Date: 10/5/2019

Version 1.0

Crisis Communications Plan Template

# 1. 0 Purpose

To provide our members a template that can be modified for your company’s use in developing a Crisis Communications Plan. The Crisis Communications Plan compliments your company’s cyber incident response plan and may be modified for use for other incident types, however the what, how, why and when you communicate critical information to your stakeholders, customers and partners would be different for each type of incident. This plan focuses communication strategies for **cyber incidents** **only.**

# 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 Crisis Communications Planning Definition**

For the purposes of this document, Crisis Communications is defined as:

“P*erforming incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. Continually monitoring for attacks or potential disaster is essential. Establishing clear procedures for prioritizing the handling of incidents is critical, as is implementing effective methods of collecting, analyzing, and reporting data. It is also vital to build relationships and establish suitable means of communication with other internal groups (human resources, legal) and with external groups (other incident response teams, law enforcement).”*

Department of Commerce, National Institute of Technology Publication 800-61r2*.*

## 4.0 Notifications/Incident Handling

A. Notification. 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: 10/5/19

Version 1.0

Crisis Communications Plan Template

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. Incident Handling. Include a description of how you expect to be notified and who will be the POC in your company for the notification, and their duties of receiving the notice. 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. Clearly document the POC’s responsibilities and define who they will communicate the notice to within your company.

If an employee notifies you that they think they believe an event has occurred, begin by collecting basic information - what systems were affected, what exactly has occurred, the time frame and who else has been informed. After this notice, obtain the services of a forensic investigator to determine if an event has occurred and the extent of the impact.

**5.0 Verification/Legal/Crisis Action Team/Formal Notices**

A. Verification. The next section in the plan should be devoted to attack verification; the process; and who in the company will be involved in the investigation. If you suspect an insider may be responsible for the incident, it is important to keep the investigation private until all the facts are known and your legal counsel advises you on next steps. If an employee removal action is warranted, then there should be procedures in place as to what co-workers or customers are told based on privacy concerns.

B. Legal. In the event the forensic examination identifies that the incident reached the threshold of a formal breach notification, consult your legal counsel as to the appropriate notifications required as governed by the regulatory agencies.

C. Crisis Action Team. As part of this planning process, you may consider identifying a team in your company who will comprise your crisis action/communications team. Team members may include HR, IT lead, legal, CFO, CEO or senior management and marketing.

Concurrent with the legal review, convene your crisis communication/management team and start to prepare a draft notification to employees, customers and stakeholders. The final incident notification should be a well-coordinated and thought-through document, since it may impact your reputation, customer relationships and stakeholders.

Once the incident verification is complete, contact your insurance agent. The agent will require the summary report from the forensic examiner and the extent of the breach implications from your legal counsel. Many of the costs for breach notification may be covered in your policy. At this time, you may consider notifying law enforcement. Additionally, your company should report the incident to the NCSS so that the incident

Date: 10/5/19

Version 1.0

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.

D. Formal Notices. Formal notifications should be developed for each audience. Notify your board and full management team once legal counsel provides their recommendations on the notices. Your management team may consider hiring an outside crisis communications consultant prior to the formal notices being sent, depending on the severity of the breach and the data that was exposed. At this time you would notify the regulatory agencies.

Formal notification takes many forms, and what you communicate is different to each audience. Your company may decide to notify stakeholders and customers through a PR firm with a formal press release and through social media. These “broad messages” should be carefully crafted to communicate to your stakeholders you have the incident well in hand and are on the road to recovery.

Breach notification letters to the regulatory agencies and to your victims are different than the notices to the public. Your legal counsel will guide you on who and when these notices should be sent. Notification to your employees should also be carefully drafted, since this might be an opportunity to educate them on cyber best practices.

In preparing the formal notice your team may include information on what you are going to do to recover and include some details in the notice - such as 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 conducted as well as the fact you reported the event to PHISH.org.

E. On-going communications. When developing the Crisis Communications Plan consider developing communication strategies for 30/60/90 day post event. Notifying your stakeholders and customers of on-going actions will go a long way in confidence building. Additionally, you may need to develop and deploy an educational campaign to your employees - there are many tips and tools on our website for you to use.

**6.0 Recovery and Restoration**

This phase includes recovery and restoration. Once an event like this occurs, your company may be offline for a few days or weeks. This 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 improve your company’s security Is the best recovery approach to take.

Include in this section guidance on how the compromise will be addressed and what will be communicated to your staff and customers. Thinking through the recovery - how long it will take, what

changes you might make and what you might want to communicate is an important step that is often overlooked. Recovery items that might impact your operations and need to be communicated to your customers and employees include:

Crisis Communications Plan Template

Date: 10/05/19

Version 1.0

* Reconfiguring the network to provide better network segmentation;
* Buying new equipment;
* Refreshing your website;
* Hiring new staff;
* Having scripted notification procedures;
* Limiting roles within the company;
* Developing new policies that impact operations;
* Improved training and new employee policies.

**7.0 Lessons Learned**

In developing your Cyber Incident Response Plan and Crisis Communications 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. Communicate what happened to the company. 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.

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

The Crisis Communications Plan and 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.

# 10.0 Applicability

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

Crisis Communications Plan Template