DATA BREACHES: MAJOR CHALLENGES FOR HEALTHCARE EXECUTIVES

A Pandora's Box of New Challenges for Business Executives and Board Members is Starting to Open

CELERIUM.com

INTRODUCTION

As challenging as data breaches are today, they are poised to become even more problematic shortly, and we are not just talking about the threats posed by AI. According to an April 2024 survey, data breaches are the top concern of CISOs (Chief Information Security Officers). However, healthcare business executives, audit committees, and boards of directors will face increased challenges and responsibilities regarding data breach defense. In the future, they may not be able to delegate or abdicate to IT the responsibility of key policies and plans regarding data breach defense.

CONTENTS

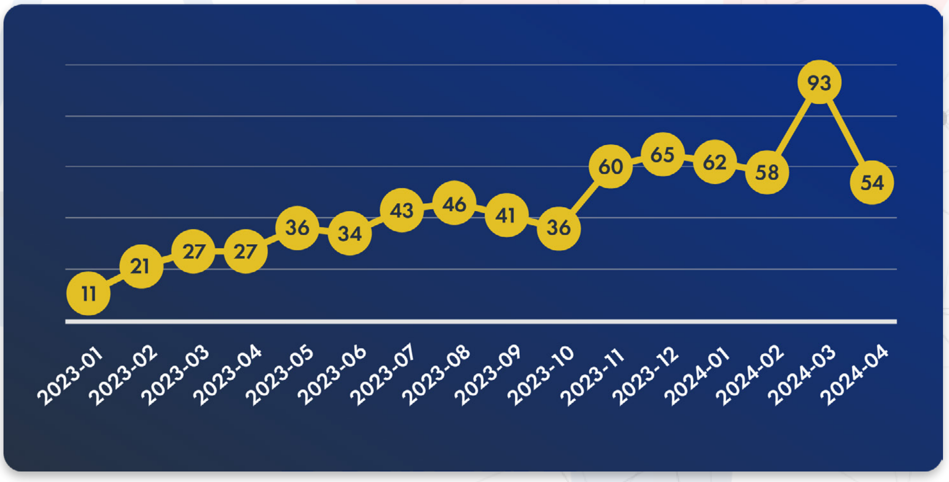
THE REGULATORY LANDSCAPE

Regulatory bodies such as HHS, SEC, FTC, FCC, DHS (CIRAC Critical Infrastructure), and recently, the FHA have increased pressure on executives and board members. Currently, much of this pressure revolves around the timing and speed of data breach disclosures, but this focus is beginning to shift. In the healthcare sector, the challenges are particularly acute and growing.

The FTC, FCC, and FHA have mandated that organizations disclose certain types of data breaches to federal agencies and customers within a few days to a month, depending on the agency. Initially, the SEC focused on protecting investors and shareholders in publicly listed companies, but now Regulation S-P also prioritizes consumer protection against the theft of PII (Personally Identifiable Information) in 30,000 "covered" financial organizations. The stakes in healthcare are higher, as patient records (PHI) can be sold for between $250 to $1,000 per record. HHS and the AHA (American Hospital Association) have taken a leadership role in combating data breaches, but the problems are intensifying.

In addition, many states have various data breach disclosure rules. California, in particular, has very large fines of up to $2,500 per negligently released record.1

Congress mandated that HHS create a public record of data breach activity, which HHS implemented via a website in 2022. Sometimes known as the "wall of shame," this site shows the alarming rate of data breaches – averaging 60 breaches per month or two per day for the first five months of 2024. Data breaches at Change Health Care and Ascension Hospital Network compound the problem, as Ascension has about 140 hospitals. Although it's unclear now if Ascension did experience a full data breach, CBS News reported it as a data breach, and a patient of Ascension Saint Thomas filed a class action lawsuit over the data breach.



Source: HHS OCR
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

THE 2024 CHALLENGES CONFRONTING HEALTH CARE

Healthcare executives, in particular, face numerous challenges related to data breach vulnerabilities, including:

- **Legacy and Networked Systems:** Hospitals often have outdated systems and complex networks of medical devices.
- **Patient Data Privacy and Safety:** Ensuring both privacy and safety of patient data is a dual challenge.
- **Regulatory Complexity:** Federal programs like the Affordable Health Care Act add layers of IT complexity, particularly in payment processing and EHR interoperability.
- **Integration and Data Sharing:** The push for increased integration and data sharing across the healthcare ecosystem introduces additional risks.
- **Cybersecurity Staffing:** Many healthcare organizations lack the cybersecurity expertise to deal with the ever-increasing cyber and data breach threats.

THE CHALLENGES OF DATA BREACH DETECTION

On the surface, data breach detection is simply an issue for IT security staff. HHS (like the FTC) wants the healthcare industry to disclose to HHS within 30 days the theft of 500 or more PHI records (as documented on the HHS website). Of course, HHS is only one regulatory agency. Some organizations in the healthcare industry may also need to report activity to the FTC, SEC (for shareholders), and DHS (CIRCIA) since parts of the healthcare ecosystem are considered to be critical infrastructure. Here are some of the data breach detection issues that warrant attention from business executives and boards:

- **Regulatory Fines:** Fines can affect the bottom line.
- **Class Action Lawsuits:** These are becoming increasingly common and costly. Recently, T-Mobile had to **pay** $350 million in response to a class action lawsuit. The healthcare industry will face similar lawsuits as Ascension now faces a class action suit.
- **Higher Premiums:** Cybersecurity insurance policies may see higher premiums after a data breach.
- **Reputational Impact:** How could your company have prevented the breach, reported it sooner, or reduced the number of patients impacted?

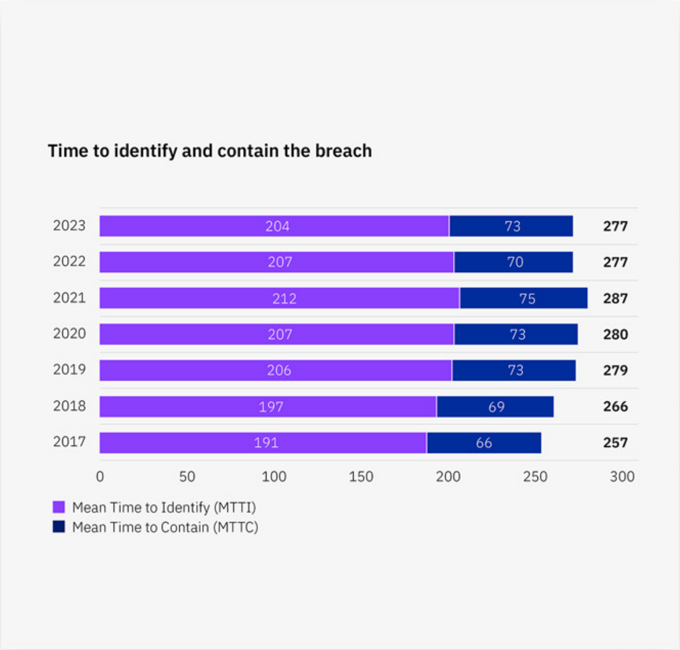
On the surface, there are indeed benefits to faster data breach detection:

- Early detection potentially catches and stops activity before more than 500 PHI records are stolen, thus avoiding the HHS disclosure requirement.
- Fewer patients impacted could mean smaller or fewer class action lawsuits and possibly smaller increases in cyber insurance policy premiums.

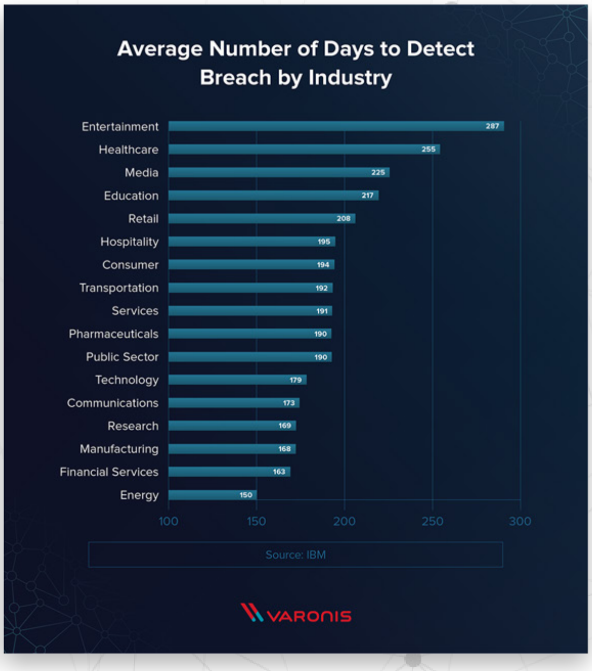
EXECUTIVE CHALLENGES IN EARLY DATA BREACH DETECTION

The often-cited IBM data breach report indicates that the average data breach detection time, regardless of industry, over the last seven years has been about 200 days or seven months.

In the healthcare industry specifically, Varonis found that the average data breach detection time is much worse. Their research indicates **the average data breach detection time in the healthcare sector is 255 days (more than 8 months!).** Of course, some breaches may take even longer to detect. For example, Samsung recently announced that it had suffered a data breach that began one year before its announcement.



Source: IBM



Source: Varonis

DHS reported that the recently discovered cyber reconnaissance (a precursor to possible data breaches) in critical infrastructure by the Chinese “Volt Typhoon” has been ongoing for five years. But what about the power of AI? IBM claims that for companies trying to harness the power of AI and EDR, data breach detection could be slashed from 200 days to 150 days (five months), which is still a long time. With hospitals having difficulty funding and finding cybersecurity expertise, the challenge of data breach detection is very problematic.

- **Technical Ambiguity:** It can be quite difficult to detect and verify that a data breach has even taken place. Focusing on early detection can lead to many “false positives.” Do business executives want to be notified about “possible data breach activity” or only when a breach is been confirmed? What if this confirmation process takes days or weeks?

- **Missing Detections:** Lack of robust detection can lead to “false negatives” which can be disastrous. Many threat actors constantly change their techniques to avoid detection through obfuscation and other measures.

- **Business Impact of Data Breaches:** This is one of the biggest challenges. Regulatory organizations typically mandate reporting only if the breach has resulted in a significant loss of PHI or PII data (often 500 records) or if it is “material” (SEC), whether because of its impact on the business or because of “qualitative” factors. These impact determinations can be very complex for IT and business operations teams to assess. For example, just last month, the SEC’s Division of Corporation Finance Director admonished all publicly held companies to “assess all relevant factors” when determining the materiality of an incident. He quoted from the SEC’s earlier cybersecurity incident Adopting Release that companies should consider whether the incident will adversely affect the company’s “reputation, customer or vendor relationships, or competitiveness.” Additional factors to consider are the “possibility of litigation or regulatory investigations or actions, including regulatory actions by state and Federal Governmental authorities and non-U.S. authorities.”

- **Corporate Focus on Speed of Data Breach Disclosure:** We are seeing early data breach disclosure submissions. In the case of the SEC disclosure system set up in December of 2023, publicly listed companies could not always quickly complete the determination of the “materiality” of a cybersecurity incident. As a result, there have been many “prophylactic” filings where companies say, “We’ve had some possible data breach activity; we don’t really know if it is material or not, but we wanted to give the SEC and shareholders a ‘heads-up.’” The SEC is not at all happy with these arguably premature disclosures, but that is the state of the industry that business executives and boards need to deal with. This explains why last month, the SEC’s Division of Corporation Finance Director decided to issue a statement cautioning companies to differentiate in their SEC filings between a cybersecurity incident determined to be “material” versus a voluntary “prophylactic” filing in situations where the materiality determination had not yet been made.

THE GROWING EXECUTIVE CHALLENGES OF DATA BREACH RESPONSE

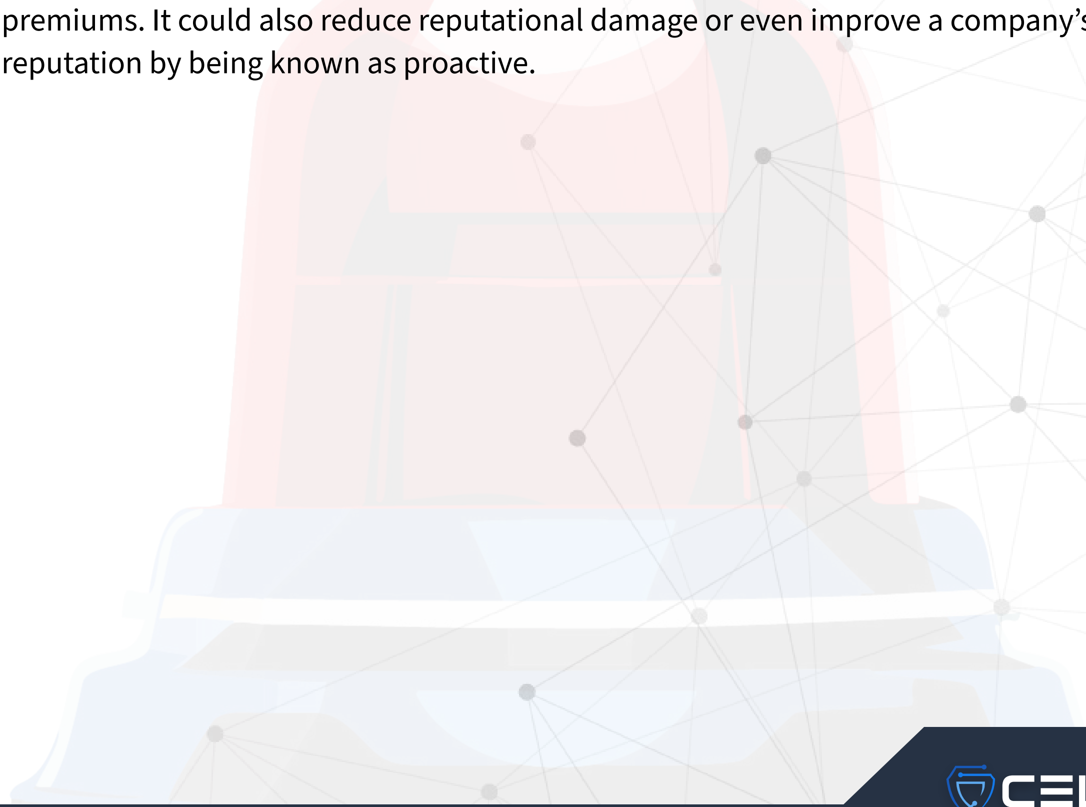
Beyond the issues outlined above related to data breach detection and disclosures are even more complex executive decisions about how to respond:

- **Pay or Not Pay Ransom:** This has been one of the common executive decisions covered by many reports.

- **When to Invoke Response:** As noted above, even the technical confirmation of a data breach can be ambiguous. Executive policies of when to bring in outside resources to better understand real breaches and possible responses (via IR firms) need to be carefully formulated.

- **Future Regulatory Requirements Regarding Response:** Today, most regulatory attention focuses on mandates for reporting and suggestions for cyber improvement (checklist guidelines compliance). Some regulators are now putting "mandate pressure" around response. The SEC has announced that over the next 18-24 months, 30,000 covered financial organizations will be mandated to create data breach response policies covering detection, response, and recovery. These response mandates will likely flow into other industries, including healthcare.

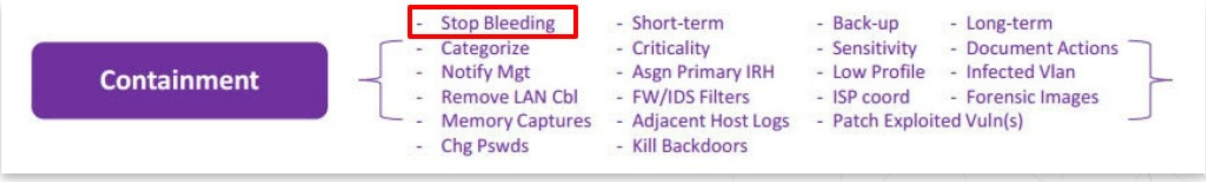
- **Early Response:** Although early detection (along with confirmation and analysis) of data breaches is widely recognized as important today, an effective early response can be even more important for the organization. Early response might reduce or avoid financial impacts from regulatory fines, class action lawsuits, and increased insurance premiums. It could also reduce reputational damage or even improve a company's reputation by being known as proactive.



A PRIMER ON EARLY RESPONSE AND CONTAINMENT

- What does data breach response really mean in the context of the larger "incident response"? Incident response covers a broad set of activities, including working with law enforcement and insurance companies, deciding whether to notify regulatory agencies, and performing forensic work to determine how the breach occurred to prevent future incidents.

At the front end of the IR lifecycle is an early step called containment. Some organizations in the IT security industry (NIST, SANS Institute) argue that containment can include a spectrum of initial and later-stage activities (e.g., patch management, forensic analysis, MFA). Here, we focus on "tactical containment," which involves:



Containment

- Stop Bleeding
- Categorize
- Notify Mgt
- Remove LAN Cbl
- Memory Captures
- Chg Pswds

- Short-term
- Criticality
- Asgn Primary IRH
- FW/IDS Filters
- Adjacent Host Logs
- Kill Backdoors

- Back-up
- Sensitivity
- Low Profile
- ISP coord
- Patch Exploited Vuln(s)

- Long-term
- Document Actions
- Infected Vlan
- Forensic Images

Source: SANS 504-B Incident Response Cycle: Cheat-Sheet

- **Stopping the Bleeding:** Blocking the active loss or theft of data from breached systems.
- **Stopping the Spread:** Preventing the spread of the breach to systems that have not yet been breached.
- **Notification to Management: I**nforming appropriate IT and business staff about these issues. This is not necessarily about notifications to regulators, customers, or patients.

PANDORA'S BOX STARTING TO OPEN FOR HEALTH CARE EXECUTIVES AND BOARDS

Most industry focus on risks has been prioritized by regulators, who appropriately emphasize faster notification to customers, patients, and shareholders so they can take timely action. However, the industry and regulators are now starting to focus on the broader impacts beyond the breach disclosure—specifically, the response side of the problem.

The situation related to Change Health Care underscores this shift. The Change Health Care incident involved data breaches, customer or patient data loss, and extortion fees of $22 million paid to an initial threat actor. More critically, it highlights the disruption caused in the entire healthcare ecosystem—not by the theft of PHI data but by delays to payments, surgery schedules, and patient care. Recent congressional hearings have primarily focused on the disruption element rather than the privacy element.

This distinction between protecting privacy (e.g., PHI records) and protecting patient safety and care has not been sufficiently articulated by the media or in congressional hearings. Often, service disruptions are not directly caused by threat actors but by the organization's action to isolate affected systems, leading to significant operational disruptions.

1. A common and understandable interpretation is that cyber attacks such as data breaches cause disruption to service in the healthcare industry. But this is not necessarily the case at all.
2. Often, when companies respond to a data breach, they implement a type of isolation-based containment which can result in the disconnection of IT systems. More refined approaches to isolation and other types of containment can be used. Still, in the current environment with pressure regarding possible regulatory fines or class action lawsuits, companies can feel the urgency to stop the bleeding at all costs.
3. Unfortunately, if systems are disconnected via isolation, they are no longer usable, thus disrupting the organization, its customers, patients, partners, and perhaps the broader healthcare ecosystem.
4. **BOTTOM LINE:** The disruption to patients, partners, and others is not always caused by threat actors (it can be if data is encrypted by threat actors). Often, the disruption is caused by the organization itself deciding to take systems offline to stop the bleeding and perform forensic analysis. These decisions are frequently business or executive decisions and not simply IT (CISO) decisions.

5. Decisions about disconnecting (isolating) or not, given the possible, if not likely, business disruption, are not necessarily new but they are becoming more and more complex – especially for business executives, given the financial pressure of regulatory fines or massive class action lawsuits.

6. We are entering a time when the response or disruption side will become more prominent because of industry impacts related to incidents at Change Health Care, Ascension Hospital, and more. There could be class action lawsuits or perhaps regulatory fines related to the response decisions made by healthcare executives.

7. Is this notion of company-created disruption true? An interesting example, as many of us know, is how an attack against the critical infrastructure company Colonial Pipeline shut down the gas supply on the East Coast for weeks. According to some industry reports, the threat actors attacked the company's administrative or IT systems related to accounting and other business operations – they did not directly attack the pipeline operations systems (the OT, ISC, and SCADA systems). It was reported that Colonial Pipeline decided to shut down its pipeline systems out of an abundance of caution. Perhaps the pipeline shutdown was the right approach – but the key issue is that it must have been an executive decision.

LEGAL PERIL FOR BUSINESS EXECUTIVES AND BOARDS: THE CHOICE OF EVILS

The legal dilemma for boards and executives involves defining policies and actions to address:

- **Privacy-Oriented Data Breaches:** With associated fines and lawsuits.
- **Disruption-Oriented Business Costs:** Impact on patients, partners, and potential lawsuits caused by operational disruption decisions.

A CALL TO ACTION FOR HEALTH CARE EXECUTIVES AND BOARDS

The Pandora's box of data breaches and resulting disruption is opening wider each day. Healthcare executives and board members need to address the creation of policies or plans that deal with the difficult "Choice of Evils" between protecting privacy (HIPAA) versus protecting business continuity that avoids disruption to companies, patients, partners, and the healthcare industry. The challenges here are formidable, but they can be effectively managed and mitigated with proactive leadership and strategic planning.

- **Review or Implement New IT Security Policies:** These policies should specifically address the conflict between privacy (avoiding regulatory fines and class action lawsuits) and disruption to a company, patients, partners, and the industry, which sometimes can be caused by isolation-based containment.

- **Advocate for Safe-Harbor Provisions:** Regulators and Congress should formally review this difficult issue and consider creating safe-harbor provisions.

CONCLUSION: A CALL TO ACTION

For healthcare executives and board members, the time to take meaningful action to address escalating data breach frequency and severity is now. By prioritizing data breach management and response at the highest levels of leadership, organizations will be better able to protect their patients, reputation, IT systems, and bottom line.

ABOUT CELERIUM

Celerium® powers active cyber defense solutions to help protect organizations and communities from increasing cyberattacks. With a rich 16-year history of facilitating cyber threat sharing for critical industry sectors and government agencies, Celerium is an established leader in providing innovative cybersecurity solutions, with solution directions based on the evolving needs of the industry.

Learn more at www.Celerium.com and follow us on X at @CeleriumDefense

CELERIUM.com

ENDNOTES

[1] For example, California has both a general statute governing the protection of consumer data, the Consumer Privacy Rights Act, Civil Code sections 1798.100 et seq. (the “CPRA”), as well as a specific Confidentiality of Medical Information Act, Civil Code sections 56 et seq. (the “CMIA”). The CMIA provides for more serious penalties that supersede those obtainable under the CPRA. With respect to covered medical information, the CMIA provides, “Any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to” statutory damages of up to $1,000 per negligently released record and administrative penalties of up to $2,500 per negligently released record. See Cal. Civ. Code §§ 56.101(a), 56.36(b), (c).