SHADOWHQ

INSURANCE USE CASE

Meet changing cyber policy requirements

Demonstrate compliance and cyber readiness to insurers

Cyber insurance has become a necessary part of doing business in the digital world. Businesses understand they need it to protect themselves from the nearly unlimited risk they are exposed to because of growing cyber threats. While no shortage of cyber insurance exists, the requirements to secure or renew a policy continue to intensify as insurance providers look to protect themselves as well.

RISKS OF NOT MEETING CURRENT POLICY REQUIREMENTS

- Higher premiums and increased risk of policy denial
- Difficulty in obtaining a policy or filing a claim
- Financial and business risk
- Reputational damage

The Challenge

Companies have become aware of the cost of a cyber breach, both financially and reputationally. Stakeholders continue to put pressure on company leadership to obtain relevant cyber policies that protect the business from additional risk. Yet securing these policies is challenging as insurance companies ramp up requirements to protect themselves — a result of the cost to insurers as breach payouts continue to climb.

Insurance companies are not in the business of providing easy payouts. A steady increase in cyber insurance claims have led to stricter requirements to obtain these policies. Companies seeking or renewing policies must demonstrate that they have the right incident preparedness in place, including the necessary cybersecurity measures, incident response solutions, disaster recovery plan, and crisis management policies to minimize their risk exposure and payout frequency.

The Solution

Companies have become aware of the cost of a cyber breach, both financially and reputationally. Stakeholders continue to put pressure on company leadership to obtain relevant cyber policies that protect the business from additional risk. Yet securing these policies is challenging as insurance companies ramp up requirements to protect themselves — a result of the cost to insurers as breach payouts continue to climb.

Insurance companies are not in the business of providing easy payouts. A steady increase in cyber insurance claims have led to stricter requirements to obtain these policies. Companies seeking or renewing policies must demonstrate that they have the right incident preparedness in place, including the necessary cybersecurity measures, incident response solutions, disaster recovery plan, and crisis management policies to minimize their risk exposure and payout frequency.

Appropriate insurance planning processes also ensure:

- The ability to navigate insurance application processes and meet cyber policy requirements
- Crisis readiness by supporting both the planning and execution side of business continuity planning and incident response
- Response readiness through log and documentation availability

Simplify insurance policies applications and renewals with ShadowHQ

Here's how:

- ✓ Enable better risk management by providing the right people with the visibility, tools and training they need to seamlessly navigate any crisis.
- ✓ Implement an audit trail that provides you with logs of all tasks, messages, updates, reports and time stamped files that your insurer may request.
- ✓ Access to a multi-purpose platform that goes beyond insurance initiatives to cover all of your business's incident response and preparedness planning, business continuity and crisis response and management needs.

Easily maintain and retain your cyber insurance policy

REQUEST A DEMO