Your Trusted Partner for IT Security & Business Continuity Solutions

Combatting Cyber Risk With A Cyber Security Incident Management Program

Understanding what's at stake and how to prepare for the "What if" that would bring chaos upon the town and schools.

Prepared for: Kevin Stokes – CIO, Town Government and Public School System

Of: The Town of Brookline, MA

5/10/2017

Prepared by:

Eric C. Dunham – Hub Technical Services, LLC | IT Security & Business Continuity | 774-573-7449 | EDunham@HubTechnical.com

44 Norfolk Avenue
South Easton, MA 02375
Tel: 508-238-9887
Fax: 508-238-1146
www.hubtech.com
sales@hubtech.com

Statement of Confidentiality

This document, the correlating proposal, written and verbal relevant dialogue, and findings will be kept confidential under mutual non-disclosure agreements between the Town of Brookline, MA and HUB Technical Services, LLC.

The contents of this document have been developed by Hub Technical Services, LLC. Hub Technical Services, LLC considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Hub Technical Services, LLC. Additionally, no portion of this document may be communicated, reproduced, copied or distributed in written or verbal form without the prior consent of the Town of Brookline, MA and Hub Technical Services, LLC.

The remainder of this document depicts information intended to assist the Town of Brookline in instituting a formal cyber security incident management program.

Table of Contents

Foreword

As a culture, we continue to increase our reliance on technology in both our professional and personal lives. The rapid evolution and proliferation of technology continues to be driven by multiple factors including the increasing ease of use, the insights/advantages to be gained, and the insatiable appetites of business and individuals who simply want "more" and turn to technology as an enabler.

*The term "cyber risk" promotes a sense of delineation and subversively diverts **business risk** to be categorically dealt with by the IT Department which is a costly mistake.*

Unfortunately, too often political and municipal leaders unknowingly overlook or underestimate the risk that can manifest from the utilization of technology in town government. I've yet to witness a municipal political candidate incorporate "managing cyber risk" into their platform and I hope I never do. My reasoning is simple; the reality is that *there is only "risk" and regardless of the category,* **political and municipal leadership own risk management.**

The proliferation of technology, the dependency and critical nature as it relates to most municipal operations coupled with the multitude of threats, actors and motivations makes an incident, whether accidental or intentional, an inevitability for all organizations. With that said, municipal organizations must apply the same level of business preparedness that occurs with a natural or manmade disaster. The type and levels of incidents that can arise from the use of technology span a spectrum that ranges from "acceptable" to "life threatening" depending on the way technology is used. This is not to say technology should be avoided, rather, political and municipal leadership need to broaden their knowledge of and prepare for what they have invited unto themselves and those they serve.

If you're a political/municipal leader and question whether you should be vested in expanding the towns risk management and incident management program(s) to include technology born risk, ask yourself some basic questions and avoid the costs of contemplating them in real time like so many others have;

- *How would the organization react in the event of a data breach affecting your department?*
- *How would a ransomware payment be debated and ultimately paid if there was no acceptable alternative?*
- *What is the obligation of the town to report the event to the public? Who would be the person identified to communicate to the public?*

"If you don't know, you know" you've got work to do!

At first glance it may seem like a daunting task to protect sensitive digital assets and to a large degree it is. It's imperative to recognize that this isn't just an IT challenge, it's a business challenge that organizational leadership must take head on. Yes, leadership may relegate the technical challenges to the domain of IT staff however they cannot relinquish the ultimate responsibility of answering to those it is used to serve. Every organization can come up with a list of "what if's" and the best time to determine what happens when that "something" happens is beforehand not amidst chaos.

There are far too many examples where the stimulant for organizations coming together internally to discuss their IT risk profile is in fact a compromise or disruption of service which exposes an internal state of disarray. Today's cyber criminals' motives and means have pulled unsuspecting organizations into a multi-faceted battle to face an adversary they may have never considered in the past. These miscreants know they have a significant advantage when they engage the ill-prepared. Compounding the challenge adversaries don't need to be external nor do they need be malicious when it comes to the potential for compromising confidentiality, integrity, and availability of IT assets. George Washington once said "To be prepared for war is one of the most effectual means of preserving peace." (Jan. 8, 1790). A wise and enduring statement relevant to our digital world he never could have imagined over 227 years ago.

If you are an organizational leader make it a point to have continuous internal dialogue about what your current risk profile is with your peer group and those you rely on in IT. Ask yourself and others the question "What would we do if ____ was compromised"? If you're an IT leader ensure you're presenting identified cyber risk as a business risk, not just a need for some widget to mitigate the latest compromise circulating in the headlines. It is unlikely there will be efficient answers for all hypothetical scenarios but therein lies your starting point. You may be surprised to learn how disparate vulnerabilities can add up to an "uh oh" moment. Continue to iterate until you're comfortable detailing acceptable risk and have a well-documented action plan to follow when "something" happens.

Eric Dunham
Cyber Security & Business Continuity Practice Lead
HUB Technical Services, LLC

This page intentionally left blank

Introduction

This document has been crafted to help the Town of Brookline better understand the importance of instituting a formal Cyber Security Incident Management Program and elevate the awareness of what is involved with doing so.

What, if anything will you say when your department is breached?

To help set the context for this document consider how the town prepares for seasonal weather conditions. Winter in Brookline is a perfect example to illustrate how the town already has required disciplines in place to deal with an array of "what if's" that may occur due to weather. Imagine it is January and you ask members of Public Safety, Health & Human Services, and Highway & Sanitation the following question individually: "How is your department preparing for the next major snow storm?" You will get three different lists of things that have, or will occur independently yet in parallel, all to react to a single "what if" scenario. Additionally, those answers will likely vary if there are three inches versus two feet of anticipated snow. Next consider how the answers might be different if the budget for clearing the streets had already been exhausted and a low-pressure system moved in and the storm intensified. The point is the different departments in the town anticipate their required actions in reaction to a "what if" and can adapt to changes on the fly. Disparate groups have executed their respective roles, provide status updates to a centralized command center, information is aggregated and the public is provided an articulate update. Experience, preparation, collaboration, and executing a plan were likely to be key factors in what enabled the best possible service to the community throughout the event.

There is a very real domain of "what if's" that many cities and towns have yet to include in their incident management purview and that's in the arena of cyber threats. The utilization and dependency on technology in service to the community of Brookline is significant and when todays cyber threat landscape is considered, a formal cyber incident management program is warranted. The absence of a program that anticipates and provides a basis for navigating through cyber incidents is often due to lack of risk awareness, required cross-functional group collaboration, and the lack of a significant incident prompting action. The Information Technology department of Brookline has recognized the need for establishing such a program and realizes that it will take a concerted effort across town government to establish, maintain, and activate if/when necessary an effective program that minimizes the impacts of a compromise that eluded existing protective controls.

Incident management is not a new concept to municipalities and those such as Brookline already have effective emergency management infrastructure and procedures in place to deal with public safety scenarios ranging from natural disasters, terrorism, loss of public service(s), and many other circumstances such as snow storms. A "cyber" incident management program is like most incident management programs in that they contain similar key elements and a life cycle which ensures the program is effective when activated. For that reason, the town has a significant advantage in establishing a cyber incident management program over organizations who have yet to prepare for significant cyber incidents.

This document will illustrate at a high level:

- Why a cyber security incident management program is important to implement.

- Insights to the current cyber threat landscape.
- Who in town government should be engaged in a cyber incident management program, and why.
- A sample framework with considerations for a program.

Why is this important?

The services Brookline town government and the school district provides are vital to health and welfare of an entrusting community that funds its very existence. By law the citizens of Brookline have certain rights and therefore expectations of the town as a collective to protect "sensitive" information and ensure that technology and data acquired in service to the community is used for its intended purposes without compromise. That might be a very sobering statement but it's the reality. Put aside the hypothetical optics of a media headline depicting a cyber incident that has exposed sensitive information of the towns people and it was determined to be the inadvertent fault of someone in your department when in fact it wasn't. Consider what would happen if without warning the technology of a department or a school was unplugged and removed from the environment by an unauthorized party. In what is called a ransomware outbreak that is virtually what happens. The purpose for presenting these scenarios is not a scare tactic. They are very real states of operational crisis that have occurred elsewhere and we hear about them and others all too often. Regardless of where technology assets reside on the towns balance sheet or who manages it, it is vital for officials to personalize the fact that they have a responsibility to actively participate in the development, management, and potentially the activation of a cyber incident management program because technology is engrained in town business. Just as with a major snow storm town government will not be held responsible for the actual snow fall but you will be answerable to how it is dealt with.

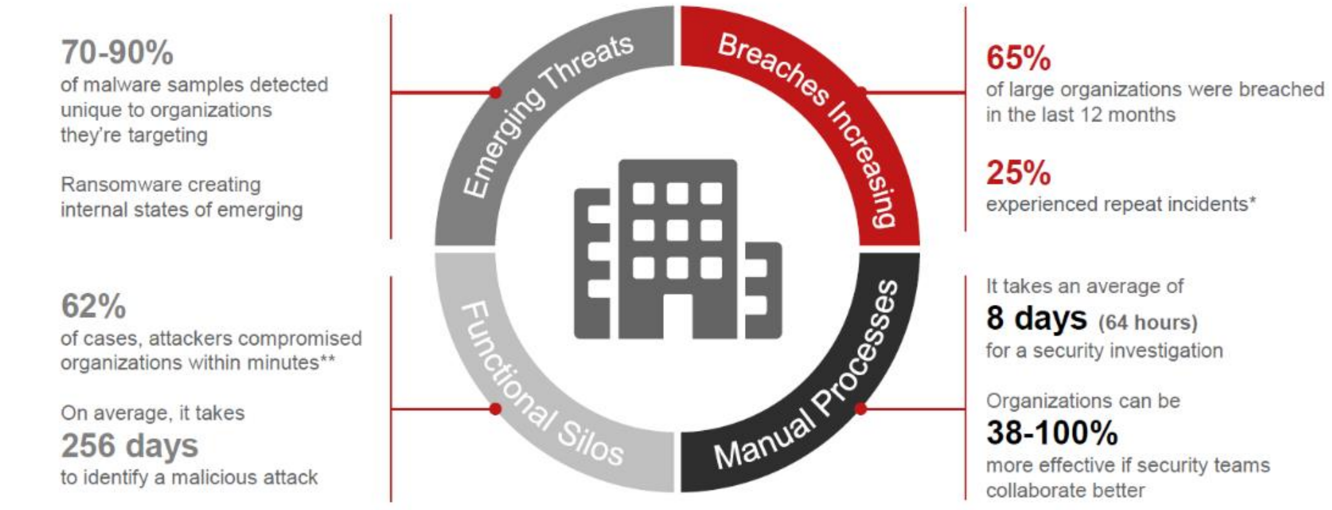
One might jump to a sense of comfort believing that the Information Technology department is there to deal with all things technology and if something were to happen "they" will take care of it. This would be an ill-conceived notion because they are not empowered to do so, nor should they be. Consider the preparation efforts of multiple departments that went into the snow storm example given earlier. In the context of cyber incident management, the Information Technology department serves as the "custodian" and "subject matter experts", not the "owner" of the towns digital assets and an endless discretionary fund. As should become evident in this document maintaining the confidentiality, integrity, and availability of the towns technology is a shared responsibility. For example, during a technology compromise incident, the IT staff members will put hands to keyboard however they won't autonomously appropriate funds to a third party electronic currency service to pay a ransom to obtain a decryption key for the towns payroll information.

This is not to suggest that non-IT employees need to become IT subject matter experts, rather department heads and key resources need to prepare for high risk "what if" scenarios. With today's threat landscape, operational best practices require acceptance that it's not a matter of if you'll experience a compromise, it's when, it could be costly, and you need to be prepared for it. It can be overwhelming, and frankly impossible to mitigate all the "what if's" when it comes to cyber security and that's exactly why an incident management program is required. Should a significant threat or incident be declared the citizens of Brookline and town government will be best served if the affected departments and others can efficiently move through the process of managing the scenario. Reflecting inwardly as yourself the question "What would happen if X happens?" If you don't have a clear understanding of how or who will take ownership of the situation there's work to do.

Understanding the threat landscape

Trying to understand all the motives and means of adversaries is futile. Believing that only one cyber incident can occur at a time is foolish, the bad guys don't take deli counter tickets and wait their turn. Often time victims are not directly targeted and only had the misfortune of encountering a threat that was dispersed into "the wild" we call the digital world. Local law enforcement will be challenged if not rendered powerless in apprehending offending cyber criminals, just consider their jurisdiction limitations. Even if State and Federal authorities are engaged their resources are limited and when they engage they must use vital time acclimating to the event before they can help. It should be apparent that this is a very complex subject that needs the attention of and very best collaborative and preparation efforts from Brookline government.

This document only serves to provide topical evidence that the development of a cyber security incident management plan for Brookline is necessary. Consider each of the insightful data points in the graphic below.



70-90% of malware samples detected unique to organizations they're targeting

Ransomware creating internal states of emerging

62% of cases, attackers compromised organizations within minutes**

On average, it takes **256 days** to identify a malicious attack

65% of large organizations were breached in the last 12 months

25% experienced repeat incidents*

It takes an average of **8 days** (64 hours) for a security investigation

Organizations can be **38-100%** more effective if security teams collaborate better

*UK Cyber Security Breach Survey, 2016 **Verizon Data Breach Report, 2015

I once had a professor state "Never has there been a time when so many knew so little about so much". While the subject matter was entirely different it is relevant to the cyber threat landscape and those who can be negatively impacted by it. The enduring challenge with cyber security is that the battlefront shifts continuously making it difficult for even those who specialize in technology to safeguard IT assets. It's not always some miscreant in a far-off corner of the world that might announce their presence with a visual indicator that they've gotten in. It's easy to imagine the adversary as some misguided student, criminal enterprise, or nation state. It's important to understand that threats and compromise can arise from the non-malicious actions of town employees as well. Bottom line, do yourself a favor and prepare for a faceless enemy that is well funded, likely to be very skilled and doesn't associate with any reasonable justification for creating the havoc they've bestowed upon you.

You might say to yourself, "We're not a bank or some Fortune 50 company, why would anyone target the town of Brookline? We're cutting budgets everywhere and don't need to consider another expense." You may think this is leading to a request for significant capital expenditures and while some may become evident after due diligence the currency of focus in cyber security incident management is "time".

From a defensive posture organizations tend to look to shrink time and adversaries will use it to their advantage by either increasing or minimizing it to suit their needs.

The time it takes to identify threats that correlate to a vulnerability which can manifest into a serious compromise is priceless to defenders. Just as important, if an actual compromise has occurred, minimizing the time to detection is critically important to eliminating further damage and recovering. On the flip side adversaries use time in different ways to achieve their objectives. In some cases, their actions are carried out quickly and discretely with a focus on minimizing the time it takes to achieve the compromise and leave the environment without a trace. In others scenarios, they will boldly announce their presence by defacing a website or splashing a message on victim's screens rendering the computer useless and look to be disruptive for as long as possible.

You might say to yourself, "We serve the community as transparently as possible, most of our information is public record that anyone can request." Admittedly, a great deal of the data the town maintains electronically is publicly available however it doesn't change the fact that the integrity of it must be maintained and there is sensitive information that must be kept confidential. Examples to consider but are not limited to; your bank account number that payroll has, a population of citizens or businesses being sent incorrect tax bills because the property values were adjusted without authorization, or maybe the names, addresses, social security numbers, and dates of birth for local veterans were stolen and sold to be used in a fraudulent manner, perhaps the personal information of families and children receiving school lunch subsidies was absconded because children's credit ratings are rarely monitored.

The variety of potential cyber scenarios that can result in discomfort, disruption, and even jeopardize public safety are only limited to the creative minds, skills, motives, and resources of an elusive subculture that is waging war against everything it encounters. As distasteful as these thoughts are they provide insight to plausible scenarios Brookline could be faced with and not be able to efficiently deal with them in turn making matters worse.

Think you're ready for an incident? Who's managing 3rd Party and Nth Party Risk?

The adage "Trust but verify" is apropos to third party relationships. At the present, there is no Town Risk/Privacy Officer, risk governance framework, or written policy pertaining to third party risk. Upon topical inquiry, it appears that third party relationships are established in an ad-hoc process absent the necessary diligence to identify, quantify, accept or divert away from risk stemming from third parties.

The critical underlying message is that third party business relationships exist and regardless of who owns the technology or who's employee(s) were at fault for a compromise, the basis for certain risk to citizens and town business has been established and needs to be incorporated into your incident preparedness and future procurement policy.

Some of the existing third party relationships secure services and others provide access to non-town-owned technology to conduct everyday business. In some cases, the risk in these relationships is centered on the storage of, access to, and use of, what is considered sensitive and/or regulated information. In other cases, it's a matter of ensuring vendors are upholding desired business standards, contractual obligations, or can restore acceptable service post-compromise in a reasonable timeframe. Be sure to include risk considerations for any device(s) a third party introduces for service delivery that can be remotely managed. Examples include parking meters, traffic lights, building automation, irrigation sprinklers, webcams, televisions, etc. It's amazing to think that even modern refrigerators and dishwashers are capable of being connected to the internet. Believe it or not, there's a potential for them to be "weaponized" and used against the town itself or others. Todays "connect everything" world has created an industry unto itself referred to as the "Internet of Things" (IoT) which has created a new paradigm of risk and incident management. If you're interested in a recent example of how 100,000+ devices were compromised and were used as the source of significant business disruption, simply do a search for "Dyn botnet" or refer to: http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.

You may be thinking "We signed a contract to outsource a particular business function, and therefore don't own any data or the technology, the vendor has the responsibility for protecting it." You may be thinking "That technology is in the "Cloud" and we don't own it therefore protecting it and the data on the platform from unauthorized disclosure is the vendor's responsibility." The reality is that the Town is likely in a position of little leverage to change existing contracts. Educate yourselves well in advance on whether you want to renew/continue a relationship, or at the least, give a business partner an opportunity to comply with your needs.

You can't assume third parties understand their own risk much less be willing to share their vulnerabilities relevant to you but that doesn't mean you avoid the topic. Even if they share sensitive insights in the comfort that the contract is signed, they may not be willing to make the necessary investments to meet your definition of acceptable risk and you should know that. It would also behoove you to understand if your third parties outsource to fourth (4th) or Nth parties. You can ask a few simple open ended questions; "Can you elaborate on how you would notify us of a compromise?", "How would your cyber insurance cover a compromise that simultaneously involves us and your five largest customers?", and if relevant, "Can you elaborate on how you're defending against situations such as unauthorized disclosure, unauthorized alteration, and unauthorized access?" These questions will start uncovering how your business partners are, or are not, protecting what's important to you.

While every one of these relationships fulfill a need they also bring about risk that the Town needs to understand and manage. The cost for not doing so can result in an array of situations such as incurring financial penalties, lost revenue, reputation damage, and most importantly the undesired disclosure of entrusting citizen's and customer's sensitive information which can manifest into a lifetime of untold distress.

There are three recommended courses of action the town should take at this stage;

- Become safer consumers. Assess the existing procurement process and ensure appropriate standardized and centralized risk vetting is factored into the process.
    - Continuously monitor and audit relationships through their duration and stipulate data destruction confirmation once a relationship concludes.
    - If the Town doesn't possess the skillset or available resources, consider taking advantage of State programs/resources or retaining a professional services firm that specializes in risk to gain a fact based understanding of risk exposure.
- Open dialogue with existing third parties and come to a consensus on what risk exists within the relationship.

    - Understand the types of data and how much of yours exists in your third party eco-system.
    - Discuss indemnification, mitigation, recourse, and compromise disclosure obligations/expectations.
    - Ensure two (2) Town parties are acknowledged in writing as the only acceptable points of contact for compromise notification; Legal Counsel, and absent an Incident Management Program Director or Risk Officer, the head(s) of Human Resources or Information Technology. These parties are also reasonable considerations for holding the initial dialogue with third party providers.
- Establish incident management protocol commensurate with the risk posed by existing third parties.
    - Have prepared external communication protocol in place for situations such as unauthorized disclosure, unauthorized alteration, and unauthorized access. This will quickly reassure the public that the Town is reasonably advocating on its' behalf.

Disclosure obligations; those that are required and those driven by morality.

We'll address two types of disclosure obligations in this section specifically legal and moral disclosures, the latter being more difficult to navigate.

Morality and the panacea of hypothetical compromises

Moral obligations must come into focus because there will likely be more scenarios where there is no legal or regulatory obligation to disclose a compromise but the sensitivity weighted against a transparency commitment to the community may obligate disclosure. Under the context of incident management, let's assume that a compromise of some sort has occurred affecting Town assets and there are no required disclosure obligations of any kind. A reaction is still necessary and any series of things may or may not happen based in part on the morality of those making the decisions at the time. There's a likelihood that moral perspectives will vary from political term to term making it even more challenging to efficiently navigate scenarios should they occur early in a new term. A documented incident management program can minimize duress, guide reactions, and in some cases, indemnify individuals from actions taken.

Morality is subjective and when you mix in politics there's bound to be varied views on the need for disclosure.

A perfect morality example is Massachusetts Data Security Law M.G.L. c.93H and regulation 201 CMR 17.00. While "indications" are, municipalities are exempt from this law the Town needs to prepare for an incident that would violate this law. Effectively this law establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records concerning residents of Massachusetts. Should any "non-municipality" be in violation there are significant ramifications so there is a precedent to head. A common misperception about this law is that it's only about encrypting sensitive data and the disclosure requirements are overlooked and sanctions are vaguely described at best in the law. Town officials must ask the question of itself, will the town report itself and follow all requirements that commercial business must, or, will the extent of the unauthorized disclosure determine the Towns action? Does the town know if the State will impose sanctions if it reports itself, what can be anticipated, is it even legally possible? It's better to gain those insights now rather than during or after a scenario. I will pass along the same advice I was given by the Massachusetts Attorney General's office when I called to ask for clarification on municipality exemption…

“consult with your legal counsel”. As of January 3, 2017 data breach notifications violating 201 CMR 17.00: Massachusetts Data Security Law M.G.L. c.93H are now posted online and can be viewed on the MA Consumer Affairs and Business Regulation website available at: http://www.mass.gov/ocabr/data-privacy-and-security/data/data-breach-notification-reports.html. Don’t be surprised when you see “exempt” parties on the list. Clearly the current State administration has set a public-sector precedent in the Commonwealth. Provided as a non-official reference, you view the verbiage of 201 CMR 17.00 in the Appendix of this document.

The organization will need to overcome the challenge of selecting a starting point in the panacea of hypothetical morality-based scenarios. A reasonable reference to help set priorities are the laws and regulatory requirements the private sector is bound to and recent news headlines. As part of the incident management programs regularly scheduled reviews it is advised to dedicate time to ensuring the “morals-dependent” incidents and protocols still align to current municipal key stake holder principles.

Learn from what others do

Legal and regulatory obligations are for the “most part” binary, meaning there is a standard or applicable law and if broken there are penalties and obligations with known parameters. This makes it a fair bit easier for organizations to align their focus and resources to avoid undesirable scenarios.

Widely known yet commonly misunderstood examples of State and Federal laws are:

- 201 CMR 17.00: Massachusetts Data Security Law M.G.L. c.93H
- Health Insurance Portability and Accountability Act (HIPAA)
- Family Educational Rights and Privacy Act (FERPA)
- Massachusetts Dispositions and Destruction of Records Law M.G.L. c.93I

201 CMR 17.00: Massachusetts Data Security Law M.G.L. c.93H

Take CMR 17 for example, while the Town is not obligated to this law that doesn’t mean it should be ignored. The town should consider the law as a best practice and make reasonable efforts to self-impose the requirements and objectives on itself to protect those it serves. If a 201 CMR 17.00 violation were to occur in any commercial business such as one of the Towns contracted third parties that utilizes “personal information” of Massachusetts residents, they have a very prescriptive process to follow and will incur legal sanctions. Familiarity with this law will also aid the Town in vetting and reviewing third parties you entrust to provide a service.

While municipalities are exempt from this law, your non-government business partners must abide by it. It’s worth noting no one is proactively auditing these parties for compliance on your behalf so it’s up to the town to conduct due diligence before and during any relationships. It’s recommended the Town regularly look through the MA Consumer Affairs and Business Regulation website mentioned above to determine if any of its service providers appear on the list.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) is a commonly known federal law that is often discussed in terms of protecting sensitive information. Per the U.S. Department of Health & Human Services the

Town (inclusive of the school district) is not bound to this law. That is because in that it is not considered a "covered entity" such as a Health Plan, Health care clearinghouse, or Health care provider. Further details are available in Appendix X. Once again we have a law that defines sensitive information and the need to protect it. The town should understand if it collects, maintains, or provides access to such information and take a lead from the law to protect it.

Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) Electronic Code of Federal Regulations: Title 34, Part 99 is federal law that governs student education records and the towns school district is obligated to this law. The laws intent is to prevent the unauthorized disclosure of certain student records and grants parents the rights to access their child's records and request they be amended. The rights granted under this law transfer to the student at the age of 18 or upon entering a post-secondary institution at any age.

The law is applicable to educational institutions/districts, and extends to third parties acting on behalf of an institution, that receive federal funding from programs administered by the US Department of Education (US DoE). If the educational institution/district does not receive funding from the US DoE then it is not obligated to the law but should adopt the governance as a best practice.

Education records are records that are directly related to a student and that are maintained by an educational agency or institution or a party acting for or on behalf of the agency or institution. These records include but are not limited to grades, transcripts, class lists, student course schedules, health records (at the K-12 level), student financial information (at the postsecondary level), and student discipline files. The information may be recorded in any way, including, but not limited to, handwriting, print, computer media, videotape, audiotape, film, microfilm, microfiche, and e-mail. (Source: 34 CFR § 99.2 "Education Records" and "Record")

There are two actions every DoE funded institution/school district needs to take;

- Annually inform enrolled student parents of their rights under FERPA
- Determine and provide public notice of what is referred to as "directory information" which the institution/district considers exempt from FERPA regulation.

More information on these two actions is provided in Appendix E – Family Educational Rights and Privacy Act (FERPA) Must Do's of this document.

For an institution to disclose directory information without prior consent, an institution must provide a notice of directory information that includes: (1) the types of information that has been designated directory information and (2) the student's right to refuse to allow any information to be designated as directory information (including the time period the student has to make that request in writing)

It's important to note that Section 34 CFR §99.32(a)(1) of FERPA stipulates recordkeeping requirements which would encompass documenting a "breach/non-authorized disclosures" however there is no obligation to report a breach to any authority or party under the law.

In terms of incident management, the school district would want to actively investigate the cause and extent of the compromise, document findings, and take corrective actions. Notifying the affected parties or making publicly known the fact that a FERPA-centric compromise has occurred falls under the category of "moral obligation". If the DoE Family Policy Compliance Office were to investigate a complaint or suspicion of unauthorized disclosure and determine a confirmed violation has occurred, it could result in the loss or suspension of all US Department of Education funding.

Massachusetts Dispositions and Destruction of Records Law M.G.L. c.93I

Massachusetts Dispositions and Destruction of Records Law M.G.L. c.93I is applicable to the Town. This law sets the standard for the disposal of records containing personal information. The Town needs to identify where this information resides and who has access to it to ensure comprehension of the requirements and safeguards that must be taken pertaining to that information. As defined in this law, personal information is a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to the resident:

a) Social Security number;
b) driver's license number or Massachusetts identification card number;
c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password that would permit access to a resident's financial account; or
d) a biometric indicator.

If for instance the Town uses a third-party technology platform on a subscription basis for maintaining and managing the towns payroll who is liable if a breach were to occur? In terms of incident management in this case it doesn't matter. The Town needs to manage the scenario and reassure the community that it is competent and advocating for its' citizens because the Town will be held accountable for selecting that provider.

Section 2 of the law indicates "Any agency or person who violates the provisions of this chapter shall be subject to a civil fine of not more than $100 per data subject affected, provided said fine shall not exceed $50,000 for each instance of improper disposal. The attorney general may file a civil action in the superior or district court in the name of the commonwealth to recover such penalties."

Moving forward, one of the things that is often overlooked upon contract negotiations and extensions is a provision to destroy all "sensitive" data upon termination of a relationship. Vendors will indemnify themselves and limit their liability at every opportunity so the Town needs to ensure legal expertise is inspecting fine print to make sure terms and conditions meet your requirements and demand missing provisions are included.

Who should be involved with the Brookline cyber incident management program

The earlier examples of "disclosure obligations" should be considered yet another indicator that cyber incident management is a team sport. The wide array of specialized domain knowledge calls for more than just a "cyber" skillset. Once an organization has consensus that a cyber incident management program is warranted determining who should be involved is the first significant challenge the body will face. Unlike a private commercial organization where there tends to be clear chain of command and declarations of responsibilities can be made without explanation, a municipal environment has a host of nuances that need to be addressed in building the program team. The organizational structure of Brookline town government has been deliberately and democratically structured to meet the functional needs of the community however this segregation can foster a cultural detriment when it comes to incident management.

In terms of a cyber incident management program, the culture needs to acknowledge that the operational autonomy of each department and committee needs to be consolidated under a single program director, with an oversight body, when a threat or compromise is discovered. Continuity and consistency are keys to being prepared for the "what if" scenarios that occur without notice. Starting with the role of a program director is critically important for many reasons including having a consistent single point of contact for determining whether the program requires activation, declaring a formal incident (which may have legal ramifications), overseeing the coordination of response resources, officially transitioning through the stages of the program, approving internal/external communications, declaring the incident/investigation conclusion, and ensuring post-incident activities take place, etc. Imagine if local law enforcement had to gain a consensus vote on next steps to deal with a received bomb threat. That's a dramatic example however it illustrates the importance of being able to act quickly, consistently, and deliberately. In a cyber incident scenario seconds' matter. The time for acquiring consensus is during the development of the protocols of the program with key stake holders. Because it is impossible to predict and plan for every "what if", it would be reasonable to consider documenting protocols which defer decision consensus to a combination of the program lead and the oversight body. Regardless of the decision-making process it needs to be documented so there is clear guidance available for key stake holders when needed.

Beyond a Program Director, seated program team members should include members of the IT department, Human Resources, Legal Counsel, the Comptroller's Office, Superintendent, Community Relations (including social media personnel), and the Town Administrator or a form of Selectmen representation. Ensure there are open channels of dialogue, potentially even team participation, with/by existing incident management teams such as the towns Emergency Management Team and potentially third party technology/data processing service providers (under non-disclosure). The program roles of each of the aforementioned vary but each plays a significant and necessary role in most if not all cyber incidents that the program will address.

With regards to which of Brookline's functional groups to include in the program, all should be considered. Determining factors should include, but are not limited to, the dependence on technology and the sensitivity of information created, accessed, or stored by the group. While one group may "own" a technical asset such as a data set, another group may heavily depend upon it and should have at a minimum visibility to how those assets are encompassed by the program and ensure all dependencies are known. Discussions of asset ownership and to what degree the program should address the asset can become "uncomfortable". This is a reaffirmation of the need for a single program director and why the program itself is needed before the "what if" incident.

While each functional department/committee has leadership, those individuals may not be the right candidate for team participation. There may be groups within town government that simply don't rely directly on technology but that will be vetted once internal program dialogue begins. Collaboration amongst functional leadership on a formal mission statement for the program is a good idea to raise awareness of the program and serve as a reference for identifying and filtering group participation and team member candidates. Now is the time to get the politics out of the way and ensure program commitment. Once team members are identified, their written job descriptions need to amended and acknowledged in written form. The program documentation should clearly articulate the roles and responsibilities of each team member and be in concert with updated job descriptions. The same holds true if secondary/back-up personnel are designed into the team structure. Additionally, appropriate measures should be prepared in the event of a failure to perform duties by all team members including the program director. Personnel compensation and union implications are beyond the scope of this document but will likely be talking points to prepare for.

It's important to understand that an effective program takes time to institute and it should be phased into the organization. Starting with a couple of groups is likely to uncover unforeseen nuances that others can address more efficiently or avoid if necessary. Technology expertise is not a pre-requisite for members to play a vital role in the team. Keep in mind the IT department serves as the technical subject matter experts and most team members will have been seated to make respective department business decisions and serve as a liaison. Think of the snow storm example and consider the individuals beyond the actual snow removal team that were involved with managing through the event on the community's behalf.

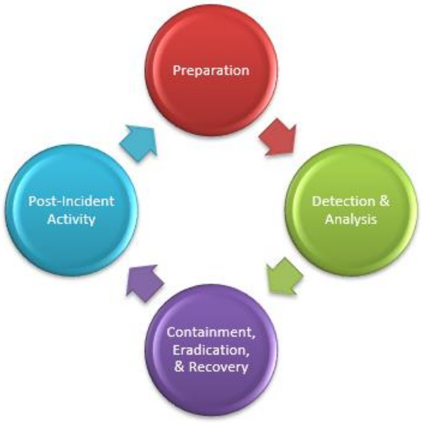
This program will clearly be a deviation from day to day workflows for all that participate. Empowerment, commitment, and a willingness to think about the business operations of the town is paramount for the program to be effective. At core of the program is a challenge to take on the "what if". Pick your team members carefully!

The Cyber Security Incident Management Program

Conceptually the organization will identify levels of acceptable risk related to things such as key assets, business process/service, and even circumstances impacting human welfare where technology is relevant. The program is intended to enable the town to effectively cope with significant cyber-related threats and incidents by organizing people, process, information, and technology in advance of unacceptable condition(s) occurring. The program will serve as a formal guideline when either control(s) are non-existent or they have been compromised and help with recovering to an acceptable state and finally, provide insights to mitigating the scenario from occurring again.

To be efficient, the program should follow a continuous life cycle that incorporates four key phases including;

(1) Preparation
(2) Detection & Analysis
(3) Containment, Eradication, and Recovery
(4) Post-Incident Activities.



Cyber Security Incident Management Program Lifecycle

The degree the program addresses "what if's is wholly dependent on what the towns acceptable risk is and what resources it's willing to commit to combatting compromise on a continuous basis. It goes without saying that efforts should initially focus on what would be considered high-value/high-risk targets and follow a prioritized plan of inclusion. It is not possible to pre-empt all possible threats and compromises so there should be protocol for "Beyond Program Scope" scenarios. Due to the fluid nature of internal and external factors such as the threat landscape, introduction/retirement of technology, and personnel, conditions that trigger program evaluation/revision should be identified and an overall assessment scheduled on a regular basis.

It must be stated that due to the sensitive nature of the program heightened discretion surrounding the program must be adhered to. Target reconnaissance is a known tactic employed by many cyber adversaries. Nearly all program information, team communication, and artifacts generated must be kept in the strictest possible confidence and used in a secure manner. Forensic and legal (prosecution and liable) positions may become a reality with some situations. Also, consider utilizing secure external storage, communication/collaboration vehicles for the program and team members. If the towns traditional voice/email and storage environments have been compromised the program may be rendered ineffective. Seek the advice of the towns legal counsel with regards to "discoverable" matters.

It is important to note here that the service acquired to generate this document was scoped to introduce cyber incident management and provide high level insights through the "Preparation" phase to determine the interest level of Brookline town government for a cyber incident management program.

Preparation

The initial phase of a Cyber Security Incident Management Program, preparation, is a laborious process that often calls on individuals to invest their time in a way they likely haven't. There is a tremendous amount of information that needs to be gathered as will be exampled later in this document. The degree of commitment to this stage will weigh heavily on the program's effectiveness. Preparation includes workflows specific to information gathering, program construction, internal training, scheduled and/or change-driven program validation and finally, launching the program.

To accelerate the information gathering process, a portfolio of standardized information gathering templates have been provided to the IT department already. The remainder of content in this topic will provide insights to each of preparation phases workflows.

Information Gathering

A sound starting point for developing an Incident Management Program is gaining an understanding of the organizations operating structure. Collecting commonly available information up front, such as organizational charts and identifying key stakeholder's helps set the stage for orienting the program. It is critical to engage the right people to define the scope of the program, a mission statement, and obtain all required investments (human & financial) for the programs development, successful utilization, and continuous evolution.

Collect information such as:

- Organizational Charts
- Business Key Stakeholders

- Identify the Program Director, oversight body, and team members
- Internal & External Specialty Functional Role Contacts
- Technical Key Resources

Understanding how and where the organization operates will provide initial context for key considerations in how the program is structured. Operational information such as regulatory requirements, service level agreements, existing relevant policies, and operational framework(s)/standards can bring early awareness of things like compliance requirements that may shape the definitions and parameters of incidents to prepare for.

Collect information such as:

- Third party service providers that the town contracts with which may be involved with a scenario or need to be called upon for assistance.
- Known regulatory and compliance requirements that must be incorporated into the program.
- Identify governing or oversight bodies that need to be part of a disclosure protocol.
- Does the organization have internal Compliance Officers and/or Auditors?
- Known audit schedules of any sort that can assist in the programs development.
- Physical locations of technology assets.

Building upon the organization and operational information gathered, the next step is to understand what technology and support services the organization utilizes. In gathering this information, it is important to gain the perspective of both the functional departments as well as the IT department. In today's world, it is not beyond the means of a business unit to acquire IT from an external source (Shadow IT) without the knowledge or support of internal IT. Regardless of how IT is acquired the Cyber Incident Management Program needs to consider all of it.

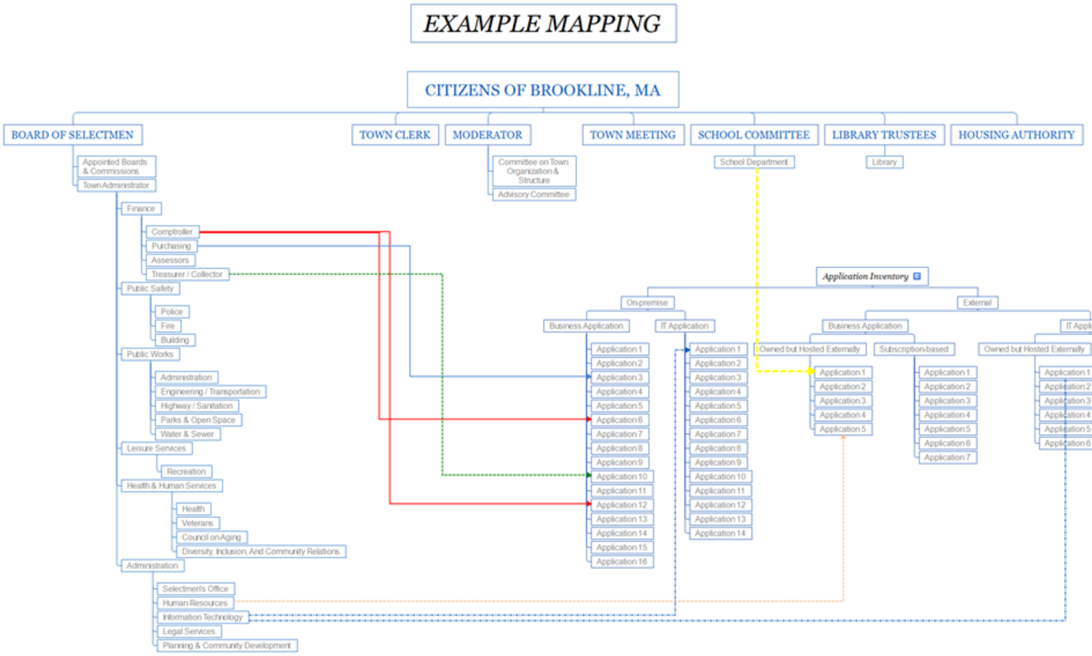
While the list(s) from the departments/committees are unlikely to be 100% accurate, acquiring their input and having them indicate level of importance to their respective business on a per data set/platform/application/service level is a necessary exercise and may prove enlightening for all parties. If the department wants an asset addressed by the program, they need to help enable that to occur. The Information Technology department will likely be able to articulate a holistic list of what is in use and illustrate technical dependencies to help define potential incident scenarios.

This is also an ideal opportunity for the organization to acknowledge who the owners, custodians, and users are of assets are on a per data set/platform/application/service basis. Multiple groups may rely on a single data set or asset so identifying chains of custody will be important for future development of program protocols.

Collect information such as:

- Application name and version
- Platform, application, or service vendor
- Utilizing business units
- Importance to business units
- Data Ownership/Governance

This information needs to be documented and can be done so with simple to comprehend maps/diagrams such as the example below.



NOTE: If multiple business units rely on an application or data set ensure one business unit does not make a decision that may negatively impact another without prior notification and/or acceptance.

Information gathering due diligence thus far will have unveiled several important attributes of the organization that will support protocols in the program. Information such as adopted operational frameworks, regulatory compliance requirements, and self-imposed policy are examples of where program development should occur.

There are several other key areas to investigate as well where deviation from written policy could be cause for detailed analysis and potentially program activation. These focus areas range from Human Resources maintained policies to legally binding documents such as non-disclosure agreements and third party service contracts. Example groups that should be solicited for input are; H/R, Legal, IT, Compliance & Information Assurance, and potentially Community Relations.

Collect information such as:

- Regulatory / Compliance Policy
- Human Resources Handbook
- Terms of Employment
- Employee On-boarding / Exiting and Suspension of Service procedures
- Non-Disclosure Agreements and Statement(s)
- Emergency Management Plan(s) / Disaster Recovery Plan(s)
- Acceptable Use Policy
- Data/Record Retention policy
- Change Control Policy
- Collective bargaining agreements

- Branding guidelines

It is a reasonable expectation of Information Technology department to ensure the organization understands what resources (human & technical) are required to support the protocols and mission statement of the program. Often organizations lack the skills and tools to effectively prevent, detect, contain, and eradicate the environment of root causes of declared incidents. It may be cost effective and necessary for the town to retain the services of a third party for incident response.

Program Development

Once team members are identified and information is gathered, documenting the program begins. If the programs mission statement has not been created and approved, it should be the first point of order. It may be necessary for team members to execute non-disclosure agreements and undergo background checks to protect themselves as well as the town, seek guidance from legal counsel and human resources. Human Resources should have amended formal job descriptions and acquired acknowledgement by all team members. The IT department should have established a secure data repository with functioning off-site backup for program content and it should be utilized for all things related to the program moving forward. If data classification, data loss prevention, or change controls have been previously instituted, ensure they take the program into account and are understood and adhered to by team members.

Fundamentally the team will:

1. Identify high-value/high-risk assets/services confirming "acceptable risk"
2. Determine dependencies
3. Hypothesize "what if" scenario's
4. Verify the absence of controls
5. Identify resources needed for Detection & Analysis, Containment/Eradication/Recovery
6. Develop protocols for #5 and internal/external communications

Internally determine the order of each functional department and their respective high-value/high-risk assets that will be incorporated into the program. Collaborate on what are believed to perceived threats and determine acceptable risk for included assets. The IT department will quantify existing controls and provide guidance on reasonable technical measures to maintain acceptable risk. This is likely to be the first time the program will generate an expense beyond the soft costs of employee resources gathering information. Costs could be generated by securing new technology for team communications, redundant content storage, new tools required for purposes such as threat detection, analysis, forensics, eradication, etc. Once the respective departments/committees understand the existing abilities to maintain confidentiality, integrity, and the availability of their targeted assets the "what if" dialogue begins.

The term "what if" has been, and will continue to be, used to cultivate a mindset of hypothetical situations. The exercise of generating the program will enable factual rationalization of existing controls against acceptable risk. The organization will be able to logically create policy/protocols and/or make investments that can expeditiously bring matters in line with acceptable states.

Be careful not to let these conversations go down the proverbial "rat hole". Identify a perceived threat or compromise and talk through the ideal process of dealing with that situation. Iterate until it's believed that an effective protocol has been documented and move on. It's best to establish a series of meaningful workflows that keep the team on task. Too much at once will quickly deflate interest and commitment in the program.

The use of a mind mapping or process development software tool will be a significant time saver. The workflows and diagrams generated will enable the team to quickly focus on the task at hand and establish a consistent and repeatable methodology to be used across departments.

Example "What if's" to work though may include scenarios of the following types:

- Unauthorized Disclosure
- Unauthorized Alteration
- Malware
- Policy Violation
- Unauthorized Access
- Unlawful Activity
- Harassment or Threats

It's important to remember not all threats are relevant or worth considering. The team must reduce considerations down to a prioritized, reasonable, and addressable set of concerns. Start with isolated scenarios, determine if effective controls are in place and identify the vulnerabilities that can be minimized, eliminated, or need to have controls/protocols established to identify indicators of compromise or reactions to compromise. To aid in setting context and the thought process a couple of examples follow. Remember, the bad guys don't take turns targeting organizations and malware released into the wild tends not to discriminate where it lands. Take caution not to be overwhelmed and commit to making small advances in the programs development. This is an iterative process that should be continuous.

EXAMPLE 1

Take malware that targets endpoint devices as a threat example to work through. It is a common root cause with a variety of impact levels. Some variants are more of a nuisance while others are crippling. Narrow malware threats down to ransomware. Ransomware does as its' name implies. The data on infected devices, and potentially wherever the device has access, is encrypted and rendered useless to the user(s) until a payment is made to an anonymous party through an electronic currency exchange such as BitCoin. The ransom amounts can range from a few hundred dollars to tens of thousands. Users typically have a short window of time to make payment and if they fail to do so, the ability to regain use of the data is lost forever. This is a very real threat that has afflicted countless individuals and organizations.

Using this example the team would need to consider a series of questions such as:

1. Is the organization vulnerable to the threat?
2. If so, who, and what data do they have access to?
3. What would happen if that data was encrypted unexpectedly?
4. Would the organization make payment, accept the loss, or restore from backup if possible?
5. If payment is acceptable, how much? Is certain data worth more than other?
6. How will payment occur? Does Brookline already have a BitCoin account?
7. What if BitCoin is not the preferred currency exchange of the adversary?
8. Is external communication of the compromise required? Who says what?

These questions provide a sense of why a cyber incident management program requires more than just the IT departments involvement. The answers may be radically different between departments and knowing desired reactions ahead of time can mean the difference between chaos and simply snubbing the bad guys.

EXAMPLE 2

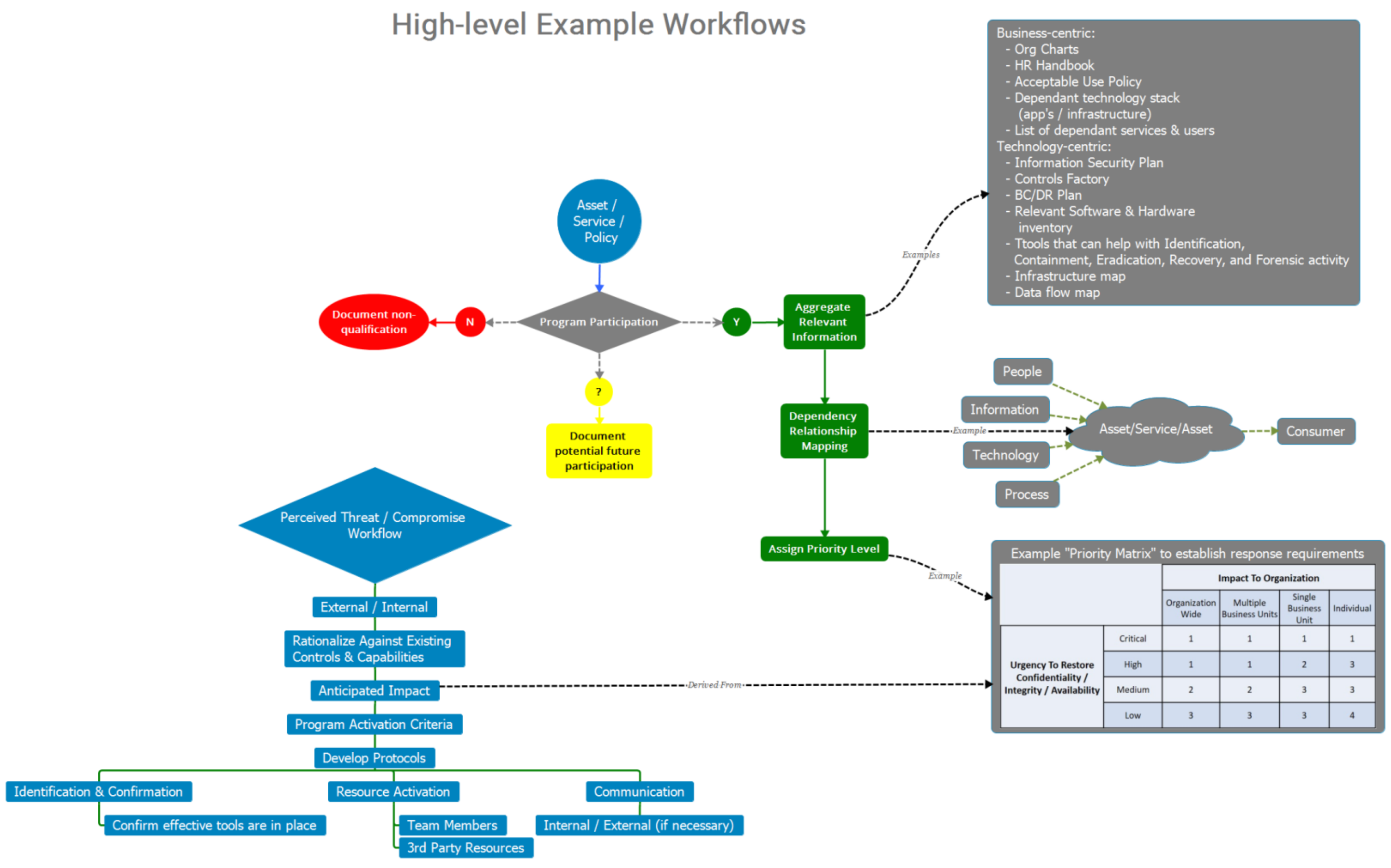
The towns website has been altered without authorization. It now contains inflammatory statements, a threat of violence if a Board of Selectmen political position is not changed to one that aligns to a hacktivist groups position, and the BrookONline page has had its links to 3rd party payment processors redirected?

Using this example the team would need to consider a series of questions such as:

1. How quickly can the site be taken off line, restored, and re-published?
2. What is the communication verbiage that needs to be used in response to inquiries? Who's authorized to make such statements?
3. Who is going to contact the Brookline Emergency Management Team, FBI, etc?
4. Is incident acknowledgement going to be posted to Brooklines social media accounts?
5. Is there a pre-recorded greeting message that can be activated on the town's main phone number and for those in IT? How often and what constitutes updating the message?
6. What happens to people who had fee/tax deadlines affected by the outage? What if someone claims they made payment while the site was altered? Can the town quickly determine whose payment was outstanding and reach out to them proactively if desired?
7. How quickly can quality assurance be conducted on the recovered/staged site before it's re-published?

As you can see from just these two examples posed by very real potential scenarios significant and potentially life threatening circumstances can occur. Having a plan in place to deal with them ahead of time will provide countless benefits for town government and the community.

High-level Example Workflows


Asset / Service / Policy
Program Participation
N
Document non-qualification
?
Document potential future participation
Y
Aggregate Relevant Information
Examples
Dependency Relationship Mapping
Example
People
Information
Technology
Process
Asset/Service/Asset
Consumer
Assign Priority Level
Example
Perceived Threat / Compromise Workflow
External / Internal
Rationalize Against Existing Controls & Capabilities
Anticipated Impact
Derived From
Program Activation Criteria
Develop Protocols
Identification & Confirmation
Confirm effective tools are in place
Resource Activation
Team Members
3rd Party Resources
Communication
Internal / External (if necessary)

Business-centric:
- Org Charts
- HR Handbook
- Acceptable Use Policy
- Dependant technology stack (app's / infrastructure)
- List of dependant services & users

Technology-centric:
- Information Security Plan
- Controls Factory
- BC/DR Plan
- Relevant Software & Hardware inventory
- Ttools that can help with Identification, Containment, Eradication, Recovery, and Forensic activity
- Infrastructure map
- Data flow map

Example "Priority Matrix" to establish response requirements

		Impact To Organization			
		Organization Wide	Multiple Business Units	Single Business Unit	Individual
Urgency To Restore Confidentiality / Integrity / Availability	Critical	1	1	1	1
	High	1	1	2	3
	Medium	2	2	3	3
	Low	3	3	3	4

Internal Testing & Training

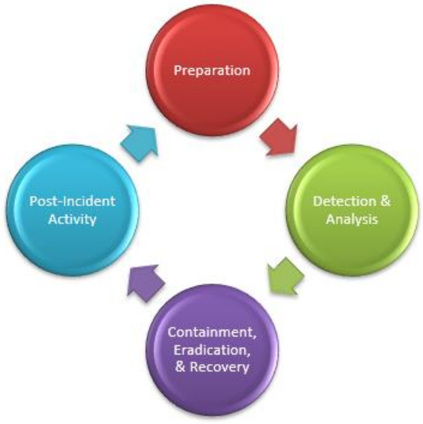
It should go without saying that the elements of the program need to be routinely assessed to ensure they are still viable and will serve as intended but we'll call it out. A documented test plan should be established and used on a periodic basis with each participating department. Table top exercises with relevant team members is a rudimentary exercise that can uncover opportunities for refinement and provide comfort and confidence in the program. Training in the form of program awareness must span beyond team members as well. The broader population of employees should have a general sense of understanding that a program exists. If they encounter a scenario that calls for concern, they should know there's a resource to turn to. This will elevate the vigilance of the user community and potentially enhance the ability to identify indicators of compromise earlier and potentially preserve forensic artifacts.

Take care to document performance during assessments for compliance reporting purposes and to identify areas for improvement or potentially communicate elevated risk to key stake holders.

Scheduled and/or Change-driven Program Validation

Ensure the program does not become stagnant and rendered useless over time. A maintenance schedule needs to be prioritized from the onset. After initial launch, there are four principle events that should trigger program inspection; an actual incident, shifting threat landscape, scheduled maintenance, or the introduction of a new control. Changes in team membership need to have documented protocols for onboarding and termination of members. The program director or an empowered designate should be tasked with updating program documentation affected by any change.

Conclusion



Cyber Security Incident Management Program Lifecycle

As depicted in this document the "Preparation" phase of a cyber security incident management program is a multi-faceted challenge. It may call on individuals to think and do things differently than what the culture and existing defined job responsibilities may prescribe. Going through the excise of understanding what legal obligations exist and determining acceptable risk from a business perspective will enable town officials to make educated decisions on how to best protect itself and those it serves. Significant cyber incidents can quickly become a problem that requires the involvement of more than just the IT department. Weighted against the potential disruption and damage that today's threat landscape poses, cross functional collaboration and planning in advance is imperative.

While the scope of this document focuses on the initial phase of creating a cyber incident management program do not dismiss the remaining three phases. They are equally important to effectively and efficiently navigating through scenarios. As indicated thoughtful preparation for "what happens" when the "what if" happens will pay untold dividends.

Appendix A - Helpful terms and considerations

This appendix has been provided to assist the Town understand additional cyber incent management considerations with regards to creating a program.

Cyber Insurance

One of the fastest growing insurance products is cyber insurance and with just cause. It simply isn't possible to achieve and maintain zero (0) risk. Most organizations have a limited capacity to prevent and react to incidents so cyber insurance presents itself as an attractive investment. The structure of cyber policies varies according to the party protected. Third party liability policies cover privacy liability, network security, media liability and regulatory action and they may carry a sublimit. First party coverage includes reimbursement coverage, privacy notification, crisis management expenses and, often, credit monitoring services. In addition, other first party reimbursement coverages may include cyber extortion, business interruption and data restoration. More insurers are offering loss mitigation and loss prevention services as well. Some commercial general liability, crime, errors and omissions, directors and officers and first party property policies may include coverage for cyber breaches. This is a topic that should be further investigated by the town.

Cyber Currency

"Bitcoin" is likely to be a new term to many and may even sound fictitious, however it's very real. If you were asked if you would accept being paid four (4) Bitcoin each pay period, you might walk away laughing for the wrong reason. Consider that at the time of this writing one (1) Bitcoin is worth $1,210 US. That might compel you to learn a bit more about Bitcoin. Another reason to learn about Bitcoin is that it is what is requested in today's most prolific cyber nuisance called "ransomware". Essentially victims of ransomware commonly have their data held hostage until a payment of Bitcoin is made to an anonymous and untraceable third party on via a cyber currency exchange. Average ransom for 2016 was believed to be in the neighborhood $800 US. Keep in mind that's per device, not all victims/organizations make their incident(s) known, and there have been public headlines depicting victim organizations having their data ransomed for hundreds of thousands of US dollars. If the town determines that there is a scenario in which it would render payment it's best to establish a Bitcoin account now, appropriate funds to it, and have a protocol in place for the addition and dispensation of funds.

Incident Definition

An incident is an adverse event affecting an information system or network, or the active threat of occurrence of such an event. The term incident implies harm or the attempt to harm. This definition provides the basis for declaring an incident however it is the responsibility of the Brookline incident handling team to officially declare an incident based on the evidence presented.

A declared incident is an incident that causes the incident response process to be implemented. Not all incidents rise to the level of a declared incident. For example, the detection of a port scan against public facing resources from the Internet could be considered the threat of an adverse event however it is unlikely that the incident response process would be implemented based on the discovery of a port scan.

Communications

Brookline will maintain secure and/or out of band communication methods for use during an incident. Such communication methods must allow for:

- Initial communication when an incident is identified (e.g. a conference bridge)
- Communication during an incident (e.g. encrypted email, encrypted voice over IP, cell phones, etc.)
- Exchange and storage of evidence (e.g. secure file storage)

Brookline will develop, maintain and test methods for notification of incident responders in the event that an incident is suspected. This notification method needs to allow all members of both core and ancillary incident handling teams to communicate about the incident in a secure way in accordance of timeframes established later in this document.

Monitoring

Brookline will maintain a program of security monitoring designed to identify indications of security incidents as quickly as possible. The program will include network monitoring (e.g. network-based intrusion detection, network traffic monitoring, full packet capture, etc.) and host monitoring (e.g. host-based intrusion detection, log monitoring, etc.)

Brookline users will sign a document annually giving their consent to being monitored. The documents for each employee will be stored for the duration of each employees' employment with Brookline. In addition, where possible, Brookline computing devices will be configured to present users with a pre-login banner advising users that:

- Access to the system is limited to authorized users only
- Unauthorized access, use or modification is prohibited
- Unauthorized user may face criminal or civil penalties
- Use of the system may be monitored and recorded
- Brookline can make use of any information collected during monitoring in any way permitted by law including turning over the records to law enforcement

Law Enforcement Notification

In the event of an incident, it may be beneficial or necessary to notify law enforcement. Whether law enforcement will be notified will be determined by the details of the case and will not be based on the characteristics, position or role of any individuals involved.

- Law enforcement will be notified in cases where illegal contraband is discovered. Illegal contraband includes but is not limited to child pornography or stolen credit card information.
- Law enforcement will be notified if evidence collected during the incident uncovers a threat to public health or safety.
- Law enforcement will be notified if the incident involves a substantial impact to a third party.
- Brookline will consider notifying law enforcement to benefit from the criminal discovery process.

Brookline security personnel will develop and maintain relationships with law enforcement including the Federal Bureau of Investigation. Membership and participation in organizations such as Infragard can be helpful in developing and maintaining such relationships.

It should be noted that if Brookline personnel receive instructions, recommendations or suggestions about how to respond to an incident during an incident, following up on those instructions could be considered acting "under color of law" effectively making Brookline personnel agents of law enforcement. Thus, evidence collected could be inadmissible in court proceedings.

Notification

Brookline will establish and maintain methods allowing Brookline personnel and others to report suspected computer security incidents. Reporting facilities could include email distribution lists, a voice mailbox, a reporting web site, etc. Brookline will ensure that information about incident reporting facilities is distributed and made available to all Brookline personnel and to any other personnel able to detect a possible incident. Incident reporting facilities and training associated with incident reporting should encourage users to include contact information when reporting a suspected incident however reporting facilities should allow for anonymous reporting.

Incident Documentation

As any incident has the potential of resulting in civil or criminal legal action, Brookline will treat all incidents as if legal action will be involved. Incident handlers will take detailed notes about all actions taken during the incident. Such notes will be written in pen in a bound notebook with numbered pages. Notes will be of sufficient detail to allow incident handlers to testify in a court of law about the incident even if such testimony occurs months or years after the incident.

Incident handlers will maintain chain of custody documentation for all evidence collected during an incident. Such documentation will include records of the circumstances around evidence collection (e.g. who collected it, where it was collected, when it was collected, etc.), information necessary for evidence integrity verification (e.g. hashes of data files) and records detailing the lifecycle of collected evidence (e.g. when it was accessed by other personnel post evidence collection). If law enforcement becomes involved, chain of custody documentation will be turned over to law enforcement when requested.

Response Team

The incident response team will consist of core and ancillary components. Core components of the incident response team will consist of the technical incident handlers. Ancillary team members include security personnel who are not specifically assigned to the core incident handling team, physical security personnel, operations (system administration), network management, legal counsel, human resources, public relations, disaster recovery/business continuity and union representation. Ancillary team member will not be involved with every incident but will be brought in on an as needed basis. Ancillary members will be trained on the overall incident handling process to the extent that their role in the process requires.

Brookline will maintain an accurate and up to date documented incident handling team roster.

Brookline will document the training each functional role of the incident handling team requires and will document the training each member of the team received.

Compensation

As incident handling often requires team members to work outside of normal business hours, above and beyond their normal job functions, Brookline will compensate members of the response team with 1.5 extra ours of paid time off for each hour of incident response work outside of normal business hours.

Response Timeframes

When an incident is declared, the members of the incident response team will assemble on a conference bridge within 1 hour of the declared incident.

When an incident is declared, qualified personnel will be on site with the capability of interacting with affected computer systems within 4 hours.

Incident handlers will prepare a report for senior management within 1 hour of beginning on site response activities. This report will detail what is known about the incident, any "known unknowns" and anticipated next steps. The initial report will also include a timeframe for the next official report.

System Access

A root, Administrator or similar privileged account will be set up on each system for use during the incident handling process. This account will be set up with a long and complex password consisting of no less than 20, pseudo-random characters. This password will be stored in an envelope in a secure location. In the event incident handlers require access to a system, the envelope will be opened providing the incident handler with the password. The password will be used throughout the duration of the incident however it can be changed by the incident handling team to one easier to enter but that meets Brookline password standards. At the end of the incident, a new password meeting the requirements defined previously in this section will be generated and placed in a sealed envelope on the secure location.

Resource Acquisition

During handling of an incident, members of the incident handling team may need to purchase equipment, services, transportation, etc. As these expenses cannot always be predicting, the incident handling team will have access to funds in the amount of at least $10,000. Access to these funds will not require prior authorization. Allocation of these funds is left to the discretion of the incident handling team lead however a detailed report of any expenditures including all receipts must be made available to senior management upon request.

Reporting/Incident Notification

During the identification phase of the incident response process Brookline incident handlers will attempt to determine whether an incident has occurred and, if so, what is the scope of the incident. This scope determination will include, to the extent possible, an inventory of affected systems and/or data. If incident handlers determine that an incident has occurred, key personnel, business partners, clients, customers and other relevant individuals associated with affected systems and/or data will be notified. To accomplish this, Brookline will maintain an inventory of systems and data. For each system or data set, Brookline will maintain a list of personnel to be notified during different types of incidents. For the purposes of notification, incidents fall into three categories; incidents involving the unauthorized disclosure of sensitive data (confidentiality), incidents involving the unauthorized alteration or modification of sensitive data (integrity) and incidents involving the disruption of access to systems, data or other computing resources (availability). It should be noted that a single incident could be categorized affecting one, two or three of the classification categories.

While it is important to ensure that all appropriate parties are notified of an incident, until a full investigation is completed, notification should be on an as needed basis. Only those individuals with a legitimate business need to know will be notified about an incident. When notification occurs, individuals will be provided with only that information about the incident that is necessary.

Training

Members of both the core and ancillary incident handling teams will receive training in line with their role on the team. At least one member of the core team will achieve and maintain an industry accepted incident response certification such as the GIAC Certified Incident Handler, the EC-Council Certified Incident Handler or the CERT-Certified Computer Security Incident Handler Certification. All members of the core incident handling team will receive technical training in incident response, incident handling, computer forensics, malware analysis and/or similar disciplines.

Ancillary members of the incident handling team will receive training per their role in the incident handling process. All members of the team will receive sufficient training to understand the overall incident handling process. All members of the incident handling team will participate in an incident handling exercise on at least a quarterly basis.

Brookline will conduct, on at least a quarterly basis, incident handling exercises. During these exercises, the entire incident handling process will be tested including methods for getting the team members on a conference bridge. At least twice per year, Brookline personnel will run through a simulated incident involving all core and ancillary team members.

Response Tools and Material

Brookline will maintain a "jump bag" containing all the hardware, software and materials necessary for effective incident response. The contents of the jump bag will include:

- Binary image creation software
- Forensic software
- Rootkit detection utilities
- Bootable anti-virus solutions
- Statically linked copies of key executable (e.g. dir, ls, netstat, etc.)
- USB hard drives sufficient for imaging Brookline hard drives
- USB thumb drives sufficient for imaging Brookline memory
- An Ethernet tap
- Cables (e.g. Ethernet, USB, serial, etc.)
- A laptop capable of supporting multiple virtual computers
- Contact lists (incident response team, vendors, contractors, etc.)
- Anti-static bags
- Desiccants
- Notebook
- Pens
- Spare battery for cell phones
- Tools (e.g. screwdrivers, etc.)
- Medical supplies (e.g. aspirin, antacid, etc.)
- Personal hygiene (deodorant, toothbrush, toothpaste, etc.)

Note: a digital forensics and incident response focused Linux distribution such as the SANS Investigative Forensics Toolkit (http://computer-forensics.sans.org/community/downloads) contains a full set of tools and utilities that may be an alternative to collecting the necessary tools and utilities individually.

System Baseline

To facilitate the incident handling process, Brookline will maintain a baseline for each system. During the system build process and as part of the change controls process, Brookline will document system configuration details including but not limited to:

- Running processes and services
- Open TCP and UDP ports
- User accounts and group membership
- Scheduled tasks
- Average processor utilization
- Average memory utilization
- Average hard drive utilization

In the event of an incident, Brookline personnel will generate another "baseline" that can be compared against the documented baselines generated during the system build or change control process. While not all incidents will result in a change to the baseline, any new accounts, group membership, processes, services, open ports, etc. can be a good indicator of changes made because of an incident.

Brookline will also maintain an accurate network diagram and hardware inventory. The diagram will detail the physical (layer 1), data link (layer 2) and network (layer 3) connectivity. The hardware inventory will include a description of each computing device, the MAC address for that device and, if statically assigned, the IP address for the device.

The inventory will also define an "asset owner" for each device. The asset owner is defined as the individual or business unit who is responsible for making business decisions about the device or about the data contained on each device. For devices containing various types of data, the inventory will contain an inventory of the data assets. For each set of data, the inventory will contain a description of the data asset and a classification label defining the business impact if that asset were to be involved in an incident affecting confidentiality, integrity or availability.

Identification

During the identification phase incident handlers have a primary and a secondary goal. The primary goal is determining whether an incident has occurred. Often, situations occur that appear to be incidents but are, in fact, hardware failures, change control issues or other errors. Furthermore, situations that would be considered incidents do not rise to a level requiring officially declaring an incident and implementing the active phase of the incident handling process. For example, detecting a port scan conducted against public facing resources from the Internet could be considered an attempt to cause harm but is unlikely to result in a declared incident. During the identification phase, incident handlers will determine whether an incident occurred and whether an official incident should be declared.

When an incident is suspected, Brookline will assign an incident handler to act as the lead. The lead handler will be responsible for coordinating all incident handling activities throughout the duration of the incident. It will be the responsibility of the lead incident handler to officially declare an incident.

While the specific steps taken in determining whether an incident has occurred will very depending on the type of incident, common steps will involve comparing the current state of any involved systems with previously created baselines. This can include attempting to identify:

- Unusual processes or services running
- Unusual network usage (e.g. open ports, established connections, etc.)
- Changes to host-based firewall settings
- Unusual registry changes, particularly those involved with automatically starting processes or services
- Extra startup items
- New or unusual user accounts
- New or unusual group membership
- Unusual scheduled tasks
- Unusual log entries
- Changes to normal CPU, memory or hard drive utilization

Depending on the nature of the incident, Brookline may also wish to run rootkit detection tools and/or malware scanning tools against suspect systems. If file system or memory forensics is required, rootkit detection and malware scanning tools should only be run after hard drive and memory images have been collected.

Computer memory contains a significant quantity of information that can be valuable in investigating an incident. Memory however, is extremely volatile and will change rapidly. Because of this, Brookline will capture volatile information including memory on any computer suspected of being involved in an incident. A tool such as "Live Response Collection" from Brimor Labs can be used for this purpose. Brookline will keep a supply of USB drives of sufficient size to collect volatile data on hand. If any computer is suspected of being involved in an incident, or if a computer malfunctions and needs to be rebuilt, volatile data will be collected. The USB drives will be labeled accordingly and will be stored for at least one month after its collection. USB drives containing volatile data will be stored in a secure location and a chain of custody record will be maintained for each USB drive. When a memory image is created, Brookline personnel will calculate at least two forensic hashes of the image using different hashing algorithms (e.g. MD5 and SHA1). The resulting hash will be recorded as evidence and will be used to ensure the integrity of the memory image can be verified.

The secondary goal of the identification phase of the incident handling process is determining the expected severity of the incident. The incident handling team should attempt to:

Understand the Incident's Background

- What is the nature of the problem, as it has been observed so far?
- How was the problem initially detected? When was it detected, and by whom?
- What security infrastructure components exist in the affected environment? (e.g., firewall, anti-virus, etc.)
- What is the security posture of the affected IT infrastructure components? How recently, if ever, was it assessed for vulnerabilities?
- What groups or organizations were affected by the incident? Are they aware of the incident?
- Were other security incidents observed on the affected environment or the organization recently?

Define Communication Parameters

- Which individuals are aware of the incident? What are their names and group or company affiliations?
- Who is designated as the primary incident response coordinator?
- Who is authorized to make business decisions regarding the affected operations? (This is often an executive.)
- What mechanisms will the team to communicate when handling the incident? (e.g., email, phone conference, etc.) What encryption capabilities should be used?
- What is the schedule of internal regular progress updates? Who is responsible for them?
- What is the schedule of external regular progress updates? Who is responsible for leading them?
- Who will conduct "in the field" examination of the affected IT infrastructure? Note their name, title, phone (mobile and office), and email details.
- Who will interface with legal, executive, public relations, and other relevant internal teams?

Assess the Incident's Scope

- What IT infrastructure components (servers, websites, networks, etc.) are directly affected by the incident?
- What applications and data processes make use of the affected IT infrastructure components?
- Are we aware of compliance or legal obligations tied to the incident? (e.g., PCI, breach notification laws, etc.)
- What are the possible ingress and egress points for the affected environment?
- What theories exist for how the initial compromise occurred?
- Does the affected IT infrastructure pose any risk to other organizations?

Review the Initial Incident Survey's Results

- What analysis actions were taken to during the initial survey when qualifying the incident?
- What commands or tools were executed on the affected systems as part of the initial survey?
- What measures were taken to contain the scope of the incident? (e.g., disconnected from the network)
- What alerts were generated by the existing security infrastructure components? (e.g., IDS, anti-virus, etc.)
- If logs were reviewed, what suspicious entries were found? What additional suspicious events or state information, was observed?

Prepare for Next Incident Response Steps

- Does the affected group or organization have specific incident response instructions or guidelines?
- Does the affected group or organization wish to proceed with live analysis, or does it wish to start formal forensic examination?
- What tools are available to us for monitoring network or host-based activities in the affected environment?
- What mechanisms exist to transfer files to and from the affected IT infrastructure components during the analysis? (e.g., network, USB, CD-ROM, etc.)
- Where are the affected IT infrastructure components physically located?
- What backup-restore capabilities are in place to assist in recovering from the incident?
- What are the next steps for responding to this incident? (Who will do what and when?)

All the above information should be documented as part of the official incident record. If an incident is declared, the incident response process will move into the containment phase.

Any information collected during the identification phase is considered evidence. As such, chain of custody will be maintained.

Containment

During the containment phase, the incident response team will take steps to ensure the incident does not get any worse. There are three distinct phases of the containment phase; short term containment, system imaging and long term containment.

Short term containment is the phase where incident handlers take steps to gain control over the incident and prevent it from getting worse. To do this, incident handlers must identify the type of incident. Types of incidents include:

- Denial of Service
- Unauthorized Disclosure
- Unauthorized Alteration
- Unauthorized Access
- Unlawful Activity
- Policy Violation
- Harassment or Threats
- Malware

If possible, incident handlers should classify the threat vector as internal or external.

The steps involved in short term containment will be largely determined by the type of incident and by the identified threat vector however common activities performed during the containment phase may include:

- Disconnect network cable
- Pull the power cable (Note: this action would result in the loss of volatile memory and may damage hard drives)
- Using network-management tools, isolate the switch port so the system cannot receive or send data… or place on an "infected VLAN"
- Apply filters to routers and/or firewalls
- Change a name in DNS to point to a different IP address
- Coordinate with an internet service provider to block or throttle network traffic

More specific containment steps will differ based on the type of incident as follows:

Denial of Service

- Determine whether the denial of service attack is being exploited locally or across the network
- Determine whether the denial of service attack is taking advantage of a technical vulnerability that can be patched or is focused on exhausting resources

	Local	Network
Vulnerability	• Identify and kill offending processes	• Identify signature of offending network packets • Implement firewall or router access controls to block offending traffic
Resource Exhaustion	• Identify and kill offending process or service	• Identify signature of offending network packets • Work with upstream ISP to block offending traffic

Unauthorized Disclosure

- Identify the method for data exfiltration
- Identify any ongoing command and control traffic
- Implement network filters to block command and control traffic
- Implement network filters as possible to block active data exfiltration
- Block, disable or change password of affected accounts

Unauthorized Alteration

- Block, disable or change passwords of affected accounts
- Identify any ongoing command and control traffic
- Implement network filters to block command and control traffic
- Identify and validate relevant backups
- Generate forensic image for additional investigation

Unauthorized Access

- Block, disable or change passwords of affected accounts
- Identify any ongoing command and control traffic
- Implement network filters to block command and control traffic
- Generate forensic image for additional investigation

Unlawful Activity

- Involve human resources as necessary
- Block, disable or change password of affected accounts
- Involve contact law enforcement
- Secure any involved computers or other computing devices
- Secure relevant logs
- Capture network traffic as necessary
- Generate forensic image for additional investigation

Policy Violation

- Involve human resources as necessary
- Block, disable or change password of affected accounts
- Secure any involved computers or other computing devices
- Secure relevant logs
- Capture network traffic as necessary
- Generate forensic image for additional investigation

Harassment or Threats

- Involve human resources as necessary
- Secure relevant logs
- Capture network traffic as necessary
- Generate forensic image for additional investigation

Malware

- Quarantine affected computers by turning off power, disconnecting from the network or isolating via network access controls
- If sufficient computers have been affected or if the malware is spreading rapidly enough, disconnect entire segments as necessary

During short term containment, it is critical that incident handlers keep a low profile. Alerting an attacker that they have been detected could cause the attacker to inflict additional damage increasing the level of harm. It may also cause the attacker to focus on covering their tracks making investigation more difficult.

Based on the resources or assets involved, notification about the incident can begin as described previously in this document in accordance with "need to know" determinations. A primary point of contact for the incident within the incident response team will be established. Communications about the incident will occur through the incident response team point of contact. No other member of the incident response team is authorized to communicate information about the incident.

Once short term containment has been completed a forensic image of any impacted computers should be created. This image is not a traditional system backup. Rather, it is a bit-for-bit copy of the entire hard drive. A forensic image will be created of any system found to contain contraband (e.g. stolen credit card numbers, child pornography, etc.) and for any system involved in an incident likely to result in civil or criminal legal action. It is recommended that a forensic image be created of systems involved in incidents where disciplinary action against a Brookline employee will be involved. Forensic images need not be created for systems affected by denial of service attacks or by systems infected with malware provided such incidents do not meet any other criteria requiring a forensic image be created.

When creating the forensic image, two hashes will be calculated for the hard drive (using different algorithms) and two hashes will be calculated for the resulting image. The hash values will be stored as evidence. Where possible, the original hard drive will be removed from the involved system and stored as evidence. If the removal of the hard drive is not possible, a forensically identical (verified via hash algorithms) image of the drive will be stored as evidence. Brookline incident handlers should consider making multiple copies of drive images (each validated via hashing algorithms). Once copy will be stored in a secure location and maintained as evidence while other copies will be used to conduct forensic analysis/investigation.

After any forensic images have been created, the goal is to move into the eradication phase. Eradication involves making significant changes to the involved systems and, as a result, may not be able to be initiated immediately after system imaging. For example, a system may have firmly established down time windows and changes must wait until those specified timeframes. In these situations, long term containment is initiated. Long term containment involves making the system as secure as possible until the eradication phase can be fully implemented. The steps taken during long term containment will be determined by the type of incident, the status of the system and the reason for enacting long term containment measures but can include:

- Patching the system
- Patching neighboring systems
- Inserting an Intrusion Prevention System (IPS)
- Null routing known malicious IP addresses
- Changing passwords
- Altering trust relationships
- Applying firewall and router filter rules
- Removing accounts used by attacker
- Shutting down backdoor processes or services used by the attacker

Long term containment is never the final state of a compromised system. Brookline will move to the eradication phase of the incident handling process as quickly as possible.

Eradication

Eradication involves removing evidence of the attackers presence from compromised systems. If the exact state of the compromised system is known and if the attacker did not gain root, Administrator, System or similar permissions on the system, eradication will involve eliminating malware, backdoors or tools placed on the system by the attacker and undoing any changes made to the system by the attacker. As necessary, data may need to be restored to the system from backups.

In cases where the exact state of the system is not known or where the attacker gained root, Administrator, System or similar permissions, eradication will involve the following steps:

- Securely wipe the entire hard drive by overwriting every block or sector of the drive with new data (binary 1's, 0's or random values).
- Reformatting the hard drive
- Installing the operating system from known good media
- Patching and hardening the operating system
- Installing applications from known good media
- Patching and hardening applications
- Reloading data from backup

Before the eradication phase is complete, Brookline will conduct a credentialed vulnerability scan of any affected systems to determine whether obvious vulnerabilities remain. Identified vulnerabilities will be corrected where possible. If correcting identified vulnerabilities is not possible, the identified asset owner will sign a document accepting the risk.

Recovery

The goal of the recovery phase is to get previously compromised systems back into production is as safe a manner as possible. This involves user acceptance testing and enhanced monitoring.

The business unit responsible for the affected system or application is responsible for conducting user acceptance testing. This testing is designed to ensure that the system or application in question functions properly. No Brookline system will be put back into production until the responsible business unit completes and signs off that user acceptance testing has been completed successfully.

Once the system has been tested, it can be put back into production however the system will be subject to enhanced monitoring. Monitoring should fall into two categories; general and specific. Specific monitoring involves identifying the changes to the system enacted by the attacker during the most recent incident. Brookline will test to determine if these "indicators of compromise" recur. General monitoring involves looking for suspicious network traffic, open ports, running services, unusual log entries, etc.

Real time testing is recommended if technically possible. If real time testing is not technically feasible, Brookline will run tests according to the following schedule:

- Hourly for the first 24 hours
- Every 6 hours for the next 48 hours
- Every 12 hours for the next 48 hours
- Once per day for the next 5 days

After this schedule, normal monitoring can continue.

Lessons Learned

Lessons learned is the final phase of the incident handling process. During the lessons learned phase, the lead incident handler will prepare an incident report. The report will detail:

- What occurred during the incident?
- Any known negative impact resulting from the incident
- The measures that were taken to respond to the incident
- Any known causes of the incident
- Recommendations for improving the state of Brookline security
- Recommendations for improving the incident handling process

The report must be finalized within two weeks of resuming production. The report, while written by the lead handler will be distributed to all members of the incident handling team who were involved in the incident. All members of the incident handling team will have the opportunity to provide feedback. The goal is to have unanimous agreement about the contents of the report however, if a member of the team does not agree about report, they will have the opportunity to have their version of events added to the official report as an appendix. The report will be provided to senior management for review.

Appendix B - 201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH

The below was taken from the Massachusetts Consumer Affairs and Business Regulation website located at: http://www.mass.gov/ocabr/data-privacy-and-security/data/ which should be consulted for current information.

Section:
17.01: Purpose and Scope
17.02: Definitions
17.03: Duty to Protect and Standards for Protecting Personal Information
17.04: Computer System Security Requirements
17.05: Compliance Deadline

17.01 Purpose and Scope

(1) Purpose

This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of this regulation are to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

(2) Scope

The provisions of this regulation apply to all persons that own or license personal information about a resident of the Commonwealth.

17.02: Definitions

The following words as used herein shall, unless the context requires otherwise, have the following meanings:

Breach of security, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Electronic, relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Encrypted, the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

Owns or licenses, receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

Person, a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.

Personal information, a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Record or Records, any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Service provider, any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation.

17.03: Duty to Protect and Standards for Protecting Personal Information

(1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

(2) Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:

(a) Designating one or more employees to maintain the comprehensive information security program;

(b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:

1. ongoing employee (including temporary and contract employee) training;

2. employee compliance with policies and procedures; and

3. means for detecting and preventing security system failures.

(c) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.

(d) Imposing disciplinary measures for violations of the comprehensive information security program rules.

(e) Preventing terminated employees from accessing records containing personal information.

(f) Oversee service providers, by:

1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and

2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 17.03(2)(f)(2) even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010.

(g) Reasonable restrictions upon physical access to records containing personal information,, and storage of such records and data in locked facilities, storage areas or containers.

(h) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.

(i) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

(j) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

17.04: Computer System Security Requirements

Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:

(1) Secure user authentication protocols including:

(a) control of user IDs and other identifiers;

(b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;

(c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;

(d) restricting access to active users and active user accounts only; and

(e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

(2) Secure access control measures that:

(a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and

(b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;

(3)Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.

(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;

(5) Encryption of all personal information stored on laptops or other portable devices;

(6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.

(7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

17.05: Compliance Deadline

(1)Every person who owns or licenses personal information about a resident of the Commonwealth shall be in full compliance with 201 CMR 17.00 on or before March 1, 2010.

REGULATORY AUTHORITY - 201 CMR 17.00: M.G.L. c. 93H

Appendix C – Excerpt from the U.S. Department of Health & Human Services web site

https://www.hhs.gov/hipaa/for-professionals/faq/513/does-hipaa-apply-to-an-elementary-school/index.html

Does the HIPAA Privacy Rule apply to an elementary or secondary school?

Generally, no. In most cases, the HIPAA Privacy Rule does not apply to an elementary or secondary school because the school either: (1) is not a HIPAA covered entity or (2) is a HIPAA covered entity but maintains health information only on students in records that are by definition "education records" under FERPA and, therefore, is not subject to the HIPAA Privacy Rule.

The school is not a HIPAA covered entity. The HIPAA Privacy Rule only applies to health plans, health care clearinghouses, and those health care providers that transmit health information electronically in connection with certain administrative and financial transactions ("covered transactions"). See 45 CFR § 160.102. Covered transactions are those for which the U.S. Department of Health and Human Services has adopted a standard, such as health care claims submitted to a health plan. See the definition of "transaction" at 45 CFR § 160.103 and 45 CFR Part 162, Subparts K–R. Thus, even though a school employs school nurses, physicians, psychologists, or other health care providers, the school is not generally a HIPAA covered entity because the providers do not engage in any of the covered transactions, such as billing a health plan electronically for their services. It is expected that most elementary and secondary schools fall into this category.

The school is a HIPAA covered entity but does not have "protected health information." Where a school does employ a health care provider that conducts one or more covered transactions electronically, such as electronically transmitting health care claims to a health plan for payment, the school is a HIPAA covered entity and must comply with the HIPAA Transactions and Code Sets and Identifier Rules with respect to such transactions. However, even in this case, many schools would not be required to comply with the HIPAA Privacy Rule because the school maintains health information only in student health records that are "education records" under FERPA and, thus, not "protected health information" under HIPAA. Because student health information in education records is protected by FERPA, the HIPAA Privacy Rule excludes such information from its coverage. See the exception at paragraph (2)(i) to the definition of "protected health information" in the HIPAA Privacy Rule at 45 CFR § 160.103. For example, if a public high school employs a health care provider that bills Medicaid electronically for services provided to a student under the IDEA, the school is a HIPAA covered entity and would be subject to the HIPAA requirements concerning transactions. However, if the school's provider maintains health information only in what are education records under FERPA, the school is not required to comply with the HIPAA Privacy Rule. Rather, the school would have to comply with FERPA's privacy requirements with respect to its education records, including the requirement to obtain parental consent (34 CFR § 99.30) in order to disclose to Medicaid billing information about a service provided to a student.

Appendix D – Family Educational Rights and Privacy Act (FERPA) Must Do's

Educational agencies and institutions must annually notify parents and eligible students of their rights under FERPA. Specifically, schools must notify parents and eligible students of the right: to inspect and review education records and the procedures to do so; to seek amendment of records the parent or eligible student believes are inaccurate and the procedures to so do; to consent to disclosures of education records, except to the extent that FERPA authorizes disclosure without consent; and to file a complaint with FPCO concerning potential violations. (Source: 34 CFR § 99.7)

FERPA does not require a school to notify parents individually of their rights under FERPA. Rather, the school may provide the annual notification by any means likely to inform parents of their rights. Thus, the annual notification may be published by various means, including any of the following: in a student handbook; in a notice to parents; in a calendar of events; on the school's website (though this should not be the exclusive means of notification); in the local newspaper; or posted in a central location at the school or various locations throughout the school. Additionally, some schools include their directory information notice as part of the annual notice of rights under FERPA. Proclaiming "directory information" is critically important to setting information handling expectations internally and externally.

FERPA permits a school non-consensually to disclose personally identifiable information from a student's education records when such information has been appropriately designated as directory information. "Directory information" is defined as information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed. Directory information could include information such as the student's name, address, e-mail address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, the most recent previous educational agency or institution attended, photograph, grade level (such as 11th grade or junior year), and enrollment status (full-time or part-time).

A school may disclose directory information without consent if it has given public notice of the types of information it has designated as directory information, the parent's right to restrict the disclosure of such information, and the period of time within which a parent has to notify the school that he or she does not want any or all of those types of information designated as directory information. Also, FERPA does not require a school to notify parents individually of the types of information it has designated as directory information. Rather, the school may provide this notice by any means likely to inform parents of the types of information it has designated as directory information.

Where to file a report: A parent or eligible student may file a written complaint with the Office regarding an alleged violation under the Act and this part. The Office's address is: Family Policy Compliance Office, U.S. Department of Education, 400 Maryland Avenue, SW., Washington, DC 20202

Appendix E - Helpful Website References:

The Official Website of the Massachusetts Judicial Branch - Code of Massachusetts Regulations (CMR)
http://www.mass.gov/courts/case-legal-res/law-lib/laws-by-source/cmr/

Office of Consumer Affairs and Business Regulation, 201 CMR 17
http://www.mass.gov/courts/case-legal-res/law-lib/laws-by-source/cmr/200-299cmr/201cmr.html

Massachusetts General Laws
https://malegislature.gov/Laws/GeneralLaws

Title XV – Regulation of Trade, Chapter 93H
https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93H

MA Consumer Affairs and Business Regulation website
Data Breach Notifications violating Massachusetts Data Security Law M.G.L. c.93H are now posted online and can be viewed online:
http://www.mass.gov/ocabr/data-privacy-and-security/data/data-breach-notification-reports.html

Ponemon Institute, LLC. Data Risk in the Third-Party Ecosystem
http://www.ponemon.org/library/data-risk-in-the-third-party-ecosystem?s

About Our Security Practitioners

HUB Tech Qualifications

HUB Tech brings to bear some of the best security professionals in the business. From experience and certification to industry involvement, presentations and teaching, HUB Tech consultants combine security expertise with business savvy, the ability to effectively communicate to all audiences and a have a deep passion for what they do to provide you with service and value unparalleled in the industry.

HUB Tech consultants achieve and maintain some of the security industry's most recognized certifications including:

- Certified Information Systems Auditor
- GIAC Certified Windows Security Administrator
- GIAC Certified Enterprise Defender
- GIAC Mobile Device Security Auditor
- GIAC Auditing Wireless Networks Certification
- GIAC Security Essentials Certification
- GIAC Certified Penetration Tester
- GIAC Reverse Engineering Malware
- GIAC Certified Incident Handler
- GIAC Certified Intrusion Analyst
- GIAC Certified Forensic Analyst
- GIAC Perimeter Protection Analyst
- GIAC Certified Security Consultant
- Snort Certified Professional

In addition, HUB Tech engages one of less than 150 people who have achieved the security industry's premier practical certification, the GIAC Security Expert, one of less than 15 people certified by SANS as a Cyber Guardian for both red and blue teams and one of less than 100 SANS Certified Instructors.

HUB TECH consultants also work to pass on security knowledge to the community via involvement with SANS teaching classes on:

- SEC401 - SANS Security Essentials – Bootcamp Style
- SEC503 - Intrusion Detection In-Depth
- SEC504 - Hacker Techniques, Exploits and Incident Handling
- SEC560 - Network Penetration Testing and Ethical Hacking
- SEC561 – Immersive Hands-On Hacking Techniques
- SEC542 - Web Penetration Testing and Ethical Hacking
- SEC440 - Critical Security Controls: Planning, Implementing and Auditing
- SEC566 - Implementing and Auditing the Critical Security Controls – In Depth
- SEC575 - Mobile Device Security and Ethical Hacking
- SEC464 - Hacker Guard – Security Baseline Training for IT Administrators
- MGT414 - SANS+S Training Program for the CISSP Exam

Business Focus and Value

While we have broad technical and industry experience Hub Technical Services, LLC focuses on business value contribution. We recognize that our clients have finite resources to safeguard their business. Our goal is to help clients identify and prioritize reasonable investments to meet their acceptable risk tolerance levels.

About Us

Hub Technical Services, LLC is a privately held information technology solutions provider based in South Easton, Massachusetts. Since our inception in 1992, the organization has been focused on serving the technology needs of Commercial, State, Local, and K-Hi Ed clients based in New England.

We adopt our client's aspirations and challenges then engage subject matter expertise to collaboratively achieve a desired objective. Our solutions expertise encompasses a broad spectrum of business technologies, professional and managed services.

Clients engage us to assess, architect, implement, and manage through the life cycle of cost effective secure solutions that drive intended business results.

We have an insatiable desire to increase the value our clients derive from a partnership with our organization. We relentlessly evolve our abilities with a certified staff of pre-sales, post-sales solutions engineers, and sales professionals that our clients and strategic business partners turn to as an extension of their organization.

Categorical expertise in:

Managed & Professional Services

Data Center Transformation

Client Computing

Information Security & Business Continuity

We have been awarded with a number of strategic state contracts in Massachusetts and Rhode Island including:

- ITC47 CAT 6 for Computer Hardware, Computer Maintenance and Services, as well as Project Management.
- ITT50 which provides access for Converged Voice and Data Networking Analysis, Architecture, Maintenance and Hardware Procurement.
- ITS53 as an IT services provider for Integration, Systems Planning, Security and Deployment Services.

Our Solution Sets

Managed & Professional Services

- Enterprise Solutions Consulting
- Infrastructure Monitoring
- Security Operations Center Outsourcing
- Executive-On-Demand Services (CIO/CISO)
- Help Desk Services
- Asset Life Cycle Services
- Managed Print Services

Data Center Transformation

- Cloud Solutions
- Hyper-Converged Solutions
- Virtualization
- Enterprise Storage Solutions
- Enterprise Networking

Information Security & Business Continuity

- Information Security Program & Policy Development
- Business Risk & Technology Vulnerability Assessments
- Penetration Testing
- Regulatory Compliance Assessments & Audit Response Services
- Information Security Awareness Programs
- Implementation & Utilization Improvement Services
- Data Classification & Protection Solutions
- Asset Management Solutions
- Identify & Access Management Solutions
- Endpoint Protection Solutions
- Secure Communications & Collaboration Solutions
- Secure Application Development Solutions
- Change Control Solutions

Client Computing

- Virtual Device Infrastructure Solutions (VDI)
- Endpoint Device Technology Solutions
- Endpoint Deployment Services
- Bring Your Own Device Solutions (BYOD)
- Mobile Device Management Solutions (MDM)
- Mobile Application Management Solutions (MAM)
- Enterprise & Personal Printing Solutions

Why Hub Technical Services, LLC

Our differentiation is in our people. We bring to bear an experienced and extensive staff consisting of highly trained and certified professionals whose sole function is to deliver exemplary service. Backed by decades of diverse professional experiences with thousands of clients we have amassed a wealth of repeatable best practices our clients benefit from.

Additionally, our internal training program consists of continuous investments in a broad curriculum ranging in matters from customer service to developing technical and business acumen relevant to our customer's needs. Our technical certifications are many and encompass a broad range of Tier 1 vendors.

The bottom line, we seek out and employ the right people and continuously invest in their professional development for our clients benefit.

Disclaimer

Warranty: Hub Technical Services, LLC warrants that the services or equipment provided complies with the statements made in the approved proposal for services and for a period of thirty (30) days from the date of signoff.

Warranty Disclaimer: Except as provided by express written warranties offered by Hub Technical Services, LLC directly to the Town of Brookline. Hub Technical Services, LLC disclaims all other warranties, conditions or other terms, express or implied, statutory or otherwise, on products or services furnished hereunder including without limitation, the warranties of design, non-infringement, merchantability or fitness for a particular purpose.

Limitation of Liability: Notwithstanding any provision contained herein to the contrary, except in case of bodily injury or death where, and then only to the extent that applicable law requires such liability, the maximum liability of Hub Technical Services, LLC to Town of Brookline or to any party whatsoever arising out of or in connection with any sale, use, or other application of any product, information, or service delivered to Town of Brookline hereunder, whether such liability arises from a claim based upon contract, warranty, tort, or otherwise, shall not under any circumstance exceed the actual amount paid by Town of Brookline for the product or service giving rise to such liability.

Disclaimer of Liability: Except in case of bodily injury or death where and then only to the extent that, applicable law requires such liability, Hub Technical Services, LLC shall not be liable for any loss of profits (even if they arise as a direct or immediate consequence of the event that generated the damages). Loss of business, loss of use or loss of data, interruption of business, nor for indirect, special, incidental or consequential damages of any kind whether under this agreement of otherwise, even if Hub Technical Services, LLC has been advised of the possibility of such loss and notwithstanding any failure of essential purpose of any limited remedy, in no case will Hub Technical Services, LLC be liable for any representation or warranty made by Town of Brookline or any agent of Town of Brookline.

Service provider indemnity: Each party agrees to hold the other party harmless, and to defend and to indemnify the other party from and against any liability, loss, costs, demand, claim, (including reasonable attorney's fees, expert fees, and other legal expenses) or cause of action for personal injury or property damage due to or arising out of the acts of that party, its agents and employees; provided, however, that, other than in instances involving willful misconduct or gross negligence, Hub Technical Services, LLC total liability to Town of Brookline under this Section shall not exceed the total amount paid by Town of Brookline to Hub Technical Services, LLC hereunder.

All opinions expressed in this document, related documentation, or any communication written or verbal do not constitute guarantees of performance or fact. All articles and tutorials presented in this engagement come with no warranty and should be followed with caution. Any reliance placed on such information is therefore strictly at the risk of Town of Brookline. Legal council should be engaged to clarify all matters related to State and Federal law.