traliant

Responding to Data Privacy and Security Incidents

4 Steps to building collaboration between CPOs and CISOs

While Chief Privacy Officers (CPOs) and Chief Information Security Officers (CISOs) sit in different parts of an organization, when a data breach or incident happens — and it's a matter of when, not if — privacy and security leaders should collaborate on a holistic approach to responding to the threat.

Without aligning privacy and security teams, organizations cannot effectively prepare for and respond to ever-changing compliance risks, regulations and challenges. We've all seen what can happen when CPOs and CISOs don't share a collaborative risk management strategy.

Consider these recent examples and stats:

A big tech giant was fined just **over $400 million for its handling of children's data,** representing the second biggest fine under the GDPR (General Data Protection Regulation). In 2021, another big tech company was fined **$888 million for the way it processed customer data.**

A leading financial services firm agreed to pay **$35 million to settle charges from the U.S. Securities and Exchange Commission involving mishandling customer data**, including violating privacy rights and not protecting personally identifiable information (PII).

82% of breaches involve the human element including social attacks, errors and misuse. and **95% of cybersecurity issues are caused by human error.**

91% of companies are not prepared to meet the CCPA (California Consumer Privacy Act) privacy rights compliance requirements and **94% are unprepared for GDPR (General Data Protection Regulation).**

The cost of an average data breach **increased 2.6% from $4.24 million in 2021 to $4.35 million in 2022.**

These four steps are among the proactive measures that organizations can take to foster collaboration between CPOs and CISOs and leverage their respective expertise and experience when incidents or breaches happen.

Develop a response plan

While each organization is different, with specific security and privacy risks, a written incident response plan should cover the basics and clearly explain the company's strategy, how it supports business objectives, roles and responsibilities and procedures to follow before, during and after an incident or breach.

Along with a response plan, the other two must-haves, according to Gartner, are developing detailed guidance and playbooks for how to handle specific types of incidents, such as ransomware, and conducting practice exercises with leadership and decision-makers across the organization to test response plans and challenge participants to react to realistic scenarios they may encounter.

Define roles and responsibilities of response team members

Beyond the core privacy and security team, a best practice is to designate a coordinator or manager, who is responsible for seeing that all bases are covered, all steps are completed and progress — from detection to notification to recovery — is continuously tracked and communicated. Representatives from HR, legal, general counsel and marketing/PR should also be part of the response team — each represents a key role in ensuring a more efficient and effective response and raising awareness of privacy and security issues across the organization.

Proactive measures can foster collaboration between CPOs and CISOs and leverage their respective expertise and experience when incidents or breaches happen.

Review and update current program and plans

There are no shortcuts to being prepared when it comes to preventing and responding to data incidents, breaches and cyberattacks. Regularly reviewing plans, policies, processes and procedures helps to ensure that privacy and security programs are aligned, both in strategy and practice, with evolving compliance risks, laws and requirements.

The International Association of Privacy Professionals (IAPP) recommends evaluating privacy programs annually. This includes developing a checklist or questionnaire to help identify areas that may require changes or updates. For example, acquiring new lines of business, undergoing technology transformations, or expanding into new markets and locations are all factors that can affect your organization's privacy profile and how personal data is handled.

Communicate, educate and train

Whether you're developing your first privacy/security program and response plan or revising the current one, it's important to engage, communicate and educate stakeholders across the organization. Regular messages to all employees from the CEO and leadership team about upcoming changes, developments and threats, such as new phishing scams and other types of cybercrime can make a big difference in raising security awareness and understanding of potential risks.

And with leadership's support, conducting ongoing employee training and sending out microlearning videos throughout the year on different data privacy and cybersecurity topics is another proactive step to encourage employees to be vigilant and prevent human error – the cause of most security breaches.

There are no shortcuts to being prepared when it comes to preventing and responding to data incidents, breaches and cyberattacks.

Fail to plan, plan to fail

Private information won't remain private if it isn't properly protected and this takes a partnership between CPOs and CISOs and their respective teams. With different backgrounds, training and experiences, CPOs and CISOs have a unique opportunity to shape strategies, policies and plans to address the evolving data security and privacy risks, inside and outside the organization, that impact employees, customers, partners, shareholders and the organization's brand and reputation.

Data breach response checklist

Not all steps are appropriate in all situations.

- [ ] Verify a data breach has occurred
- [ ] Contain and mitigate the breach
- [ ] Convene the data breach response team
- [ ] Investigate the breach to collect data
- [ ] Coordinate with cyber insurance
- [ ] Report the breach to federal and state regulators and law enforcement, if appropriate/required
- [ ] Analyze the legal implications of the breach
- [ ] Develop a communications plan
- [ ] Notify third parties of the breach, if appropriate/required
- [ ] Notify affected individuals (data subjects), if appropriate/required
- [ ] Set up mitigation resources, including credit monitoring, call center services, etc.
- [ ] Provide litigation support
- [ ] Review breach response
- [ ] Review security policies and training
- [ ] Dispense advice and counsel on limiting risks and future breaches

About Traliant

Traliant, a leader in compliance training, is on a mission to help make workplaces better, for everyone. Committed to a customer promise of "compliance you can trust, training you will love," Traliant delivers continuously compliant online courses, backed by an unparalleled in-house legal team, with engaging, story-based training designed to create truly enjoyable learning experiences.

Traliant supports over 14,000 organizations worldwide with a library of curated essential courses to broaden employee perspectives, achieve compliance and elevate workplace culture, including preventing sexual harassment, DEI, code of conduct, and many more.

Backed by PSG, a leading growth equity firm, Traliant holds a coveted position on Inc.'s 5000 fastest-growing private companies in America for four consecutive years, along with numerous awards for its products and workplace culture. For more information, visit our website and follow us on LinkedIn.

Sources: IBM - https://www.ibm.com/security/data-breach; Verizon - https://www.verizon.com/business/resources/reports/dbir/; Gartner - https://www.gartner.com/en/articles/3-ways-cybersecurity-leaders-can-prepare-for-a-breach; IAPP - https://iapp.org/news/a/how-to-prepare-for-that-inevitable-data-incident/; World Economic Forum - https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education; Varonis - https://www.varonis.com/blog/cybersecurity-statistics; Cytrio - https://www.businesswire.com/news/home/20220726005290/en/Mid-2022-Research-from-CYTRIO-Shows-Most-Companies-Remain-Exposed-to-CCPA-and-GDPR-Compliance-; https://www.dlapiper.com/en/us/insights/publications/2022/1/dla-piper-gdpr-fines-and-data-breach-survey-2022/; Meta - https://www.cnet.com/news/privacy/meta-fined-400m-for-failing-to-protect-childrens-privacy-on-instagram/