Radar[®] Privacy

Is Your Privacy Program Creating Value?

Privacy teams work twice as hard to earn a budget and prove value within organizations. With this checklist, privacy leaders can demonstrate instant, visible business impact and prove value across departments to establish privacy as a value driver.

While Privacy is younger than their counterparts in Legal or Compliance, the expanding scope of privacy regulation is showing us the untapped potential for Privacy leaders to drive value through increased efficiency, cost — and time — savings, and trust-building consistency.

n		



くへっ

SCORE YOURSELF: How mature is your privacy program?

Use this checklist to see where your incident response process aligns to the key functions that prove value

Low +1 point Medium +2 points High +3 points Critical +4 points

Identification & Investigation

Y	Applied In My Business	Key Privacy Incident Response Functionality	Business Impact	Efficiency Gains	Quantif Risk Mitigation	able Value _{Cost Savings}	Trust Building	
	+3	100% customizable dimensions that features multi-jurisdictional capability	High	1	\bigtriangledown	\$	-	
	+3	PII automatically mapped to applicable regulations	High	1	\bigtriangledown	\$	-	
	+3	Centralized portal and unique workflow for all functional areas	High	1	-	\$	-	

Assessment

3237	+2	Up-to-date Legal Library with Regulatory Watchlists	Medium	1	\bigtriangledown	\$	-
	+2	Industry-specific assessments (e.e=g. NAIC)	Medium	1	\bigtriangledown	-	-
	+3	Integration of internal policies, including 3rd-party notification obligations	High	1	\bigcirc	\$	
	+3	Automated assessment based on applicable laws with multi-facet and multi-region assessment capability within a single incident	High	1	\bigcirc	\$	
	+4	Quantification of the risk of harm	Critical	1	\bigcirc	\$	
	Deci	sion					
	+2	Central repository to manage incidents with individual assessment statuses	Medium	1	\bigcirc	\$	-
	+3	Accelerated mean time to incident resolution for all incident types without counsel	High		\bigcirc	\$	
	+3	Defensible Decision based on 100% consistent process	High	1	\bigcirc	\$	
	+4	Automated decision support guidance	Critical	1	\bigcirc	\$	2.0.0
	Noti	fication					
	+2	Notification capabilities integrated with assessment results	Medium	1	-	\$	-
	+3	Notification Letters Management: Third- Party Notifications and Industry-specific notification obligations	High	1	-	\$	225
A c	Anal	ysis					
2 000	+2	IR Trends Analysis based on user-defined categories	Medium	1	-	\$	-
	+2	Configurable reports/records	Medium	1	-	\$	-
	+2	Incident Remediation & Root Cause Analysis	Medium	1	\bigtriangledown	\$	
	+3	Incident Response Benchmarking Data	High	1	\bigtriangledown	\$	

Your Privacy Program Maturity Score:

How does your program compare with the privacy value gained from Radar Privacy?

35+ = Great! You're paving the way and proving value.

30-34 = Good. You're proving value but there's room to improve.

20-29 = OK. You've got the basics and are ready to mature your privacy program.

<19 = Needs improvement. Your program may benefit from an intelligent incident response solution.

Proving value is about increasing efficiency and building program maturity

As workloads amass for privacy, compliance, and security professionals, employing an intelligent incident response solution can provide immediate relief and long-term business value to catalyze efficiency and equip teams with actionable means to reduce risk, save time and cost, and build value – *and we can prove it*.

Radar" Priva	cy vs Others		
Key Features	What / Why	Radar Oth	
Automated Incident Risk Assessment	What is completely automated assessment that considers all relevant risk factors involved in a specific princy inclusion and programmatically undysters into them haved on all applicable data. What is dry understanding and the specific principal and the specific		
Playbooks	What create and assign customizable workflows for consistent execution across teams, involve the right stakeholders at each stage of incident management and sut a framework for scalable growth, Why holices the time sport investigating and closing incidents with well documented, repeatable processes while improving compliance, trause a repeatable, audit-compliant growth,	•	
Global Breach Law Library	What: Up-to-date library of global data breach notification laws that are mapped to an automated risk assessment, including regulatory watchfields that track proposed and recently passed legislation. Why: Tasily access and review laws that apply to privacy incidents. Assess incidents with up-to- date data breach and inclusion laws.	•	
Incident Management Decision Intelligence	what people publics and constitute deviationing -offend deviaed free parameted automation that enables a sophisticated breach investigation and reveals notification obligations and recommendations. Automated behaviology to solve the most complex challenges of data breach matagement with increased operad and accuracy.	•	
Automated Third-Party Notifications	What: Automatic consideration of third-party contractual notification obligations in addition to applicable laws and regulations during the risk assessment of an incident. Why: Assess, manage, and automate your contractual data breach notification obligations with clients and both upstream and downstream entities.	•	
Incident Dimensions	What collaboration and comparable incident suppress system for handstate latents to run playbooks in order to resolve privacy and non-privacy incident's with patential automation. Why involvement and incident multiple dimensioner, tensue the swift and accurate resolutions of an incident by unlifying all tamms, each focused on their dimension, to work together in core solution; simplifying concerning counter the solution and accurating limits to incident resolution;	• 0	
Multi-Region & Multi-Facet Incidents	What: Capacity to assess multiple jurisdictions and different situational faces to surface all notification obligations while in a single incident encord. Why: Streamline incident evaluation from Discovery to Assessment to Resolution for even complia incidents invelving multiple jurisdictions and multiple facess.	•	
Real-time Trend Analysis and Reports	What: Summary of incidents over time to facilitate analysis and trends and enable easy reporting. Why: improve visibility of privacy incident management performance and most the various data analysis and reporting needs for multiple stakeholders.	•	
Benchmarking Metrics	What: synthesis of aggregated and anonymized data to generate comparative incident response management metrics that benchmarks year organization across the industry and with peers. Why: cauge your privacy incident response management performance with others to reaffirm business genatis and improve operational efficiency.	•	

How much value can you create for your company?

See how savings from Radar Privacy compare to other leading incident management solutions.

Get the Guide

OR VISIT radarfirst.com/resources/privacy-incidentmanagement-software-comparison-infographic/

@RadarFirst

radarfirst.com | info@radarfirst.com | 844.737.3778