Date: 03/28/19

Version 1.0

Cyber Incident Response Plan Template

# 1. 0 Purpose

To provide our members a template that can be modified for their company’s use in developing a Cyber Incident Response Plan. The plan defines how your company will respond; how to minimize damage and downtime and how to comply with regulatory reporting requirements.

# 2.0 Cyber Incident Definition

For the purposes of this document a Cyber Incident is defined as:

“an occurrence that - actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality or availability of information or an information system; or constituents a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.”

Department of Homeland Security, U.S CERT

**3.0 Types of Cyber Incidents**

There are a number of different incidents that can affect your business, and it is impossible to write a plan for each type. This plan covers approaches for common attack vectors in order to give your company advice on developing a response plan. Different types of incidents merit different response strategies. For the purpose of this plan template, the types of attack are:

* Web - an attack from a web application or service;
* Email - an attack through email attachments;
* Improper Usage - unauthorized use; violation of acceptable use policies;
* Loss or Theft of Equipment - lost or stolen equipment;
* External - removable media - compromised peripherals ;
* Fraud - cyber criminals who manipulate data to steal, conduct criminal activities;
* Brute Force - attacks via online manipulation of data or networks to destroy information or information systems.

## 4.0 Notifications

A. How and when your company is notified of a cyber incident is of critical importance, since many new data breach laws require your company to notify authorities within 72 hours of an incident. If you are a NY business covered under 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies, you are required to “notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred.”

Date: 03/28/19

Version 1.0

Cyber Incident Response Plan Template

For the 23 NYCRR 500 regulation, a cyber event is defined as:

“any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such information system.”

Since timing is so critical, document in writing what has been communicated to your company, time, date and description. Identify who will be responsible for receiving the event notification from your IT provider and ensure all employees are trained on how to handle a call notifying your company of a cyber event.

B. Under the notification section of the plan, include a description of how you expect to be notified. If you have an IT security provider, or you are obtaining services from others, and they detect an incident, you will be notified. Clearly think through who in your company should be notified, what information they should collect and what the provider recommends. If an employee notifies you that they think they believe an event has occurred, begin by collecting basic information - what systems are affected, what exactly has occurred, the time frame and who else has been informed.

**5.0 Verification/Forensics**

The next section in the plan should be devoted to attack verification. Before any action is taken in terms of further notifications, hire a forensic investigator to assess the extent of the event. A cybersecurity forensics specialist will conduct a thorough investigation to determine extent of damage, what data was stolen, what equipment was damaged, etc. The examiner will remove the affected systems, copy the hard drive image and conduct the investigation at their lab. You should expect that this investigation may take several days to weeks to complete. In the meantime, you will need to recover from the lost data/or equipment and continue to operate your business.

Once you obtain a preliminary analysis of the attack, and depending upon the extent of the incident, you may need to obtain legal advice on next steps. If personally identifiable information (PII) has been stolen, you will be required to conduct a data breach notification in your state, which also might include federal regulatory bodies. Starting the legal review of the situation at this stage would be prudent.

Concurrent with the initial legal consultation, it may be advisable to contact your insurance agent, if you have previously obtained cyber insurance. Many of the costs for breach notification may be covered in your policy.

**6.0 Containment**

After the initial forensics review, the investigator may recommend further containment activities, such as taking all activities offline, until the incident is resolved. If the initial notification from your provider (described in Section 4.A) recommends disconnecting to prevent further damage, it is imperative that the recommendation be captured and communicated correctly to the company’s decision maker. This one decision may be the single most important action taken that prevents your entire company’s system to be destroyed, requiring weeks of recovery time and additional costs.

Date: 03/28/19

Version 1.0

## 6.0 Formal Incident Notification

Upon completion of the forensics investigation, obtain a written summary from your investigator. Present the findings to your legal counsel. Your attorney will guide you on who needs to notified and the procedures in which to do so. At this time, you may consider notifying law enforcement. Additionally, your company should report the incident to the NCSS so that the incident can be reported to DHS. NCSS will share the data anonymously under our ISAO, so that your company can be protected from litigation and further legal liabilities under the Information Sharing Act of 2015.

Concurrent with the legal review, convene your crisis communication/management team and prepare an official notification to employees, customers and stakeholders. The formal incident notification should be a well-coordinated and thought-through document, since it may impact your reputation, customer relationships and stakeholders. Include if possible, your company’s improvements or recommendations from a lessons learned perspective. As an example, if you found that the company’s system was compromised via a phishing attack, you could provide examples of the email and the training you have since conducted or that you reported the event to PHISH.org, so others can learn from your mistake.

**7.0 Eradication and Recovery**

This phase includes wiping clean any hard drives that were infected, installing and/or updating software or possibly reconfiguring the network. Once an event like this occurs, and your company is offline for a few days or weeks, it might be an excellent time to reconfigure how the network is segmented and access is controlled. Thinking through an eradication and recovery approach now, may convince your leadership team to set aside funds to improve your security. Using a disaster to rebuild and make changes to improve your company’s security Is the best recovery approach to take.

Hopefully, your team has developed a data recovery and back-up plan, so that if new equipment is purchased, or the network is re-configured, your company can restore from the data that has been backed up offsite.

Include in this section guidance to the company on how the compromise will be ameliorated. If malware infected your company, wiping disks and restoring software and recovering the data may be needed. However, you will need to think about which systems will need to be brought up first and what data needs to be recovered. While there are many attack vectors and the recoveries will be different, you can lay out guide lines for your team to consider, such as:

* Reconfiguring the network to provide better network segmentation;
* Encrypt all data or all sensitive data at rest;
* Buy new equipment;
* Refresh your website;

Cyber Incident Response Plan Template

Date: 03/28/19

Version 1.0

* Hire a full time IT security professional or increase your spending on IT;
* Obtain cyber insurance;
* Have scripted notification procedures;
* Improve training.

**7.0 Lessons Learned**

In developing your Cyber Incident Response Plan, include a section on conducting a lessons learned activity for your company. The activity could be a half day event, as an offsite or a stand-down day. Conducting this activity can assist in helping your company learn from the event - what went well and what didn’t. Information learned through this activity can drive change - such as providing more training, providing more money to IT security, improving dialogue up, down and across the organization, encouraging team members to speak up and not be criticized and finding that much need energy to change the way work is done. There might be opportunities to teach others business processes that are not well understood and the data that is critical to be protected. Consider hiring an outside facilitator, document what is learned and develop an action plan to correct.

Lastly, encourage your employees to speak up. Often they are your first line of defense in reporting that something is ‘just not operating” as it should. Employees who admit they clicked on a link, should never be punished, but encouraged to speak up. We all make mistakes!

**8.0 Testing, Up Keep and Leadership Commitment**

The Cyber Incident Response Plan should be dusted off, at least once a year to make sure the plan is still valid with your business circumstances. Have your CEO sign the document. Conduct a desk top exercise once a year to test the plan and train your employees.

**9.0 Key Points of Contact**

The Plan should include a list of key personnel - their responsibilities and contact information. A crisis event is not the time to find a lawyer, or to find an electrician. At the end of the plan, list out all the possible key personnel, (and back up if possible). Verify that these individuals understand their role in the event. Update the plan yearly to ensure everyone’s contact information is correct.

# 9.0 Applicability

A. This policy is applicable to all company employees, all sites and any service that is provided at alternative sites.

Cyber Incident Response Plan Template