KAREN STEPHENS

Karen is CEO and co-founder of BCyber, an agile innovative group who works with SMEs to protect and grow their business by addressing their cybersecurity and governance risk gaps by demystifying the technical.

Surviving a breach: step one - be prepared

"We've been hacked" are not words you want to hear on Christmas Eve or the last day before a long weekend, or ever (it's called strategic timing). And with your files being encrypted at between 6,000 and 10,000 files per minute, time is not on your side.

The time to plan how you react to a ransomware attack is not after it has happened, but beforehand. People need time to think, brainstorm ideas and agree on actions and roles. These are not activities you want to undertake mid ransomware attack. You need a controlled, practiced response, and you can mount such a response only if you have time: time to plan, implement and practice.

Here are six ideas to get you started when you are planning your attack response. NOTE: this is not an exhaustive list, I am sure you can come up with many more ideas.

1. **The Dream Team:** Who is going to be involved in spearheading the response? If you're an SME it will be a combination of internal and external people. Do all team members know their roles and do you have the contact details of all members? Who is to lead and coordinate your response?
2. **Important Documents:** How do you intend to access your Disaster Recovery Plans, your Continuity or Contingency Plans when all your systems are down? And are they accessible by all team members all the time?
3. **External Support:** Many SMEs have limited internal technology support so, outsource their technology to external providers. Do you know what support they provide? Does it need to be supplemented by specialist support and/or legal advice? If the answer is yes, are they on a retainer? And do you have all their contact details?
4. **Communication:** How do you plan to communicate to the team, your staff and your clients if all your systems are down, ie there is no VoIP, email, Teams, website, etc?
5. **The Insurer:** One of the first calls should be to your insurer (if you have insurance). Do you know who to call? And who is going to be doing the calling? Does your breach response plan meet the requirements set out in your insurance policy?
6. **Desktop Exercise:** Have you practiced what you will do in the event of a breach? Have you had everyone in the same room (or teleconference) and walked through your breach action plan with them?

BCYBER®

in www.linkedin.com/in/karen-stephens-bcyber/

W www.bcyber.com.au

E karen@bcyber.com.au

twitter.com/bcyber2

youtube.bcyber.com.au/2mux