



Best Four Ways for SMBs to Defend Against a Breach

TechHouse researched the issue and identified the following from the 2018 IBM breach report, [accessible here](#).

The Best Protection is Prevention & Preparation



Criminal attacks cause 48% of all breaches.

Human error accounts for 27%.

System glitches cause 25%.

1. **Incident Response (IR) Team:** have a team comprising personnel from IT, legal, compliance, and stakeholders alongside forensic specialists and crisis management.
2. **Extensive Use of Encryption:** ensure that only people with a decryption key can access encrypted information. Use multiple layers of encryption simultaneously for best effect.
3. **Business Continuity Management (BCM) Involvement:** simplify crisis response with standardized communication, threat awareness, and proactive risk management.
4. **Employee Training:** teach personnel to identify common risks and utilize standard safety measures.

The Effects of a Breach on Business, Global Averages



The post-breach cost per capita averages \$151.



Breaches generated 3.4% abnormal customer churn.



A breach takes, on average, 266 days to identify and contain.

For businesses in or related to health, stop by our [webinar](#) on July 12 for a breakdown of defenses and best practices in your industry.