cloud managed networks

30 Via Renzo Drive, Unit 4
Richmond Hill, ON L4S 0B8
Canada

1.877.238.9944

https://cloudmanaged.ca
info@cloudmanaged.ca

CREATING YOUR BREACH RESPONSE PLAN

Doing it Now, Will Save You Thousands Down the Road.

By Jane-Michèle Clark

Unfortunately, creating a breach response plan is really about preparing for the inevitable. Equally unfortunate, less than 50% of Canadian firms have ransomware or network breach response plans in place.

Knowing ahead of time who will respond to what, and how, is critical.

Experts estimate that having a breach response plan in place can save companies hundreds of hours in recovery time – because the sooner you get started, the easier it is to contain the problem and the havoc it can wreak on your organisation.

This can often translate into hundreds of thousands of dollars in savings, too. Especially if you get sued. You are legally responsible to properly protect a person's personal data and to respond quickly and professionally in the event of a breach.

In terms of protecting the data, you will be required to prove that not only do you have facility security measures in place, but that you have taken network and device precautions in the form of firewalls, data encryption, use of different servers, etc.

You will also need to show that you have strict admin and governance policies in place related to data access, storage and backup. You must also prove your organisation has regularly-updated incident response plans that can be deployed in a moment's notice. It goes without saying, of course, that these plans must be printed out and displayed in your IT Centre, as well as having been given to everyone dealing with data security. If you are hacked, you may not be able to access your computers to figure out what to do first, next and later.

You must also provide a step-by-step guide for your other employees.

In terms of response requirements, having a preparedness plan that shows how you will reduce harm to an individual if their information is taken, will go a long way in your favour in a court of law. It may also help you with the press – something that can be important when you are not allowed to reveal specifics about the nature of your breach.

cloud managed networks

What needs to be in your plan?

- The name of the designated executive responsible for being the key decision-maker. This person will coordinate the response and act as liaison between management and the response team.
- A clear articulation of your chain of command – and who is responsible for doing what, in what order. The names of all contact people, along with their personal email (not one that is attached to your company URL), home, cell and work phone numbers must be included and updated every three months. Or less. Yes, having their company email address is important, but you do not want to use it in a breach – assuming it even possible to do so.
- In addition to the corporate people to be contacted, you need to include the names and full contact info for the following:
  - Your legal team. Yes, you need lawyers on standby for such a situation. They can guide you, especially in the area of what information falls under the category of client-solicitor privilege.
  - Third-party technical experts, including your computer forensic expert.
  - PR experts (if you use a third party).
  - The Privacy Commissioner, if applicable to your organisation/industry.
- A clear articulation of the difference between data theft, data loss, compromised devices and a network breach – and how each will be detected and identified, and by whom. This includes having clear documentation of procedures and logs that can be used to pinpoint the time and place of the breach and what transpires afterwards.
- How you will respond to physical data theft versus lost or damaged data (think natural disaster or power-related problems, etc.) versus a network breach. How you will deal with ransomware, an understanding of what your insurance company's policy is related to ransomware, and the next steps that must be taken vis-à-vis the criminal, law enforcement and your insurance company.
- An inventory of applications and other programs running on your network, along with documentation on logs that can be used.
- Define your containment and eradication procedures. You need to specify what systems need to be taken off-line or disconnected from the network, what functions need to be disabled, etc., in what situations, and by whom.
- Define the notification and reporting processes for each type of breach.
- Communications plans for informing employees, clients, suppliers and other stakeholders as well as the press.

cloud managed networks

For all scenarios, you will need to assemble a cross functional team that includes senior people from all networks used by the organisation. The team should include, at very least, IT and data experts, finance, legal and compliance, corporate communications and government affairs representa-tives.

Together, you need to consider the implications of breaches in various parts of your organisation, the appropriate steps to take – including who needs to be notified.

As you go through these tabletop exercises, something that should be done quarterly, protocols and procedures will need to be updated and your preparedness plan printed again. And again, each time you meet – with the most recent update date clearly displayed.

Would else you need to do?

- Ensure that everyone in your organisation knows what to do if a breach is suspected. According to multiple manufacturers and legal experts, even when companies do have breach preparedness plans in place, they often neglect to tell anyone outside the IT department.
- Indeed, 88% of employees report they have no idea of what to do if they are hacked.

Train your employees on how to respond by simulating a data breach and performing tabletop testing regularly.

- Run drills every quarter. Not only do you want to see if your system can be attacked, which you will know from your regular vulnerability assessment and penetration testing, you need to practice what to do if someone's device is hacked, or there is a breach on your network. After every drill, you need to reassess your practices and protocols.
- Work with a third-party expert to ensure your firm has up-to-date security software and processes in place – and that your system is monitored 24/7.
- Have robust network and data backup and disaster recovery plans in place – and test their effectiveness regularly.
- You can also visit the Canadian Centre for Cyber Security at https://cyber.gc.ca/en/ for more information.

You might also be interested in reading, "Been hacked? Here's what you must do next – 5 Steps", one of Cloud Managed Networks' blog posts.

Or visit us on Linkedin for "8 tips for handling a crisis".

If you would like help setting up your plan, or need advice related to vulnerability assessments and penetration testing.

Please contact us at info@cloudmanged.ca or (416) 429-0796 or 1.877.238.9944 (Toll Free within North America).