If cyber attackers find their way in, this is the coverage your clients want waiting.

Key Data Breach Facts[1]

90%
of attacks are financially motivated.

1/3
of incidents were data breaches where confidential information was compromised.

65%
of data breaches stemmed from external agents, and 35% stemmed from internal agents.

70%
of system intrusion incidents come from ransomware attacks.

95%
of breached assets are servers.

A rise in social engineering attacks has been seen across nearly all industries.

Data breaches don't discriminate.

Data breaches happen all the time, to all kinds of businesses, for all sorts of reasons.

- A lost phone holding customer account information
- An email sent with unencrypted records
- Paper documents thrown away instead of shredded
- A hacker accessing confidential files

No matter the cause, they can expose a business to lawsuits, a damaged reputation and lost customers.

General Liability Choice® data breach coverage is comprehensive protection for your clients if a breach happens and prevention resources to reduce the chances.

Your clients' reputations. Their customers' data. Help safeguard both.

If your clients collect, store or use personally identifiable information (PII) like Social Security numbers, driver's license numbers, financial account numbers and medical histories, then data breach coverage should be part of their overall risk management program.

Protection. To help pay for expenses associated with a breach, we offer midsize businesses data breach protection as an optional coverage enhancement to General Liability Choice. In case you need higher limits or other coverages, our Hartford Financial Products unit offers a full range of Cyber coverages.

Prevention. We can also help protect your clients with tips to reduce the likelihood of a breach.

Solid layers of protection.

Available on a claims-made basis, General Liability Choice data breach includes:

Data breach expense coverage

Notification expenses. Notifies those whose PII was breached, and includes:

- Overtime wages of employees and the cost to hire others to assist with the notification process
- Development, preparation, production, and distribution costs of printed matter used in the notification process

Fees and costs. Includes those your clients incur for:

- Professional crisis management law firms
- Public relations or media relations firms to mitigate negative publicity after a data breach

The Hartford

Solid layers of protection. (continued)

Monitoring services. Covers the cost of providing victims with credit, fraud, public records and other alerts for up to one year.

Good faith advertising services. For radio, television, internet, or print media responses to reduce negative publicity and restore your clients' public image after a data breach.

Legal services reimbursement. For verification that your clients are complying with statutes and regulations regarding notifications when a breach occurs.

Forensic (information technology) services reimbursement. For investigation to determine the nature and extent of the data breach and what type of PII may have been accessed.

Limits up to $250,000 per claim are available. A per claim deductible applies to first party expense coverage.

Defense and liability coverage

Defense and indemnification when your clients are legally responsible for a data breach. Includes:

- Civil awards
- Settlements
- Judgments

Limits up to $500,000 per claim are available. Data breach defense and liability claims are not subject to a deductible.

Prevention resources.

As insureds of The Hartford, your clients will have access to our proprietary cyber portal which provides:

- Tips and resources to help minimize the chance for a breach and safeguard PII
- Access to state data breach laws
- Risk management tools, including self-assessments, best practice guides, templates, sample incident response plans, and data breach cost calculators
- White papers, blogs and webinars from leading privacy and security practitioners
- Up-to-date cyber-related news and events, including examples of privacy and security-related events
- Information on how to create a data breach incident response plan
- Access to a panel of third party incident response service providers and data breach experts who, for a fee[2], will:
  - » Provide pre-incident services to help protect your business before a cyber threat occurs
  - » Assist you with an incident response plan in the event of a breach or help you determine if a breach has occurred and its severity

Preparedness matters for businesses of all sizes.

They may not make the evening news, but companies with fewer than 1,000 employees are the most frequent victims of data breaches.

What the law says about notification.

No one likes to be the bearer of bad news, but when data breaches happen, your clients are required to notify their customers by law. In fact, almost all states and the District of Columbia require it.

Some mandate notification of affected individuals only. But more than half say businesses must notify third parties, too, including:

- Credit bureaus
- State attorney general offices
- State police
- State departments of consumer affairs

Your clients may even be required by law to provide victims with credit monitoring and/or ID theft protection for a period of time.

The cost for all of these services adds up to five figures quickly, depending on how many records were breached. Add in liability damages and your clients could be facing a serious financial threat to their businesses.

Learn more. Contact your underwriter or visit **TheHartford.com/mmagent** for tools and resources.

The Hartford

[1] Verizon 2024 Data Beach Investigation Report.

[2] Depending on the coverage you purchased, such fees may be paid by us up to the applicable limit.