

CLARITY PREEMPTS CHAOS

THE ANSWERS YOU NEED FOR BREACH PREPAREDNESS

ASK THESE FIVE QUESTIONS TO ENSURE YOU'RE READY FOR A BREACH:

1. What is our plan?

When pivoting into response mode, who will take the lead? Have roles and responsibilities across the organization been established? Does the plan include procedures for incident categorizations and possible scenarios?

2. How are we testing our plan?

This is vital to ensure the plan is effective. How often is it tested, and has it been tested since the last significant change in the organization?

3. What incident response resources are lined up?

It is helpful to have a firm—or multiple firms—on retainer. They can respond immediately with specialists in the event of a suspected or confirmed breach, and they can often help with your crises communication strategy.

4. Are we investing in cyber liability insurance?

To help mitigate risk exposure and offset costs, more and more firms are choosing to have a cyber liability insurance policy.

5. Who is our legal counsel?

Legal counsel can provide guidance to navigate the tricky notification and regulatory requirements in the case of suspected or confirmed breaches.



BREACH PREPAREDNESS CHECKLIST

- ☐ Establish and document a plan
- ☐ Identify who will take the lead on the plan
- ☐ Confirm roles and responsibilities across the organization
- ☐ Agree on the schedule and criteria to test the plan
- ☐ Test the plan
- ☐ Line up incident response resources
- ☐ Consider purchasing cyber liability insurance
- ☐ Establish legal counsel

BREACH PREPAREDNESS KEY CONTACTS

Legal Lead:

Executive Lead:

Compliance Lead:

Investigation Lead:

Incident Response Team Lead:

Incident Response Team Members (internal):

Incident Response Team Members (external):

Endpoint Analysis Lead:

Network Analysis Lead:

Backups Administration:

Systems Administration:

Communications Lead (internal):

Communications Lead (external):

Communications Approval:

Print additional copies
of this checklist:

www.rapid7.com/breach-preparedness

Learn about
Rapid7 Incident Response Services:

www.rapid7.com/incident-response

Save Rapid7's breach response line to
your emergency contacts:

1-844-727-4347 (1-844-RAPID-IR)