THE CHIEF PRIVACY OFFICER'S GUIDE:

EVOLVING FROM PRIVACY INCIDENT RESPONSE TO PROACTIVE READINESS

WHY PROACTIVE INCIDENT MANAGEMENT IS FOUNDATIONAL FOR THE MODERN ORGANIZATION

BREACHRX

TABLE OF CONTENTS

EVERY COMPANY DEALS WITH INCIDENTS

The question isn't if incidents will occur; it's when. In fact, privacy incidents occur a few times a month, ranging from misdirected emails to lost laptops or exposure of personal identifiable information (PII).

Governments are cracking down with regulations in an attempt to protect the consumer. Gartner predicts that 75% of the global population will be covered by at least one regulation by 2023[1], and over four of five all companies worldwide will encounter at least one privacy-focused data protection regulation in the same year[2]. Even incidents involving just a few records will require compliance.

The majority of privacy executives know these statistics well. Industry leaders discern how to use the opportunity to elevate their privacy departments.

CEO PRIORITIES, COMPANY GROWTH, AND INCIDENT MANAGEMENT ARE DIRECTLY RELATED.

While CEOs say growth is their #1 priority[3], they rank privacy incidents as the biggest threat to their top line[4]. Nearly half (44%) of CEO respondents say data privacy is top-three policy impacting their business[5].

Chief Legal Officers (CLOs) agree: listing data privacy, compliance, and cybersecurity as the most critical issues for business, even above compliance[6].

1. https://blog.didomi.io/en/privacy-transparency-opportunity-not-a-burden
2. https://www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022
3. https://www.gartner.com/smarterwithgartner/ceos-see-growth-in-2021-marked-by-3-shifts
4. https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2022.html
5. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/top-policy-trends.html
6. https://www.acc.com/clo2021

HOW YOU RESPOND TO INCIDENTS SETS YOU APART

"Over 75% of the global population will be covered by at least one regulation by 2023."

GARTNER

"It is not the incident, but the incident response which fails organizations and teams."

RAHUL BHARDWAJ,
CISO – APAC, KROLL

Companies can no longer wait to shift from reacting to privacy incidents, to managing privacy incidents proactively. Otherwise, they risk the liability of inaction.

Assuming a proactive posture means shifting from incident "response" to incident "management." Rather than continuing to rely on status quo manual processes and spreadsheets to react to privacy incidents, forward-thinking Chief Privacy Officers (CPOs) and privacy counsel are elevating their approaches with a more programmatic approach. This means getting ahead of privacy events by:

- Creating dynamic, tailored incident response plans
- Working across departments to coordinate privacy incident roles & responsibilities
- Incorporating regulations and contracts into workflows
- Automating processes to enable teams.

A proactive incident management program is foundational to a privacy department. Just as the Security Operations Center (SOC) is the heartbeat of security teams, the program that surrounds the privacy corollary is just as vital, and it is integrated with security.

Proactive incident management is foundational. The following sections explore how you can make that shift.

4 ELEMENTS
OF PRIVACY INCIDENT MANAGEMENT MATURITY

To transition from reacting to privacy incidents into proactively managing them, leaders shift from a human-driven manual process to one that is technology-enabled and human augmented.

We've developed a proprietary maturity model that defines five stages of the privacy incident response journey. It reflects interviews with nearly 130 privacy and security leaders, as well as a dozen strategic advisors, who transformed their privacy programs to get more proactive. They've broken down the journey into a few key elements.

THE PRIVACY INCIDENT MANAGEMENT MATURITY JOURNEY

	DENIAL	REACTIVE	MANAGED	SYSTEMATIC	PROACTIVE
Program Maturity	No incident response plan	Generic incident response template	Detailed incident response plans	Routine updating and implementation of IR plans	IR is core to privacy program
Org. Maturity	No full-time privacy headcount	Dedicated privacy responsibilities	Incident response team + responsibilities	Defined and detailed privacy workflows	Privacy + security response integrated
Regulation & Contract Maturity	Little to no in-house knowledge of applicable privacy regulations	Some tracking of regulations + obligations	Active tracking of regulations + obligations	Centralized management of global regulations + contracts	Proactive integration of regulations + contracts into incident response workflows
Tech. Maturity	No system in place	Manual processes + spreadsheets	Spreadsheets + basic ticketing system	Basic system + manual exercises	Automated processes + exercises

LET'S DIVE INTO THE FOUR ELEMENTS OF EACH PHASE

1. PROGRAM MATURITY.

Similar to the idea of security by design, leaders need to build privacy into their organizations' programs, processes, and products from the start. Otherwise, it's bolted on, less effective, and more expensive. Proactive privacy organizations acknowledge that today's privacy landscape is dynamic, with a growing body of regulations and contractual obligations. The first step to becoming more proactive is acknowledging that incidents occur regularly and that managing those incidents is core to any privacy program.

For example, one fintech company prepared to go public by strategically outlining all facets of privacy incident response: outlining playbooks for all possible scenarios, defining roles for each; distributing responsibility across relevant teams; automating regulations and contracts into workflows; and building cultural value around reducing risk. Today, the organization deftly responds to privacy events with the confidence that it's honoring shareholder and customer interests.

2. ORGANIZATIONAL MATURITY.

The foundation for organizational maturity involves defining the privacy team roles and responsibilities, establishing clear privacy processes, and cultivating a relationship with security. Without clearly laying this out, managing privacy incidents can quickly become chaotic and inefficient, with different teams tripping over each other.

Greenhill, a leading investment bank, developed organizational maturity by streamlining efforts and outcomes across privacy and security teams. By working together, Greenhill centralized roles, activities, and workflows in a single platform, dramatically saving time, focusing effort, and improving communication. They also know exactly who needs to do what when incidents occur.

"Breach response is very manual and prone to a checklist mentality, which leads to a lot of mistakes."

AL RAYMOND, CONSUMER & COMMUNITY BANK PRIVACY OFFICER, JPMORGAN CHASE

HOW GREENHILL DEVELOPED ORGANIZATIONAL MATURITY

Greenhill, a leading investment bank, developed proactive organizational maturity by orchestrating its privacy and security teams. Together, the teams centralized roles & responsibilities, regulations & contracts, and dynamic workflows in a single platform—dramatically saving time, focusing effort, and improving communication.

LET'S DIVE INTO THE FOUR ELEMENTS OF EACH PHASE

3. REGULATION & CONTRACT MATURITY.

There's no way to overstate the importance of comprehending regulatory and contractual obligations. There are now over 180 regulations for data privacy in 128 countries[7], some of which require incident reporting in 24-48 hours, and many more on the way. While the average cost of a data breach in the U.S. is $9M[8], legal missteps and contractual mistakes can add to the cost or lead to a CPO being held personally liable.

Industry leaders mature privacy incident management by incorporating regulations and contracts into automated workflows that adjust for each situation and any new laws, even as obligations change.

4. TECHNOLOGICAL MATURITY.

Automation is critical for scaling legal teams, as growing bodies of regulation make it untenable to keep throwing people at the problem. This is likely why over one-third of GCs and CPOs purchased incident response software in 2021, and 15% more planned to buy incident response software in the next 12 months.

One customer data platform provider used technology to make their small team exponentially more efficient, effectively adding new bench strength and resources with the privacy incident management tool.

CPOs, CLOs, and GCs must deeply understand these four elements to successfully transition from one phase to another.

"Completely manual mitigation approaches don't scale."

FORMER CISO, VANGUARD

"Most response plans keep security and legal teams isolated in their own swim lanes. "Throwing things over the wall" throws up communication obstacles and can inhibit smart, collaborative response."

FORMER CISO, CYLANCE

7. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
8. https://www.securityinfowatch.com/cybersecurity/press-release/21123576/ponemon-institute-ponemon-institute-reveals-68-of-organizations-were-victims-of-successful-endpoint-attacks-in-2019

3 STEP CHECKLIST FOR PROACTIVE INCIDENT MANAGEMENT

Shifting to a proactive approach requires more than just planning out a response ahead of time. It requires laying a foundation of people, process, and technology that will enable the business, integrate with security and adjacent departments, and orchestrate coordinated workflows when privacy events occur.

Legal and privacy executives help their teams mature into proactive privacy incident management by following three steps.

"Successfully managing an incident begins and ends with how well you are prepared to address it."

STEVE MANCINI,
CISO, ECLYPSIUM

STEP 1
PREPARE

- Prioritize incident management
- Build relationships with security counterparts and other internal partners, helping them understand privacy and legals' roles
- Organize and document which teams and roles should execute which tasks for different events
- Maintain automatically-updated regulatory information and keep tailored playbooks up to date
- Organize and update contractual obligations in one place
- Run incident simulations and tabletop exercises

STEP 2
RESPOND

- Tailor response action items to your organization's needs
- Automatically assign tasks to team members
- Facilitate cross-functional processes and update stakeholders in real time with built-in collaboration tools
- Separate on-the-record and off-the-record communication
- Provide a safe haven where teams can communicate outside operational environments that might be compromised during an incident

STEP 3
MANAGE

- Make incident management a foundational and routine activity
- Measure and report on the types and frequency of incidents and on response efficiency, so privacy teams can analyze and improve their performance, share with the C-suite and the board
- Conduct detailed post-incident analysis, improve readiness and response postures, increase efficiency

WHAT SUCCESSFUL PROACTIVE INCIDENT MANAGEMENT LOOKS LIKE

A proactive privacy incident posture that's effective reflects the size of your organization.

GLOBAL ENTERPRISES

In the heat of the moment, relying on lengthy playbooks and manual processes won't work. Instead, industry leaders diminish their businesses' exposure to privacy incidents by orchestrating privacy incident management with technology that:

- Automates processes
- Enables tabletop exercises
- Customizes tailored plans to reflect real-time situations
- Incorporates regulations and contracts into workflows
- Integrates privacy and security response
- Measures progress
- Enables the business

Such organizations also prioritize leadership alignment, ensuring all members of IT, legal, privacy, and security departments understand and embrace their strategic role in privacy incident response.

INDUSTRY LEADERS DIMINISH BUSINESS EXPOSURE BY ORCHESTRATING PRIVACY INCIDENT MANAGEMENT WITH TECHNOLOGY.

"Companies need to take a fresh approach to information risk discovery. They need tools that generate key insights, drive automated playbooks, and aid their users in making timely, actionable decisions for risk mitigation."

FORTUNE 100 CYBERSECURITY EXECUTIVE

HIGH-GROWTH ORGANIZATIONS

Fast-growing companies have additional constraints of budgets and talent shortages[9]. While leadership alignment still matters for the best organizations of this size, privacy incident program success takes a leaner, more technology-assisted form. High-growth privacy professionals help their organizations lay a solid foundation to achieve privacy readiness early on. They augment their privacy incident response by:

- Appointing privacy champions in different areas across unique teams
- Defining playbooks for all possible incident types
- Accounting for regulations and contracts in their processes and workflows
- Conducting frequent rehearsals
- Investing in technology that can scale with their business to orchestrate privacy and security response

The above is particularly true for high-growth companies in financial services, high tech, healthcare, and digitally-driven, critical infrastructure—and is likely a big reason why year-over-year spend on privacy technology is up 30%[10].

The relationship between organizational growth, CEO priorities, and proactive privacy incident management is clear. As breaches increasingly infiltrate mainstream media and boardroom discussions, the importance of how your company responds will keep pace.

9. https://www.wsj.com/articles/competition-for-compliance-officers-intensifies-amid-regulatory-pressures-11642623091
10. https://iapp.org/resources/article/privacy-governance-report/

"Companies should consider having tools like BreachRx at the ready to help them act before, during, and after an incident, from a compliance perspective. They also need to improve their privacy and security programs overall to maintain trust with customers and regulators."

ALEXANDRA ROSS,
GLOBAL DATA PRIVACY
EXECUTIVE, AUTODESK

ABOUT BREACHRX

BreachRx empowers privacy and legal teams to get ahead of privacy events. The privacy incident management platform helps businesses reduce risk by moving them beyond traditional spreadsheets and documents into an actionable, dynamic SaaS platform that keeps pace with evolving regulatory and contractual obligations. The platform strengthens privilege protections in ways that traditional alternatives cannot. Built by legal and security experts for their peers, the company was founded by Anderson Lunsford, CEO, and Matt Hartley, Chief Product Officer.

THE VALUE OF BREACHRX

By enabling privacy teams to get more proactive in their privacy incident response and management, the BreachRx platform measurably reduces the cost of a breach by over $2.5M on average (based on the 2020 Ponemon Cost of a Breach study). This savings amounts to over 22x the return on an organization's annual investment in the BreachRx platform.

"It was easy to see how BreachRx's automation for incident response and data breach processes would allow us to proactively elevate our approach."

JOHN SHAFFER,
CIO, GREENHILLZ

"BreachRx helps automate the end-to-end process and eliminates a lot of mistakes and missed opportunities."

AL RAYMOND,
CONSUMER & COMMUNITY PRIVACY OFFICER,
JPMORGAN CHASE

To learn more about BreachRX, please visit www.breachrx.com.

Follow BreachRX on Twitter and LinkedIn.

REQUEST A DEMO