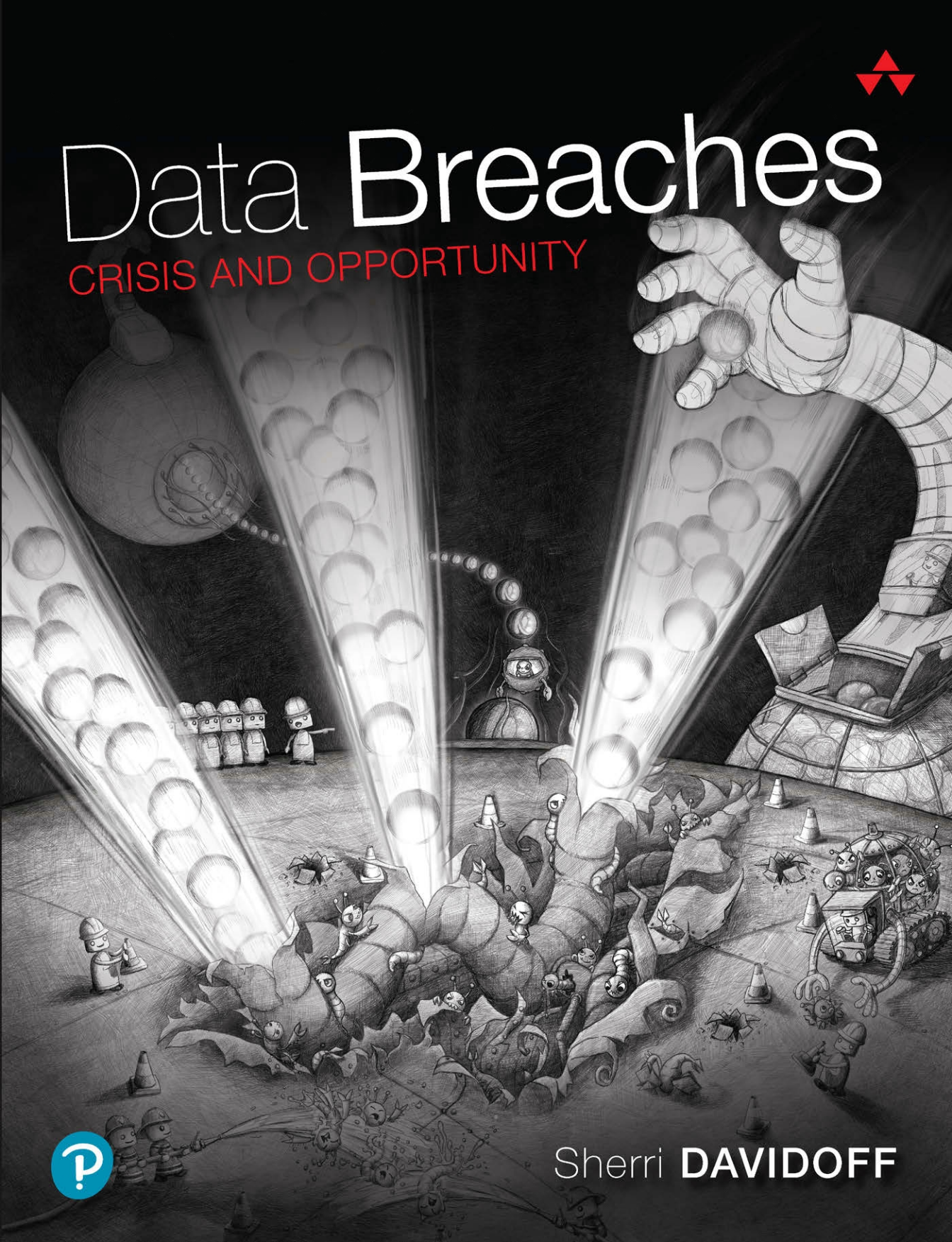
Data Breaches

CRISIS AND OPPORTUNITY



Sherri **DAVIDOFF**

Data Breaches

involved actually cared quite deeply about what occurred, and put a lot of time, effort and resources into it."

ChoicePoint was acquired in 2008 for $4.1 billion by Reed Elsevier, the parent company of LexisNexis.

4.7.3 Changing the World

Security expert Bruce Schneier pointed out that the economics did not incent data brokers to protect consumer data. "The hundreds of millions of people in ChoicePoint's databases are not ChoicePoint's customers. They have no power to switch credit agencies. They have no economic pressure that they can bring to bear on the problem. . . . ChoicePoint doesn't bear the costs of identity theft, so ChoicePoint doesn't take those costs into account when figuring out how much money to spend on data security. In economic terms, it's an 'externality.'"[103]

The ChoicePoint case illustrated to the U.S. public and legislators that:

- Absent laws, information brokers did not effectively protect consumer information from exposure.
- Information brokers would not notify consumers of a data breach out of the goodness of their hearts, but instead required clear legal and/or financial incentives.
- Breach notification legislation *worked*, at least in some cases.

"Responsible handling of such records is every bit as important a public safety issue as is the proper disposal of hazardous waste," wrote Atlanta pundit Scott Henry in the aftermath of the ChoicePoint breach. "If it turns out that ChoicePoint's gross negligence doesn't violate current law, the laws are clearly inadequate. It's encouraging that legislators in Georgia and around the country are already drafting laws that would help prevent—or at least provide reasonable notification of—a similar security breach."[104]

As a result of the ChoicePoint breach, laws across the United States were enacted to hold organizations accountable for notifying consumers of a breach, therefore also indirectly providing incentive to reduce breaches. By June 2005, 35 states had introduced data breach notification laws, and at least 22 states had enacted laws by October of that same year.[105]

The World Privacy Forum later called ChoicePoint "the *Exxon Valdez* of privacy." While many breaches have been compared to *Exxon Valdez* crisis, the ChoicePoint case is perhaps its closest equivalent. Like the *Exxon Valdez* spill, ChoicePoint wasn't the first disaster of its type or the biggest (not even close). It was, however, the most visible to the American public and resulted in the creation of new laws and greater oversight. The ChoicePoint breach helped the public understand that organizations require clear incentives in order to act in the best interest of the public.

---

103. Schneier, "ChoicePoint."

104. Scott Henry, "ChoicePoint," *Creative Loafing*, February 23, 2005, http://www.creativeloafing.com/news/article/13017248/choicepoint.

105. Milton C. Sutton, *Security Breach Notifications: State Laws, Federal Proposals, and Recommendations* (Moritz College of Law, Ohio State University, 2012), 935, http://moritzlaw.osu.edu/students/groups/is/files/2012/02/s-sutton.pdf.

In other words, the ChoicePoint breach didn't just change ChoicePoint. It changed the data brokerage industry and the world.

Adapt

"A data breach can't be undone," says Karen Sprenger, an 18-year veteran of the digital forensics industry. The best you can do is learn from it. "Adapt" is the final phase of our DRAMA breach response model.

Your organization will almost certainly change as a natural process following the breach. You can also put your organization in a better position by *consciously* adapting in proactive ways, such as:

- Implement more effective security procedures, including both technical and policy changes.
- Improve logging and monitoring infrastructure.
- Obtain comprehensive data breach insurance.
- Build better crisis management and crisis communications plans.

By adapting proactively and wisely, you can maintain the value of your organization and reduce the risk of future breaches. When your organization emerges, it can be "well and whole"—but it will be different.

4.8 Before a Breach

Now that we've analyzed a data breach crisis from beginning to end, inside and out, let's go back to the beginning. What could ChoicePoint have done to handle its breach more effectively?

Data breaches represent crises, which by their nature are often fast moving and unpredictable. "You need to be ready in advance and take time to prepare with a multidisciplinary team," said Chris Cwalina. For ChoicePoint, a major failing was simply that it had not developed any crisis management plans for recognizing or responding to a potential data breach. As a result, it stumbled over and over—particularly in the prodromal and acute phases, which require a quick response.

"The lack of a plan or the infrastructure to handle a data breach created problems in disseminating information and handling public relations," observed researchers from North Carolina State University who analyzed the ChoicePoint breach.[106]

But where does planning start? The fundamental problem at ChoicePoint—and indeed, in many organizations—is that no one had been tasked with oversight for data breach crisis planning in the first place.

106. Otto, Antón, and Baumer, "ChoicePoint Dilemma."

4.8.1 Cybersecurity Starts at the Top

The data breach crisis planning process is most effective when it is driven from the executive level, and managed by a risk officer or chief information security officer (CISO), outside of IT. Ideally, it should be integrated with an enterprise crisis management effort.

It turned out that ChoicePoint had never assigned responsibility for managing information holistically, throughout the enterprise. As a result, ChoicePoint's team was not only forced to create response procedures on the fly; they even created whole positions that, in retrospect, should already have existed. For example, the notification letter that ChoicePoint sent to consumers was signed "J. Michael de Janes, Chief Privacy Officer."

CSO magazine pointed out that de Janes was "actually the general counsel for ChoicePoint. His description of responsibilities on the ChoicePoint website does not include privacy. It seems that ChoicePoint just needed a privacy officer, and fast."[107]

The company *did* have a very accomplished CISO at the helm: Rich Baich, who had been named "Information Security Executive of the Year in Georgia" during 2004, "in recognition of his accomplishments in the realm of information security."[108] He was a Certified Information Systems Security and Privacy Professional (CISSP) and also a Certified Information Security Manager. His book, *Winning as a CISO*, (ironically) was published in June 2005, while the ChoicePoint crisis still burned.

When the ChoicePoint data breach erupted, Baich was publicly roasted and called a "fraud and discredit to the position of the CISO." He responded by pointing out that the breach was not a "hack," arguing that issues with customer vetting processes were not his responsibility.

"Look, I'm the chief information security officer. Fraud doesn't relate to me."[109]

And indeed, it didn't. Despite the fancy title ("Chief,") ChoicePoint's CISO was siloed inside the IT department, which was fully separate from the unit of business that handled customer vetting and access policies. Although on paper ChoicePoint had someone who might appear to be "in charge" of information security, in reality, due to Baich's placement within the organization, it was not possible for him to manage information security or coordinate a breach response across all business units, as was truly necessary.

Cybersecurity incident response teams have traditionally been built and led from within the IT department. This might have made sense when most cybersecurity incidents were handled by IT staff, without major risk to the organization as a whole. Viruses, spam, inappropriate use, equipment loss—all of these cases were once handled within IT, with little planning or involvement from other departments.

Over the years, as data breaches have become more of a concern, organizations have started to realize that planning for data breaches must be a coordinated effort involving stakeholders from across the organization. While your IT department may be perfectly capable of managing the *technical* aspects of a data breach, it is rarely the case that an IT manager is in a position to effectively plan for or manage an enterprise-wide crisis response strategy, which typically

---

107. Scalet, "Five Most Shocking Things," 29.

108. "ChoicePoint CISO Named Information Security Executive of the Year in Georgia 2004," *Business Wire News*, March 19, 2004, https://www.businesswire.com/news/home/20040319005030/en/ChoicePoint-CISO-Named-Information-Security-Executive-Year.

109. Scalet, "Five Most Shocking Things."

involves a diverse team such as representatives from legal, public relations, human resources, risk management, executive management, and other departments. Furthermore, since data breaches often expose flaws within IT (including process deficiencies, resource allocation issues, and more), it is often most effective to have data breach planning managed by a team outside the IT department, thereby reducing the potential for conflict of interest.

"Information Security should [not] necessarily be under IT," said Chris Cwalina. "Incident response is in essence a risk management function. And an incident response team should have appropriate support and visibility in the organization or it will be difficult to make progress. Also, it is so important for legal to be part of the incident response function and investigative process. Security analysts and lawyers need to spend a lot of time together and learn to speak one another's language. This is critical."

"[T]he CISO can't just work in the tech space," said Michael Assante, chief security officer (CSO) of American Electric Power. "They have to start looking at business processes."[110]

"[T]he extent to which fingers are pointed at [Baich] speaks volumes about how broadly CISOs have come to be regarded as protectors of information, no matter the threat," wrote *CSO* magazine. "[W]hat happened reflected a wholesale failure of ChoicePoint's approach to security governance."[111] ChoicePoint had never fully evaluated or addressed the risks of a data breach at a holistic, enterprise level. This gap stemmed directly from the fact that ChoicePoint had never assigned responsibility for doing so *to a person who had an appropriate breadth of access within the organization*. Despite *CSO* magazine's damning assessment of ChoicePoint's information security program, this failure is repeated over and over in organizations everywhere, even to this very day.

In order to successfully manage cybersecurity, and its sister, data breach response, an executive-level person needs to be engaged, with oversight by the board of directors or other top stakeholders. All too often, we give a person responsibility for "information security," but it cannot truly be meaningful unless that person is placed high enough in the organization to actually oversee information management *across the whole enterprise*.

Within a month of ChoicePoint's breach notification, the company announced that it had hired Carol DiBattiste, former deputy administrator of the U.S. Transportation Security Administration, to take on the new role of "chief credentialing, compliance and privacy officer" for the company. This new role reported directly to the board of directors. "[W]e need a strong voice outside the day-to-day business that is responsible for customer credentialing, compliance and privacy," said John Hamrem, chair of ChoicePoint's privacy committee. "Having a person of Carol's stature join us is vital to our efforts to have the kind of policies, procedures and compliance programs that build confidence as well as set a standard for the industry."[112]

---

110. Scalet, "Five Most Shocking Things."

111. Scalet, "Five Most Shocking Things."

112. Associated Press, "ChoicePoint Names DiBattiste Chief Credentialing, Compliance and Privacy Officer," *Atlanta Business Chronicle*, March 8, 2005, https://www.bizjournals.com/atlanta/stories/2005/03/07/daily6.html.

4.8.2 The Myth of the Security Team

Cybersecurity and data breach response aren't solo efforts. Large organizations typically have an information security team, which is tasked with both proactive cybersecurity and incident response.

Data breaches, however, are crises that reverberate throughout the organization—and beyond. They cannot be designed or executed solely by the "information security team," however convenient that might seem. Response planning efforts must reflect the crisis itself and involve stakeholders throughout the organization and out into the broader ecosystem, such as:

- Legal
- Public relations
- Customer relations
- IT
- Cybersecurity team
- Insurance
- Human resources
- Physical security
- Finance
- Executive team
- Board of directors
- Forensics firms
- Customers
- Former IT staff
- Key vendors/suppliers

When developing a data breach crisis response function, management must engage all of the key stakeholders regularly. The frequency and depth of involvement varies for each stakeholder, but in order for crisis response plans to be effective, this involvement must be ongoing throughout the lifespan of the organization.

Develop

The great military strategist Sun Tsu said, "Win first, then do battle." This maxim is as true for data breaches as it is for war. "Develop" is the very first phase of our DRAMA breach response model, and it encompasses the activities that must occur before a breach happens. Organizations need to develop and maintain data breach response plans in order to minimize the negative impacts of a breach. Make sure your data breach crisis plan is initiated at the executive level and includes all key stakeholders throughout the enterprise.

4.9 Conclusion

ChoicePoint was a catalyst for change. From a historical perspective, the crisis was game changing, resulting in a dramatic shift in public perception, new laws, and even the birth of the term "data breach."

The ChoicePoint breach also demonstrates the importance of developing your data breach crisis management function in advance and ensuring that it is aligned with your organization's key risks. The breach was far more explosive and impactful because of the company's lack of response, particularly in the early stages of the crisis. At the same time, the company did, suddenly, adapt midcrisis and was able to manage the chronic phase effectively, which helped to restore confidence and value.

In this chapter, we analyzed the ChoicePoint breach in the context of Steven Fink's four stages of a crisis:

- Prodromal
- Acute
- Chronic
- Resolution

We also reviewed the capabilities that your organization needs to have in place in order to manage our data breach crisis:

- **Develop** your data breach response function.
- **Realize** that a potential data breach exists by recognizing the signs and escalating, investigating, and scoping the problem.
- **Act** quickly, ethically, and empathetically to manage the crisis and perceptions.
- **Maintain** data breach response efforts throughout the chronic phase, and potentially long-term.
- **Adapt** proactively and wisely in response to a potential data breach.

The ChoicePoint crisis teaches us that, as the name implies, we have choices at each stage of the crisis. An organization, however, is not an individual, and it requires coordination and planning in order to ensure that smart decisions are made and acted upon.