INCIDENT RESPONSE RETAINER

HOW TO SAFEGUARD YOUR BUSINESS FROM A CYBERSECURITY INCIDENT

Overview

A cyber attack can strike your organization when you least expect it. Therefore, it is important to have a safeguard plan to not only minimize the threat, but also the resulting damage in the case that your business is faced with a security breach. Setting up an Incident Response Retainer (IRR) contract for your business will ensure that you are protected when it matters most.

Key Takeaways

- Learn about the various types of retainers and their benefits.
- Identify which retainer is the best fit for your company.
- Determine how to select the proper incident response firm.

LIFARS
your digital world, **secured**

CONTENTS

LIFARS
your digital world, secured

BREAKDOWN

As of 2016, 85% of companies have an existing incident response retainer, are planning to expand their service, or are planning to implement one in the next 12 months, according to a Forrester Research Survey. By choosing an IR retainer and an experienced cybersecurity firm, companies are able to improve their overall security posture by appointing breach investigations, ransomware removal, and maturity assessments.

Incident Response Retainers Defined

An incident response retainer(IRR) provides your company with a specific plan of action and a trusted partner on standby in the event of a cybersecurity incident. After the FS-ISAC's regulations were updated by Homeland Security Presidential Directive 7 in 2003, Incident response retainers have become standard practice for regulated businesses to assure the timely availability of services to investigate and prosecute threats and attacks in the cyberspace. This proactive method is typically organized in one of three types of annual contracts with differences in structure and execution. Some providers require you to buy a pre-paid number of hours to establish a relationship, but others require no financial commitment.

Retainer Benefits

1. On Demand, Fast Access
to Top IR Talent for Less Expense

2. Improve Breach Response
Due to Familiarity with your Company's Environment

3. Set Terms Ahead of Time
to Ensure Best Protection and Fit for your Business Needs

An Incident Response Retainer provides an independent assessment and a guaranteed response time to any incident that may occur within an organization, whether it's 3:00pm or 3:00am. Another benefit is that your trusted team has the background and knowledge of the company's environment, and can provide expert services without the expensive costs of hiring an internal resource.

CHOOSING A RETAINER

To determine the best retainer to suit your organizational and security requirements and business objectives, consider the following elements:

- Response Time
- Regulatory Obligations
- Budget Allocation
- Unused Hours
- Incident Escalation and Severity

Incident Response Retainer Models

1. Tier 1: Contractual Agreement
2. Tier 2: Assurance Measure
3. Tier 3: Comprehensive Model

Feature	Tier 1	Tier 2	Tier 3
Pre-negotiated terms	Yes	Yes	Yes
27/7 service	Yes	Yes	Yes
Service Level Agreement (SLA)	Yes–Best Effort	Yes	Yes
Incident Preparedness Services	No	Yes	Yes
Discounted Hours	No	Prepaid + hours as needed	Yes As needed

LIFARS
your digital world, secured

TIER 1: CONTRACTUAL AGREEMENT

"Best Effort"

This contract model is colloquially called the "Best Effort" model because time expectations for remote or onsite assistance, often detailed in an SLA, are not specified. It acts as a promise by the IR retainer to put forth its best effort in helping your organization, but doesn't prescribe the specific actions and responsibilities of the IR firm. There generally is no bidding war involved to provide services nor the ability to penalize the vendor for not responding to a phone call.

Advantages	Disadvantages
• Quick Negotiation • Emergency Security • No initial Cost • Fulfill Legal Requirements	• Lower Response Time • Not Recommended

Details

The advantage of using Contractual Agreements is that they tend to be quick to negotiate because they address the basic levels required of vendor due diligence. In this pricing model IR vendors are hired to render services, as needed, often on an emergency basis, at an agreed upon hourly rate. The "Best Effort model" is often written to easily clear the legal requirements set by a prospective client, however, the ability to demand more from the vendor, such as pre-purchasing hours, are uncommon.

Depending on the number of incidents and threat actors involved, the recommended response time varies. High priority targets facing elite cyber hackers would need the quickest SLA in order to respond to the lightning fast breaches that organized crime groups execute. Companies that face less severe threats can typically accept the risks that come with slower SLAs. Best Effort SLAs are not recommended, but they can help provide requirements for various factors, such as legal requirements, without having a high initial cost.

TIER 2: ASSURANCE MEASURE

Insurance Plan

This model is used mainly by organizations that do not have a dedicated Incidence Response team. Offering a combination of SLA and pre-purchased hours, this type of pricing plan allows your firm to address specific problems with certainty that the vendor will go beyond its best effort to resolve and fix these cyber incidents. This type of contract is modular, and the pre-purchased hours can often be used for other, non-IR related services. Any additional hours are billed at a specified rate, which is generally higher. Other services that are often included with this pricing model include resource training and a tabletop exercise to test all aspects of detection and response. A gap analysis and holistic review of your IR plan and its procedures as well as recommendations for software/hardware are also common procedure.

Advantages

All those from Tier 1 Plus:

- Pre-purchased hours at discount
- Specified incident response plan
- Transferable hours for non-IRR
- Resource training

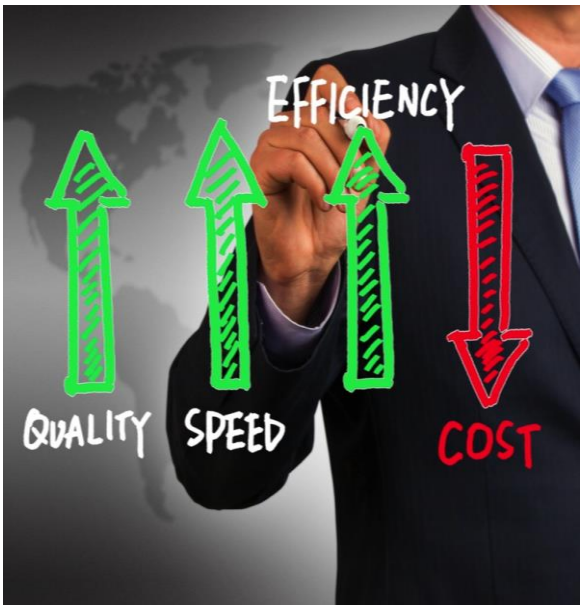
Details

What is advantageous about this type of contract is that the time for delivery is specified in the SLA and the vendor contractually agrees to fulfill phone calls as well as remote and onsite assistance. Companies interested in this type of pricing model often want a vendor to fill their need for dedicated, on-staff, IR personnel. They believe the probability of a breach is lower, or the associated fines don't justify the added costs of hiring an internal IR resource. This type of contract is great for companies that experience several large incidents a year lasting a few weeks each, as well as some smaller incidents lasting a couple of days. This is because they need the additional support for these times of increased work volume, however they do not need the number of staff to warrant internal hiring.

TIER 3: COMPREHENSIVE MODEL

Best Protection

The most comprehensive Incident Response contracts are structured to augment the capabilities of your existing, in-house staff. In this model, clients are getting SLA, pre-paid hours, and an additional team of dedicated IR professionals. The general structure allows for pre-paid hours and an SLA for on-call, remote, and onsite assistance. The pricing is agreed upon, and additional hours are usually purchased in bulk. This pricing model is similar to the Tier 2: Assurance Measure IR Retainers, but the difference is that 30-50% is allocated for pre-paid hours.



Advantages

All those from Tier 2 Plus:

- Access to advanced malware detection systems
- Network forensic investigative tools
- Secure code scanning platforms
- Threat intelligence mappings
- Endpoint threat hunting systems

Details

The advantage of this model is that you are hiring vendor staff to augment and act as an extension of your internal team. The hired response team is familiar with your internal team and its capabilities. The IR vendor provides your company with its outside expertise, toolkits, and partnerships with other vendors in the market. Having an external team can provide a set of fresh eyes to detect weaknesses that may not have been seen by the internal team due to a familiarity bias.

CHOOSING AN INCIDENT RESPONSE FIRM

Regulation

An increase in cybercrimes has spurred regional and industry-specific cybersecurity regulations and the resulting fines and penalties for non-compliance. Although most SLAs will include the core requirements of nearly all cybersecurity regulations – monitoring, management and reporting – the depth of service offered and the choice between automation and human support to fulfill contractual agreements could be the factor that saves your organization from losing money.

Companies serving the cybersecurity, digital forensics and incident response (IR) space are creating pricing models designed to highlight their core capabilities and support the business objectives of their clients. It is important for organizations looking to hire a firm to understand how pricing models support their business needs and address the dynamic nature of cyber threats.

Questions to Ask

Questions to ask when evaluating an Incident Response firm should determine if the vendor has a clear understanding of your objectives and requirements. Questions to consider include the geographic proximity of the team to the critical infrastructure of the company, how short the response time can be, and experience working with law enforcement or other government and regulatory agencies. Taking just one example, parameter of response time, could be divided to on call consultation, remote assistance and on-site time specified response. As we can see, each parameter can contain a separate call to action among the incident response team, and the enterprise under IRR coverage. It is important that internal teams' communication and strategy aligns with the IR vendor teams, and provides a path to successfully execute crises incident response forensics investigations.

THE LIFARS DIFFERENCE

Benefits of a LIFARS IR Retainer

High Flexibility

24/7 Support

Constant Communication

Customized Security Plan

We create a holistic Incident Management strategy with a detailed Incident Response plan that ensures your corporate brand integrity stays in tact in the event of any cyber-attack. With our IR Retainer, we will map out a step-by-step program together that is tailored to your organizational needs and objectives. Extra hours will be used to strengthen your company's cybersecurity posture.

Premier Response Time

When a cyber-attack strikes, time is money. An Incident Response Retainer from LIFARS guarantees a near-instant response with record breaking turnaround time. We provide superior speed and accuracy in execution. Security incidents happen, but the impact on your business can be dramatically reduced with a rapid and precise response.

Access to Our Expert Team

One of the main perks of an IR Retainer is an assigned response time that is crafted specifically for your organization, broken down by location with remote assistance included. This means we guarantee "feet on the street" as needed—the emergency team will indeed parachute to your doorstep when you need us the most.

Calculated Budget Protection

Think it's tough to capture budget before a data breach occurs? We get it, but what happens after the fact? The longstanding scramble for large sums of unplanned cash flow to remediate damages that could have been prevented is not worth the wait, or the internal argument that often ensues. Prepare for the worst with budgeted hours assigned to incident response before it's too late.

LIFARS CUSTOM RETAINER OPTIONS

Services	Description
Paid Retainer	Prepaid IR service hours to assure customer perks such as reduced hourly rates or better SLA.
Proactive IR Preparation	Services created to increase familiarity with your company in order to more efficiently respond to an incident. This includes readiness assessment, table-top exercises, and documentation reviews.
Retainer Flexibility	The capability to use other services offered by LIFARS during the term of the retainer contract.
Security Assessment	Services customized to identify issues in your organization—such as threat hunting to uncover an existing breach or penetration testing services to determine your overall risk posture.
Retainer Rollover	Allows retainer money to be used for other services after the term of the retainer contract instead of requiring that these services be used during the contract term.
Discounted Rate	A discounted rate, offered for an early contractual engagement.
Contract Only	The minimum contract level, which describes terms and conditions, but no hours have been prepaid.

LIFARS

your digital world, **secured**

Contact Us to Learn More

www.lifars.com | 212.222.7061 | info@lifars.com | Twitter: @LIFARSLLC

LIFARS is an Elite Cybersecurity Intelligence firm based in New York City specializing in: Incident Response, Digital Forensics, and Cybersecurity Intelligence.