DATASHEET

RadarFirst

The True Cost of Office Productivity Tools for Incident Management

Your office productivity tools may be jeopardizing the health of your privacy, compliance, and security teams.

Your office productivity tools may be costing you more than an annual fee. While they offer critical productivity support for communicating and collaborating, for a privacy or security team, they can also generate inefficiencies—and organizational risk—when used as the foundation of a home grown incident assessment and response system. They simply aren't purpose-built to be event-specific tools.

The solution: RadarFirst. Use purpose-built, market leading incident response solutions to eliminate process and communication inefficiencies, accelerate your speed to notification decisioning, and bring a high level of defensibility to your teams' incident management approach.

Common Office Productivity Tools:

Office productivity tools are critical to the infrastructure of both individual teams, as well as entire organizations. Some of the most common office productivity tools used by Fortune 500 companies and startups alike include:

- Spreadsheets
- Email
- Shared Document Systems
- Ticketing Systems
- Team Communication Tools

Shared spaces to communicate, collaborate, and manage tasks are some of the top benefits to teams when these essential tools are used in collaboration with one another—and have become even more valuable in the age of remote work environments. Privacy, compliance and security teams, however, need more than optimized workflows and shared work spaces to efficiently and effectively respond to data breach incidents.

Challenges to Home Grown Incident Management Systems:

Home grown incident management systems can be comforting in their familiarity, and are often "the devil we know." Common barriers to adopting a new solution typically focus on resource constraints, from limited budgets to concerns over intense onboarding timelines.

However, when we understand how the challenges to using office productivity tools for building out homegrown incident management systems can potentially add up to costly organizational risk and inefficient use of employee resources, it becomes easy to make the ROI case for investing in a purpose-built incident management solution, like RadarFirst, that collaborates with, and optimizes, already embedded office productivity tools and systems.

RadarFirst

Challenge:

Ever-changing laws and regulations

State, federal, and global privacy and security laws are an ever-evolving—and ever-increasing—landscape of regulations that are next to impossible to stay ahead of using manual processes and tools, such as spreadsheets or documents

Consequences:

The potential consequence of using a manual system to maintain a law overview is both the **under, or over, notification of regulators, stakeholders, and customers when an incident occurs**, either of which can increase fines and penalties, and decrease trust. Additionally, internal resources, or high-priced external counsel, are required to survey laws and update these systems.

Realities of human error and subjectivity

The most dedicated and diligent professionals in an organization are often aligned with the compliance, security, IT, or privacy teams. But, ultimately, humans are humans, prone to error and influenced by subjective thinking. Office productivity tools may offer workflow automation, but can't account for subjective decision-making still inherent within a workflow.

Subjectivity, and simple human error, account for many common privacy incident causes. For instance, auto filling the wrong recipient when sending out an email that contains sensitive data. While no solution or tool will ever fully eliminate the possibility of error, automating the incident notification decisioning process, a critical step in the incident management lifecycle, can help **reduce the costly consequences of both human error and bad actors**.

Scalability of privacy, compliance, & security teams

The demand on compliance, security, and privacy teams is increasing at a rapid pace; they need the ability to scale the pace at which they operate, potentially without added headcount, and their digital footprint with ease and speed. While individual office productivity tools are often easily scalable by adding additional users, tight budgets might prevent hiring. These tools also don't support the scalability of a team's efficiency and effectiveness in a significant way when it comes to an essential aspect of their roles: incident management.

When a critical team, like privacy or security, can't appropriately scale their efforts to meet organizational needs and regulatory or consumer expectations, the consequences can have a **costly impact on the organization's bottom line, from loss of trust to fines and penalties** for under notifying regulators and stakeholders about breaches, or even a simple delay in notification. And, let's not forget the human cost as employees are required to work longer hours.

RadarFirst

Which challenge resonates most with your team? Reach out to RadarFirst to learn more about how we can solve for the risk-generating gaps in your home grown incident management system >

Not event-specific

Office productivity tools, from email to spreadsheets, offer essential collaboration opportunities, but are passive solutions for communicating and data gathering, and do not support event-driven demands of teams involved in privacy, security, and compliance-based incident management and response.

Event-focused teams that rely on manual systems built on office productivity tools are at a much higher risk of over or under notifying regulators and stakeholders than teams that have embedded purpose-built, automated solutions into their work. The **consequences of both under and over notifications can be costly, to the tune of millions, in fees and fines**—as well as the loss of customer trust, the cost of which can have years or decades long impacts on an organization's bottom line.

Event audits or recalls

It's not uncommon for data incidents, which occurred years ago, to be called into question, whether through an audit or legal action.

Office productivity tools require compliance, privacy, or security teams to review years of emails, looking for keywords, and then piecing together a comprehensible story from the email narratives. This **time consuming process is certainly fraught with error** as teams are likely to miss important content, particularly given tight time constraints.

Inconsistencies inherent in manual processes

Manual, homegrown processes, particularly those built on top of office productivity tools, are inherently inconsistent as they rely on human decision-making versus automation and technology to follow and complete steps.

A critical measure of an effective and risk-mitigating incident management solution is consistency, i.e. defensibility. Without automated incident management solutions that drive forward the digital transformation of key organizational teams, such as privacy, compliance, and security, proper documentation of incident assessments cannot be assured—and **an organization's defensibility of their notification decision making process may be called into question by regulators and stakeholders** when the inevitable privacy or security incident occurs.

RadarFirst

Enter-RadarFirst

RadarFirst offers a purpose-built incident management solution that addresses privacy, security, and compliance incident assessment and notification decisioning via patented technology and streamlined automation. The Radar® platform offers two award-winning products to drive the digital transformation of security, privacy, compliance, and IT teams.

Radar® Privacy

Radar® Privacy, powered by RadarFirst's patented Breach Guidance Engine™, features automated risk quantification for expedited breach notification decisioning. The solution automates the privacy risk assessment and immediately solves the most complex questions after a breach occurs:

1. Does this breach require us to notify regulators or affected individuals?
2. What is our risk of harm analysis for each jurisdiction or region?
3. How much time do we have to meet our breach notification obligations?

Radar® Privacy enables an exhaustive investigation that ensures all critical details from an incident are captured, and automatically and seamlessly connects that critical data to the appropriate breach notification laws.

Radar® Compliance

Radar® Compliance is a configurable rules and assessment engine. The solution offers organizations the ability to define their own notification triggers and obligations to stakeholders, from federal regulators to the board of directors. Highly configurable, Radar® Compliance is able to address a wide variety of incidents, including but not limited to cyber events, health and welfare, operational interruptions, and internal compliance.

By operationalizing compliance, risk, and cyber requirements with their associated internal and external notification obligations, Radar® Compliance shortens the time spent getting to a notification decision, freeing up resources for incident investigation, and providing a transparent process to all stakeholders. The result is a company-wide streamlined compliance process that enables cross functional collaboration and risk mitigation between IT, InfoSec, cybersecurity, privacy, legal, HR and compliance teams.

RadarFirst Integrations with Office Productivity Tools

Collaboration is the key to mitigating organizational risk, not only between teams, but between tools, platforms, and solutions. RadarFirst integrates seamlessly with a growing number of office productivity tools, including: Slack, Microsoft Teams, IMAP (e.g., Gmail, Outlook), CSV Uploads, Jira, and BambooHR.

RadarFirst

Use Case

Loss of Electronic and Paper Information

While out to dinner on a Friday evening, a key financial employee of a B2C business left their backpack in a parked car. The backpack contained a computer with downloaded files as well as paper reports, both revealing the personal information of customers and employees. The car window is smashed and the backpack is stolen.

When the employee discovers the theft upon their return to their parked car, they call law enforcement to report the crime. The employee also sends an email to "incidents@company.com," via an IMAP integration to Radar® Privacy, and includes the key incident information, along with pictures of the initial police report and the car window. The employee received a confirmation email that the incident was indeed received by the Radar® platform, and therefore in the hands of the privacy team. Additionally, the privacy team received an alert via Microsoft Teams of the created incident to ensure the investigation and assessment process would not be delayed until the privacy team returned Monday morning.

The affected company's Microsoft Teams and IMAP email integrations to Radar® Privacy enabled this timely data incident reporting that otherwise may have been delayed for several days over the weekend. And, thanks to RadarFirst's patented Breach Guidance Engine™, the privacy team was able to swiftly determine whether or not to notify regulators, and within what timeframe.

Previously, a similar incident may have taken the privacy teams weeks to identify, investigate, and assess, and required significant guidance from outside counsel. The collaborative integration of office productivity tools with RadarFirst's automated incident management products accelerated the team's breach resolution, from discovery to notification, ensuring the appropriate stakeholders were notified, within the required timeframe, and only as required by law, safeguarding the organization's trust, reputation, and their bottom line.

Schedule a demo to streamline your incident management processes.

INFO@RADARFIRST.COM | 1.844.737.3778

Schedule a Demo

RadarFirst

Learn more at radarfirst.com

RadarFirst's award-winning incident management solutions are trusted by organizations in heavily regulated industries to reduce risk and simplify compliance with global data breach laws.