servicenow

Privacy management needs a new playbook

START >>

In 2021

60% of the world's population is online generating

1.7 MB of data per second

2.5 quintillion bytes (million trillion) per day

74 zettabytes per year

while at the same time

230,000 new malware samples are being created every day

The amount of data generated in 2024 will grow to **149 zettabytes** [1]

Everything generates data

With the digitalization of everything we do, our personal data is everywhere. It's very easy to build a profile of who we are. The personal information (PI) we give away is transformed into something precious–and used to train machines to be smarter. The Google searches we do with health questions or as we research hobbies give away information about us. We probably share the most on social media as we stream music and movies, attend virtual exercise classes, and connect with others. With connected devices we control the temperature in our houses and monitor our children. Even our cars have been digitalized–providing more valuable data.

There is a common analogy that compares personal data to oil: information powers today's most profitable corporations, just like fossil fuels did for those of the past. But unlike oil, data is easier to extract and spill. Every day, hundreds of companies we may not even know exist gather facts about us. This precious information flows to academics, law enforcement, attackers, and nation-state hackers—as well as plenty of companies trying to sell products and services.

44%

of breaches involve customer personal information/data [2]

26%

involve employee personal information/data

Most data breaches involve personal information

Because PI is so precious it's the most sought-after data in an attack.

For organizations, the exposure of PI is the costliest to remediate. In general, customer PI cost an average of $180 per lost or stolen record, 12% higher than the average cost per record.[2] Determining which accounts have been impacted, communicating with customers, and providing credit services is just the beginning. For better or worse, breaches are not the biggest source of privacy risk—employees are.

50%

Of privacy incidents originate with employees [3]

45%

Of employee-driven privacy failures are intentional

servicenow

Customer privacy concerns are increasing

Studies have shown that many customers don't feel enough is being done to safeguard their data in large part because of the media attention when data records are lost. According to findings, most customers are concerned about their data privacy and said their concern about data privacy has increased over the past 12 months.

79%

Concerned about privacy [4]

21%

Concerns have increased in last 12 months

"It feels like a broken record when discussing data privacy regulations because every year data privacy regimes continue to grow in jurisdictions around the globe. But as repetitive as it can be, it is still the truth. The frameworks and regulations that enterprises need to manage continue to explode. End users are struggling with the sheer volume of regulations and need help with the regulatory change management...."

- Ryan O'Leary research manager, Privacy and Legal Technology at IDC

Privacy management practices aren't keeping pace

Many organizations are in reactive mode regarding managing privacy risks. They act when a risk has been identified or a new regulation must be implemented. Not only is there no common taxonomy, the are are no standard processes or frameworks to ensure redundant controls are being created or to manage the potential explosion of controls. There's simply very little time to put anything in place. The growing number and complexity of privacy regulations will continue to stretch privacy and compliance teams.

To put the explosion of privacy regulations into perspective, in the last 3 years, 128 out of 194 countries have put in place legislation to secure the protection of data and privacy, while 19 other countries have draft legislation in place. That's 76% of all countries.[5]

servicenow

Silos of data and tools lead to errors and omissions

In addition to the expanding number of data privacy regulations, organizations are also dealing with the growing volume of data across a patchwork of databases and endpoints–essentially silos of data. Unfortunately, these endpoints are becoming increasingly dispersed with remote work continuing to be the norm.

With every department or functional group managing data privacy with their own processes and tools, there is a lack of visibility, integrated reporting, and accountability at the enterprise level. For an enterprise view of privacy risk or during an audit, compliance and audit teams must piece together information across multiple departments. The task of determining what data is affected, where it's stored, and how it's used is monumental. It could take weeks, and by the time the report is completed the data is stale.

And the amount of data continues to grow. This makes it more and more difficult to not only report on compliance but also to limit the risk.

Inefficient privacy management practices:

#1. Reactive, based on new risks and regulations

#2. Lack of visibility across the growing silos of data and tools

#3. Manual processes and a lack of skilled employees can lead to errors and omissions

Manual processes can't scale

Many organizations, even if they are using commercial products, still have too many manual processes and too few skilled people doing the work to manage privacy risks. When attestations, impact assessments, notifications, and issues are all created and tracked manually it's too easy for things to fall through the cracks leading to errors, omissions, and unnecessary risk.

If organizations want to scale, It's impossible to track dates and status or communicate and collaborate with a swirling mass of spreadsheets, email, phone calls, and even sticky notes. This is especially true when you consider that regulations require organizations to ensure customer data is protected even when it's shared with third or fourth parties. The saying "You can outsource your business services, but you can't outsource the liability" is too accurate.

Does anyone remember the third party responsible for one of the many data breaches this last year? Probably not, but everyone remembers the company that was breached. It's essential to ensure third parties have the proper processing and safeguards in place to protect PI.

servicenow

What should the privacy management playbook enable?

A new privacy management playbook should focus on privacy management practices that allow organizations to embed privacy compliance and risk management into daily work and integrate it across the enterprise in real-time. This will support privacy by design concepts and protect an individual's privacy.

.

Privacy by design is a framework based on proactively embedding privacy into the design and operation of IT systems, networked infrastructure, and business practices.[6]

#1

Go from reactive

Reactive, based on new risks and regulations

To proactive

Continuously monitor controls for compliance

Train employees on best practices

Proactive management of privacy risk and compliance

Privacy management should be proactive not reactive. Fire drills are inevitable, but they should be the exception to be avoided. How?

- By continuously collecting information to spot emerging risks or identify when there is a compliance failure before it becomes an audit finding.
- A single taxonomy should be in place so everyone is speaking the same language and new regulations can be more easily imported.
- The existence of a governance framework when a new regulation is implemented would allow for controls already in place to be used to reduce redundancy–and the time it takes to test for compliance.

Having skilled employees who understand privacy practices is essential, in addition to training to ensure all employees are prepared to handle personal data. Including a record to prove employees have completed training is a best practice.

Training prepares employees to effectively do their jobs and keeps privacy teams on top of risks. Additionally, when it's not a constant fire drill, people can be more forward-looking and begin to get in front of the explosion of regulations.

#2

Go from siloed

Lack of visibility across the growing silos of data and tools

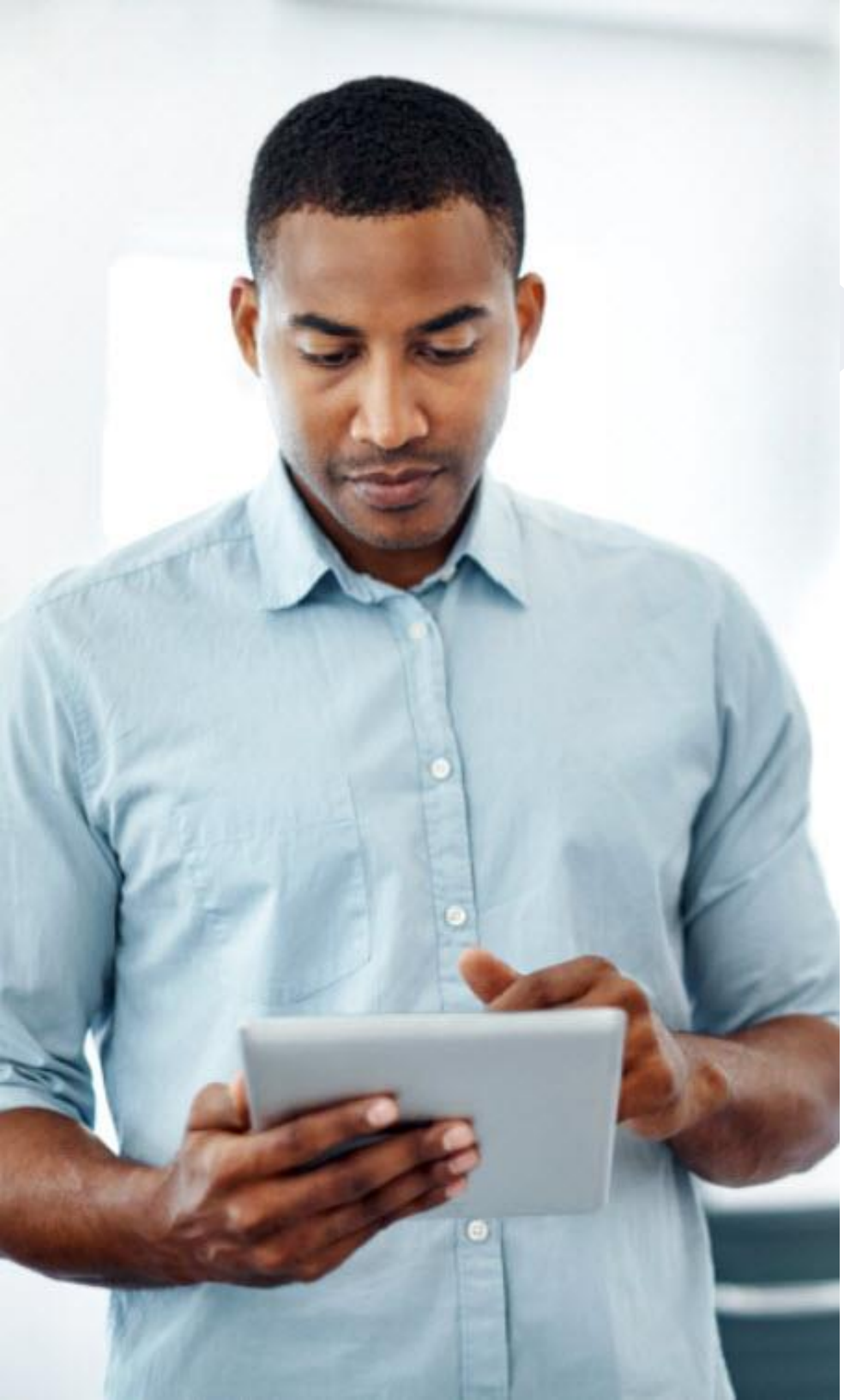
To integrated

Cross-functional workflows keep privacy top of mind for all departments

Embed privacy by design into daily work

Instead of everyone working in silos, privacy management programs should provide a central repository that supports cross-functional workflows, which could be embedded in everyday activities. In this way, privacy management can support the concept of privacy by design.

New applications, projects, vendors should be screened to determine if they process personal data during the evaluation phase, NOT after they are implemented or on-boarded. A single repository for the enterprise is key to allow for privacy or compliance teams to establish workflows that put these checks in place across the variety of departments and functional groups that are involved.



servicenow

Integrate privacy management across the enterprise

The ability to request a privacy screening assessment must be easily accessible for all application or process owners–on their mobile devices, through chatbots, and in their familiar employee portals. Only when processes that support privacy by design are invisibly embedded in daily workflows for all employees, will privacy management become a natural part of the fabric of an enterprise.

The other benefit of a platform with a single repository is the ability to achieve security by design alongside privacy by design. It's vital to build in security best practices to protect data. Using cross-functional workflows security vulnerabilities or incidents that impact personal data can effectively be communicated to privacy teams.

Additionally, providing visibility into the status of the remediation efforts is key to a strong privacy posture.

Security by design is an approach to software and hardware development that seeks to make systems as free of vulnerabilities and impervious to attack as possible through such measures as continuous testing, authentication safeguards and adherence to best programming practices.[7]

#3

Go from manual

Manual processes and a lack of skilled employees can lead to errors and omissions

To automated

Automate data lookup to make screening the exception not the rule

Smart issue management helps ensure issues with customer requests are quickly addressed

Enable the adoption of smart processes

And of course, privacy management should make employees' jobs easier so they can do more with less.

For example, if an existing application or vendor is involved in a change of process or update, automation can be used to save time. Automatically discovering whether a vendor or application accesses PI and providing an impact assessment greatly increases productivity because a screening assessment is not necessary.

Issues get addressed faster by using artificial Intelligence (AI) to assign an individual or group to work on an issue based on previous assignments. AI can also be used to group similar issues or suggest remediation tasks that have been assigned for similar issues in the past

Having a single platform and source of intelligence here is again critical. It enables cross functional workflows and access to necessary information to determine whether PI is involved. For example, using the single source of intelligence, it should be clear that PI is not mapped to Photoshop, but it will be for Slack.

servicenow

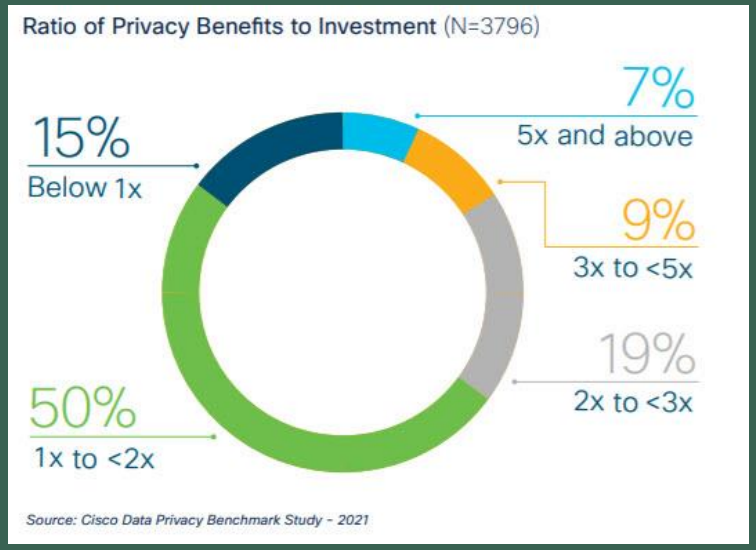
Reap the benefits

There are several benefits to having a new playbook that includes a real-time, integrated, and automated approach to privacy management.

Organizations can:

- Stay on top of privacy risks and regulations to avoid fire drills and unnecessary risks
- Unify and scale enterprise-wide data privacy governance to help ensure privacy by design is embedded across the enterprise
- Efficiently support customer data privacy rights and build trust

Doing so will create a much more mature privacy management program. A little investment in privacy practices can go a long way.



Privacy investment returns value

Organizations with more mature privacy practices are realizing much greater business benefits from privacy than those with less mature practices. Benefits range from reducing sales delays to improving a company's reputation, and of course building trust with those customers who are concerned about the protection of their personal data. According to a recent survey 35% of organizations are seeing an ROI of at least 2x and 16% are seeing 3x or above. The implication is that privacy investment continues to return significant value.

Across the six areas of benefits measured, 85% to 91% of mature organizations are realizing these benefits, compared with 68% to 74% of medium-maturity organizations, and only 45% to 55% of those with low maturity.[8]

93%

Of organizations are reporting at least one privacy metric to the board [8]

14%

Of organizations are reporting five or more privacy metrics to the board

Reporting privacy to the board

And finally, privacy management has become a business conversation at the highest levels. Today, executives are reporting privacy metrics to the board. This highlights the importance organizations are placing on privacy—and the costs, benefits, and risk it entails.

Among the most reported metrics are privacy program audit findings, privacy impact assessments, and data breaches.

Reporting at all levels of the business is easier with a comprehensive risk and privacy program that provides on-going status reports.

Next steps to building a better privacy management playbook

Below are some next steps to build a better privacy management playbook that will ultimately allow you to keep pace with the risks created by the growing amount of personal data that's generated, support increasingly complex privacy regulations, and build trust with your customers.

- Adopt a single platform and data repository
- Implement the necessary controls and indicators to continuously monitor risk and compliance, including third parties
- Embed privacy by design concepts into employees' daily workflows through service portals, mobile, and chatbots
- Automate cross-functional processes and utilize AI where you can.

Find out more about how ServiceNow can help you manage privacy risk and compliance across the enterprise at www.servicenow.com/risk

1. FinancesOnline 53 Important Statistics About How Much Data Is Created Every Day
2. Ponemon cost of a data breach report 2021
3. Gartner Security & Risk Management Summit May 18-20, 2020 Germany
4. Entrust State of Consumer Data Privacy Survey 2021
5. UNCTAD Data Protection and Privacy Legislation Worldwide
6. Deloitte Privacy by Design Brochure https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF
7. TechTarget What is Security by Design https://whatis.techtarget.com/definition/security-by-design
8. Cisco 2021 Forged by the Pandemic: The Age of Privacy, Data Privacy Benchmark Study

<< BACK