What's the Difference Between Compliance & Security?

Compliance

vs

Security

- Government regulated and mandated
- Binary - you're compliant or you're not
- Technologically vague
- Requires ongoing management
- Prioritizes documentation

- Risk Management
- Shades of gray
- Defined by risk profile
- Commonly thought of as an IT issue
- Can be **highly secure** and still not **compliant**

Compliance Mandates Security



What's Security?

Definition: the quality or state of being secure, such as:

- a. Freedom from danger - safety
- b. Freedom from fear or anxiety

Firewalls



Encryption



Backup



Spam & Virus



The Importance of Trust

20%

Patients are lost by
practice annually on
average

68%

Appointments come
from existing patients

83%

Patients would
recommend a
practice they trust

82%

Patients will stick to a
practice if they trust
it

The Importance of Technology



62% of patients want to communicate with providers through email



64% of patients schedule online



61% of patients say digital services are important when choosing a physician



2/3 of patients would switch providers for access to their records online

Bad News

17,000

medical records
breached per day on
average

89%

of healthcare
organizations have
experienced a breach
over the past 2 years

86%

of mistakes are
administrative

HIPAA & Cybersecurity Basics

Why Care About Cybersecurity?

On average, more than **1 in 10** sensitive files are open to every employee

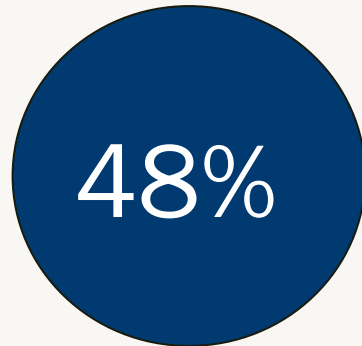
The average cost of a data breach in the healthcare sector was **\$4.45 million** in 2023

Over 50% of organizations have more than **1,000** files open to every employee



Insights on Data Breaches

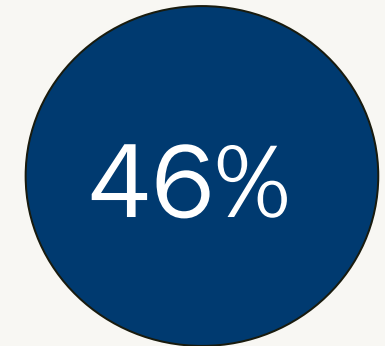
Among both small and large healthcare providers, **more than half store more than 90% of patient data digitally**; such as patient records, medical histories and billing records.



of large healthcare providers say they had experienced a data breach in the past



of small practices had experienced a breach in the past



of small practices said human error was the leading cause of a data breach

An Industry Under Attack

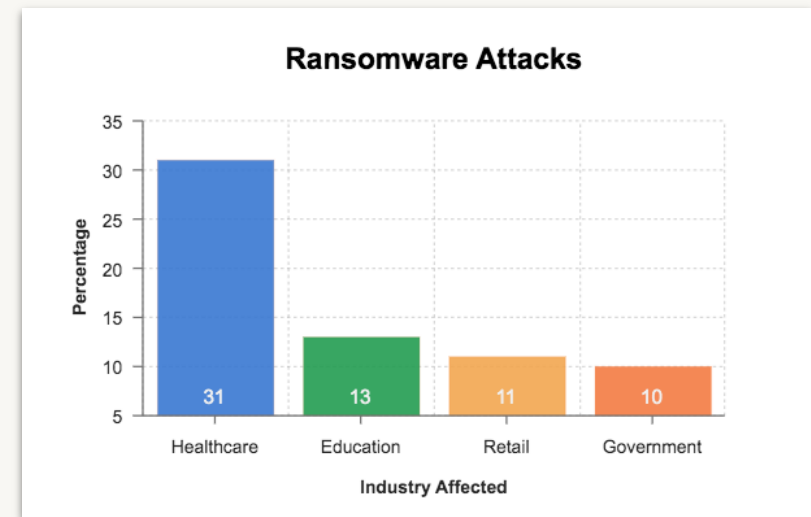
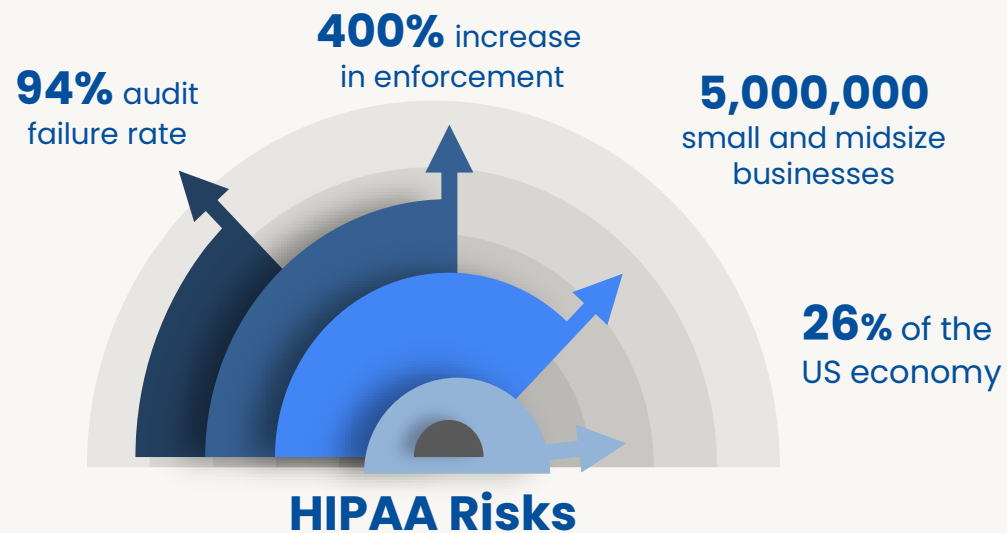
- 93% of healthcare organizations have experienced a data breach over the past three years
- 62% of administrators feel inadequately trained and/or unprepared to mitigate cyber risks
- Small to midsize organizations are primary targets for hacking
- Hacking/IT represents the majority of healthcare cyber breaches

What's Ransomware?

“Malware that attempts to extort money from a computer user by infecting and taking control of the victim’s machine, file, or documents”



Why Healthcare & Compliance?



Causes of Violations/Breaches



Phishing



Lost/Stolen
Devices



Vendor/
Hacked



Theft

Do you have proper safeguards in place?

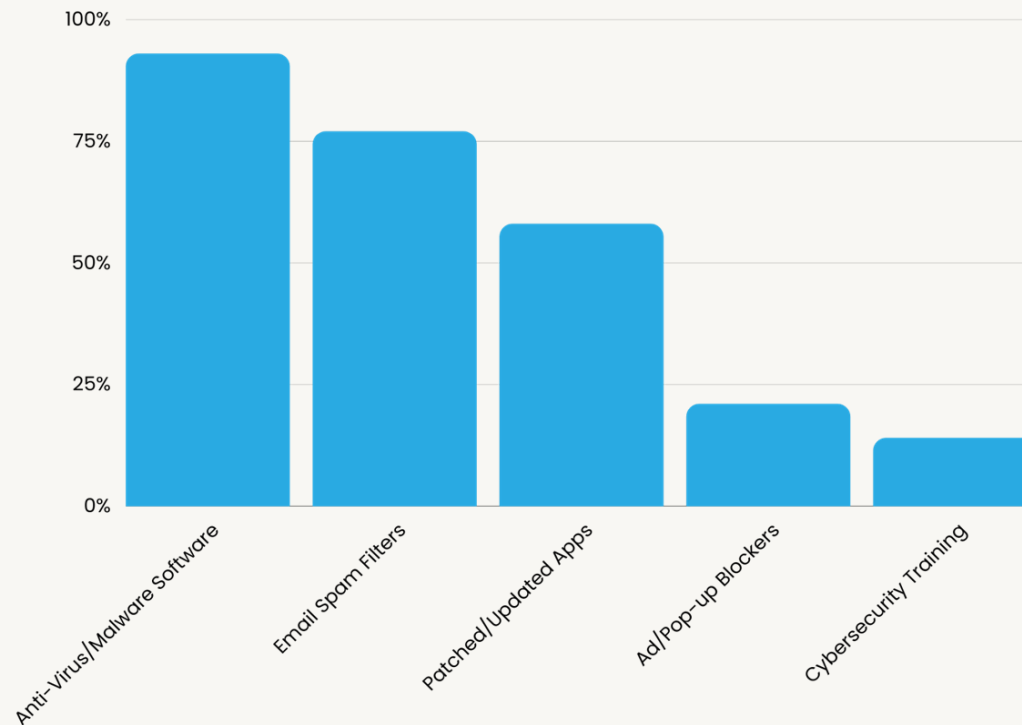
In Reality, Tech *Isn't* Usually the Problem...

86% of IT-related incidents occur as a result of ***administrative error***

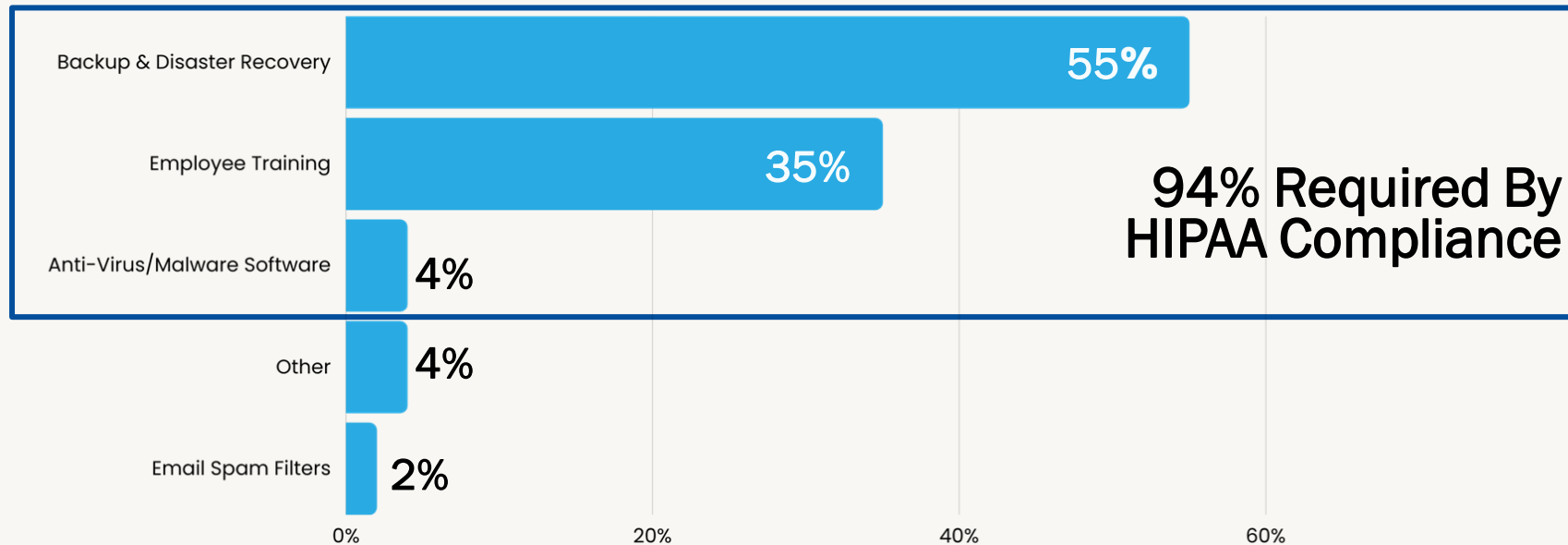
The #1 reason breaches occur is a mistaken belief that current security is “good enough”

CompTIA's International Trends in Cybersecurity report

Ransomware Outsmarts Today's Top Defense Measures

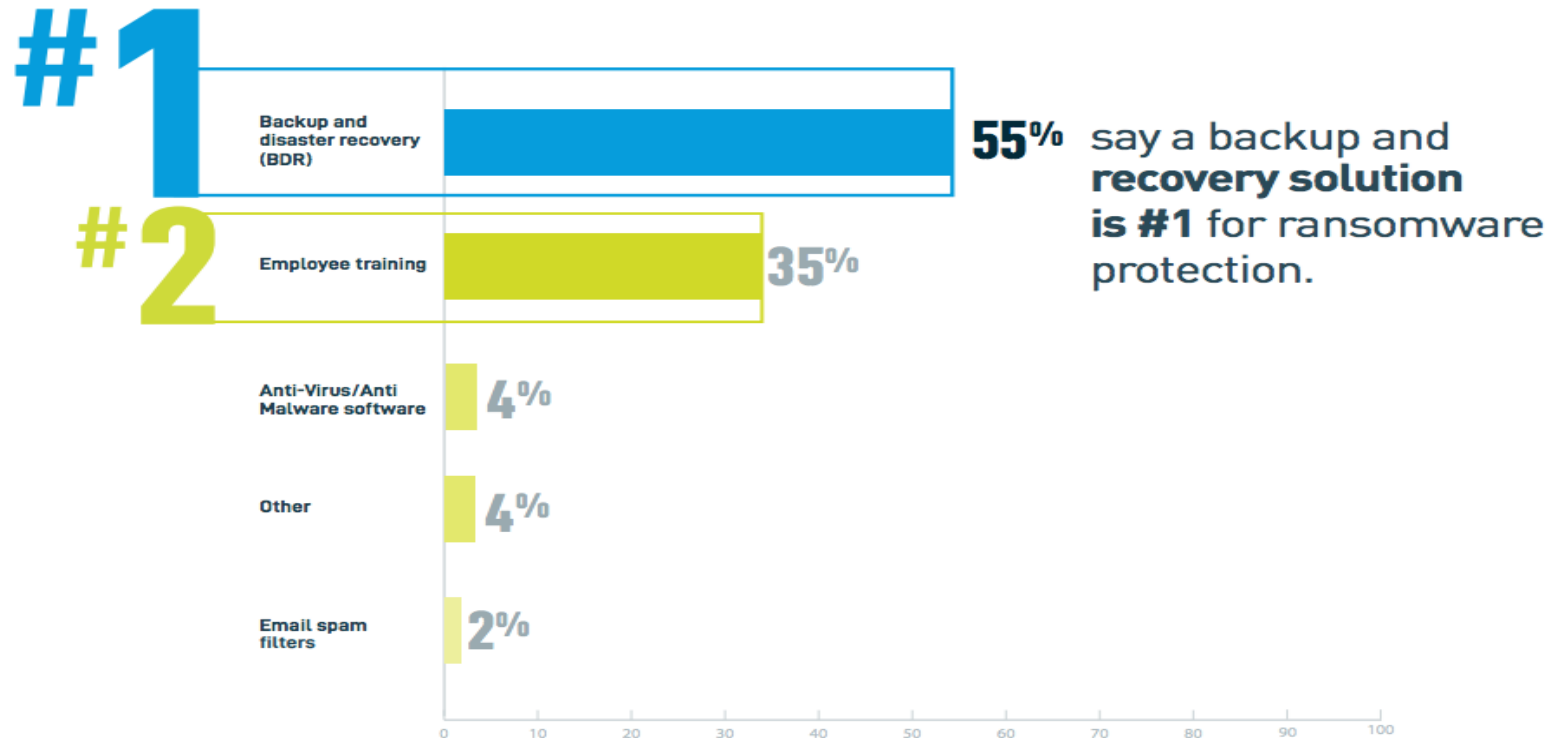


Backup & Disaster Recovery - Most Effective Ransomware Protection



BACKUP AND DISASTER RECOVERY (BDR) MOST EFFECTIVE RANSOMWARE PROTECTION

► Of the following, which would you say is most effective in terms of business protection from ransomware?



94% Required
by HIPAA
Compliance

Fines, Fines, Fines

A healthcare plan members were able to access PHI of other members for two days and had reported two breaches in 2016 and 2019.

\$1,300,000

In a health system, hackers accessed PHI of 2.81 million individuals.

\$1,250,000

A California-based psychiatric medical group was fined for right of access failure.

\$25,000

A Licensed Professional Counselor in Pittsburgh was fined by HHS for a right of access failure.

\$15,000

A mental health and substance use disorder provider in Massachusetts was fined for potentially violating the HIPAA Right of Access.

\$70,000

A medical group had a network incident that affected 230,572 patients due to a data file placed on a server separate from their client hosting environment.

\$25,000

HIPAA Compliance & Security

Assessment of Risks: remediate vulnerabilities

Training: staff knowing what to look for and how to identify attacks

Policies & Procedures: stops ransomware infection before it takes hold

Encryption: protect the sensitive information

Backup: practice 3-2-1

Disaster Planning: restoration of access to data and getting back to business

What Can You Do Right Now?



Get HIPAA Compliant



Restrict unnecessary access



Passwords



Keep anti-malware up-to-date



Show your members what to look for



Ensure a backup plan

AUDIENCE Q&A

FINAL THOUGHTS

- A recording will be emailed to you in 2 weeks. It will include the presentation slides.
- Take our survey immediately after the webinar has concluded.

THANK YOU!

PAID FOR BY

