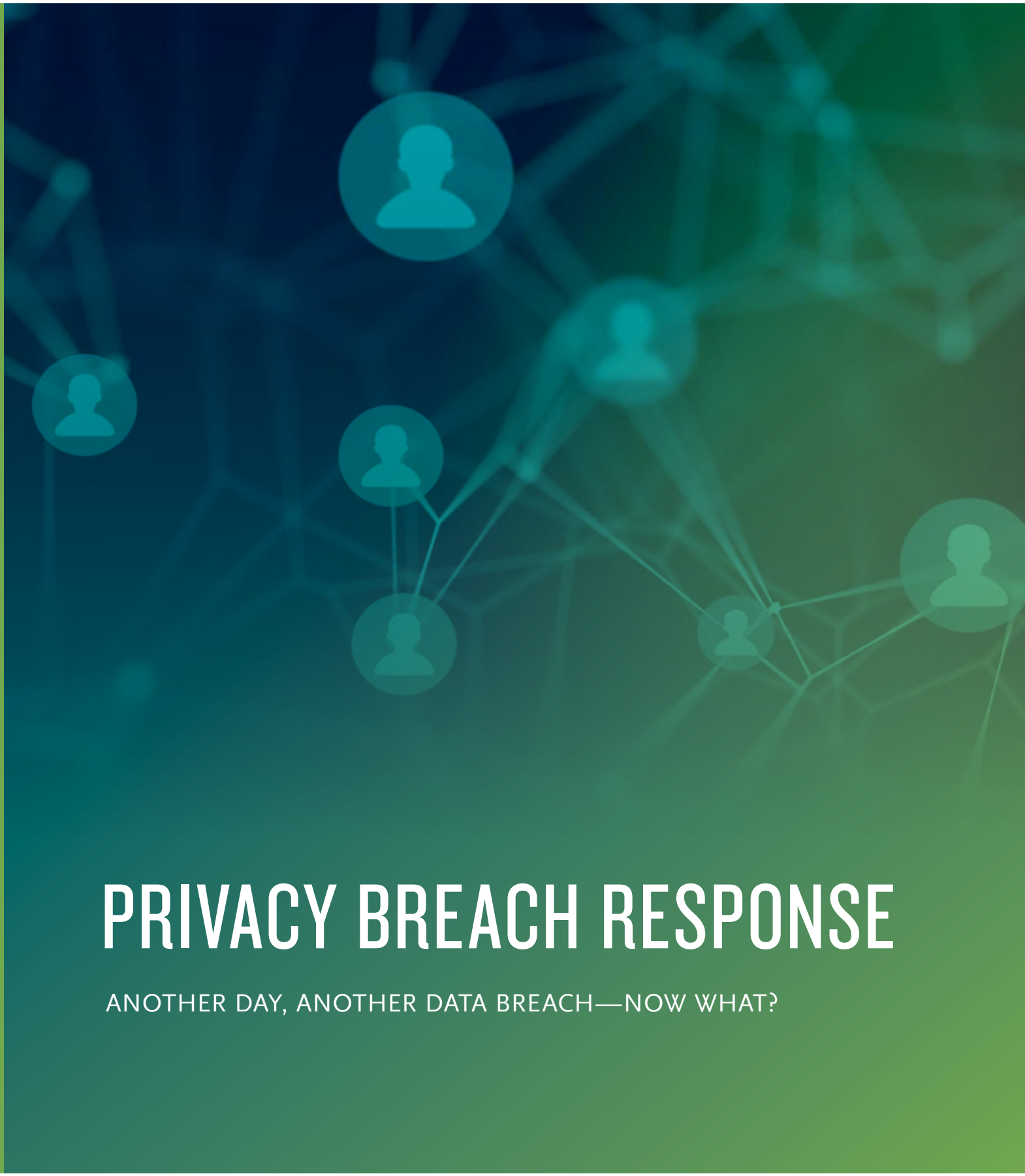
Booz | Allen | Hamilton



PRIVACY BREACH RESPONSE

ANOTHER DAY, ANOTHER DATA BREACH—NOW WHAT?

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

WITH EVERY DAY SEEMINGLY BRINGING ANOTHER DATA BREACH, HACK, OR EXPLOIT, IT'S NO LONGER "WHAT IF" BUT "WHEN" AND "HOW BAD."

Having an established Privacy Breach Response program puts the necessary processes, policies, tools, and people in place so that you are prepared when your organization encounters a breach of personally identifiable information (PII). Booz Allen created the Privacy Breach Response service offering to help organizations implement a comprehensive program integrated with existing computer or security incident response programs with the goal of reducing overall enterprise-wide privacy risks.

DEFINING THE ROLE OF PRIVACY BREACH RESPONSE

... for an organization to successfully implement a Privacy Breach Response program, there needs to be a deliberate cultural shift that moves away from only reactive response to proactive education and preparation.

Privacy breach response starts with the Chief Privacy Officer, Senior Agency Official for Privacy, or Privacy Official, but certainly doesn't end there.

Successfully implementing privacy breach response includes obtaining buy-in from your organization's senior leaders, bringing the right stakeholders (e.g., IT Security, Security Operations, Legal, Human Resources, and Public Relations staff) to the table, building relationships and partnerships across your organization, and finding ways to integrate into existing computer or security incident response processes.

The Privacy Official should be at the center of developing and implementing the Privacy Breach Response program—from the creation of a privacy breach tracking and reporting process, to designing notification templates, to assessing third-party contract terms and requirements related to breach response. Depending on the maturity of your organization and Privacy Program, some of these components may already exist or you might be starting from scratch. Regardless, for an organization to successfully implement a Privacy Breach Response program, there needs to be a deliberate cultural shift that moves away from only reactive response to proactive education and preparation.

Using an awareness campaign, this program can be appropriately socialized within an organization to ensure every employee understands their roles and responsibilities. Information about privacy breaches should be included in any annual and role-based privacy training, but creating separate targeted awareness materials, specifically around identifying and reporting privacy breaches, will help distribute information on new processes and policies in place.

2017 U.S. DATA BREACH STATISTICS AT A GLANCE:

- Average total cost of a data breach was $7.35 million
- Average number of breached records per incident was more than 28,000
- Average cost per breached record was $225

With the likelihood of a recurring data breach increasing to 27.7% globally, the need to remediate the issue quickly and improve prevention tactics is vital to a healthy breach response program.[1]

[1] "2017 Cost of Data Breach Study: Global Overview." Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview, IBM Security, June 2017, www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&.

PRIVACY BREACH RESPONSE IN PRACTICE

SCENARIO 1

Human Error—The Biggest Culprit

An HR employee sent a list of 100,000 former employees' names and social security numbers to an incorrect email address without the proper encryption. Now the data has been exposed and notifications and credit monitoring are required due to the risk of identity theft. Leadership is concerned over the size of this breach, the cost to the organization (both financial ramifications and damage to reputation), and the ease with which it could have been prevented.

How privacy breach response can help:

Our team can handle this breach from reporting to notification, including:

- Investigating the causes of the breach, from routine processes to organizational policy
- Collaborating with the security operations team(s) to recommend remediation steps to recover the breached data and lower the risk of reoccurrence
- Developing training to increase privacy breach awareness and implementation of data loss prevention tools
- Compiling and presenting information for leadership on the details of the breach, combined with metrics on similar breaches to best inform decisions regarding individual notifications and future policy

SCENARIO 2

Making a Plan for Your Plan

New federal regulations have been released that require your organization to develop a Breach Response Plan. Your organization has an existing policy, but you're unsure how to address all the new requirements nor which requirements are important for your organization given limited funding and resources.

How privacy breach response can help:

Our team can assess the new requirements within your environment and help create new policies and procedures from development to implementation by:

- Examining existing policies and comparing against new requirements to produce a gap analysis, highlighting areas in need of development and improvement
- Drafting a new policy document and reconciling organizational feedback
- Finalizing policies and aiding in implementation across your organization, including developing standard operating procedures, job aids, and training to ensure consistency of implementation

SCENARIO 3

Exercise Regularly as Part of a Healthy Routine

Your organization has just finished remediating a major breach, but many of the vital players were unaware of their roles and responsibilities, resulting in delayed remediation efforts and individual notifications. Key stakeholders within the organization were unaware of where to find the appropriate resources for dealing with a breach, and those who were had out-of-date information. Given the fast pace and public attention to the breach, your organization has identified the need to practice a standard breach response.

How privacy breach response can help:

Our team can prepare all the resources necessary to run a tabletop exercise and provide operational support during the exercise, including:

- Creating a scenario and injects to simulate the timeline of an actual breach
- Preparing instructions and other materials to facilitate practicing breach remediation across the organization
- Reviewing lessons learned and stakeholder feedback for implementation in new standard operating procedures and revised resources, including job aids and tip cards, to support ease of reporting and remediation in future breach situations

ABOUT BOOZ ALLEN'S PRIVACY BREACH RESPONSE SOLUTION

Booz Allen understands the importance of developing a comprehensive Privacy Breach Response program.

We help a wide variety of organizations prepare for what's next and advise both federal and commercial organizations on how to modernize traditional Privacy Breach Response programs to more effectively manage and mitigate privacy risk across the enterprise. As thought leaders in next-generation privacy considerations, Booz Allen understands the complexities of the changing privacy landscape and the impact on how organizations handle PII when building new programs and services. Our experience and expertise can help organizations develop and implement a comprehensive privacy management approach that minimizes risks while satisfying your business needs. Organizations need a Privacy Breach Response program to ensure everyone knows what to do when a breach occurs. Implementation of this program would have to be risk-based and dependent upon resources, with fully resourced privacy programs being able to stand up a Privacy Breach Response program more quickly and less resourced offices having to prioritize based on the organization's risk tolerance.

Key components of this strategy include the following steps:

1. Full privacy breach response lifecycle management process for training, tracking, reporting, investigation, mitigation, remediation, and notification of breaches.
2. Privacy breach response policy and/or plans to ensure compliance with federal, state, and industry requirements and best practices.
3. Data loss prevention tools and services.
4. Regular tabletop exercises to test capabilities and ensure proper processes and policies are in place within an organization.

Like any successful initiative, this is not a "one-and-done" activity; it's a process that requires ongoing effort.

Maintaining continuous awareness of your organization by promoting open dialogue with key stakeholders and ensuring your privacy breach efforts are being integrated with existing Computer or Security Incident Response Programs are keys to having a successful Privacy Breach Response program in your organization.

HOW BOOZ ALLEN CAN HELP

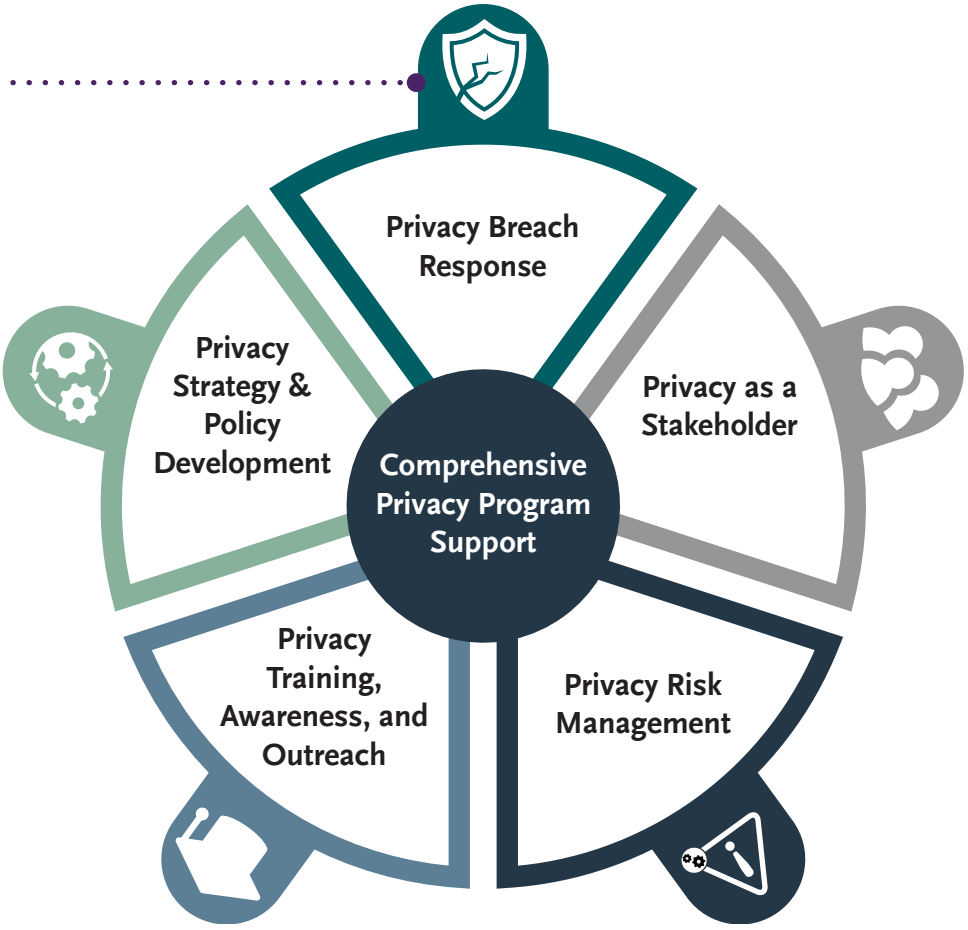
Our Privacy Consulting Team comprises industry experts with experience in both the commercial sector and the Federal Government, who have built full-scale enterprise privacy programs.

Our depth of experience allows us to bring best practices from one organization to another, while customizing the need to fit the privacy program and organization at hand. We have assisted clients with developing and maturing their Privacy Breach Response programs and analyzing new and emerging requirements to ensure organization compliance. We understand the importance of creating a roadmap for success and have worked with clients to develop privacy priorities and documentation that complies with federal and industry privacy requirements and is built to fit the organization's needs.

We have a team of privacy experts equipped and ready to help you:

- Assess any existing privacy breach response processes and policies, identify issues/gaps, and provide recommendations
- Develop, implement, and test new privacy breach response policies and procedures
- Assess needs for technologies, tools, and services to support the Privacy Breach Response program

BOOZ ALLEN'S PRIVACY SERVICE OFFERINGS



PRIVACY BREACH RESPONSE

- Design and implement a privacy breach response process including training, tracking, reporting, investigation, mitigation, remediation, and notification
- Develop a privacy breach response policy to formally document all processes, procedures, roles, and responsibilities
- Identify and implement data loss prevention technologies
- Conduct privacy breach tabletop exercises to ensure processes and policies are in place and functioning properly

About Booz Allen

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that—together—we will find the answers and change the world. To learn more, visit BoozAllen.com.

For more information, please contact:

LIZ TRIBELLI
tribelli_elizabeth@bah.com

DIANNA CARR
carr_dianna@bah.com