CONTACT:
Research Section
5000 NASA Boulevard, Suite 2400
Fairmont, WV 26554
Ph: 877-628-7674
Fax: 304-366-9095
Web: www.nw3c.org

Cyber Intrusion and Data Breaches (2017)

The terms "data breach" and "cybercrime" are often used interchangeably, and though closely related they are not synonymous. The simplest definition of cybercrime is "criminal activity or a crime that involves the Internet, a computer system, or computer technology."[1] In the course of most cybercrime, some form of data breach is likely to take place; however, not all data breaches require the use of a computer. A data breach is an incident in which "an individual's name, Social Security number, driver's license number, medical records or financial records (credit/debit cards included) are potentially put at risk because of exposure. This exposure can occur either electronically or in paper format."[2] The loss of personally identifiable information (PII) during a data breach can be very damaging, regardless of whether the breach is the result of a hacker or the many other methods.

How They Occur

Who comes to mind when we think about cybercriminals? The most likely images are of state-sponsored computer hackers working in a foreign country maliciously attempting to hack state secrets from top-secret government computer systems. Recall for example, five Chinese military members were indicted by the U.S. Justice Department after conducting similar cyber attacks.[3] Another example might be the masked faces of the '*Anonymous*' hackers pursuing social change by engaging in "hacktivism" (Hacktivism is the act of hacking, or breaking into a computer system, for a politically or socially motivated purpose)[4]. Their most recent efforts include cyber attacks following controversial police shootings on the websites of Cleveland, Ohio;[5] Ferguson, Missouri;[6] and Albuquerque, New Mexico.[7] A third example might be a gang of criminals attempting to hack into databases to steal identity information that is later sold on the black market.[8] Most recently, there is the case of ongoing debate about the alleged Russian influence in the 2016 U.S. presidential election. Still another possibility might be simply an image of the junior high school kid with seemingly limitless computer skills, such as the two 14-year-olds who hacked a Bank of Montreal ATM machine during their lunch hour.[9]

All of the above events arguably involve examples of cybercrime and most of these incidents include a data breach; however, as previously noted, not all data breaches involve the use of a computer. When examined in total (which we will discuss later in this paper), the data breaches resulting from cyber intrusions or hacking only account for less than 30% in the last 10 years. [10]

There are several organizations that specialize in tracking reports of data breaches in the United States. In order to develop a meaningful database of sufficient size, NW3C combined the reported incidents of multiple sources and carefully eliminated any duplication. The result was a data set containing more than 5,000 reported incidents over the past decade, throughout the United States.

The sources used for the NW3C analysis are as follows:

- **The Identity Theft Resource Center (ITRC)** - is a non-profit organization that provides free services and victim assistance to consumers.[11] ITRC tracks and reports data breaches on a yearly basis that involve the compromise of sensitive personal information that could be used in identity theft.
- **The Privacy Rights Clearing House** - is a non-profit organization that provides a long list of services pertaining to the preservation of privacy including maintaining a database of reported data breaches dating back to 2005.[12]
- **The Breach Level Index, by Safenet** - tracks data breaches and categorizes them according to type of breach.[13]
- **The U.S. Department of Health and Human Services Office of Civil Rights** - investigates complaints of data breaches and tracks the number of data breach incident complaints reported each year going back to 2003.[14]
- **Publications**
    - Hackread (www.hackread.com)
    - Govtech magazine (www.govtec.com**)**
- **Online Blogs**
    - www.identityforce.com/security
    - www.bleepingcomputer.com
    - www.threatpost.com
    - http://thehackernews.com/
- **State Attorney Generals Web Sites**
    - California AG's website breach list https://oag.ca.gov/ecrime/databreach/list
    - Massachusetts AG's website breach list http://www.mass.gov/ocabr/data-privacy-and-security/data/data-breach-notification-archive.html

These organizations are widely recognized as valid sources of data breach information. All of the organizations use similar sources and methods of gathering data, thereby providing with comparable reporting standards for analysis.

It is important to note that the statistics reported by these sources do not represent the total number of data breach incidents occurring in the U.S. There are unquestionably data breaches that, for a variety of reasons, are not reported. In many instances, victims of a data breach may not yet know their system has been breached, therefore they have not reported the breach. There may be instances in the private sector that are intentionally not reported for a variety of reasons including: avoiding loss of customer confidence, fear of a negative impact of stock prices.

Many of the reporting agencies that track breach report incidents classify individual incidents according to the type of entity experiencing the breach. The main categories generally include business (sometimes further segregated by retail, financial or other), medical, government/military, and educational entities. An analysis of the data provides an opportunity to determine the degree of targeting for each type of entity. This allows the development of a picture regarding higher or lower propensity of data breach in any category.

Each of the sources shows that reported data breach incidents may be broken down into a few broad categories that capture the various methodologies by which the holder of records (the

victim) can experience a data breach. One challenge posed to analyzing information from multiple sources, is that the sources do not necessarily utilize the same classifications for the causes of the reported data breach. Depending on which source information was obtained, the classification of the cause/type of breach varied to some degree, making selection of a standardized method of classification an important aspect of NW3C's research.

The following is the list of standardized classifications:

- ***Unintentional Insider:*** data breaches resulting from the unintentional action or omission of a member of an agency resulting in the compromise of otherwise confidential information including, but not necessarily restricted to Personally Identifiable Information (PII). The data may be electronic or in document form. The disclosure can be the result of:
    - Failure to properly secure paper documents so as to protect the confidentiality of their contents.
    - Inadvertent exposure of PII in the normal course of business, for example, improper packaging of a document to be mailed in such a way as to expose PII
    - Inadvertently posting confidential information to a website belonging to the agency.
    - Failure to adhere to proper cyber security protocols such as using properly constructed login credentials and properly safeguarding them.
    - Failure to observe proper email procedures resulting in a successful phishing attack.
    - Failure to adhere to proper security protocols involving wearables and portable devices capable of storing digital information to memory.

- ***Hacking or malware*****:** Cyber intrusion by an outside entity that may compromise PII. Also included in this category were the ransomware attacks, regardless whether the reporting agency claimed that confidential information was compromised. Early forms of ransomware did not necessarily involve the potential compromise of PII, but as the practice evolved the ability to access, alter, or even remove information from the system under attack, developed to a significant degree.

- ***Malicious Insider Attacks*****:** Records compromised when someone within an organization, having otherwise legitimate access, abuses their credentials to access information illegally for their own purposes.

- ***Lost or Stolen Devices*****:** Lost or stolen electronic communications devices such as desktop computers, lap tops, portable hard drives, thumb drives, smart phones, copiers with the ability to retain information in digital memory, that may contain confidential PPI. Also included in this category are incidents involving improper disposal of electronic devices in which hard drives are not properly wiped of confidential information.

- ***Unknown***: Those instances of data breach where the cause of the compromise of confidential information is unable to be determined. There are, for example, reports of PII appearing on web sites and blogs catering to hackers where it is impossible to

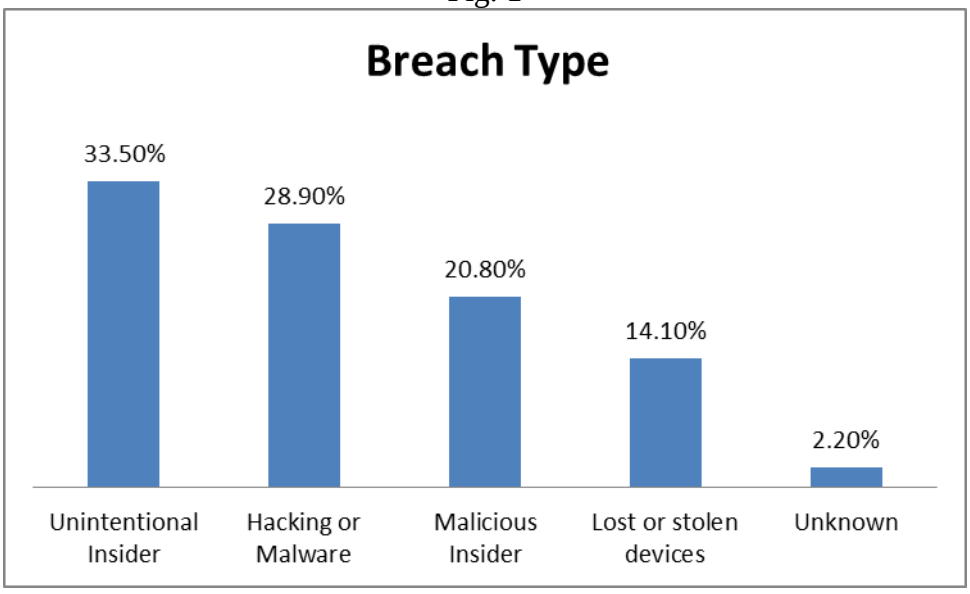
determine how that information got to the site in the first place. The owners never noticed or at least reported having experienced a breach and while the information is obviously of a confidential and protected nature, there is no explanation as to how it was obtained.

Several of the sources of data breach report lists, subdivided the reports by the sector involved; for instance, data breach incidents involving the medical field were classified separately from those occurring in the retail, education, or government fields. NW3C used those sources that differentiated by sector, to gain a better understanding of the degree to which the various sectors were reporting cyber intrusion/data breach incidents. Where the breaches did not differentiate, NW3C was forced to review all reports and classify where possible. Our analysis showed that *Business/retail* was the highest category accounting for 39.14% of the total; Medical/Health Care followed with 29.87%, and the *Education* and *Government/Military* categories came in third and fourth, with 14.83% and 14.07% respectively.

The ultimate focus of NW3C's research is state and local government data breaches. The original *Government/Military* category often included everything from hacking incidents involving NASA, the FBI, IRS and the U.S State Department, to data breaches suffered by individual cities and small villages. For analysis, we isolated and analyzed the category of government even further to distill state, county and municipal governmental entities from federal and military. By eliminating those instances of data breaches that involved federal government and military entities, it was possible to examine more closely the rate at which state, county, and municipal government entities fall victim. After distilling the data, there were 1,800 instances of reported data breach of various types from 2005 to the end of 2016 in the data set.[15]

From the information contained in the sample, we examined the sources and/or causes of the reported breach incidents for state and local government (see Fig. 1). Perhaps the most interesting feature of the results was that more than half (71.1%) of all reported data breaches in the last ten years are not the result of hacking (which only accounted for 28.9%), but are more accurately attributable to personnel and organizational issues.

Fig. 1



Costs and Statistics

Before examining how to mitigate the danger and how best to handle a data breach if/when one occurs, it is helpful to examine the potential costs of failing to adequately address the problem. The results of an independent study sponsored by IBM and conducted by the Ponemon Institute, covered a survey sample of entities that had suffered data breaches during the fiscal year 2016. The results of their survey showed that within the U.S.:

> *The average cost for each lost or stolen record containing sensitive and confidential information increased from $217 to $221. The total average cost that organizations paid increased from $6.53 million to $7.01 million.*[16]

A quick reference to the cost per record in the above paragraph ($221) should sufficiently illustrate the potential cost of not addressing the danger of data breach. In addition to the cost per record stolen, we must also take into consideration any incidental issues that arise following a cybersecurity breach. After a breach occurs, an emergency response team should identify the holes within their IT security system, determine how to close those holes, and review and adapt the response protocol as needed. It is also important to attempt to identify the responsible parties and prosecute. All of these measures add to the overall cost and are not easily computed.[17]

In addition, the response team should attempt to decide what services to offer the potential victims. Detection and notification of possible exposure should be the obvious first step. In the private sector and banking industries, a generally followed protocol for exposure of a customer's PII caused by a data breach typically includes timely notification of potential victims and the provision of some level of identity theft protection (at the expense of the holder of the dataset that was compromised). This may include credit-monitoring services provided to potential victims at the cost of the record holder. In government, this may prove cost prohibitive, but it is normal to afford some level of service to those who are inconvenienced by a breach; even if it is only a hotline used to refer victims to investigative services or counseling.

Investigation and recovery are often among the more costly expenses in the post-data breach process. According to the results of a survey of cybercrime victims, the average amount of time cybersecurity breach victims took to investigate, restore service and verify resolution of the incident was six months to detect that a cyber intrusion has occurred and two additional months to contain the issue.[18] For a municipality relying on an IT system to handle even a moderate amount of its routine business, this may prove disastrous.

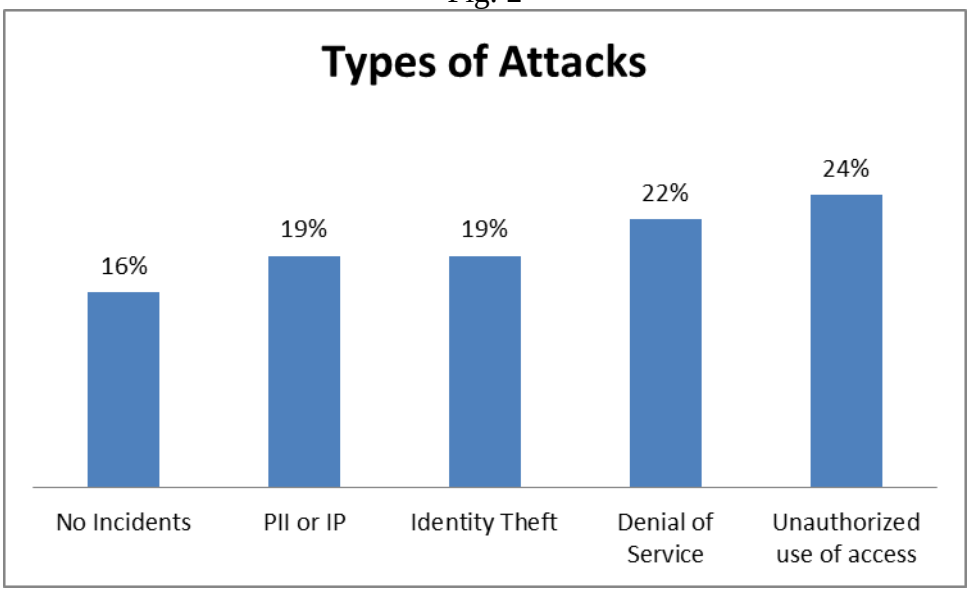
Loss of the IT function can be debilitating and costly, but a larger cost may be in the illegitimate use of the lost PII. Exposure of thousands of citizens' PII to the risk of identity theft can pose some serious problems for any governmental entity. Both the FBI and the Federal Trade Commission (FTC) note that identity theft is one of, if not the fastest growing crime in America.[19] According to the Identity Theft Resource Center 2016 data breach report, "the number of data breaches in 2016 hit an all-time high of 1,093, representing a 40% increase over the prior year."[20]

In an article written in April 2013, the marketing director of McAfee stated that "the number of malicious programs written to steal your information has grown exponentially to an estimated

130 million from about 1 billion in 2007".[21] These numbers only refer to software programs specifically designed to steal large quantities of personal information (hacking). It does not account for possible causes of data loss, which may include malicious insiders, lost or stolen electronic data storage devices, improper disposal of electronic digital information storage devices, etc.

In 2013, a partnership of the computer Emergency Readiness Team, (CERT) Division of Software Engineering of Carnegie Mellon University and the U.S. Secret Service conducted a survey of more than 500 U.S. businesses, law enforcement services, and government agencies. The below illustration (Fig. 2) is a breakdown of responses from those government agencies in reference to data breaches and their results.[22]

Fig. 2



Of the agencies surveyed, only 16% reported having experienced no data breaches of any type. 19% reported data breaches that resulted in the loss of PII or intellectual property (IP), but were unable to conclude that identity theft had taken place because of the breach. Another 19% reported verifiable incidents of identity theft because of their breaches. Denial of service was reported by 22% of the respondents, while 24% found their files and/or web sites had been altered in some manner. Finally, 24% of respondents reported the malicious insider threat or instances of unauthorized access and use of data, systems and networks.

Governmental entities do not normally have to concern themselves with some of the issues of the private sector; hence, the costs of a data breach may be slightly lower. For example, retail entities have to contend with loss of customer loyalty or lost revenue from copyright infringement (IP theft). While governmental entities may not be obligated to provide the types of relief that large corporate entities like Target, Home Depot or financial institutions and banks typically provide their customers who have personal information compromised by the company's data breach, there are still costly ramifications to suffering a data breach.

A significant portion of the potential costs of a data breach include investigation/prosecution of the incident and personnel costs of IT specialists.[23] After a breach it is common for IT specialists to work around the clock to determine the source of the attack, the extent of the compromise of sensitive information, and recover any lost information that may still be recoverable. Their task involves not only restoring the security of the system that was compromised, but also identifying and preserving evidence that may be needed for the investigation and potential prosecution of the perpetrator.

They also have to identify the weakness that led to the breach and correct it so that a repeat does not take place. There are also costs of clerical personnel required to make the appropriate notifications and assist residents in navigating the now damaged system. These costs can all add up to an impressive price tag. Disruption of critical IT services for prolonged periods can potentially constitute significant cost to a governmental entity, particularly if that entity uses its IT infrastructure to collect taxes, bill for services, maintain taxation records, etc. In addition, arranging for clerical staff to handle these types of repetitive tasks until the IT system can get back online will add to the cost of recovery. Recovering from any data breach incident could very easily wreak havoc with a tightly constructed municipal budget.

To complicate matters, the majority of governmental IT systems typically provide services to local law enforcement and other emergency service organizations. In a recent survey (conducted by NW3C)[24] of the members of the Major Cities Chiefs Association—an organization made up of the 68 largest municipal police agencies in the U.S. and Canada—it was found that only 50% maintain their own IT system, separate from that of their parent government agency. The degree to which police agencies of any size maintain their own IT systems is not fully known, however, it would seem reasonable to believe that it is rare for a police department to be large enough to maintain its own IT system, making the governmental entity the one responsible for securing that law enforcement organizations cyber security. Regardless of the particular arrangement, the sensitivity of the information law enforcement agencies routinely have access to, increases the importance of maintaining appropriate levels of security. Law enforcement necessarily has access to databases that the typical private sector entity or even other departments within the typical governmental organization would never be able to access. The extremely sensitive nature of the information residing on a police department's portion of the larger IT system cannot be overemphasized in this discussion. Compromise of databases containing PII of tax payers, governmental employees, politicians, property owners, or others doing business with a state, county, or local government is a serious problem.

A breach of information on a law enforcement agency's computer system that results in the compromise of information related to confidential informants, witnesses in criminal prosecutions, victims of sex crimes, child abuse or domestic violence cases, legally protected information related to juvenile offenders, are all very serious issues, many of which can actually compromise the administration of justice and potentially re-victimize victims of crime and negatively impact the outcome of criminal trials. A compromise of confidential information at this level could even pose a threat to the safety of complaining victims, witnesses, informants or undercover officers.

The Ferguson, Missouri officer involved shooting incident is a classic example of the damage a hacked IT system servicing a police agency can cause. The hacker group *Anonymous* claimed responsibility and left warnings. "If you abuse, harass or harm the protesters in Ferguson we will take every web-based asset of your department and federal agencies off-line."[25] Since that time the PII of the Chief of Police, photos of his home, his wife and daughter were released on the internet. Access to confidential personnel information of city employees will expose the safety and security of every police officer, firefighter, council member and chief executive of the municipality. Where information regarding complainants names and addresses in criminal actions result in witness intimidation, threats against crime victims, exposure of the identity of victims of sex crimes—all of which could turn into serious problems for the entity maintaining the compromised system.

The negative impacts of this type of information being exposed are potentially far more serious than identity theft. The responsibility for securing that information is, therefore, that much more critical. The degree to which the holder of the data is ultimately liable for breaches that result in damage to the credit of those who's PII resides in their system or, as in the case of the law enforcement entity whose personnel information is exposed, results in the very real danger of exposing officers to potential physical danger, will be examined later in this paper.

How likely is my city/county to become a victim?

One of the challenges in dealing with issues involving IT security and the potential of a data breach is urging government administrators to take the threat seriously and address the problem. In a world of tighter budgets, allocating resources to prevent and/or respond to cyber intrusions could very easily take a back seat to seemingly higher-priority spending issues. In 2010, a report by the National Association of State Chief Information Officers (NASCIO) notes that 50% of states reported spending less than 3% of their IT budget on security. The private sector spends 5% or more and state spending on cybersecurity is actually trending downward.[26] And yet, the media continues to carry report after report of state and local IT systems being compromised by outside malicious attacks (hacking). The city of Wichita, Kansas e-procurement website was hacked in October 2013, potentially compromising the private financial information of vendors that have done business with the city and current or former employees who have been reimbursed for travel and other expenses since 1997.[27]

In other examples, the city of Chicago, Illinois suffered a data breach not once, but three times. The first breach occurred in 2003, a second in 2006 and then again in 2012 in which the records of 1.3 million voters were compromised.[28] In 2007, a laptop containing the personal information of 280,000 city of New York retirees was stolen from its assigned user.[29]

Turkish hackers were responsible for intrusions into a Student-run TV station in Oswego, New York. The municipal database of taxpayers in Akron, Ohio, the web pages for Lansing, Michigan, and the police department in Mobile, Alabama, are all recent example of how vulnerable information may be on governmental systems.[30] The above attacks were classified as cyber vandalism because, although they did not steal any PII, the hackers posted slogans in support of their particular cause on the web sites, defacing and disabling them in the process.

In February 2014, a virus hit Portland Oregon City Water Bureau's billing staff and the Revenue Bureau through the city's computerized billing system.[31] In June 2014, what was described as a massive data breach affecting hundreds of Miami-Dade County, Florida employees was revealed when a county employee's personal information was discovered being used to file fraudulent unemployment claims and commit credit card fraud.[32]
In April of 2016, the Lansing Michigan Board of Water and Light (BWL) fell victim to a ransomware attack and was forced to pay $25,000.00 to foreign hackers. The total costs or recovery however, far exceeded the ransom payment.

> In addition to paying a $25,000 ransom to unidentified foreign hackers, BWL incurred costs of cyber forensics, the cleaning and testing of 700 to 800 laptops, desktops and servers, the replacement of an extensively infected server, and $400,000 in cybersecurity upgrades that brought the total to about $2.4 million.[33]

The list could go on almost indefinitely. The analysis conducted by NW3C currently stands at 1,800 governmental entities reporting data breaches through data breach; in reality, the number is likely to be far higher since more than a third of the reported incidents in our sample stated they were unable to determine whether PII was compromised and it is generally accepted that there are likely hundreds of entities out there who have been hacked or suffered a data breach but are unaware of an incident or its repercussions.

A final observation on cost is that it makes a very persuasive case for investment in appropriate measures to prevent, detect, and respond to data breaches. In a survey conducted of entities who have suffered a data breach and had to go through the recovery process, it was found that "data breaches drive increased spending in data security, according to 61% of respondents, the average increase [in post breach spending] is 20% [of the original cybersecurity budget]."[34] The International Data Corporation (IDC) publishes a yearly report predicting the projected IT security spending for various sectors in the U.S. economy. According to IDC:

> The industries that will see the fastest growth in their security investments will be healthcare (10.3% Compound Annual Growth Rate), followed by telecommunications, utilities, state/local government, and securities and investment services. Each of these industries will experience CAGRs above 9.0% over the forecast period.[35]

The argument of the IT supervisor to the governmental executive approving the budget then should be, "*pay for appropriate security now or pay more for recovery later*."

The Civil Liability Question

"In the wake of data breaches among U.S. retailers, many believe the risk of legal liability and costly lawsuits will escalate."[36] In 2011, the U.S. Department of Defense was hit with a $4.9 billion law suit for a data breach in which the PII of almost 5 million soldiers was compromised.[37] The suit asked for only $1,000.00 per victim, but considering the number of victims of the breach, the price tag sky rocketed. A question that is invariably discussed when dealing with this issue involves the potential for civil liability as it applies to the owner of the database of PII.

One of the hallmarks of American society is that you can pretty much be sued by anyone for anything. Even if the case gets thrown out of court early on, it's still likely to take up a good

deal of time, cost money in terms of legal resources needed to respond, and generate a great deal of needless anxiety. That means that all that can really be addressed is whether or not you're likely to be held accountable for the various problems that may occur when hosting, using, maintaining, or relying on massive data sets to do business.

At the current time, there are 47 states within the U.S.[38] that have specific legislation requiring reporting data breaches that involve compromise of confidential personally identifiable information. There are similarities in many of the states as to the numbers of PII records that have to have been compromised to cross the legislated threshold to trigger the reporting responsibility, variations in the amount of time between first learning of a breach and the responsibility to report, and the penalties for failure to adhere to the legislation, however, the important issue here is that the majority of states have at least taken the matter seriously enough to have legislated a reporting requirement. The issue of liability that a governmental entity is likely to be faced with is, or at least should be a question of considerable concern. The problem appears to be new enough that there are no hard fast answers. Case law is developing as civil suits against the holders of breached data sets are winding their way through the court systems. In an effort to gain some understanding of what the issues are and where we stand currently, with respect to civil liability borne by a governmental entity suffering a data breach, NW3C's research staff and research attorney has studied the problem and the following discussion represents the current situation as it exists, at least as of the writing of this white paper.

State and Local Government Cyber-Liability

State and local governments (and their component agencies) need to proactively secure their digital assets against criminal access and use before they become victims of cyber-criminals – and to take steps to mitigate the damage caused by anything that slips through their defenses. In 2015, NW3C reviewed reports of over 300 data breaches, exposing over 400 million identities, and over 362 thousand ransomware incidents.[39] It's not a question of if governmental entities are being targeted – most state and local agencies had at least 6 breaches in the past two years[40] and almost five times as many identities were compromised by government data breaches in 2015 than by all retail breaches combined.[41] The cost of data breaches is at a new record high ($221 per compromised record),[42] and damages from these incidents routinely run into the millions of dollars (an average organizational cost of $7 million per incident in 2016)[43]. It's also not a question of leaving it to your IT department – the agency CEO needs to be involved in this. The impact of these decisions is organizational and systemic, and risk points located in organizationally insignificant locations can lead to tremendous financial losses.

What Could Go Wrong?

The immediate risks inherent in a data breach are fairly well-known (namely expensive and/or burdensome lawsuits from those affected by the breach). There's certainly no reason to downplay those risks. Even suits that don't succeed can tie up manpower and drain other departmental resources through drawn-out discovery and deposition proceedings. Suits that do succeed can, of course, take millions from your budget or from the state's general fund. The direct damages caused by the breach are just the beginning of the analysis, however. A class-action lawsuit from citizens whose credit card information was exposed through your online fee-payment system will hurt – but relatively few of them will have suffered direct,

unreimbursed losses. Their losses were generally absorbed by their banks and insurance companies. What about your personnel whose personal information, including names, addresses, dependents, vehicle description, are made public and potentially placed in danger? What do you tell the residents of your municipality, county, state, whose PII is laid open to identity thieves. How do you deal with the loss of public trust that accompanies this type of scandal?
Think of the sorts of information that your organization collects and/or processes. How could that information be misused?

- Financial information could be used to commit fraud
- Personal identifying information could be used to commit identity theft
- Personal information on children, witnesses, informants, victims of crimes, and other vulnerable populations could be used to violate their privacy or facilitate crimes against them
- Information on regulated business could be used by business rivals
- Information on governmental bidding, contracting, or economic development plans could be used to competitive advantage
- Information dealing with active investigations (civil, criminal, or administrative) could be used to compromise those investigations
- Sensitive information could be made public
- Personal information on government employees could be used to exact revenge for unpopular decisions

Mille Lacs County, Minnesota and Mikki Jo Peterick were forced to jointly pay $1 million to people whose Minnesota Driver's License records were impermissibly accessed by Peterick while she worked as a child support investigator for the Mille Lacs Department of Family Services. No allegations were made of the use to which such information might have been put.

-Settlement Agreement, Candace Gulsvig et al v. Mikki Jo Peteric et al., US District Court for the District of Minnesota, Civil File No. 13-cv-1309 (JRT/LIB) https://www.knowyourrights.com/SiebenCarey/media/News_PDF/Settlement-Agreement.pdf

For that matter, how would your organization recover from losing access to any of this information? Crypto-ransomware (malicious software that encrypts a victim's data and then offers to sell the victim the decryption key for a price) infections are on the rise[44] and have already crippled hospitals, police departments, and other vital cornerstones of public infrastructure. Medfield, Massachusetts lost its municipal computer network to ransomware for a week[45] and more than 700 police departments across the nation have been hit.[46,47,48] Do you have a plan in place for when you're hit next?

Similarly, you should think over the sorts of devices that your agency uses, and what sort of internet connectivity and functionality they have.

- Are you not sure what would go on that list? That's a fairly bad sign.[49]
- Internet-enabled video feeds may be intercepted (video and/or audio)
- Internet-enabled vehicles may make themselves more vulnerable to theft or sabotage
- Smart controls may be used to sabotage, monitor, or manipulate connected devices

These aren't just abstract hypotheticals. Smart meters run by local utilities have been getting hacked to commit utility fraud since at least 2009,[50] Iranian hackers gained control of New

York's Bowman Dam's sluice systems in 2013,[51] and 2016 saw the first major cyberattack launched from compromised internet-connected consumer devices.[52]

What Would You Be On The Hook For?

Negligence

Being sued for negligence is always a possibility in situations where people experience loss. There's just no way around it. To be liable for negligence, first your state has to allow you to be held liable (more on that later). Secondly, it must be shown that you had a duty (generally, a "duty of care"), that you breached the duty (generally, by not exercising "reasonable care"), and that the breach of duty caused the damage in question ("proximate cause").

While private citizens are the most immediate victims of many data breaches, they also typically constitute the least well-positioned class for bringing negligence actions. Negligence requires both a duty and harm. The duty part is generally assumed – the entity who collects and holds onto someone else's private information (especially when that process is mandatory) owes a duty of care to the people whose information is being held. Harm, however, is a different matter. A negligence claim requires that the harm (a) occur, and (b) occur because of the defendant's failure. Many private negligence claims will fail here. The vast majorities of consumers who suffer from data breach-related fraud are immediately reimbursed by their banks (and therefor have already been made whole, so far as the law is concerned). Any further damages are purely speculative.

Past that, the private citizen must show that any harm that they suffered occurred because of this breach. In this case, the very ubiquity of data breaches in today's society provides some unexpected respite. Many individuals' personal information will have already been compromised before your incident, and they may have a great deal of difficulty proving that your data breach was the one that the criminal was using (especially if the criminal was never prosecuted, which is fairly typical).

One grey area here is credit monitoring. Some courts have held that having to pay for credit monitoring services is a harm that the victims are actually suffering now, is a reasonable step to mitigate the harm, and that it is a direct result of knowing that their information was compromised in the breach in question. [53] Others courts (the majority) have held that credit monitoring services are not a harm that was created by the defendant's lack of care (but, rather, a harm that the plaintiff has chosen to inflict upon themselves[54]), or that they are, essentially, a repackaging of a speculative future harm for which the plaintiff would only be able to recover if and when it happened.[55]

As previously mentioned, however, the individual citizens are unlikely to be the most worrisome party to bring a negligence action against you. The financial institutions impacted by the breach may come after you to recover the money that they reimbursed their customers, as well as for associated costs (investigations, credit monitoring, etc.). Unlike similarly-situated private individuals, these institutions will be in a far stronger position as they will be suing you not for

speculative damages, but real damages that they have already incurred.[56] They are also far more likely to use a legal team with deep experience and expertise in these sorts of actions.

While it isn't related to negligence, it is worth pointing out that some institutions (such as credit card companies) may also have provisions in their payment acceptance agreements that may subject you to contractual penalties for not following proper data security practices.[57]

Sidebar: Sovereign Immunity

Sovereign immunity is, historically, the sovereign's privilege not to be subject to suit in his own courts unless he wishes to be. The Supreme Court has held[58] that the Eleventh Amendment re-affirms that states also possess sovereign immunity and are therefore immune from being sued in federal court without their consent.

However, a "consequence of [the] Court's recognition of pre-ratification sovereignty as the source of immunity from suit is that only States and arms of the State possess immunity from suits authorized by federal law."[59] The natural follow-up question is which entities are arms of the state and which aren't. That answer, unfortunately, varies widely by state. In some states, counties are seen primarily as political subdivisions of state government.[60] In others, they're seen primarily as private corporations.[61] Likewise, cities and municipalities generally lack sovereign immunity,[62] but some states will extend it, at least in some cases (such as when the city is functioning more as an extension of the state government and less as a corporation).[63]

Exceptions exist even when an entity is otherwise covered. For example, "immunity does not extend to a person who acts for the state, but [who] acts unconstitutionally, because the state is powerless to authorize the person to act in violation of the Constitution."[64] Additionally, the basis of sovereign immunity (as applied to states) is that they can't be sued without their consent. Where they have given their consent (by statute, for example), sovereign immunity offers no protection.

The long and the short of it is that this is a discussion for you to have with your legal counsel.

Statutory Penalties

42 U.S.C. § 1983 (Civil action for deprivation of rights) creates civil liability for violations of Constitutional rights (e.g., the Due Process Clause).

The argument that government action has resulted in taking something without due process of law is generally advanced only after something tragic has happened. For instance, this line of reasoning was invoked in a 2008 case where a disgruntled ex-boyfriend gained unauthorized access to 911 information. He then used the information to track down and murder his girlfriend's new boyfriend.[65] At that point, it can be argued that the government's actions (in releasing the data) deprived the victim of life, violating the Due Process Clause. (Which reads: "No State shall deprive any person of life, liberty, or property, without due process of law ...") Of course, since the Due Process Clause includes deprivation of property as well as life, there's no reason why it couldn't be invoked in cases of identity theft just as easily. (It's just that the case law so far is heavily skewed towards instances of loss of life.)

The Due Process Clause, generally, doesn't create an affirmative duty for the state to protect its citizens from the acts of private individuals. However, there are two standard exceptions to that rule. One is when the state has taken custody of someone (in which case, the fact that the state is preventing them from acting as they see fit to protect themselves creates a duty for the state to offer them reasonable protection). The other is when the state created (or enhanced) the danger in the first place.

While the Supreme Court has yet to officially adopt a theory of state-created danger, it's been used in the 2nd, 3rd, 6th, 7th, 8th, 9th, 10th, and 11th circuits, and D.C. Each circuit enumerates its test for state-created danger a little differently, but the 3rd circuit's is a good representation.

To prevail on a state-created danger claim in the Third Circuit, a plaintiff must prove the following four elements:

> (1) the harm ultimately caused was foreseeable and fairly direct;
>
> (2) a state actor acted with a degree of culpability that shocks the conscience;
>
> (3) a relationship between the state and the plaintiff existed such that the plaintiff was a foreseeable victim of the defendant's acts, or a member of a discrete class of persons subjected to the potential harm brought about by the state's actions, as opposed to a member of the public in general; and
>
> (4) a state actor affirmatively used his or her authority in a way that created a danger to the citizen or that rendered the citizen more vulnerable to danger than had the state not acted at all.[66]

Three of those prongs are not very good news in the case of unauthorized access or a security breach. Depending on just what sort of information is obtained, the harm may or may not be foreseeable and fairly direct (prong 1). In today's age of widespread digital crime, however, it doesn't take much imagination to form a foreseeable and fairly direct link between the release of sensitive data and a significant harm or loss. Similarly, the person whose information was compromised is certainly a foreseeable victim of the act (prong 3) (or, in the case of a larger data breach, a member of a discrete class of persons subjected to potential harm). For that matter, through creating the data system in the first place (and, in the second place, by protecting the data in whatever manner that it was protected), a state actor used their authority to create the danger (or, at least, to make the citizen more vulnerable than if they had not done so) (prong 4).

Help comes from the second prong (a state actor acted with a degree of culpability that shocks the conscience). But what is culpability that "shocks the conscience"? That's a little harder to pin down. It's a standard with a good pedigree, at least. The U.S. Supreme Court has stated that "for half a century now we have spoken of the cognizable level of executive abuse of power as that which shocks the conscience."[67] But what, exactly, have they meant by that for the past 50 years? That's harder to say.

The courts have generally acknowledged that the "shocks the conscience" test is situational. Behavior that's understandable in a high-pressure situation is less understandable when the person has time to deliberate and come to an unhurried judgment. In an extremely tense environment, an actual intent to cause harm is usually required. On the other end of the spectrum, deliberate indifference has been acknowledged to be enough when the state actor has ample time to think things through. Some courts have even suggested that actual knowledge of a risk of harm is unnecessary when the risk is so obvious that it should be known.

So, where does that leave us? That's a good question, and one that can't be answered outside of court, I'm afraid. All we can do at this point is look at other cases and get a general sense from them. Consider the 2008 case involving the release of 911 information: this was a situation where the murderer was aided by his coworkers in the 911 call center who knew of his emotional state and pulled up the relevant records for him anyway. The coworkers' behavior was considered to be potentially so indifferent to the victim's safety that it could shock the conscience.

On the other hand, in a case where the names, addresses, social security numbers, and phone numbers of two arresting officers and their immediate families were given to a defendant in a drug trial (or rather, his lawyer, who provided him with copies),[68] the city's human resources department and the employee who released the information were considered, as a matter of law, to be guilty of negligence at most (mere negligence is not enough to shock the conscience).

The main difference between the cases, for our purposes, is that, in Phillips, the government employee knew that something was wrong with the general situation and supplied the information anyway (as they knew that their coworker was emotionally distraught and wasn't supposed to be accessing the files of his ex-girlfriend and her new boyfriend), while in Hart, the idea of the files ending up in the wrong hands hadn't occurred to the employee, who had assumed that everything was routine. There's certainly a difference there, but there's no clear line. Unfortunately, there's no real guidance yet that directly addresses computer security breaches as state-created dangers. However, it looks like it would take an extremely damning fact pattern for a computer security problem to be more than negligence, at least the first time any such problem emerges. After the agency's aware of the problem, though, a finding of deliberate indifference becomes increasingly likely.

Section 5 of the FTC Act prohibits unfair acts or practices. In this context, "unfair" means that it "causes or is likely to cause substantial injury to consumers", "cannot be reasonably avoided by consumers", and "is not outweighed by countervailing benefits to consumers or to competition".[69] While the FTC Act only applies to persons engaged in commerce, accepting money in exchange for services arguably puts local governments in the thick of it. The FTC has routinely alleged that failure to employ "reasonable and appropriate" security measures to protect personal information and files was an unfair act or practice.[70]

The tort of Public Disclosure of Private Facts occurs when someone publishes non-newsworthy, private facts that are so intimate that their publication would be offensive to a reasonable person. So, to start with, it's hard to see maintaining an information system as "publishing" the information. Even if the information is given to a select list of people- say,

government employees in the course of their work - it's not considered publishing unless the information is disseminated to the public at large (such as in a periodical). Distributing information to a closed list of individuals, rather than the general public, does not constitute publication. That said, the comingling of private and public web pages on the internet makes the accidental public posting of private information far from impossible.[71]
Privacy can also be framed as a Constitutional matter, however, as one of the liberties protected by the Due Process Clause. This brings it back to a 42 U.S.C. §1983 action (discussed at the start of this section), however.[72]

Post-breach notification laws exist in every state but Alabama, New Mexico, and South Dakota.[73] These laws typically impose penalties for failures to promptly notify people whose information was compromised in a data breach. This can result in potentially expensive consequences if your agency's response to a data breach incident doesn't follow legal requirements.

Managing Your Agency's Risk Exposure

Hardening Your Systems

Security in the modern world has two main components – the machines and the users. Your IT team needs to maintain their training and certifications, keep abreast of the most recent security developments, and have the manpower, access, resources, and support to implement the changes needed. On the user side, users must be trained in proper security practices – and then monitored and/or tested to make sure that the abstract knowledge has actually translated into the desired changes in behavior. Your whole organization, from top to bottom, needs to be well-trained and vigilant in order to maximize operational security.

That said, maximizing computer security across all aspects of your organization is rarely a realistic goal. Assuming that you instead need to maximize benefits per dollar spent, a little preliminary research may be in order. Liability analysis of corporate entities has shown that, on average, 92% of all computers in such organizations contain assets representing a total liability of between $25,000 and $250,000 (not counting servers, which contain more than $300,000 in potential liability). 5% contain liabilities under $25,000, and 3% contain over $250,000 in liability.[74]

While it isn't a given that an analysis of corporate liability patterns is perfectly generalizable to a government context, there are enough similarities to suggest that merely identifying and better securing the most potentially damaging 3% of your agency's computers will have a disproportionately positive impact on your potential liability. In a hundred-machine office with one server, this means that concentrating on just three machines and the server may reduce your agency's risk exposure by more than $1 million.

Insurance

Don't trust that your standard, brick and mortar errors and omissions policy will cover you in the case of a successful cyber-attack. The right cyber insurance can soften the blow of from

those incidents that make it past your defenses. There are more than 40 companies offering such coverage,[75] however, and their products are far from standardized.

Your risk assessment team needs to conduct a cyber risk assessment, determine where your current gaps in coverage exist, and identify policies that completely fill the gaps. Bear in mind that just a few words difference between policies can have a radical impact on your coverage.

Things to look for:

- **Exceptions for rogue employees need to be drawn as narrowly as possible**
    - It might be unrealistic to ask an insurer to cover you for any and all actions taken by rogue employees – but the damage that an ill-intentioned (or even misguided) person with legitimate access to your information resources could do is often enormous.
        - Example: An employee uses a personal electronic device (such as a smartphone) to transmit sensitive, work-related information, in flagrant disregard for established policy. They lose this device at a bar. Your state laws require you to notify everyone whose data might have been compromised. Are you covered for the notification costs?

- **Your coverage shouldn't require an external actor to be the proximate cause of the loss**
    - Companies with policies in place to protect against external actors penetrating corporate security have been denied coverage for losses stemming from social engineering attacks (where employees are manipulated into performing actions on behalf of attackers).
        - Example: *Ameriforge* Group, Inc. was hit by a phishing attack (an attack that relies on fraudulent messages made to seem as if they originated from a trusted source) that impersonated the company's CEO to its director of accounting to secretly transfer $480,000 in regards to a sensitive business acquisition. The accounting director complied, only to find out a week later that the transfer was unauthorized. The criminals were long gone by that time, and the money was unrecoverable. While *Ameriforge* had a robust cyber insurance policy, it only covered fraudulent transfers made by hackers – not legitimate (if mistaken) transfers made by employees.[76]

- **Your coverage should be as neutral as possible, in regards to technology and techniques**
    - Information technology and criminal techniques are both evolving rapidly. Even if you manage to secure coverage that completely covers your current exposure in the current environment, it's hard to know that your original assumptions will all still be valid six months out, much less years later. Where possible, don't tie your coverage to specific technologies that you use, or to specific criminal attacks that you anticipate.

        - Example: Suppose that you take out a policy to cover you in case of a malware infection, but it specifies that your insurer will pay for the cost of repairing, restoring, or replacing the systems (whichever is cheaper). The computers controlling your automated 911 system get hit by ransomware, demanding money to restoring your systems. You pay up, in the interest of public safety. Since you allowed yourself to be bound to one particular method of responding to the incident (though one that would have made sense before 2013), your insurer is unlikely to reimburse you.

- **Get coverage for contingent business interruptions**
    - A policy will often cover the direct damages resulting from an attack – but the direct damages aren't always where the bulk of your agency's troubles will lie. You need to be covered not only for the costs of dealing with being targeted by cybercrime, but for the costs that accrue because you were dealing with the crime. In a standard business, these might largely be opportunity costs – the cost of lost sales and profits. In a government context, this is far more likely to be the cost of government services being unavailable – which can range from an annoyance to a matter of life and death. In 2016, the indirect costs associated with a data breach were almost twice as high as the direct costs. ($145 per person vs. $76)[77]
        - Example: Going back to the example of your 911 system being targeted, let's assume that your city is targeted by Anonymous and they launch a denial of service attack against your 911 systems, flooding them with fraudulent 911 requests. Your IT department is able to get the problem sorted out within a day or two, and no hardware is actually damaged. Your direct damages are relatively minor – maybe a bit of overtime or hiring on a few short-term workers. But the indirect damages (the consequences of a community being without effective 911 capability for a few days) are potentially much, much higher – and many parties are likely to try to pass those costs on to you.

- **Your coverage should include your legally-mandated response to incidents**
    - States may require you to act in certain ways after an attack, and these required actions are not generally without cost, at least in manpower. Figure out what you'll be required to do in case of an attack and make sure that the cost of it is already bundled into your insurance. Most insurers offer this sort of policy.
        - Example: The University of Utah incurred $3.3 million in costs in notifying their hospitals' 1.7 million patients of a third-party data breach that impacted them, as they were required to do by statute. They didn't have specific cyber insurance, and their general insurer refused to cover the loss.[78]

- **Be wary of accepting a duty of care**
    - While it should almost go without saying, any component of your insurance that specifies that coverage is contingent on proper behavior on the part of your agency invites your insurer to do everything in their power to show that your agency didn't live up to its obligations. While it's unlikely that any insurance company could be persuaded to part with such requirements entirely, it's vital that you note where such requirements are embedded in your policy, that you bring it to the attention of your top administrators, and that you get your insurer to sign off that your specific policies meet their requirements (making sure that your employees actually follow said rules is slightly tougher, mind you).
        - Example: Cottage Health System suffered a data breach in 2013. The data breach allegedly occurred because Cottage Health (or a third party vendor) stored medical records on a completely unsecured system that was accessible from the internet. A class action lawsuit against the nonprofit prevailed to the tune of $4.1 million, for which Cottage Health looked to its insurance for coverage (it was covered for privacy injury claims and privacy regulation proceedings to $10 million, with a $100,000 deductible). The insurer refused to fund the settlement however, on the grounds that an exclusion to the policy precluded coverage for failure to follow minimum required practices.

          The insurer claimed that the hospital system failed to implement the procedures and risk controls identified in its insurance application. Notably, it claimed that the data breach was caused by Cottage Health's "failure to regularly check and maintain security patches on its system, its failure to regularly reassess its information security exposure and enhance risk controls, its failure to have a system in place to detect unauthorized access or attempts to access sensitive formation stored on its servers and its failure to control and track all changes to its network to ensure it remains secure among other things."[79]

- **Consider a policy that covers intentional acts by your agency that may nevertheless generate liability.**
    - A cyber insurance policy is often thought of as a way to protect against accidents and crimes. These are not the only things that can generate liability, however. Your agency may at some point intentionally engage in online or computational activities that are later deemed to be subject to civil liability.
        - Example: A data processor, Federal Recovery Acceptance, Incorporated (FRA), processed payments for Global Fitness. Global Fitness later entered into an asset purchase agreement with L.A. Fitness that included transferring its account data (which was held by FRA). FRA retained several key bits of information (such as credit card data) and refused to release them without significant extra compensation. Accordingly, the

purchase price for Global Fitness dropped dramatically. FRA had cyber error and omissions coverage which read:

> SECTION I—ERRORS AND OMISSIONS LIABILITY COVERAGE
>
> 1. Insuring Agreement
>
> a. We will pay those sums that the insured must pay as "damages" because of loss to which this insurance applies. The amount we will pay for "damages" is limited as described in Section III–Limits Of Insurance in your CyberFirst General Provisions Form.
>
> b. This insurance applies to loss only if:
>
> (1) The loss arises out of "your product" provided to others or "your work" provided or performed for others;
>
> (2) The loss is caused by an "errors and omissions wrongful act" committed in the "coverage territory";
>
> (3) The "errors and omissions wrongful act" was not committed before the Errors and Omissions Retroactive Date shown in the CyberFirst Declarations or after the end of the policy period; and
>
> (4) A claim or "suit" by a person or organization that seeks "damages" because of the loss is first made or brought against any insured[80]

"Errors and omissions wrongful acts" were defined as "any error, omission or negligent act".[81] FRA turned to its insurer to shield it from the judgment against it and the insurer refused, on the grounds that, though it was arguably a wrongful act to withhold the data, it was not an error, omission, or negligent act. The insurer prevailed in court.[82]

- **Strongly consider obtaining retroactive coverage.**
  - Given that most data breaches aren't discovered for more than six months[83], it's important to consider retroactive coverage dates. Many insurers are willing to write policies covering activity that occurred as much as two years prior. Without it, you won't be covered for acts that occurred before the policy date, even if they weren't discovered (much less claimed) until after the coverage date.

- **Make sure that your coverage matches your exposure in magnitude as well as type**.
  - Data breach liability can easily reach into the millions. There's simply no point in securing insurance that won't significantly cushion that blow. Work with your risk assessment/management team to make sure you've got enough insurance to cover what you need.

- **Be cognizant of any applicable sub-limits** (limits on an insurance policy that provide reduced coverage for specific types of loss).
    - While your main policy might cover you for a large enough amount to provide for your safety, be aware that you may not always be able to call upon the full strength of your policy. Insurers often limit how much they will cover in particular instances.
        - Example: A $10 million primary policy is likely to have a $2-$5 million sublimit for regulatory actions.[84]

Don't expect to obtain cyber insurance overnight – this isn't a well-explored, standardized product and it's worth it to insist on multiple face-to-face meetings with insurers to make sure that they understand your needs and that you understand what they can offer.

Action Items

1. **Talk to your legal team** – Is your agency protected from data breach litigation by sovereign immunity? What are your legal duties in case of a breach? What contractual data security obligations has your agency incurred?
2. **Talk to your facility managers** – What equipment is internet-enabled (regardless of whether or not such features are actually used)? Have they informed IT of each one, even if the online features aren't being used? Just because you aren't using the functionality doesn't mean that nobody else can! What protections do these devices have against being hacked? What could happen if they were?
3. **Talk to your risk assessment team** – Of all the information that your company handles, which puts it at the most risk? How much risk are you carrying, in terms of information? Where is that information at risk of exposure? Which computers in your organization contain the most potential liability?
4. **Talk to your IT team** – Is your agency compliant with relevant data security standards? If not, how do you get there? Are your employees (at all levels!) receiving security training? Can IT harden the targets you identified in items 2 and 3?
5. **Talk to your financial team** – Do you have relevant insurance? What does it cover? Does your coverage match your exposure?

The Response/Current Efforts

A detailed discussion of the process of dealing with data breach issues is far too technical and complex for the purposes of this white paper. Considering the speed with which technology evolves, any such attempt would likely be outdated before the work is published. Rather than attempt to provide a the step-by-step description of how to go about dealing with a cyber intrusion or a data breach, it is more productive to deal with the policy and procedure aspects of the process and leave the technical details to the IT experts. The IT manager should be charged with staying current on threats to cybersecurity and recognized industry standard best practices for addressing those threats. They are the content experts to whom top-level executive government administrators turn when a data breach occurs. In turn, it is the responsibility of that top-level administrator to assure that the municipal IT security measures are up to industry

standards and that a viable incident response protocol is in place. This necessarily means working together with the IT manager not only when an incident occurs, but at budget time and throughout the year to assure that the confidential records necessary for government to function, are protected to the greatest degree possible.

> *Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. Continually monitoring for attacks is essential. Establishing clear procedures for prioritizing the handling of incidents is critical, as is implementing effective methods of collecting, analyzing, and reporting data.*[85]

There is a multitude of sources for recommended technology and software related measures that should be considered when preparing for and responding to a cyber intrusion incident. A review of a number of noted authorities on the topic revealed striking similarities in their recommended course of action for an effective incident response.

- The Software Engineering Institute of Carnegie Mellon University published a paper[86] outlining a plan involving 18 high-level tasks that need to be addressed in preparation for the inevitable cyber intrusion.
- The SANS Institute, specializing in research and education in computer security and internet security issues, published their recommended 20 Critical Security Controls for Effective Cyber Defense[87].
- Verizon, in its 2014 Data Breach Investigations Report, addressed the broader issues of data breach involving cyber intrusion and recommended several measures designed to prevent, prepare for and remediate the cyber intrusion based data breach.[88]

Without getting bogged down in the technical aspects of cybersecurity, it is safe to say that malicious intrusions (hacking) pose problems that are normally addressed with firewalls, anti-virus software and various other technical methods. As the analysis of reported incidents of data breach discussed above indicated, this type of data breach only accounts for a little over 29% of reported incidents. Keeping up with the latest in threat prevention is an ongoing battle. As programmers come up with stronger security measures for IT systems, hackers are continually working to find their vulnerabilities. As they discover those vulnerabilities, software designers are continually trying to find ways of addressing them. The best anyone can hope for is that the IT manger stays abreast of the latest development in both threats and threat prevention and is able to convince the chief executive of that level of government to incur the expense of dealing with the threat before a data breach takes place.

Lost or stolen devices can be addressed to some degree with measures such as data loss prevention software, encryption or anti-theft software that prohibits unauthorized access to a device. Where a lost laptop or digital storage device is encrypted, the information contained is at least safe from compromise even though it may be lost. It may be possible to obtain software for institutional portable electronic devices, equipped with tracking capability so recovery is more likely. Hopefully a backup exists and recovery will be relatively simple.

These two categories combined (Hacking and Lost or Stolen Devices) still leave more than 60% of all reported data breach incidents attributable to some form of non-technical action. This

means that those data breaches involve incidents where policy and training are likely to be the most effective tools for dealing with issues such as inappropriate access by an insider, malicious insider activity, or accidental disclosure of confidential information.

The importance of training employees and those having access to a system cannot be overstated. One analysis of reported data breach incidents found:

> *..in the vast majority of espionage attacks, hackers gained access to computer systems through 'spear-phishing'; e-mails carefully tailored to an individual employee, official or executive, including a compromised link or attachment. E-mail attachments accounted for 78 percent of espionage attacks, according to the report*.[89]

A comprehensive list of preventive measures and recovery processes is too lengthy for the purposes of this work, however, throughout our research, it became clear that the majority of sources dealing with the problems of data breach and cybersecurity seemed to share the same ideas on how to best protect a system from intrusion as well as preparing for the inevitability of having to deal with an intrusion. The most frequently recommended measures gathered from a number of authoritative sources that may help mitigate the threat of a data breach of any sort include:

- **Ensure the IT manager remains current on threats as well as security measures:** IT managers need to stay abreast of the threat environment as well as the latest developments in threat management and response and keep top level executives briefed is a requirement. Appropriate budgetary resources must be properly allocated to assure that the IT system is protected (at the very least) to accepted industry standards.

  This is a particularly challenging area for a couple of reasons. As technology and the environment of electronic communications and digital data management are always changing, staying on top of the latest trends can be quite challenging. Conveying an understanding of the importance of these changes to the top-level executives who may not fully understand highly technical issues can pose another challenge for the IT manager. When a data breach takes place, a victim comes forward in civil court seeking damages, and the IT system is found to fall below "industry standards", the media portrays and the public tends to see the governmental entity as being responsible for having allowed their IT system to operate without following best practices in prevention. This lack of diligence may expose the municipality to charges of negligence (see legal analysis above) and raise the question of liability.

- **Executive Involvement:** Involvement of top-level executive management, those to whom the IT manager reports, is a critical part of the equation. Although the topic is often challenging for those not trained in IT security issues, it is imperative that the executive(s) responsible for building the budget regularly communicate with and take seriously, the information pertaining to system security provided by the IT manger.

- **Provide access only as needed:** Have an established well thought out and comprehensive policy on user access to the IT system. Be very careful of allowing access to third parties with whom you are contracting. If it is necessary to provide access

to an outside third party, be sure to review their security measures and that it does not provide a weak spot for intrusion into your system.

- **Keep close track of those portable electronic devices with access to the IT system:** Inventory and audit the number of portable devices in use to assure that they are where they belong, being used for what they were intended to be used for, and that they are equipped with the most up-to-date protection possible. Also, inventory and audit the programs in use on those electronic devices. Be certain that employees have not managed to install software programs allowing remote access to work terminals from personally owned computers, Smartphone's, etc.

- **Strictly enforce password policies:** Maintain a policy of regularly changing passwords of users, assuring users select satisfactorily strong passwords. Also, maintain clearly written, understandable policies regarding access and use of the IT system, educating users, monitoring adherence to those policies and most of all, enforcing the regulations of those policies. Policies are of little use if they are not enforced with appropriate, corrective action when violations are identified.

- **Security training to reinforce policy:** Periodic employee training and monitoring are critical parts of the prevention process. It is quite common for management to publish a new or updated policy, circulate a signature document for everyone to sign indicating that they have read and understand the contents of the new policy and stop there, waiting for the first violation to cause a disciplinary issue or civil suit before taking any further action. By the time a policy violation is detected or a civil action is filed, the damage is done. When dealing with data breaches, that damage is likely to be far more wide-spread than the employee being disciplined or the one or two victims who have decided to bring suit.

- **Restrict remote access:** Closely monitor remote access by employees who may use portable computers during work-related travel. Also limit and/or closely monitor any remote access into your system by outside vendors, contractors and service providers if they exist. Where it is necessary for a third-party vendor or service provider to have access to a governmental IT system, be sure that the process is carefully vetted, appropriate safeguards are in place on the third party's IT system and that the personnel adhere to periodic monitoring.

- **Deploy effective anti-virus software:** Ensure IT professionals stay abreast of and adhere to current industry standards on anti-virus software and anti-intrusion measures. Also, ensure that the IT professional in charge of the system is regularly staying on top of the latest developments in malware and intrusion methodologies as they evolve.

- **Look for suspicious activity on the network**: Daily use of any system will typically yield some form of identifiable standard or pattern. Knowing what is normal will allow the abnormal to be more easily identified and dealt with. Periodic audits of activity, looking for anomalies that stand out from otherwise normalized traffic patterns can help avoid a data breach before it happens.

- **Restrict IT system use to business only**: Prohibit surfing the net, social media or anything non-work related on work-site computers. Depending on the position of the employee, there may need to be limited exceptions, but to the greatest extent possible, restrictions should be established and enforced.

- **Have an effective Incident Response Plan in place BEFORE the data breach:** the plan should require periodic assessment and modification as technology and system intrusion methodology evolves. Complete support of top management is necessary to maintain an effective defense against data breach so management needs to be continually briefed on the status of the plan, its required modifications, the results of periodic reviews and newly emerging threats, etc.

- **Maintain a plan for effective customer notification and remedial action**: When PII is compromised it is essential to have a plan to notify those affected by the breach. If possible, provide identity theft prevention instruction and counseling and identity theft monitoring services by a recognized provider. Establish a hotline for dealing with reported identity theft incidents that may be the result of the breach. Having an effective response plan in place could help mitigate civil claims of negligence as well as the inevitable political fallout from such an event.

- **Testing and auditing:** Stage simulated data breach events to rehearse and evaluate response to a potential data breach incident. Diligent periodic reviews of incident response plans are a necessary element of any effective response strategy. As threats change, prevention strategies must also change. The environment is a rapidly evolving one and as such response plans should evolve with it in order to remain effective.

- **Cyber intrusion insurance**: Insurance companies have recognized this issue, and there are vendors in the field who will provide insurance to cover such events.

- **ALWAYS REPORT**: Make sure to report all data breaches as required to the appropriate law enforcement authority. "Forty-six states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information."[90] Helpful sites for reporting cybercrime and data breach incidents include:

    - Your State Attorney General's office. A comprehensive list of all AG's by state is provided at the following: http://www.naag.org/naag/attorneys-general/whos-my-ag.php

    - FBI at the Internet Crime Complaint Center located at: http://www.ic3.gov/media/annualreports.aspx

    - Your local U.S. Secret Service Electronic Crimes Task Force: Comprehensive state by state list located at http://www.secretservice.gov/ectf.shtml

    - Your local law enforcement state or local law enforcement agency.

Research indicates that a strong security posture, incident response planning, business continuity management, and a Critical Incident Security Officer (CISO) with enterprise-wide responsibility

decreases the per capita cost of data breach incident.[91] A good incident response plan that is reviewed and updated regularly, practiced periodically, and managed effectively will help reduce the likelihood that the entity involved is found to be responsible for not having taken all the precautions feasible to prevent a data breach.

The availability of a team of personnel specifically trained to not only respond from the IT perspective, but to minimize loss and even restore service is necessary. Having trained personnel in the criminal investigative field who know computer forensics is also critical to proper response. Restoring service and recovering lost information is only one aspect of the recovery process. Identification of forensic evidence for investigative purposes for use in a court of law after the perpetrator of a data breach is identified is another critical aspect of response.

"For More Information"/Links

The 2014 Verizon Data Breach Investigations Report provides a good analysis of preventive measures for each individual type of data breach by type. The report is located at http://www.verizonenterprise.com/DBIR/2014/

The Federal Trade Commission maintains an Identity Theft Resource Center located at http://www.consumer.ftc.gov/features/feature-0015-identity-theft-resources

U.S. Department of Justice on Identity Theft and Identity Fraud; http://www.justice.gov/criminal/fraud/websites/idtheft.html

SANS Institute, Critical Security Controls for Effective Cyber Defense, http://sans.org/critical-security-controls/

Cybersecurity Incident Response: Are we as Prepared as We Think? http://www.lancope.com/ponemon-incident-response/

Computer Security Incident Handling Guide. National Institute of Standards and Technology Special Publication 800-61 Revision 2 Natl. Inst. Stand. Technol. Spec. Publ. 800-61 August 2012, located at; http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

CERT Software Engineering Institute of Carnegie Mellon University maintains a Guide to Insider Threats and information on dealing with Insider threats at http://www.cert.org/insider-threat/index.cfm

"Information Security Handbook," from the National Institute of Standards and Technology http://dx.doi.org/10.6028/NIST.SP.800-100

"Guide to Protecting the Confidentiality of Personally Identifiable Information," National Institute of Standards and Technology. Special Publication 800-122. (April 2010) http://ssrn.com/abstract=1671082.

"Prevent Identity Theft with Responsible Information-Handling Practices in the Workplace," from the Privacy Rights Clearinghouse www.privacyrights.org/ar/PreventITWorkplace.htm

"Prevent Identity Theft with Responsible Information-Handling Practices in the Workplace," from the Privacy Rights Clearinghouse www.privacyrights.org/ar/PreventITWorkplace.htm

National Conference of State Legislatures. Security Breach Notification Laws. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

International Association of Chiefs of Police, Law Enforcement Cyber Center. http://www.iacpcybercenter.org/

Maintenance and Revisions: NW3C's Research Division

Legal Analysis: Christian Desilets, Research Division

This project was supported by Grant No. 2015-BE-BX-0011 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Smart Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

[1] Definition courtesy of Dictionary.com, located at: http://dictionary.reference.com/browse/cybercrime
[2] Identity theft Resource Data Breach Reports, published November 25, 2014 located at: http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf
[3] Chinese Hackers Infiltrated U.S. Companies, Attorney General Says. From Ashley Fantz, CNN, May 19, 2014 located at: http://www.cnn.com/2014/05/19/justice/china-hacking-charges/
[4] Definition taken from Tech Target located at; http://searchsecurity.techtarget.com/definition/hacktivism
[5] FBI Probing 'Anonymous' Hack on Cleveland's web site, Nov. 24, 2014 located at: http://www.aol.com/article/2014/11/24/fbi-probing-anonymous-hack-on-clevelands-website/20998522/
[6] Anonymous Hackers to Ferguson Police, 'We are the Law Now'; The Washington Times, Nov. 21, 2014 located at: http://www.washingtontimes.com/news/2014/nov/21/anonymous-hackers-to-ferguson-police-we-are-the-la/
[7] Albuquerque Police Department website Hacked in Cyber-Attack, Anonymous Takes Credit for Crash of APD Website. March 30, 2014 located at: http://www.koat.com/news/albuquerque-police-department-website-hacked-in-cyberattack/25239274
[8] Russian Hackers Amass Over a Billion Internet Passwords. By NICOLE PERLROTH and DAVID GELLESAUG. 5, 2014, located at: http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?_r=0
[9] Kids With Operator's Manual Alert Bank Officials: "We Hacked Your ATM", Bank of Montreal gets Schooled by Kids Who Accessed Owner's Manual Online. by Dan Goodin - June 9 2014, located at: http://arstechnica.com/security/2014/06/kids-with-operators-manual-alert-bank-officials-we-hacked-your-atm/
[10] Privacy Rights Clearing House home page, located at: https://www.privacyrights.org/
[11] Identity Theft Resource Center home page, located at: http://www.idtheftcenter.org/
[12] Privacy Rights Clearing House home page, located at: https://www.privacyrights.org/
[13] Breach Level Index web site located at: http://breachlevelindex.com/#!home
[14] U.S. Department of Health and Human Services, Office of Civil Rights web site located at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/complaintsyear.html
[15] NOTE: NW3C will continue to add information to our data set as breaches are reported. January 1, 2017 was selected as a cutoff point for this research only for purposes of this report.
[16] 2016 Cost of Data Breach Study: United States, Ponemon Institute, June 2016. Retrieved on 1/5/17 from https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03094usen/SEL03094USEN.PDF
[17] Ibid.
[18] Ibid
[19] August 14, 2013 – Identity Theft: The Fastest Growing Crime in America by Sean Trundy located at http://www.fraudfighter.com/counterfeit-detection-id-verification/bid/94512/Aug-14-2013-Identity-Theft-The-Fastest-Growing-Crime-in-America
[20] Identity theft Resource Center 2016 data breach report, located at; http://www.idtheftcenter.org/2016databreaches.html
[21] Identity Theft, Growing Costly to Victims, by J. Craig Anderson in USA Today, 4/13/13, located at http://www.usatoday.com/story/money/personalfinance/2013/04/14/identity-theft-growing/2082179/
[22] U.S. Cybercrime: Rising risks, reduced readiness: Key findings from the 2014 US State of Cybercrime Survey co-sponsored by the CERT Division of Software Engineering Institute at Carnegie Mellon University and the United States Secret Service. P.5 Located at http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf
[23] 2016 Cost of Data Breach Study: United States, Ponemon Institute, June 2016. Retrieved on 1/5/17 from https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03094usen/SEL03094USEN.PDF
[24] Survey of Major Cities Chiefs Association, 2016, conducted by NW3C, presented at 2016 IACP conference, October, 2016.
[25] How Anonymous Hackers Changed Ferguson Missouri Protests, by David Hunn, McClatchy News Service August 13, 2014, located at http://www.govtech.com/local/How-computer-hackers-changed-the-Ferguson-protests.html
[26] Cybercrime Hits Small Towns. By Todd Newcombe, December 2011, located at http://www.governing.com/topics/technology/cybercrime-hits-small-towns.html
[27] WPD, FBI Investigation Website Hacking Case, Van Williams, 10/8/2013, located at http://www.wichita.gov/Government/News/Pages/2013-10-08b.aspx

[28] 5 worst City Data Breaches, Chicago Board of Elections, by Mary Jander, Managing Editor, Future Cities, February 13, 2013 located at http://www.ubmfuturecities.com/author.asp?section_id=359&doc_id=524364&page_number=2
[29] Ibid.
[30] Turkish Hackers Causing a Nuisance in Anytown USA, by The Information Institute, located at http://aldwychassociates.com/informationinstitute/turkish-hackers-causing-a-nuisance-in-anytown-u-s-a/
[31] Portland computer System OK after Virus Strike, by Brad Schmidt, McClatchy News Service, February 5, 2014; located at http://www.govtech.com/local/Portland-Computer-System-OK-After-Virus-Strike.html?utm_source=related&utm_medium=direct&utm_campaign=Portland-Computer-System-OK-After-Virus-Strike
[32] Massive Data Breach Affects Hundreds of Miami-Dade County Employees, Friday June 6, 2014 by Dan Krauth, NBC news. Located at http://www.nbcmiami.com/news/local/Massive-Data-Breach-Affects-Hundreds-of-Miami-Dade-County-Employees-262169331.html
[33] Lansing State Journal, *Was BWL Prepared for a Ransomware Attack?* Reed, Steven R., November 25, 2016, located; http://www.lansingstatejournal.com/story/news/local/2016/11/25/bwl-prepared-ransomware-attack/94332454/
[34] The Post Breach Boom, by the Ponemon Institute, February 26, 2013, located at; http://www.ponemon.org/blog/the-post-breach-boom
[35] *Worldwide Revenue for Security Technology Forecast to Surpass $100 Billion in 2020, According to the New IDC Worldwide Semiannual Security Spending Guide;* Press Release, October 12, 2016, located at; http://www.idc.com/getdoc.jsp?containerId=prUS41851116
[36] U.S. Cybercrime: Rising risks, reduced readiness: Key findings from the 2014 US State of Cybercrime Survey co-sponsored by the CERT Division of Software Engineering Institute at Carnegie Mellon University and the United States Secret Service. P.5 Located at http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf
[37] Defense Department Facing $4.9 Billion Law Suit Over Breach. In SC Magazine, Oct. 17, 2011, located at; http://www.scmagazine.com/defense-department-facing-49b-lawsuit-over-breach/article/214600/
[38] National Conference of State Legislatures web site; located at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx retrieved January 20, 2017
[39] 2016 Internet Security Threat Report: Government, Symantec Retrieved on 1/4/2017 from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-government-en.pdf?aid=elq_&om_sem_kw=elq_3732438&om_ext_cid=biz_email_elq_&elqTrackId=f1f3aad23c4c4cd081363eed333cbb87&elqaid=2909&elqat=2, page 9.
[40] State of Cybersecurity in Local, State & Federal Government. Ponemon Institute LLC. (2015) Retrieved on 1/10/2017 from https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-2563enw.pdf
[41] 2016 Internet Security Threat Report: Government, Symantec Retrieved on 1/4/2017 from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-government-en.pdf?aid=elq_&om_sem_kw=elq_3732438&om_ext_cid=biz_email_elq_&elqTrackId=f1f3aad23c4c4cd081363eed333cbb87&elqaid=2909&elqat=2, page 52
[42] 2016 Cost of Data Breach Study: United States, Ponemon Institute, June 2016. Retrieved on 1/5/17 from https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03094usen/SEL03094USEN.PDF
[43] 2016 Cost of Data Breach Study: United States, Ponemon Institute, June 2016. Retrieved on 1/5/17 from https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03094usen/SEL03094USEN.PDF
[44] https://us.norton.com/ransomware/article
[45] Ellement, John R. (2016) Hackers extract $300 ransom from Medfield after "locking" town network. Boston Globe, February 2, 2016. Retrieved on 1/10/17 from https://www.bostonglobe.com/metro/2016/02/02/town-medfield-pays-ransom-free-computer-system/oHZB3bYC20lW39kSJJsrKI/story.html
[46] Ransomware Holds Captive PC-files of Collinsville Police. (2014, January 7). Retrieved April 20, 2015, from http://www.spamfighter.com/News-19056-Ransomware-Holds-Captive-PC-files-of-Collinsville-Police.htm
[47]Goodin, D. (2014, June 7). We "will be paying no ransom," vows town hit by Cryptowall ransom malware. Retrieved April 20, 2015, from http://arstechnica.com/security/2014/06/we-will-be-paying-no-ransom-vows-town-hit-by-cryptowall-ransom-malware/
[48] Distant, D. (2014, November 13). Dickson County Sheriff's Malware Ransom: Police Pay Hacker to Release Their Files. Retrieved April 20, 2015, from http://www.christianpost.com/news/dickson-county-sheriffs-malware-ransom-police-pay-hacker-to-release-their-files-129674/

[49]Search engines for connected devices exist and can help you identify which of your devices might be online. https://www.shodan.io/

[50] FBI: Smart Meter Hacks Likely to Spread. Krebs on Security. April 12, 2012. Retrieved on 1/10/17 from https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/

[51] Walters, Riley (2016). Cyber Attacks on U.S. Companies in 2016. Issue Brief #4636. Retrieved on 1/10/17 from http://www.heritage.org/research/reports/2016/12/cyber-attacks-on-us-companies-in-2016

[52] Gallagher, Sean (2016). Douple-dip Internet-of-Things botnet attack felt across the Internet. Ars Technica. Retrieved on 1/10/17 from http://arstechnica.com/security/2016/10/double-dip-internet-of-things-botnet-attack-felt-across-the-internet/

[53] It was foreseeable, on these facts, that a customer, knowing that her credit or debit card data had been compromised and that thousands of fraudulent charges had resulted from the same security breach, would replace the card to mitigate against misuse of the card data. It is true that the only plaintiffs to allege having to pay a replacement card fee, Cyndi Fear and Thomas Fear, do not allege that they experienced any unauthorized charges to their account, but the test for mitigation is not hindsight. Similarly, it was foreseeable that a customer who had experienced unauthorized charges to her account, such as plaintiff Lori Valburn, would reasonably purchase insurance to protect against the consequences of data misuse.
Anderson v. Hannaford Bros. Co., 659 F.3d 151, 164–67 (1st Cir. 2011)

[54] We hold that respondents lack Article III standing because they cannot demonstrate that the future injury they purportedly fear is certainly impending and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm. We therefore reverse the judgment of the Second Circuit and remand the case for further proceedings consistent with this opinion.
Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1155, 185 L. Ed. 2d 264 (2013)
(While this case dealt with privacy advocates fearing that their calls were being intercepted, and the steps that they took to mitigate that risk, it is generalizable to our current discussion)

[55] Although Appellants have incurred expenses to monitor their accounts and "to protect their personal and financial information from imminent misuse and/or identity theft," they have not done so as a result of any *actual* injury (e.g. because their private information was misused or their identities stolen). Rather, they prophylactically spent money to ease fears of future third-party criminality. Such misuse is only speculative—not imminent. The claim that they incurred expenses in anticipation of future harm, therefore, is not sufficient to confer standing.
Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011)

[56] The Defendant first moves to dismiss all of the Plaintiffs' claims for lack of standing. In order to establish standing under Article III, a plaintiff must show an injury that is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." The Supreme Court has held that "threatened injury must be *certainly impending* to constitute injury in fact, and that allegations of *possible* future injury are not sufficient." The Supreme Court has also noted, however, that standing can be "based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." Here, the financial institution plaintiffs have adequately pleaded standing. Specifically, the banks have pleaded actual injury in the form of costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs for customer fraud monitoring, and costs due to lost interest and transaction fees due to reduced card usage. These injuries are not speculative and are not threatened future injuries, but are actual, current, monetary damages. Additionally, any costs undertaken to avoid future harm from the data breach would fall under footnote 5 of Clapper, specifically as reasonable mitigation costs due to a substantial risk of harm. The injuries, as pleaded, are also fairly traceable to Home Depot's conduct, specifically the alleged failure to implement adequate data security measures. A favorable ruling would also redress these monetary harms. The Defendant's motion to dismiss for lack of standing should be denied.
In re: The Home Depot, Inc., Customer Data Sec. Breach Litig., No. 1:14-MD-2583-TWT, 2016 WL 2897520, at *3 (N.D. Ga. May 18, 2016)

[57] The complaint alleged that Fifth Third has contracts with MasterCard and Visa that require compliance with operating regulations adopted by each credit card organization and that TJX and Fifth Third similarly have a contract that requires TJX to comply with such regulations.

It further alleged that TJX and Fifth Third ignored security measures required by the operating regulations—for examples, that signatories deploy a firewall configuration, protect stored data, encrypt transmission of cardholder data, and track access to cardholder data and network resources.

In re TJX Companies Retail Sec. Breach Litig., 564 F.3d 489, 494 (1st Cir. 2009), as amended on reh'g in part (May 5, 2009)
[58] In Hans v. Louisiana, 134 U.S. 1 (1890).
[59] Northern Insurance Company of New York v. Chatham County, 547 U.S. 189 (2006)
[60] Coffey, Amanda (n.d.), Local Government Sovereign Immunity 201: Florida, American Bar Association. Retrieved on 1/6/2017 from www.americanbar.org/content/dam/aba/.../state_local_government/SovImm201.pdf
[61] Lake Country Estates, Inc. v. Tahoe Regional Planning Agency, 440 U.S. 391, 401 (1979)
[62] Jinks v. Richland County, 538 U.S. 456, 466 (2003)
[63] Anthony, David, and Beth McMahon (2000), Sovereign Immunity: Can the King Still Do No Wrong?, Virginia Lawyer. Retrieved on 1/6/2017 from www.vsb.org/docs/valawyermagazine/apr00anthony_mcmahon.pdf
[64] Althouse, Tapping the State Court Resource, 44 Vand. L. Rev. 953, 973 (1991)
[65] Phillips v. County of Allegheny, 515 F.3d 224 (3rd Cir. 2008)
[66] Bright v. Westmoreland County, 443 F.3d 276, 281 (3d Cir. 2006) (internal quotation marks and footnotes omitted)
[67] County of Sacramento v. Lewis, 523 U.S. 833, 846 (U.S. 1998)
[68] Hart v. City of Little Rock, 432 F.3d 801 (8th Cir. 2005))
[69] 15 USC § 45
[70] [E]xposure of consumers' personal information has caused and is likely to cause substantial consumer injury, including financial injury, to consumers and businesses. For example, Defendants' failure to implement reasonable and appropriate security measures resulted in the three data breaches ... the compromise of more than 619,000 consumer payment card account numbers, the exportation of many of those account numbers to a domain registered in Russia, fraudulent charges on many consumers' accounts, and more than $10.6 million in fraud loss. Consumers and businesses suffered financial injury, including, but not limited to, unreimbursed fraudulent charges, increased costs, and lost access to funds or credit. Consumers and businesses also expended time and money resolving fraudulent charges and mitigating subsequent harm.
F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 622 (D.N.J. 2014), motion to certify appeal granted (June 23, http://www.kristv.com/story/34074845/ccisd-443-former-students-social-security-numbers-displayed-on-internet2014), aff'd, 799 F.3d 236 (3d Cir. 2015)
[71] Cruz, Eddie (2016) CCISD: 444 former students Social Security numbers displayed on internet, KrisTV.com http://www.kristv.com/story/34074845/ccisd-443-former-students-social-security-numbers-displayed-on-internet
[72] We hold that because disclosure of the officers' addresses, phone numbers, and driver's licenses, as well as the names, addresses, and phone numbers of their family members, placed the officers and their families at substantial risk of serious bodily harm, the prior release of this information encroached upon their fundamental rights to privacy and personal security under the Due Process Clause of the Fourteenth Amendment. Because the City has not shown that its prior actions narrowly served a compelling state interest, its release of this personal information to defense counsel in the Russell case unconstitutionally denied the officers a fundamental liberty interest. Having deprived the officers of a constitutional right, the City is liable to them under § 1983 for any damages incurred.
Kallstrom v. City of Columbus, 136 F.3d 1055, 1069–70 (6th Cir. 1998)
[73] http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
[74] Data Breach Risk Brief, MSP Intelligence, SolarWinds MSP. Retrieved on 12/14/2016 from http://f6ce14d4647f05e937f4-4d6abce208e5e17c2085b466b98c2083.r3.cf1.rackcdn.com/data-breach-risk-brief-pdf-4-w-2873.pdf
[75] Greenwald, Judy (2015). Cyber Insurance Policies Vary Widely and Require Close Scrutiny, Business Insurance 5/10/2015. Retrieved on 1/9/17 from http://www.businessinsurance.com/article/00010101/NEWS06/305109992/Cyber-insurance-policies-vary-widely-and-require-close-scrutiny
[76] Firm Sues Cyber Insurer Over $480K Loss, Krebs on Security (2016). Rerieved on 1/9/17 from http://krebsonsecurity.com/2016/01/firm-sues-cyber-insurer-over-480k-loss/
[77] 2016 Cost of Data Breach Study: United States, Ponemon Institute, June 2016. Retrieved on 1/5/17 from https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03094usen/SEL03094USEN.PDF
[78] Vijayan, Jaikumar (2010). Insurer says it's not liable for University of Utah's $3.3M data breach. Computerworld. Retrieved on 1/10/17 from http://www.computerworld.com/article/2518592/data-security/insurer-says-it-s-not-liable-for-university-of-utah-s--3-3m-data-breach.html

[79] Greenwald, Judy (2015), Insurer Cites Cyber Policy Exclusion to Dispute Data Breach Settlement. Business Insurance. Retrieved on 1/10/17 from http://www.businessinsurance.com/article/20150515/NEWS06/150519893

[80] Docket No. 28 Ex. B, CyberFirst Technology Errors and Omissions Liability Coverage Form, Section I, at bates number PRMT000923, Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., Inc., 103 F. Supp. 3d 1297, 1298 (D. Utah 2015)

[81] Id, at Section II, 3, at bates number PRMT000926

[82] Defendants argue that Travelers' duty to defend remains until any uncertainty as to coverage has been resolved. While this is a correct statement, the Global action provides no such uncertainty. To trigger Travelers' duty to defend, there must be allegations in the Global action that sound in negligence. As discussed above, there are no such allegations. Further, this is not a situation, like the one found in *Benjamin v. Amica Mutual Insurance Co.*,which would occur if Global had pleaded alternative causes of action, some of which would trigger the duty to defend. Rather, none of Global's allegations involve errors, omissions, or negligence. Therefore, Travelers has no duty to defend
Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., Inc., 103 F. Supp. 3d 1297, 1302 (D. Utah 2015)

[83] Osborne, Charlie (2015). Most companies take over six months to detect data breaches. ZDNet. Retrieved on 1/10/17 from http://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/

[84] Greenwald, Judy (2015). Cyber Insurance Policies Vary Widely and Require Close Scrutiny, Business Insurance 5/10/2015. Retrieved on 1/9/17 from http://www.businessinsurance.com/article/00010101/NEWS06/305109992/Cyber-insurance-policies-vary-widely-and-require-close-scrutiny

[85] Computer Security Incident Handling Guide. National Institute of Standards and Technology Special Publication 800-61 Revision 2 Natl. Inst. Stand. Technol. Spec. Publ. 800-61 August 2012, located at; http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

[86] An Incident management Ontology, Mundie, D. Ruefle, R. et. al. Carnegie Mellon University, located at http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=426836

[87] SANS Institute, Critical Security Controls for Effective Cyber Defense, located at http://sans.org/critical-security-controls/

[88] Verizon 2014 Data Breach Investigations Report, located at http://www.verizonenterprise.com/DBIR/2014/

[89] Cyber Attacks on the Rise, Money is the Main Target. David R. Baker, McClatchy News Service April 22, 2014, located at; http://www.govtech.com/security/Cyberattacks-on-the-Rise-Money-is-Main-Target.html?utm_source=related&utm_medium=direct&utm_campaign=Cyberattacks-on-the-Rise-Money-is-Main-Target

[90] Privacy Rights Clearing House home page, located at: https://www.privacyrights.org/

[91] 2014 Cost of Data Breach Study: Global Analysis, sponsored by IBM, independently conducted by Ponemon Research Institute LLC, May 2014, p. 11 located at; http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis