k_Street Consulting

WHITE PAPER

Best Practices for Developing an Incident Response Plan

k_Street

Cyber Incident Response Plans (CIRP), like computers themselves, are not as simple as they seem on the surface and should be modular. When considering your CIRP, breaking sections down into smaller elements may reduce the overwhelming nature of developing a comprehensive strategy.

Please note these recommendations are meant as a general guideline. Governmental or classified data, as well as employee or customer financial data, personable identifiable information, private health information and information related to citizens of the European Union may require greater care, security measures, and response than discussed here. Please consult a lawyer to determine what regulations and laws apply to your environment.

From the start, view the CIRP as a part of a larger IT master plan and how it interacts with the other components of that plan. Next, look at the CIRP from both reactive and proactive perspectives. Events that hold the potential of data loss should be treated the same as events that have caused data loss. From there, break down your actions into the key parts of incident response: **Identify, Contain, Address, Recover, and Postmortem**. Plan for both specific scenarios as well as general responses based on resources impacted and severity of incident. After the incident itself has been resolved, what a company does next, from legal obligations to public relations, is just as crucial.

Let's go into a little more detail on what we mean by breaking your plan down into smaller, more manageable sections and how you should shape your perspective and approach when developing your plan. In the larger scheme of things, your CIRP should be a component of, and dove tail with, your grand IT Master Plan containing your policies and standards (*rules of doing things*), procedures (*how to do things*), the CIRP (*what to do when things go wrong*), and disaster recovery or business continuity (*how to recover when things go really wrong*).

The CIRP itself is also broken down in to various components. These of course need to be highly customized to the specific needs, scenarios, geolocation and regulations of each individual firm. The goal of this method is to create a decision tree that no matter who "grabs the book", they will have a

tool to help them make a decision and take action quickly. In incident response time is critical and hesitation is damaging.

The first compartmentalization of a broad CIRP is between proactive and reactive. Most people view incident response as purely reactive but it should be treated in a proactive manner as well. A user getting a new computer or a new phone is an incident. When they do so, the device being replaced becomes a potential conduit for data loss. Phones have company email, contacts and sometimes even password lists. Quite often, especially around the holiday times, the IT department is not even aware that someone has replaced their phone without taking necessary precautions. At a minimum, phones should be factory wiped before handing them down or trading them in. With new computer equipment, the former system's hard drive needs to be securely wiped before being put back into inventory or disposed of. In general, try to think of any method or medium used to transmit or store data and determine what events put this data at risk. Those are your potential incidents and need proactive responses to prevent loss.

Reactive responses are innately more urgent. The common practice for incident response breaks down into the following steps: **Identify, Contain, Address, Recover, and Postmortem**. All of these steps need to be swift but accurate. A misidentification or misdirection in action could cost time and data.

Identification of an incident can come in many forms. Hopefully it's from a deterrent employed detecting the incident as its happening so immediate action may be taken. All too often it's after the fact when the detritus of a breach is discovered (*where did that user account come from?*) or when the ramifications are felt from data being publicly released (*WikiLeaks*) or used to compromise people (*identify theft*) or compromise resources (*breaking into other systems*). Identifying is broken down into determining root cause and determining damage. It is critical to determine the actual root cause. You may be responding to "no one can access company files" when the actual incident you need to respond to is "one of our systems got Ransomware". The incident may seem to be "We're under a denial of service attack" when the real issue might be that attack is a smoke screen for the extraction of data (also known as a "sneeze attack"). Knowing the difference is key to reacting quickly and correctly.

Once the incident is identified, stop the bleeding. **Containment** can be broken down into two facets, active and passive, depending on the incident identified. If it's an active incident happening right now e.g., your files are in the process of being encrypted, data is being downloaded, or there is a denial of service attack, you might need to take dramatic action. This may be unplugging a system from the network or shutting down the company access to the Internet. But do what it takes to stop loss of data. By passive, we mean the damage has already been done. You've discovered someone has broken into your network, data was leaked, or a laptop was stolen. The response is still just as urgent, but you can be more precise in your tools and methods such as changing everyone's password rather than cutting off the Internet and stopping business.

Addressing the problem is fixing the root cause. Someone may have stolen a password and broken in. You changed all passwords to mitigate the damage, but you still need to remedy the actual cause. Was there a key logger on someone's computer? Then we'll need to scan, find out and fix it in addition to the password changes. The addressing of an incident needs to be thorough; the cause may not be the cause. In our example it may have been the key logger that gave away the password that allowed the breach, but it may have been a free game downloaded that allowed- and will allow again- the key logger to be installed.

Recovery is the most dependent upon being prepared before any incident has occurred, and arguably the one that should have the most resources and focus of a company because it's not only essential to an incident response but to overall business continuity in times of disaster. Recovery may be divided into two phases: **immediate / temporary**, and **permanent**. The goal in recovery from an incident, as it is during a disaster, is to first get the business working again- temporary, and second, to get back to a state of normalcy- permanent. If equipment or services are down, it may be temporarily running off of backup resources until the primary resources are restored. If data was damaged, it may be restoring from backups but then needing to rekey missing information until you are up to date.

During the recovery phase, keep in mind who or what is affected. Internal users? Outside customers? The company brand or intellectual property? With data breaches and compromised security, recovery is not limited to just the restoring of data or repairing equipment. Recovery may also entail addressing regulatory compliance requirements, disclosure to regulatory bodies or governmental agencies, and notification to the impacted persons and the public. In turn, this may require you to involve a public relations crisis team depending on the extent and damage to the brand. Disclosure is broken down into Authority (FBI, USSS, regulators, etc.), Impacted (customers, users, employees), and Public (news outlets). Depending on the type of data, geolocation of data, and your industry regulations, you may be required to report to governmental authorities and the users or customers that a breach has occurred within a defined timeframe and possibly provide reparations such as free credit monitoring. Any medical information covered by HIPPA, any personally identifiable information (PII), any information that could be used for identity theft, or any account information such as login names and passwords are all examples of how types of data should trigger the need for notification.

Again, when you disclose is dependent upon the type of data and regulations. The Electronic Code of Federal Regulations states that a telecommunications carrier must report a breach to both the FBI and the US Secret Service "no later than seven days" (47 C.F.R. § 64.2011). Yet, as we have seen in other cases, disclosure is not necessarily always immediately after discovery. There are several cases of high profile data breaches in which the disclosure was years after the occurrence. Had LinkedIn™ announced their data hack in 2012 when it occurred, it would have been one of the largest breaches at the time. By waiting until 2016, the loss was rather small in comparison to Home Depot™ and Target™ and subsequently damage to the brand was minimalized. Between 2012 and 2016, the incident was under internal review thus the investigation was not considered closed which would have triggered the requirement for disclosure.

Conversely, a stark contrast to the LinkedIn breach is the now infamous 2017 Equifax™ breach. In this case Equifax publically announced their breach within just a couple of months of the incident. The attackers gained access between May and July 2017. Equifax publically announced the breach September 7th 2017. Even with only a two month delay, the firm was publicly skewered for withholding information for that length of time. It is reasonable to say that the damage from the Equifax was greater in both sheer numbers of users affected and harm caused to these users, but these are just two examples to demonstrate how responses and disclosures varied. How and when you should notify greatly depends upon the laws and regulations covering your industry, the type of data affected, the officers of your company, the marketing department or a damage control public relations team perspective, and ultimately your legal counsel. Your plan will need to take in consideration these factors as well as what action to take afterwards as this type of public announcement in turn impacts the company's brand and reputation.

The last phase to an incident response is the **postmortem**. Postmortem is lessons learned, and like the rest of our steps, is done in manageable parts:

1. How did we handle the situation?

2. Can we do better? and;

3. How do we prevent it from happening again?

Postmortems are essential. They improve the process and prevent reoccurrences. Unless gross negligence was at the heart of the issue, they should not be used for finger pointing or blame as people trying to protect themselves may prevent the real causes from coming to the surface leaving your firm exposed yet again.

When composing the guide, the process itself should include setting up a round table discussion, putting together your response team, determining how to categorize incidents so you won't have to write a plan for every conceivable contingent, a step by step scenario for example and testing purposes, and directions on how to test and update the plan.

By considering how to break down your cybersecurity incident response plan into various smaller components, you will be able to easily produce a comprehensive strategy to cover a wide range of incidents.

But remember, always have good backups.

If you would like further information, or assistance with implementing any of these suggestions, please do not hesitate to contact K_Street Consulting for professional, certified, cyber security service.