Watering down the risk of data breaches

SUBSCRIBER CONTENT:
Dec 6, 2016, 10:15am CST

Steven Blumenthal

I've had bad experiences with water. Gushing from burst pipes and broken washing machines, water has repeatedly defied my attempts to keep it contained. But I need water, so I maintain my plumbing, use water sensibly and clean up the mess after a leak.

Why am I talking about water? Modern businesses need data like we need water. It is not feasible for organizations to stop using data or to lock their data down so it's secure, but not usable. Instead, businesses should approach data security with attention to incident prevention and response.

Businesses should maintain a strong data security posture, including conducting regular reviews of their information technology systems to identify weaknesses. Organizations in certain industries are required to engage an outside security firm to perform annual risks audits, but we recommend this for all businesses.

Just like water conservation, businesses should control their data flows. Each company should determine who has access to what data and why they have access to it.

Identifying data flows should be part of every new project, and audits should be conducted at least annually. The results of data flow analyses can be used to conduct regular maintenance on data "plumbing," including limiting access to essential personnel and "flushing" data the business no longer needs.

Data flow analyses are also good tools for developing and implementing internal data security training. Human hands are usually the culprit behind data security incidents. Implementing training programs that explain why data security is important provide information about threats and vulnerabilities and instruct personnel how to respond to incidents.

No matter how watertight a company's "data plumbing" is, data security incidents will happen. Plan for leaks by developing, deploying and practicing a data security incident response plan with these steps:

Identify the occurrence and scope.
Contain the incident and mitigate its impact.

Notify affected individuals.
Learn, evolve and mitigate any future similar incidents.

Developing an incident response plan should be a multidisciplinary effort involving a company's IT, legal, human resources and public relations teams. Drills should be used to identify weaknesses, enhance response strategies and facilitate ongoing communication among the members of the incident response team.