Gridware

THE EXPERT'S GUIDE:

MANAGING A CYBER SECURITY BREACH OR INCIDENT

29 JULY 2019

GRIDWARE.COM.AU

HOW TO MANAGE A CYBER SECURITY INCIDENT

Introduction

Maybe it's the moment you've been dreading for years, or perhaps it's a threat that you've been relatively oblivious to. Either way, your business has suffered a significant breach, and you're not quite sure how to handle it.

It's important to act quickly and carefully – making the right moves now can dramatically reduce the effects your organisation faces. The right decisions can help to limit the extent of the attack, minimise any disruptions to your business or clients, and control any potential legal ramifications.

The moments after a breach are stressful and confusing, so Gridware is here to help. We've come up with a rough guide for your organisation to follow so that it gets out of this mess with the least damage possible.

Point 0. Incident Response Plan

Ideally, your organisation will already have an incident response plan that dictates how it should respond and recover from a cyber event or data breach. Having a plan in place makes the process much smoother and easier. If your organisation hasn't already been breached yet, it should develop a comprehensive plan as soon as possible.[1]

Let's assume a worst-case scenario, that your organisation doesn't have a response plan when a breach strikes. What should it do?

1. Contain the breach (0-3 Hours)

As soon as a breach is detected, the first step is to contain it. This will limit the damage, prevent things from getting worse, and ensure that your business can get back to normal as soon as possible.

How your organisation contains a breach will depend on the nature of the breach. Before you can properly contain it, you will need to find out how it occurred, whether data is still being accessed in an unauthorised manner, who is normally able to access the data and in what manner.

Once you have this preliminary information, you can begin to take steps to stop the unauthorised data access. This can range from simple measures like taking away access privileges from malicious insiders, or it may necessitate completely shutting down the system. It's important that you don't take any actions which may destroy evidence – this could be critical in the later stages.

If you organisation has cyber cover under an appropriate insurance policy, you should consider immediately notifying your Insurer in order to comply with the terms of your policy. Your Insurer will also help you assess the claim and appoint a cyber security vendor to assist you with containing the breach. Your policy may also cover you for legal advice as a result of a security incident.

1. Australian Cyber Security Centre, 'Guide to Incident Response Plans (1 July 2019) <https://www.cert.gov.au/ci-big-business/general-guidance/guide-incident-response-plans>

2. Get Expert Assistance (3-12 Hours)

If your organisation has been breached, it may not have the right expertise to handle the situation appropriately. If this is the case, it's generally best to engage outside security specialists such as Gridware.

We can use our experience to act swiftly and make sure the breach is handled properly. Our approach can help to limit the extent of the breach, speed up the recovery and minimise any disruptions to your business.

3. Assess the Data Breach (12-72 Hours)

Once you have contained the breached, your organisation can begin assessing it in more depth. This involves finding out as much information as you can about the breach, such as:

- What logs are available in our systems, firewalls and emails?
- What type of personal information was accessed?
- What caused the breach and how extensive was it?
- How could the breach harm the affected individuals?
- How can this harm be mitigated?

Once your organisation has further insight into the breach, it will have a greater understanding of the risks and how these can be addressed in an ideal manner.

4. Review the Breach (72 hours – 1 Week)

Once these steps have been conducted, organisations should complete a thorough review of the breach. This can enhance your organisation's understanding of the problems, lead to plans for preventing similar breaches in the future, and also result in new ideas for ways to improve its response.

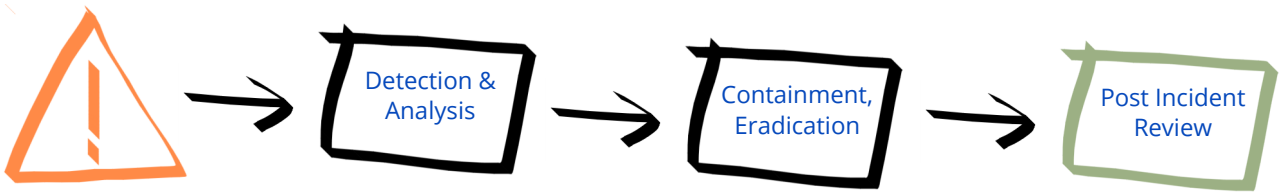
It might be worth asking:

- What controls are we implementing immediately to prevent the issue from reoccurring?
- What are the long term initiatives that we will undertake to improve our security for the future?

Gridware recommends preparing a post incident review that can be used by management, or provided to financial institutions, legal counsel, authorities or regulators if requested.

A post incident review should also include recommendations for improving the organisation's ability to withstand, respond and recover from any future incidents.

FIGURE 1. FLOW CHART OF TYPICAL INCIDENT RESPONSE PROCESS



5. Notify If Necessary (Up to 30 Days)

In certain situations, organisations covered by the Privacy Act (this includes government agencies, businesses and charities with annual turnovers of more than $3 million, among others) will be required to notify both the affected individuals and the Australian Information Commissioner.

Some regulations, such as those under the Notifiable Data Breach Scheme under the Privacy Act require reporting certain data breaches to the Privacy Commissioner within 30 days of being aware of the incident. In these cases, you may require the advice of a law firm that specialises in cyber security matters such as privacy and data breach notification legislation. More information on where to report can be found here at https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach/

It is also worth mentioning that you may have reporting obligations under the EU General Data Protection Regulations (GDPR).

If your organisation has suffered a misdirection of funds, or fraud that resulted in financial loss, you should also consider notifying your State Police and reporting the Cyber Crime to ACRON (Australian Cybercrime Online Reporting Network) at https://www.cyber.gov.au/report

Each breach should be considered on a case-by-case basis to determine whether there is a serious risk of personal harm to the affected individuals. If there is, they must be notified. Notifications should inform the individuals about what has happened, as well as how they may be affected. They should also include possible mitigation strategies, such as changing passwords or raising awareness of potential scams that may come as a result.

In cases where there is limited risk, such as if the data was encrypted, your organisation may not need to notify the individuals. These kinds of notification may cause unnecessary stress to those that receive them, or cause them to become desensitised to the risk. This is why an appropriate evaluation of the risks is so critical.

> "Recent data released by the Office of the Australian Information Commissioner (OAIC) reveals that in 2018 it received 812 notifications as part of the notifiable data breach scheme. That means that the OAIC received data breach notifications from 73 Australian companies per month, with the number of companies reporting growing by 7% each quarter."

Make the switch to Gridware

If your organisation has not yet suffered a cyber incident, you're in a good position to seek advice early about your capabilities to respond to a breach, the strength of your security controls and any gaps in processes that may be the cause of a future cyber event.

Contact us today and learn why more Australia companies are choosing Gridware as their incident response partner.

SYDNEY
Level 13
333 George Street
Sydney NSW 2000
T +61 9158 7304

MELBOURNE
Level 13
114 William Street
Melbourne VIC 3000
T +61 3 9020 7626

GRIDWARE.COM.AU