

# What is Incident Response Retainer (IRR)?

All businesses face cyber attacks. When successful, they not only cause disruption, but also allow cybercriminals to steal personal information, which can harm both businesses and their customers.

Having a plan in place to deal with cyber attacks is obviously essential. Many businesses create incident response plans to do just that. However, an alternative is to pay for the Incident Response Retainer (IRR) service.

So what is Incident Response Retainer and does your business need it?

## What is Incident Response Retainer?

Incident Response Retainer is a service agreement with a cybersecurity service provider - the contract states that if a business is the target of a cyber attack, the provider will arrange for the necessary services. to react to it.

Incident Response Retainer provides an alternative to hiring security personnel to develop an incident response plan. They are ideal for small businesses that want to prepare for such attacks but don't have their own cybersecurity staff.

## How much does Incident Response Retainer cost?

Incident Response Retainer comes in a variety of price points. Some providers charge an upfront fee while others only charge after their service is used.

### No upfront fees required

Many providers offer the service without requiring upfront fees. Simply an agreement to provide services if needed and detail what types of services are included, as well as the cost of those services.

### Prepayment required

Other providers require businesses to pay for a certain number of hours each year. These hours are then used in the event of a cyber attack. If this does not happen, those agreed upon hours can often be used for other services, such as penetration testing.

## What does Incident Response Retainer include?



Incident response tools are typically designed to provide everything needed to defend against cyberattacks. Exactly what is included will depend on the price and what is deemed necessary. Here are the main services that should be included.

### **Incident response plan**

Any IRR will include an incident response plan. This is simply an action plan to deal with common cyber attacks. The plan is usually developed in conjunction with the business's management or IT staff. Most plans will include steps the business also needs to take in the event of an attack.

### **Classification of incidents**

The IRR will include a security expert ready to categorize any potential cyberattacks. This person will answer the phone and determine if a security incident is a real attack and what to do about it.

### **Incident response**

The IRR will include a security expert or team that will respond appropriately to any attack. They are responsible for performing most of the steps of an incident response plan such as damage limitation, threat removal, and system recovery.

Incident Response Retainer will also include a detailed list of exactly what services are and are not included. Many IRRs also include a guarantee that the provider will initiate a response to an attack within a certain amount of time.

## **What are the advantages of Incident Response Retainer?**



Incident Response Retainer is an increasingly popular cybersecurity product. Here are the advantages of paying for an IRR.

### **Reduce damage**

The main advantage of the incident response tool is that it has the ability to reduce the damage caused by a cyber attack. A successful attack can cause a business to shut down for hours and personal information stolen. Incident Response Retainer is designed to reduce damage and can protect your business data in the event of a breach.

### **Peace of mind focus on business**

Having an Incident Response Retainer means you are prepared for an attack. It also allows your employees to focus on other things. If someone at the business believes an attack is going on, they can contact an expert, rather than trying to figure it out on their own.

### **No need to train or hire security staff**

Some businesses would benefit from having security on staff, but that's not always practical. Small businesses in particular often cannot afford to hire IT professionals. Purchasing an Incident Response Retainer offers a more affordable alternative. It allows a business to benefit from security expertise without paying a security specialist.

### **Price control**

Whether you choose to pay in advance or later, the price of support is clearly stated. Incident Response Retainer is very useful for companies with limited budget and want to know the price in advance.

### **Extra services can improve defense**

The upfront IRR includes the ability to hire a provider to perform additional services such as penetration testing. Many of these additional services are useful for finding vulnerabilities in the network and making attacks more difficult. Therefore, choosing an IRR and taking full advantage of the time it is in the agreement can strengthen

the security posture for the business.

## Should you hire an outside incident response service?

Whether a business should outsource incident response services depends on size and budget. Outsourcing provides a way to get professional incident response without hiring staff. For smaller businesses, this may be a more sensible fit than hiring unnecessarily full-time employees.

A large business can benefit more from having an in-house team. An internal team will only protect one business, may have more specific knowledge of the threats facing an individual business, and provide additional security services more often. .

You finished reading the article "**What is Incident Response Retainer (IRR)?**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.