Smart Cyber Defenses Demand a Strategic Approach and Recognized Best Practices

SETTING THE SCENE

Health and life sciences executives working amidst an increasingly digitized landscape face sizable cybersecurity and information security challenges and risks. In healthcare, a highly digitized industry landscape means a much bigger attack surface compared to other industries. Although paper records can't be breached, digitized ones can. Beyond breach of patient records, ransomware attacks that disrupt operations may even prove fatal for patients and healthcare consumers.

Cyberattacks are now often a well-calculated, well thought-out, and highly strategic endeavor involving smart political know-how, skill, and sophistication. Here, organized criminals and cyber gangs are often highly trained, well-prepared, well-funded, supported, and sometimes even protected by foreign governments.[1]

According to Kelvin Dickenson, Senior Vice President, Risk and Compliance, SAI360, leaders such as Chief Information Officers (CIOs) "are constantly learning about compliance costs, the ongoing evolution of cybersecurity, the implementation and execution of digitization, artificial intelligence, and the Internet of Things across healthcare and life sciences, and so much more tied to health information technology (health IT).

Healthcare organizations face ongoing threats from phishing schemes, and backdoor vulnerability exploits. When it comes to Protected Health Information (PHI), healthcare providers are the most frequent victim of breaches, more so than payers or other participants. In addition to direct attacks, the risk presented by third parties is critical. Business associate (BA) involvement in breaches is steadily Increasing. Whether attacks occur directly or through a vulnerable third party or BA, they can prove disastrous, leading

"What they are finding is having inadequate technology and controls in place to manage healthcare's sizable attack surface exposes their organizations to unnecessary risk to patient data and organizational operations."

SAI360
RISK FROM EVERY ANGLE

1 https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed

to things like large regulatory penalties, information held at ransom, patient data being stolen and sold behind the scenes, and even an entire organization having to activate business continuity and disaster recovery plans.

"A quick online search or glance at mainstream media headlines reveals healthcare insurance plans, hospitals, clinician groups, and others in the healthcare sector remain in the spotlight for all the wrong reasons," said Kelvin. The headlines are usually tied to the aftermath of a cyber event, leading to reputational damage, expansive data losses, heavy fines, and significant organizational disruption, perhaps even needing to suddenly go fully offline, losing access to medical record information, delaying medical procedures, or diverting patients to different medical facilities.

There is typically significant organizational disruption as well. For example, providers may lose access to medical record information, be forced to go offline, need to delay medical procedures, or divert patients to different medical facilities.

Why is healthcare information so valuable? Patient records include an inherent wealth of data—including PHI. PHI details a person's care information, personal details, health history, insurance details, and payment information.

Because of its highly detailed and personalized information tied to someone's lifelong medical identity—one single healthcare data record may be worth up to $250 on the black market versus $5.40 for the next highest value record[2], a payment card. Stealing this information can allow someone to commit medical identity theft, buy prescription drugs or send a Medicare claim on someone's behalf, and more.[3]

PHI also reveals information about people's individual health stories, family health history, or medical appointment history, for example. Access to a health record gives details of prescriptions, operations, participation in health programs, diagnoses, and hospital stays. Compare this to personally identifiable information in retail or banking, for instance, such as credit card data, which can be changed if compromised.

"In short, you can get a new credit card number but not a new health history. This is why healthcare is an ideal target that once breached, remains compromised," emphasized Kelvin.

Bad Actors are Making Moves

Ransomware, cyberattacks, and breaches are becoming more widespread. This means large-scale patient data theft is becoming more commonplace—meaning more incidents, and more people are affected in each incident.

Cybercriminals deploying ransomware, for instance, now have more opportunities than before to use phishing, social engineering, and of course unpatched backdoor vulnerabilities.

What Does This Look Like in Action?

- Phishing and ransomware attacks are now the most significant security incidents affecting healthcare organizations4
- Nearly one in two healthcare cybersecurity professionals say the most important security breach they went through within the past twelve months was a phishing attack, with 17 percent saying ransomware4
- Email-based phishing attacks account for nearly three in four—71 percent—of big security breaches, with over one in four saying voice phishing (vishing) and nearly one in four saying a significant smishing (SMS phishing) attack4
- The first compromise point for 15 percent of attacks was social engineering. And phishing was the most common way into an organization, accounting for 71 percent of attacks[4]

In the meantime, the COVID-19 pandemic increased the number of incidents and their severity. Although healthcare providers account for most of these incidents, BA incidents have been increasing since COVID-19. IT incidents, as opposed to improper disposal or loss, make up the overwhelming majority of events and a large majority of breaches, as highlighted below:

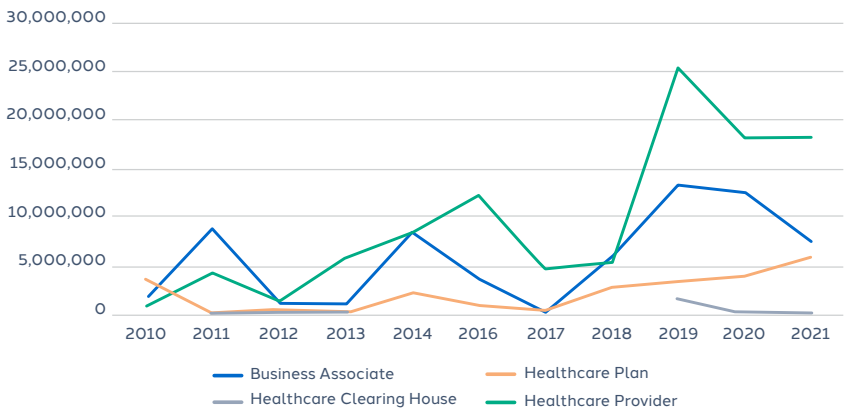
2 https://www.trustwave.com/en-us/resources/library/documents/2019-trustwave-global-security-report/

3 https://www.coverys.com/knowledge-center/Healthcare-Patient-Data-and-the-Black-Market

4 https://www.infosecurity-magazine.com/news/phishing-top-threat-to-us/

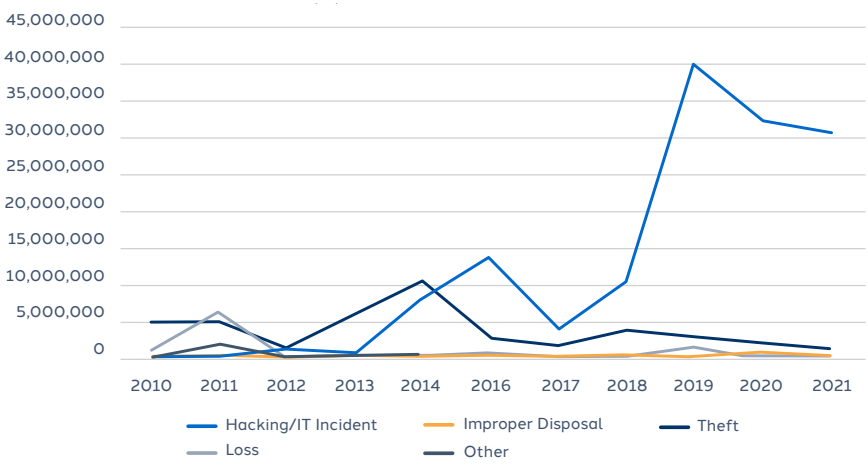
BREACH TRENDS:
HHS OFFICE FOR CIVIL RIGHTS REPORTED BREACHES REVEAL THE CHALLENGE

Individuals Affected 1



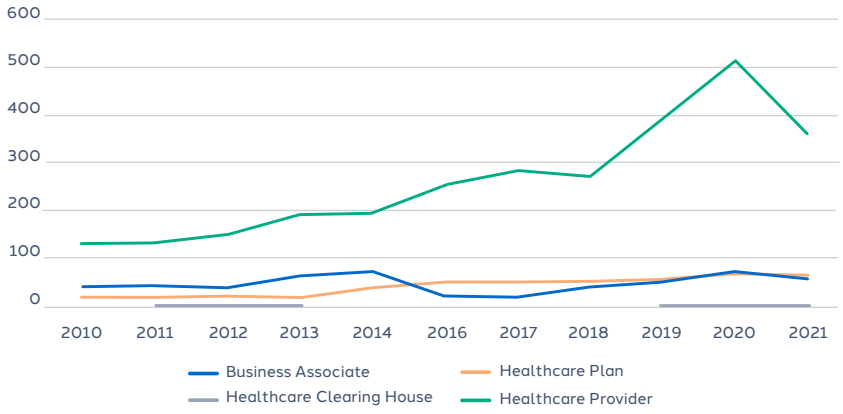
Trend data excludes 2015 due to an outlier event affecting nearly 78 million records that year.

Individuals Affected 2

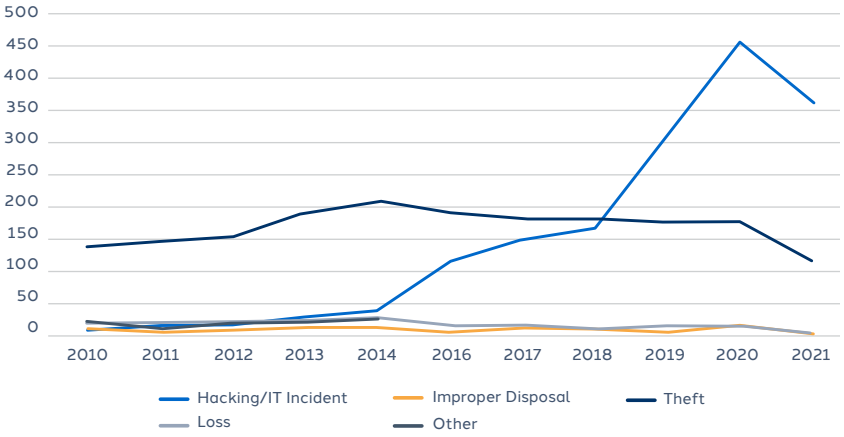


Source: SAI360 Analysis of HHS OCR Data on breaches of 500 records or morerecords that year.

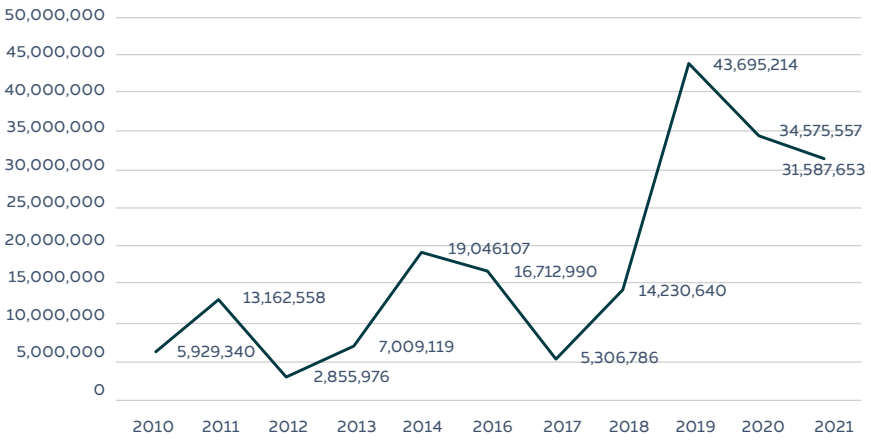
Breach Events 1



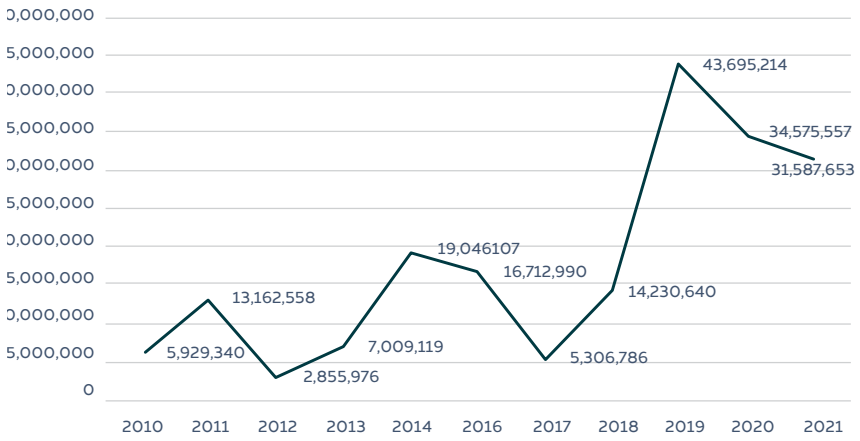
Breach Events 2



Total Individuals Affected



Total Events



A Small Sampling of Those Who Have Recently Been Hit the Worst

In 2022 alone, over 48 million people (more than the entire population of California[5]) across nearly 600 organizations were impacted by healthcare data breaches.[6]

One of 2022's most sizable healthcare data breaches was the OneTouchPoint ransomware attack incident where an unauthorized individual got access to personal patient information such as health assessment details and member identifications across 35+ organizations including Geisinger, Kaiser Permanente, and Humana, just to name a few.[7]

5 https://www.infoplease.com/us/states/state-population-by-rank

6 https://healthitsecurity.com/features/this-years-largest-healthcare-data-breaches

7 https://healthitsecurity.com/features/this-years-largest-healthcare-data-breaches

Top 5 2022 Data Breaches

In 2022, there were 11 reported healthcare data breaches involving over 1 million records and 14 more data breaches involving over 500,000 records. Most of these breaches were tied to hacking circumstances. A common thread here was ransomware or people trying to commit extortion.[8]

At the beginning of February 2023, the U.S. Department of Health and Human Services Office for Civil Rights had 877 cases under investigation that affected nearly 79 million Americans. These investigations were tied to events including hacking and IT incidents, unauthorized access and disclosure, theft, and loss. These breaches involved places with more than 500 users.[9]

Just a few of the most recent breaches from 2023 as of the time of this writing include:

- **February 2023:** Tallahassee Memorial HealthCare in Florida had to shut down its IT system, cancel surgeries, and divert patients following an IT security issue. It also had to work offline following this ransomware attack.[10]
- **February 2023:** Banner Health paid $1.25 million to settle a cybersecurity breach that affected nearly 3 million people.[11]
- **January 2023:** Health insurer Lifetime Healthcare Companies paid $5.1 million to settle a data breach affecting over 9 million people.[12]
- **January 2023:** Hacker activity caused files to be stolen from the Howard Memorial Hospital, potentially compromising over 53,000 patients' information.[13]

Cybercriminals commonly gain entry and access through phishing, social engineering, or backdoor attacks that exploit long-standing vulnerabilities IT departments have not yet patched or mitigated. Oftentimes, this happens because IT departments find themselves stretched too thin with responsibilities. Or perhaps do not yet follow a recognized framework to identify and mitigate these types of risks.

Covered Entity	People Impacted	What Happened
OneTouchPoint, Inc., WI	4,112,892	Ransomware attack
Advocate Aurora Health, WI	3,000,000	Pixel-related impermissible disclosure via websites
Connexin Software, Inc., PA	2,216,365	Hacking incident and data theft
Shields Health Care Group, Inc., MA	2,000,000	Hacking incident and data theft
Professional Finance Company, Inc., CO	1,918,941	Ransomware attack

Source: HIPAA Journal, 2022 Healthcare Data Breach Report [14]

"It is crucial to update cybersecurity and enterprise risk management practices to reduce the probability of a cyber event. As is informing all colleagues, business associates, and other third parties, across levels about the severity and potentially disastrous effects of cyberthreats and the policies they must follow to reduce the risk," Kelvin said. "Ultimately, healthcare leaders must know this: It is not if a data breach will hit your organization; it is when."

3 Key Takeaways

1. Expect your organization will be hit with a breach or attack if it has not already
2. Acknowledge preparation is critical
3. Health information is exponentially more valuable for bad actors than other types of personal data

8 https://www.hipaajournal.com/2022-healthcare-data-breach-report/#:~:text=There%20were%2011%20reported%20healthcare,involved%20ransomware%20or%20attempted%20extortion.

9 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

10 https://www.fiercehealthcare.com/health-tech/tallahassee-hospital-takes-it-systems-offline-postpones-procedures-after-apparent-cyber

11 https://www.hhs.gov/about/news/2023/02/02/hhs-office-for-civil-rights-settles-hipaa-investigation-with-arizona-hospital-system.html

12 https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/excellus/index.html#:~:text=Entities%20%26%20Business%20Associates-,Health%20Insurer%20Pays%20%245.1%20Million%20to%20Settle%20Data%20Breach%20Affecting,affiliates%20Excellus%20Health%20Plan%2C%20Inc.

13 https://www.beckershospitalreview.com/cybersecurity/hacker-steals-files-from-arkansas-health-system.html#:~:text=Nashville%2C%20Ark.,stole%20files%20from%20its%20network.

14 https://www.hipaajournal.com/2022-healthcare-data-breach-report/#:~:text=There%20were%2011%20reported%20healthcare,involved%20ransomware%20or%20attempted%20extortion.

Beyond Data Alone

Ransomware attacks' potential negative public health impacts

Ransomware bad actors have found the healthcare industry to be an ideal target. Typically, they can shut down systems until a ransom is paid. Forty-two percent of health delivery organizations have faced two ransomware attacks within the past couple of years, according to a 2021 survey.[15] At least one in three of these organizations attributed the ransomware attacks to a BA or other third party.

A ransomware attack requires quick thinking for effective mitigation. For example, the 100-bed Jackson Hospital in Florida used physician chatting software—which was maintained via an outside vendor. This became infected in January of 2022 with ransomware. It then stopped connecting to patients' medical records and charting systems. They immediately closed the facility's computer systems to isolate the ransomware so it would not cause further damage.

Still, complications arose.[16] For several hours, Jackson Hospital's physicians had to process notes, prescriptions, and more non-digitally via contingency plans. And physicians facing an offline emergency room charting system had to acquire emergency room patient records from elsewhere in the hospital.

Situations like this are unfortunately becoming more common. They can impact patient care—to the point where not acting quickly enough and in the right way can become a life-or-death situation.

Almost 71 percent of health delivery organizations say a ransomware attack meant that patients had to stay longer than originally anticipated.[17] The same percentage of health delivery organizations also say because of ransomware attacks, patients' medical procedures and tests had to be pushed out to a future date. This caused more people to experience adverse health outcomes because they were unable to get the care they needed when they needed it.

More than one in three health delivery organizations say that they have witnessed more complications from medical procedures post-ransomware attack.[18] One in five even say cyberattacks caused an increase in patient mortality.

In some situations, the intention of attacks is not about financial motivation; but rather about threatening the lives of others and endangering public health.[19]

3 Key Takeaways

1. Healthcare organizations are attractive ransomware targets
2. Ransomware attacks require puttinga game plan together—and urgently
3. The need to protect yourself is key and ransomware can lead to diminished care outcomes and even an increase in deaths

15 https://securityintelligence.com/articles/hospital-ransomware-health-care-data/

16 https://www.cnn.com/2022/01/16/politics/florida-hospital-ransomware/index.html

17 https://securityintelligence.com/articles/hospital-ransomware-health-care-data/

18 https://securityintelligence.com/articles/hospital-ransomware-health-care-data/

19 https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed

A Brief Snapshot of Ongoing Regulatory Shifts

The greater implications of cyber threats are clear: Healthcare organizations and their cybersecurity leaders now more than ever need IT risk management and third-party risk management software, strategies, and technologies to safeguard privacy, security, organizational resilience, and financial viability.

There are 4 critical areas where control is urgently needed:

- Internet of Things (IoT) and the way that hospital systems are connected online
- Medical devices and medical monitoring devices
- Building fundamentals like HVAC, heating, cooling, and water management
- Multiple billing and other databases

Said Kelvin, "Addressing a wide range of organizational needs, from safeguarding IT assets to monitoring building operating, protecting data storage, and more must remain a key executive imperative. When it comes to cyber risks and data privacy, healthcare and life sciences CIOs face formidable and complex regulatory uncertainty, and opportunities through their leadership and technology initiatives.[20]

At an organizational level, the solution is to leverage technology to monitor the current industry and broader IT risk landscape to predict and prepare for changes and upheavals in real time. It lies in driving ongoing organizational resilience via solid data protection measures, BA risk management, and increased transparency about risk management needs and capabilities.

In the meantime, there is increasing pressure sparked by regulatory pushes and a shifting regulatory landscape to improve health IT processes across the board and increase patients' privacy rights. For instance, in 2022, notable progress was made toward potentially passing the American Data Protection Act.[21]

Additionally, nine U.S. states in 2023 have already introduced privacy bills. These new regulations are, of course, incremental to the existing federal standards such as the Health Insurance Portability and Accountability Act (HIPAA), passed in 1996 to improve patient data access and protection. HIPAA, amended in 2009 with the HITECH Act, which was then amended again in 2021, encourages electronic health record (EHR) usage and implements strong repercussions for compliance failure.[22]

In 2021, the HITECH amendment meant HIPAA-covered entities were required to choose Recognized Security Practices (RSP) according to what best fits their business needs. Covered entities are compelled to ensure their cybersecurity defenses are both effective and efficient by following U.S. Department of Health and Human Services/Office of Inspector General (HHS/OIG) guidance on best practices.

In 2022, the Department of Health and Human Services' Office for Civil Rights (OCR) imposed more financial penalties23 for those who violated HIPAA than in any other year. As a result, there have been 22 investigations that led to settlements or civil monetary penalties, with most financial penalties in 2022 below $100,000.[23]

3 Key Takeaways

1. Regulatory requirements will continue to increase
2. Streamlining and automating processes, reporting metrics, and more is critical
3. Holistic, real-time, and proactive organizational vantage points are necessary

20 Gartner - Healthcare and Life Sciences Business Driver: Uncertainty and Ecosystem Risk, Published 20 January 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

21 https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2023/

22 https://www.sai360.com/resources/grc/healthcare-grc/hitech-act-comes-with-obligations-a-carrot-and-a-stick-blog

23 https://www.hipaajournal.com/2022-healthcare-data-breach-report/#:~:text=There%20were%2011%20reported%20healthcare,involved%20ransomware%20or%20attempted%20extortion

Strong It Risk And Third-Party Risk Management Programs Are Of Critical Importance

Solid organizational protection now involves a multi-faceted approach. It is critical to identify and understand risks and the likelihood they may affect your organization, how you can prepare today for tomorrow's unknown, and how you can work to protect your data, reputation, patients, and operations. A best practice framework will include a wide array of controls including backup and restoration controls, endpoint protection, vulnerability patching across all systems, incident management processes, and user access rights access. [24]

Healthcare organizations are seeking new ways to implement holistic approaches to protect sensitive data, safeguard operations, have a strong incident response plan underway, and know what to do next if an attack hits. For example, to stay up-to-speed while managing health IT risks, organizations are enhancing IT policy training to include employee courses on phishing attempt, and social engineering.[25]

The good news is, thanks to standards and frameworks, organizations can better address IT security and create blueprints and game plans.[26] Many CIOs' strategic planning approaches implicitly assume current business and technology trends will continue, and do not include processes to adapt and change in response to changing market signals within a planning cycle.[27] Oftentimes, this comes down to a lack of awareness, urgency, or understanding of why best practices and technological solutions need to be implemented. Much work remains to be done to get and stay ahead of the curve.

Healthcare organizations need a program that puts recognized frameworks into play in a measurable, reportable, and auditable manner. And in a way that allows them to assess where gaps exist, and implement new controls to mitigate.

As organizations look to develop agile responses to the evolving risk landscape, those that will be successful in the future will rely heavily on third-party technologies, data, and offerings28 to meet or exceed their business objectives. Doing so helps risk professionals make sense of emerging risk trends before—not after—they become mainstream. And it helps ensure your programs are not outdated, decreasing the chance of organizational disaster.

Interestingly, according to Forrester's 2022 research data, although most Enterprise Risk Management (ERM) decision-makers—69 percent—say improving their ability to name and address risks from the third-party ecosystem is a top-of-mind risk management priority, only 20 percent identify third-party risk.[28]

Effective and efficient IT risk and third-party risk management demands an integrated technology solution and not simply another spreadsheet or siloed technology offering. According to Forrester's Research Inc., the majority of organizations—75 percent—say their third-party risk program is manual.[28]

3 Key Takeaways

1. Volatility and ongoing transformation demand new capabilities and vantage points
2. Third-party capabilities improve business operations
3. Technology bundles drive efficiency

24 https://www.sai360.com/resources/grc/whitepaper-seize-control-of-your-cybersecurity

25 https://www.sai360.com/resources/grc/healthcare-grc/hitech-act-comes-with-obligations-a-carrot-and-a-stick-blog

26 https://www.sai360.com/resources/grc/whitepaper-seize-control-of-your-cybersecurity

27 Gartner - Healthcare and Life Sciences Business Driver: Uncertainty and Ecosystem Risk, Published 20 January 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

28 Forrester report, The State of Third-Party Risk Management 2022

Knowing What You Don't Know: Why Awareness Is Critical

Keeping up to date on security awareness is far from a one-and-done process. Ongoing training revisions are necessary. After all, a reported 19 percent of data breaches are caused by human error, with an additional 15 percent connected to no-longer-supported legacy software.

Here are just a few ways to know what you do not know more clearly[29]:

- Use threat intelligence data services
- Implement technical controls, such as email filters that block embedded links
- Understand how threats are rebranded and repackaged over time
- Implement a strong program with controls and policies based on a recognized framework

Addressing Compliance Issues Head-On Demands An Informed, Engaged, and Calculated Approach

It is important to emphasize that information privacy and security concerns still are a top risk area.

In short, if you know what your biggest risks are up front, it becomes easier to focus on an action plan and prepare your organization accordingly.

Stolen or compromised data and massive operational disruption aside, enforcement agencies are an additional risk. According to 70 percent[30] of our survey participants, this is something most healthcare organizations say they have already had to do, said our Healthcare Compliance Benchmark Survey Report.[30] Both the OIG and the Department of Justice (DOJ) say having an effective compliance program can serve as a mitigating component when analyzing culpability that might decrease or worsen penalties and/or settlement terms.[29]

What do organizations' risk assessment results tend to look like now? Three-quarters of our survey respondents say their organization addresses risk assessment results by incorporating identified risk issues in annual compliance internal audit work plan, updating policies and procedures to improve internal controls, and changing and enhancing compliance training on identified risk issues. Given the regulatory burden of HIPAA and other PHI laws, it is not difficult to see how a robust IT risk and third-party risk management program is essential to this.

29 https://securityintelligence.com/articles/hospital-ransomware-health-care-data/

How SAI360 Supports Health IT Risk Management

This is where SAI360 comes into play. As CCOs, CISOs, and Boards continue making sense of evolving regulations, new and creative methods used by cybercriminals to steal valuable information from unsuspecting parties, and other vulnerabilities, SAI360 helps organizations stay ahead of the curve.

At SAI360, we supply IT risk mitigation and management, like an in-depth cybersecurity protection layer. We work to ensure organizations are resilient, can support business integrity, and keep their operations running as intended in case of unauthorized access, user disclosure of data, server disruptions, ransomware attacks, and data loss.

The SAI360 IT Risk Management module equips organizations with a best-practice IT security program including multiple frameworks such as NIST CSF, NIST 800-53, ISO27001, and more, along with pre-defined assessment templates and robust reporting. Users can track steps from assessments to completion and monitor risk scores to decide future action.

With SAI360's fully integrated risk and compliance platform, an IT security program goes beyond finding risks and managing controls tied to assets. It also equips users to centralize a library of policies with automated record-keeping of authors, reviewers, and revisions. All information is organized in one single place. For those currently trying to manage IT risk in spreadsheets, switching to the platform can be a game changer.

Beyond IT risk management, SAI360 has modules needed to support a full patient of the elements needed for a full patient data privacy and security program, including the ability to streamline policy management, regulatory change management, and incident management. We help keep employees educated on how they can prevent breaches and attacks by sharing best practices for success. And we offer interactive procedural checklists, target measurements, and other capabilities that can be unrolled anytime and anywhere.

To help prevent a breach, and provide the best path forward if you do, SAI360 has the solutions to manage, measure, quantify, and report appropriately. We also help organizations understand how new and emerging risks are likely to shape business models and demand future technology investments.

Key reasons SAI360 should be at the top of your list to partner with include:

1. Highly referenceable healthcare customer base, with two in three SAI360 customers providing essential (key) services across healthcare, pharmaceuticals, and beyond
2. Market- and analyst-recognized leading risk management platform
3. Easy to buy, easy to own all SaaS subscription model
4. Interoperability of all modules delivered on the same common architecture
5. User-configurable advanced workflow and forms configuration engine
6. Support services like project initiation and setup and post-implementation support

FINAL THOUGHTS

It all comes down to improving prevention, transparency, automation, real-time communication, risk analysis, and staying out of negative media headlines.

Take action to protect your organization and strengthen your IT risk and cybersecurity posture. Understand and implement best practices now to adopt enterprise-wide risk analysis. Your organization, those you work with, and those you serve all depend on you taking the right steps before it is too late.

Interested in learning more about SAI360's Data Security solutions?

Request a demo.

Our unified approach to risk sets us apart

Today's complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform and Learning solution that spans the entire risk spectrum.

Risk Management Solutions

- Enterprise & Operational Risk Management
- Regulatory Change Management
- Policy Management
- Third-Party Risk Management
- Internal Control
- Internal Audit
- Incident Management
- Conflicts of Interest (COI) Disclosure Management
- IT & Cybersecurity
- Business Continuity Management

Ethics & Compliance Learning Solutions

- Anti-Bribery & Anti-Corruption
- Competition & Anti-Trust
- Conflicts of Interest
- Data Protection & Privacy
- Information Security
- Exports, Imports & Trade Compliance
- Harassment & Discrimination

SAI360 RISK FROM EVERY ANGLE

SAI360 is giving companies a new perspective on risk management. By integrating Governance, Risk, Compliance (GRC) software and Ethics & Compliance Learning resources, SAI360 can broaden your risk horizon and increase your ability to identify, manage, and mitigate risk. See risk from every angle.
Visit www.sai360.com.

149950 0224