ARMOR BULLETIN - HEALTHCARE: FALL 2020

UPDATES ON HITRUST

In the healthcare industry, securing data protects more than the bottom line; it safeguards the privacy and dignity of patients by controlling who can and cannot view their most personal information.

CONTENT

A HEALTHCARE INDUSTRY UNDER ATTACK

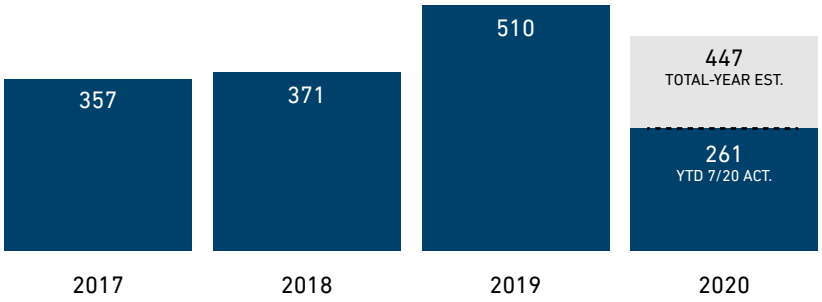
As a cybersecurity software company, Armor works with many healthcare and healthtech companies to secure their sensitive applications and related data as part of compliance with HIPAA.

Across the industry, 2019 was a difficult year with a record high number of breaches. Though 2020's estimated breaches are projected to be lower, they clearly represent an overall upward trajectory in breaches year after year. Fortunately, the number of records exposed through July 2020 is only 6.7 million, a far cry from 2019's high of 41 million records.

HITRUST develops, maintains, and provides broad access to its widely-adopted common risk and compliance management frameworks, related assessment, and assurance methodologies.

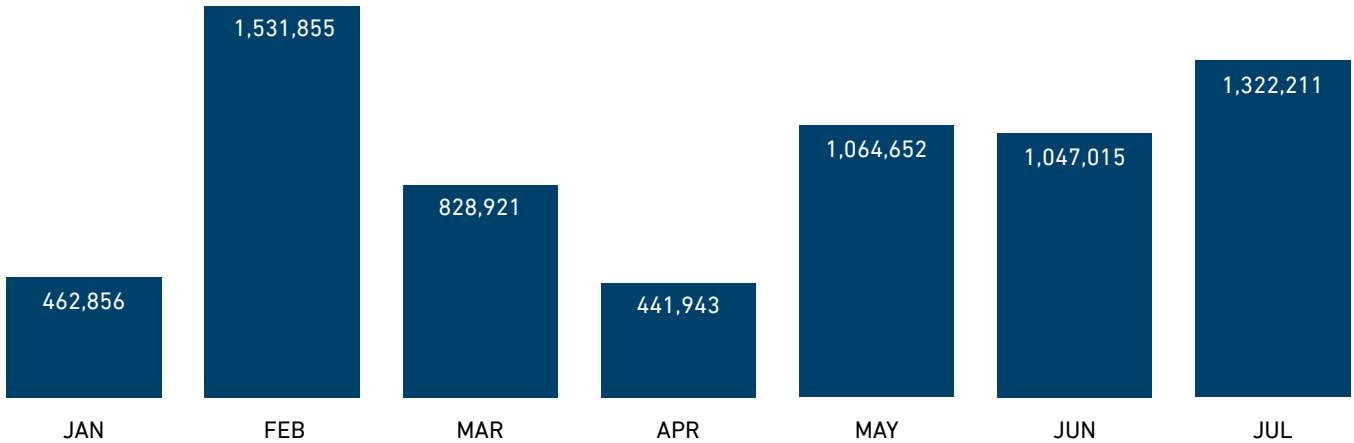
— HITRUST Alliance

BREACHES BY YEAR



Source: Armor

HEALTHCARE RECORDS BREACHED IN 2020



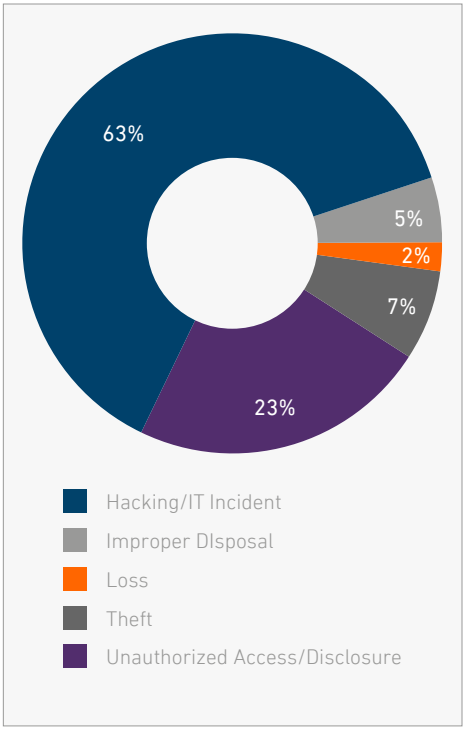
Source: HIPAA Journal

ACCIDENTAL AND INTENTIONAL CYBER RISK IN THE CLOUD

Healthcare and healthtech organizations face challenges as they seek to leverage cost efficiencies in the public cloud.

In addition to defending against a changing threat landscape, these organizations must put controls and processes in place to protect from inadvertent exposure of data as a result of misconfigurations, "honest mistakes," and even negligence on the part of employees or third-party vendors.

Intentional and accidental cyber risk are two sides of the same coin, and organizations must consider both when deploying sensitive applications and data into the public cloud.



COMPLIANCE WITH HIPAA

When the Health Insurance Portability and Accountability Act (HIPAA) was signed into law in 1996, it fundamentally changed how health information was treated across the industry. However, despite the weight of the legislation, it soon became clear that requirements and guidelines were, at times, vague and poorly defined.

Founded in 2007, the HITRUST Alliance was established with the intent to provide an actionable framework for complying with HIPAA guidelines, and it developed the HITRUST Common Security Framework (CSF). In recent years, the HITRUST Alliance began incorporating other security, compliance, and privacy frameworks into the CSF. This incorporation has helped healthcare and healthtech organizations, subject to or pursuing alignment with other frameworks outside of HIPAA such as PCI DSS, do so more efficiently.

HITRUST CSF

14 CONTROL CATEGORIES

49 OBJECTIVES

155 CONTROL REFERENCES

THE 14 CONTROL CATEGORIES

0.0	Information Security Management Program	**7.0**	Asset Management
1.0	Access Control	**8.0**	Physical and Environment Security
2.0	Human Resources Security	**9.0**	Communications and Operations Management
3.0	Risk Management	**10.0**	Information Systems (Acquisition, Development, & Maintenance)
4.0	Security Policy	**11.0**	Information Security Incident Management
5.0	Organization of Security Policy	**12.0**	Business Continuity Management
6.0	Compliance	**13.0**	Privacy Practices

CSF VERSIONS

VERSION 9.4.1

HITRUST CSF version 9.4.1 represents the latest iteration of the framework.

VERSION 9.4

Released on June 22, 2020, as HITRUST CSF version 9.4, the HITRUST Alliance continues to expand on the versatility of the framework. In this update, the HITRUST Alliance incorporated the Department of Defense Cybersecurity Maturity Model Certification (CMMC) into the CSF. Version 9.4 also saw updated NIST SP 800-172 r2 mappings for stronger alignment of controls.

VERSION 9.3

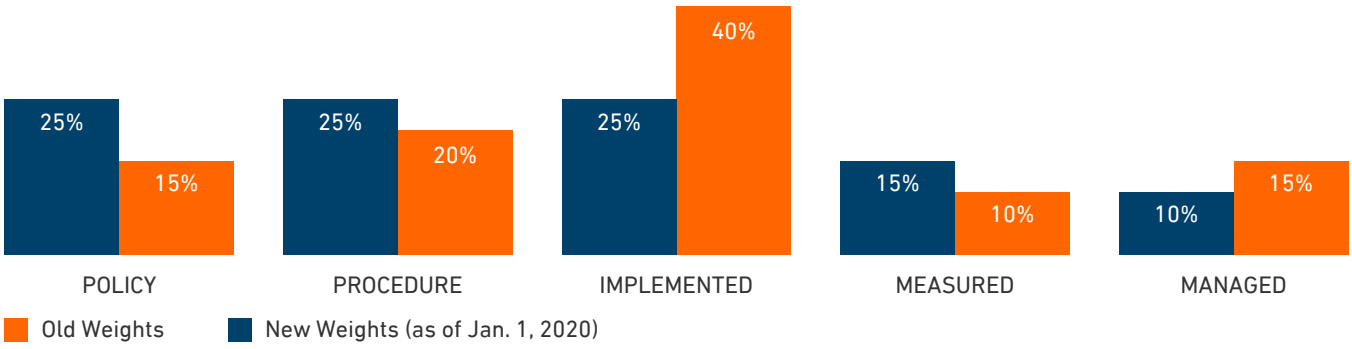
The version addressed requirements of the California Privacy Protection Act (CCPA) 1798 and the protection of consumer data as well as opt-out processes. It also incorporated The South Carolina Insurance Data Security Act 2018 (SCIDSA) 4655, which requires organizations to have a cybersecurity program and report cybersecurity incidents.

WHAT'S NEW WITH HITRUST CSF IN 2020

WEIGHTING SCALE

Effective Jan. 1, 2020, HITRUST Alliance adjusted HITRUST CSF's PRISMA weighting scale to place more emphasis on the actual implementation of controls.

CHANGES TO HITRUST PRISMA MATURITY MODEL WEIGHTING SCALE



Source: HITRUST Assurance Advisory 2019-007

SHARED RESPONSIBILITY PROGRAM

HITRUST Alliance also released its Shared Responsibility Program, which is intended to bring clarity and specificity on the division of responsibilities between cloud service providers and their customers. This is particularly useful given that CSPs' shared responsibility models can be too broad and vague with no additional documentation to spell out exactly what each layer of the model implies.

COVID-19 RESPONSE

HITRUST Alliance put out perspectives and "alternative approaches" to third-party attestation of controls through use of tools such as video conferencing.

WHAT TO EXPECT THROUGH 2021

You can expect to see additional enhancements to the HITRUST CSF to incorporate further controls and guidance around privacy frameworks. As of July, California, Nevada, and Maine had signed bills addressing data privacy. More than a dozen states had legislation in some stage of introduction and review. (Source: IAPP)

OUTCOME OF COVID-19

Expect further discussion and codification of "alternative approaches" to internally-driven, third-party attestation of controls through use of tools such as video conferencing.

VERSION 10.0

HITRUST CSF Version 10.0 will be released in Q4 2020 and will likely roll out further frameworks broadening the CSF's appeal across more industries.

ABOUT ARMOR

Armor is a global cybersecurity software company. We simplify protecting data and applications in private, public, or hybrid clouds as well as help organizations comply with major regulatory frameworks and controls. We know security is complex; it doesn't have to feel that way.

HITRUST CSF-CERTIFIED SOLUTIONS

Armor is certified by HITRUST whose framework is designed to simplify HIPAA compliance requirements by providing prescriptive compliance guidelines.

To accelerate your compliance with HITRUST, check out Armor.

SOURCES:

- HIPAA Journal – July 2020 Healthcare Data Breach Report
- Full-year 2020 estimate performed by Armor.
- HITRUST Assurance Advisory AA 2020-007 – September 3, 2019
- "US State Comprehensive Privacy Law Comparison," - The International Association of Privacy Professionals – July 2020
- HITRUST Alliance Shared Responsibility Program

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167