The Need for An Incident Response Plan

In today's world, Cyber threats and attacks are becoming the norm. There is not one single business or corporation that is immune from these threats. It seems like that no matter how much an entity does to fortify its defense perimeters; the Cyber attacker will find a way to circumvent it and inflict whatever possible damage that he or she can.

Such kinds of attacks can range from the theft of confidential information and data about your customers to launching extremely sophisticated Ransomware attacks, in which the Bitcoin is the only acceptable form of "ransom payment." Consider some of these statistics:

*Over 70% of business entities have reported that they have been a victim of a major Cyber-attack in just the past 12 months;

*The automotive industry reported a 32% increase in detected incidents;

*There was a 60% increase in Security breaches in the healthcare sector alone;

*There was also an astounding 527% increase in Cyber related incidents in the power and utility industry.

These statistics further substantiate the fact Cyber-attacks can occur in any industry as well. Now, consider, some of the financial losses that are associated with this:

*The average cost of a single corporate data breach reached $3.5 million, an increase of 15%;

*Each record that is hijacked or stolen from a database costs a business on average $145.10.

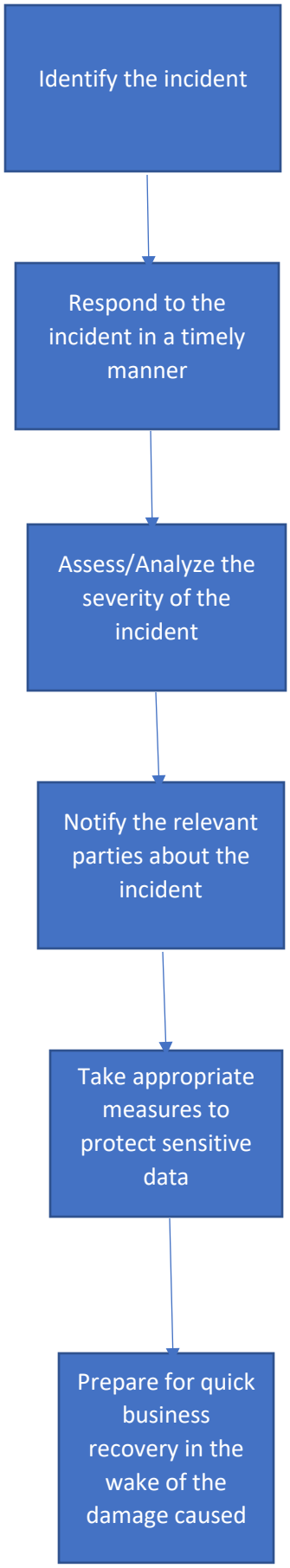
The unfortunate truth is that many Cyber-attacks are so covert and stealthy that they can often go unnoticed for a long period time. Thus, this is where Incident Response becomes absolutely critical. It can be specifically defined as follows:

"The process by which an organization handles a data breach or Cyber-attack, including the way the organization attempts to manage the consequences of the attack or the breach. The goal is to effectively manage the incident so that the damage is limited in recovery time, costs, and brand reputation". (SOURCE: 1).

However, it is important to note that responding to an incident as soon as it has been discovered becomes absolutely crucial. The above definition states that a process must be used, but it must be a defined and orderly one.

For example, there must be a clear line of communication, specific roles and duties must be assigned to each team member of the IR team, but most importantly, there must be a mechanism put into place which allows the IR team members to report back as to what they have discovered. From here, then the next action items can be quickly determined and enacted upon.

In other words, the IR process must detail how to handle just about any type or kind of Cyber-attack. This process must be viewed as literally an emergency plan (such as a step by step policy) in order to increase the chances that a business entity will be able to resume back to normal operations in a quick and efficient manner. This process can be diagrammed as follows:


Identify the incident
Respond to the incident in a timely manner
Assess/Analyze the severity of the incident
Notify the relevant parties about the incident
Take appropriate measures to protect sensitive data
Prepare for quick business recovery in the wake of the damage caused

The Risks and the Needs Associated of Going Offline

When a business or a corporation is hit by a Cyber-attack, one of the first questions that often gets asked is just how much the IT Infrastructure has been damaged, or even if the Cyber attacker is still lurking around trying to infect other systems in the process of confusion and mayhem. It is in these instances that the thought of shutting down the entire IT Infrastructure or just parts of it in order to prevent further damage comes to mind.

While this might be a tempting option to utilize, there are certain risks that are inherent with doing this, as this is often considered one of the most drastic scenarios to take. For example, in a complete shutdown, information and data might be lost that may never be recovered.

Or, if the software development team is working on a mission critical application for a customer this could mean that the source code could be lost, thus resulting in a much-delayed delivery once operations have been restored back to normal. A complete shutdown would not only greatly impact the entire organization, but its customers as well, especially if they are depending upon mobile apps in order to conduct their daily activities.

A direct shutdown can also mean that any Forensics evidence could also be lost, thus greatly impeding any subsequent investigations.

Shutting down any systems, or going offline, is greatly dependent upon the magnitude of the Cyber-attack which has just occurred, and the systems and processes that are being directly impacted. This is not a decision to be taken lightly, as sometimes it may have to be made in just a matter of minutes.

For instance, if the IT staff could quickly calculate the risk of any downtime incurred versus the time it would take to just remedy an infected system. If it is discovered that the situation can be quickly patched and there is no sensitive data that has been impacted, then there is no need to go offline.

But this is not the only permutation to take into consideration. There are others that can be taken into account by mere observation of the server logs. For example, if it was discovered that a Cyber attacker is trying to gain access to just a certain network component of the IT Infrastructure, then a partial shutdown is warranted in order to prevent this unauthorized access from occurring. In this regard, a partial shutdown is a much more preferable, and less drastic approach to take than a complete shutdown.

But there are those instances where a complete shutdown might be needed. For instance, if the Cyber-attack involved the use of malware or worms, these can be spread very quickly to other systems and can literally bring an organization to its knees. In order to prevent this from happening, it may be decided quickly to go completely offline in order to prevent the malware or the worms from causing further damage by spreading itself.

Thus, determining which systems, and processes need to be shut down or brought offline is also a direct function of their level of importance to a business or corporation. This is best ascertained by conducting a Business Impact Analysis, also known as a “BIA”.

This document will help to quantify the exact level of the importance of these assets, what they are used for, and the impact they will have to have an organization if they are indeed brought offline. The BIA can thus be used to determine if an impacted area of the of the IT Infrastructure can just be protected

while a patch is being quickly developed, or if it is better to take that particular area either partially or completely offline.

It is important to note that this decision is a combination of considering both quantitative and qualitative variables, there is no hard and fast rule for making it, and it will be unique to each and every business and corporation.

The Benefits and the Needs for Fast Time to Detect and Time to Respond Periods

When an organization is hit by a Cyber-attack, the IT Staff obviously needs to respond as quickly possible to the incident. Any wasted time will simply translate more downtime in the end, which will mean lost revenue, brand recognition damage, and worst of all, lost customers. Thus, the need for an orderly and precise Incident Response Plan is a must, and this will be reviewed in more detail later in this whitepaper.

But, responding as quickly as possible to a Cyber-attack also brings about some benefits to it as well. Some of these are as follows:

1) The downtime, if any, will be minimized. Therefore, the business or the corporation will be able to come back to full operations quickly, assuming that there is a proper Incident Response Plan put into place and that all sensitive data has been backed up properly and can be accessed efficiently and quickly. The end result is that, depending upon the severity of the Cyber-attack, the financial bottom line of the company should not be too greatly impacted. Also, responding quickly to an incident will mean that any vulnerabilities that have exploited by the Cyber attacker will be minimized, and also reduce the risk of the same incident happening to a different part of the organization.
2) Quickly responding to a Cyber threat and immediately notifying your customers as to what happened could in the long run, actually win new business. For example, when you communicate to your customer in a timely manner, it shows to them that not only do you take your due diligence seriously, but that you also care about them on a much more personal level as well. In fact, this is where many organizations fail, because many customers do not know they too have become a victim until a much later in point in time. In these instances, very often a letter is mailed out, thus leaving an "impersonal effect". So, the manner and the timeframe in which a customer is contacted can also make a huge difference. A phone call to the customer from a member of the management team shortly after an incident has taken place would leave a much more "personalized effect"; it will prove to them that by taking the time and effort to use this mode of communication you take their security very seriously as well. Thus, in the end, this personal touch will create a much more favorable, and long-lasting impression to the customer, which could bring in more repeat as well as referable business later on.
3) After an organization has been hit by a Cyber-attack, one of the key areas that will be looked into by management is filing a claim with the respective insurance company in order to be compensated for the associated costs incurred with restoring business operations. Showing your agent that you responded quickly to the incident by having a well-crafted Incident Response Plan will not only mean that you will receive your claim money quickly, but you could also receive policy discounts in the future.
4) By responding in a timely manner to any kind of Security breach, this will allow for a thorough investigation to follow in an expedient fashion as well. This will mean that evidence will still be

fresh and intact, thus allowing for any Forensics information and data to be collected quickly as well. This of course translates into evidence that will be admissible in a court of law, and which can also be used to bring the Cyber attacker to justice.

5) Typically, after a Cyber-attack, the larger corporations and businesses (such as those in the Fortune 500) might be required to release what is known "Electronically Stored Information", or also known as "ESI" for short to the Federal Regulatory Authorities and Law Enforcement Agencies. The quicker that an organization can respond to a Security related incident, the greater the chances that the ESI will remain intact, and can be produced quickly when questioned. Any delays in this regard by the entity could result in very stiff fines and penalties by the authorities.
6) Responding quickly to a Cyber-attack will create a subsequent, proactive Security mindset amongst the IT staff of any kind of organization, large or small. This in turn will lead to what is known as a "Targeted Security Monitoring" environment. This occurs when the IT staff can identify many types of Cyber threat vectors before they increase in their degree of severity, thus giving you a greater chance of mitigating them in the future. With a reactive Security mindset, not only will incident response time be much slower, but you will be forced to devote all of your resources in figuring out what exactly is transpiring to just one incident, thus leaving the organization much more vulnerable to being exposed to other Cyber-attacks at the same time.

Responding quickly to Security incident means also that the right team needs to be put into place as well at the business or corporation. The following matrix illustrates who should be involved in responding to an incident:

Title	*Role*
Team Leader	Responsible for the overall incident response; will coordinate the necessary actions that need to take place.
Incident Lead	Responsible for coordinating the actual response.
IT Contact	Responsible for communications between the Incident Lead and other members of the IT staff.
Legal Representative	Responsible for leading the legal aspects of the incident response.
Public Relations Officer	Responsible for protecting and promoting the image of the business entity during an incident response.
Management Team	Responsible for approving and directing Security Policy during an incident response.

The Importance of Communications in Incident Response

Just as much as it is important to have a clearly defined Incident Response Plan and having the Incident Response team in place, the lines of communication are also equally important. Responding to a Cyber-attack can be chaotic enough, and this does not need to be made worse by not communicating with the members of the Incident Response in a clear and succinct fashion. After all, reducing the downtime as much as possible is one of the key goals of Incident Response, and any improper communications can

only further exacerbate a tense situation even more. The importance of Effective Incidence Response communications (also known as the "Crisis Communications Plan") encompasses three key areas:

1) Communications Internal to the Business or Corporation:

By maintain open lines of communications, this will help to minimize the risk of any sensitive information from being inadvertently released to third parties. Any unauthorized release of information could impede any subsequent investigation. It will also serve as a vehicle in which to minimize any rumors or speculation as well.

One of the best methods to have good communications is to ensure that each part of the Incident Response Plan covers how information and data will be relayed amongst the team members that are responsible for that specific component of the plan. For example, the mechanisms that will be used to communicate with each other need to be clearly defined. For example:

- Will there be a central hotline for the team members to call into?
- Will there be a main command center from which all communications will be centralized and then dispersed amongst the Incident Response Team members?
- What will be the main vehicle(s) of communications-wireless devices, Smartphones, etc.? Will each member of the Incident Response Team has a dedicated device for IR communications, or will their current work issued device(s) be suffice enough?
- What will be the form of communications? For instance, will be it E-Mail, actual phone conversations, text messages, instant messages, etc.?
- How often will these lines of communications be tested in order to ensure that they will work quickly and efficiently when they are needed?

2) Communications for Compliance Related Issues:

After a Cyber-attack has occurred, a business or corporation now has to formally report to the federal authorities what exactly has happened, the extent of the damage that was caused, and which parties were impacted (for instance, customers, suppliers, other 3rd party vendors, etc.). If there is a time delay or failure to report this, it is quite possible that the organization could face severe financial penalties. In other words, this aspect of the IR communications process should be a part of the planning process, instead of making it a reactionary one. In this aspect, the legal department from the organization must also be included. For example, they can assist in determining how the affected parties should be notified, and how exactly the Security breach should be communicated. This aspect is very important, so that a violation of any regulatory or privacy requirements does not actually occur.

3) Communications with the Media:

In this aspect, the public relations department needs to be involved in any Incident Response communications. They can act as a conduit for building up a good rapport with the local and state law enforcement agencies when reporting the occurrence of a Cyber-attack. They can also help prepare the proper documents that are needed to relay information to the public such as Press Releases, announcements, and other forms of disclosure statements. It is also important to have a member of the IT staff be involved in this part of the IR communications process as well, so that they help break down all of the so called "techno-jargon" into a language that will

be easily and clearly understood by the public. It is important to note that the documents here will not contain each and every aspect of what exactly has transpired, therefore, it is crucial that the two sides (the designated PR and IT staff members) from the organization work together in a harmonious fashion to help ensure that the information which is communicated to the public is not taken out of context.

The bottom line is that by having effective Incident Response communications, an organization could actually win praise amongst customers, investors, regulatory agencies, and even the public by being open, honest, and forthright in a timely manner after it has been impacted by a Cyber-attack.

In summary, the key benefits of effective Incident Response communications are as follows:

- It will help to increase an overall sense of heighted Security awareness amongst the employees of the organization;
- It can help to mitigate the degree of severity of a Cyber-attack;
- It can help reduce the time it takes to respond to a Cyber-attack;
- It can help the business entity identify a threat before it actually happens;
- It will help to remind employees of the organization as to what matters most in a crisis situation. For example:

  *We care about our investors and customers;

  *We are responding to the Cyber-attack in a quick and timely fashion;

  *We will cooperate with investigative authorities to determine what happened who did it.

The Incident Response Communications (Crisis Communications) Plan

As we have just reviewed the three key areas in quick Incident Response is critical, it is at this point that crafting the actual Incident Communications plan becomes crucial. It is important to note that each plan will be very unique to a business or a corporation, therefore the exact requirements that needs to go into such a plan will vary.

In these instances, it could prove to be very beneficial for an organization to actually hire an outside company that specializes in creating such plans. The biggest advantage of this is that the Incident Response Communications plan will be created from an unbiased and neutral perspective.

But, the general components that should be included in this plan should include the following:

1) Identify who will be specifically involved on the Incidence Response communications team:

   In this component of the plan, it is very crucial that the right people from all of the departments of the business or corporation are selected. Once selected, all of these individuals must then understand the gravity of their responsibilities, as they must be able to respond quickly at a moment without hesitation. They key individuals that need to be included on this team include the following:

   *The CEO, CFO, and the CIO or CISO:

*A representative from the Public Relations department;

*A representative from the Investor Relations department;

*A representative from the Human Resources department;

*A representative from the Sales and Marketing department.

It is also important that at least two individuals from these respective departments should be trained in how to handle any communications or queries from the media. Also, an alternate to each representative should also be picked in case the primary representative cannot be reached during the time of a crisis.

2) Have mechanisms in place where employees can help communicate any unforeseen threats:

   In this regard, there should be an open line of communications where feedback from employees is solicited across all departments of the organization, and at all levels. The goal here is to have the ability to report any new threats and even new ideas for the continuous refinement of the Incident Response communications process to the appropriate representative of the IR Communications team (as just described). By having this particular line of communications in place, a proactive Security mindset will thus be instilled amongst all employees of the business or corporation.

3) Create and develop the messaging around the risks that have been identified:

   After the representatives have been selected and the open lines of communications set forth, the next step is to create the messaging for each kind of Cyber risk that the organization is prone to. Obviously, the details of what will be communicated to the public and other key stakeholders will vary if an organization is actually hit by a Cyber-attack. But at this point in the Incident Response Communications plan, it is important to have at least the messaging template prepared so that the designated representatives of the various departments will be able to communicate with confidence and effectiveness.

4) Create the Internal Contact Roster:

   This component of the Incident Response Communications plan is deemed to be one of the most important. After all, once a business or corporation is hit by a Cyber-attack, the first thing that will come to mind is contacting the department representatives to determine exactly what is happening and to what degree the damage is. In this regard, it becomes critical to have all of the contact information (which includes work E-Mail, personal E-Mail, work cell number, personal cell number, and even home telephone number) for each of the department representatives. All of this contact information should be documented in an easy ad quick to read format, such as that of a call tree. Also, it is important to include all of this contact information for the alternate department representative as well. The bottom line here is that all of the contact information must be up to date and confirmed at least once a month for any changes.

5) Identify and establish relationships with the key stakeholders of the organization:

Apart from communicating with employees and the department representatives, it is also equally important to reach out to the stakeholders that have a vested interest in the well being of the organization in the time of a crisis. Such individuals include the following:

*Investors and shareholders;

*Customers and business partners;

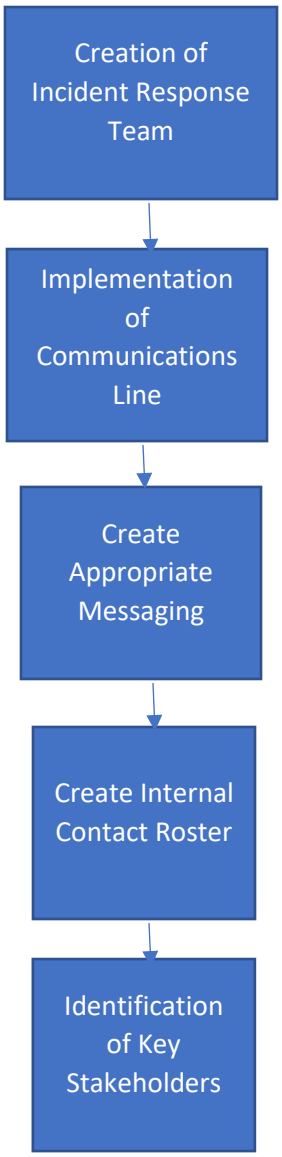
*Suppliers and distributors;

*Any relevant government official at the local level.

This particular component of the Incident Response Communications plan is an often overlooked one; therefore, it is important to include all of their contact information in the call tree as well. The call tree should be made available to all department representatives (including their alternates) and key stakeholders in printed, electronic, and online formats.

Finally, it is important for a business or a corporation to not focus on just preparing for just one type or kind of Cyber-attack. Rather, a holistic view should be taken, which will thus allow you to prepare for ***any*** Cyber-attack.

These components of the Incident Response Communications plan can be diagrammed as follows:



How to Report a Security Incident to Internal Stakeholders

As it has been discussed throughout this whitepaper, the need to respond quickly and to communicate on a real-time basis after an organization has been hit by a Cyber attack is very critical. But also, just as important is the need to communicate after the Cyber-attack has been specifically identified and it's the effects of its impact has been resolved.

After all, people will want to know what exactly has happened, the damages and/or losses it has created, and what can and will be done in the future to prevent it and similar attacks from occurring.

In these instances, it is imperative to communicate all of this to parties that are both internal to the business or corporation (such as the employees, executives, board of directors, investors – these are considered to the "internal stakeholders") as well as external (such as the partners, clients, suppliers, distributors, etc. – these are considered to the "external stakeholders").

Thus, withholding any kind of information about the Cyber attack could lead to a serious level of mistrust and misunderstandings. Therefore, the representatives of the Incident Response Team have to open and forthright as to what exactly transpired.

How this information will be ultimately disseminated to the internal stakeholders is entirely up to the organization – there is no hard and fast rule for this. For instance, it could take place as a memo, an E-Mail, or it could even be posted on the company intranet.

But in the end, perhaps having an open forum where the internal stakeholders are physically present could be the best venue to take. Taking this approach will allow for a real time Questions/Answers to take place, and also the internal stakeholders will feel that their input and suggestions will be valued and taken seriously.

But, in order to decide what will be formally communicated to the internal stakeholders, a defined process must be followed, which is as follows:

1) Triage the Situation:

   The three fundamental questions about the Cyber-attack must first answered. These are also known as the four "W's":

   *Whom specifically launched the Cyber-attack?

   *Why did the Cyber attack (in other words, what was the underlying motive)?

   *What parts of the organization did the Cyber-attack effect?

   *Where was the Cyber-attack launched from?

2) Decide the specific medium in which the internal stakeholders will be notified:

   As mentioned, this could take place either in a print, electronic, or direct person approach. But whatever the decided medium is, it is important that all messages (such as E-Mails and Texts) be kept within the Incident Response Team until the above questions have been fully answered.

3)Manage the Timing of the Communication:

In this step, the internal stakeholders need to be told the venue of how they will be informed of the Cyber-attack, and when such communications will actually occur.

4) Rehearse the message:

At this stage, it will be important to conduct a dress rehearsal of the actual message that will be communicated amongst the internal stakeholders. For example, if it is in a print or electronic form, it will be important that all members of the Incident Response Team review it carefully before it is distributed. Or, if it will be open forum based, then the presentation that will be given needs to be practiced, as well as the Question/Answer session, where it will be important to brainstorm any potential items that could be questioned by the internal stakeholders.

How to Report a Security Incident to External Stakeholders

The external stakeholders the business or corporation are primarily your customers, and even the suppliers and distributors that you currently work with. But, it is the customer that drives revenue into your business, and if their confidential information or data (these include mostly credit card numbers, social security numbers, passwords, PIN numbers, etc.) has been compromised by a Cyber-attack, not only do you have a moral obligation to notify them as to what happened, but you also have a legal one as well. a

This has been brought under the legislation know as the Data Security Breach Notification Act of 2015. This clearly states that an organization must take all precautions to protect customer data, and to inform them in a timely manner after a Security breach has actually taken place.

It also requires for entities to provide such notifications to all law enforcement and investigative branches at the federal, state and local levels. If this is not done, a business or a corporation could face very harsh financial penalties and fines, and even criminal ones as well.

But, reporting a Security breach to your external stakeholders requires a different approach than reporting to your internal stakeholders. This is primarily driven by the fact that the latter will be a much smaller group of people, versus the former, which will obviously be much larger.

As it was discussed earlier in this whitepaper, calling customers individually and notifying them as to what happened adds a “personal touch” in the communications process. Of course, this option is only feasible if you are a smaller business entity with a smaller customer base.

What protocols should be followed in notifying customers if you are a much larger business with thousands of customers? In these instances, sending out a letter to them in an expedient fashion would be the most prudent venue to take. But before the letters are drafted and sent off, very careful thought needs to be given as to how they will convey the message, that basically, their confidential information and data are at risk.

Here are the key areas that are to be considered:

1) Give very careful consideration to the tone and the voice of the letter:

In these instances, it is important to keep the language of the letter as soft as possible. In other words, it should be kept to the point, no-nonsense, and easy to read and understand. This will help to reassure your customer base that you are looking after their best interests, and that you will take care of them no matter how much efforts are needed on your part.

2) Tell your customers exactly what happened:

   There is no need to reveal each and very bit of information, but your customers have a right to know as to what exactly transpired. This includes how the Cyber attack occurred, what was impacted, and the severity of it, and what the plans are to prevent this from happening again. Most importantly, you need to tell your customers that you are working closely with investigators and law enforcement in order to track down your hijacked information/data before even further damage occurs (such as subsequent Identity Theft Attacks). Also offer to them free credit monitoring and Identity Theft protection. you are even important to include the relevant contact information so that they reach out to you with any concerns or questions.

3) Consider the audience of your customer base:

   If your business is large enough or virtual in nature, the chances are that you will probably have customers that are international as well. You may be thinking at this point, if they are in a different country, why should they be notified? The bottom line is that they are still your customer, and the fact still remains that their information and data resided on your servers; so therefore, you still have a legal obligation to inform them that their information and data are at risk. Therefore, it will be important to draft a letter in their respective language. In this regard, hiring a translator in the respective a language is therefore a must. This will ensure that any nuances in the language translation will not cause any further misunderstandings.

4) It must be understandable:

   Just as it is important as it is to communicate what exactly happened and what has been impacted by the Cyber-attack, it is also equally important that the letter be understandable to read. In other words, there is no need for the techno-jargon, keep the substantial portion (which is about the Cyber-attack) to use bold headings and bullet points. Try to keep this part down to just a couple of paragraphs. Remember, when a customer reads this kind of letter, they normally just skim it at first. Therefore, the importance of the letter and the gravity of the situation must be conveyed the first time your customers read the letter.

Finally, after the letter has been drafted into its final form, an attorney should also review it to make sure that it complies with the federal laws, as described previously in this section.

Conclusions

This whitepaper has examined the importance of the importance of appropriate and proper Incident Response to a Cyber-attack. A number of key topics were reviewed, ranging from the business need to an effective plan to how communications should be handled. In today's world, staying ahead of the Cyber attacker is much like a cat and mouse game. For example, hardly a business or corporation has recovered from a Cyber-attack, the next one is on the way or already even there.

There will really is no absolute way to prevent a Cyber attack or similar Security breach from occurring. In the end, the only thing that can really be done is to mitigate the risk of it from actually happening, and minimizing the impact of it should an organization become an unfortunate victim. It not only takes sophisticated Security technology to do this, but it also takes a great deal of human vigilance and having proactive mindset.

By having a well-defined Incident Response Plan (which also includes the Crisis Communications Plan), an entity can be at least assured that downtime will be as minimal as possible, but most importantly, that their brand and reputation will be protected as well.

Sources

1) www.digitalguardian.com
2) www.netiq.com
3) www.searchsecurity.techtarget.com
4) www.darkreading.com
5) www.technet.microsoft.com
6) www.securitymagazine.com
7) www.dpkpr.com
8) www.blog.investorrelations.com
9) www.everbridge.com
10) www.alertopps.com
11) www.businessinsider.com

Executive Summary

This is a white paper that focuses upon the importance of timely Incident Response and Communications when a business has been impacted by a Cyber-attack. The topics covered as follows:

*The Need for An Incident Response Plan;

*The Risks and the Needs Associated of Going Offline;

*The Benefits and the Needs for Fast Time to Detect and Time to Respond Periods;

*The Importance of Communications in Incident Response;

*The Incident Response Communications (Crisis Communications) Plan;

*How to Report a Security Incident to Internal Stakeholders;

*How to Report a Security Incident to External Stakeholders;

*Conclusions.