INFRAGARD

JOURNAL

June 2019 - Issue 1, Volume 2

Critical Infrastructures:
Chemical
Commercial Facilities
Communications
Critical Manufacturing
Dams
Defense Industrial Base
Emergency Services
Energy
Financial Services
Food and Agriculture
Government Facilities
Healthcare and Public Health
Information Technology
Nuclear Reactors, Materials and Waste
Transportation Systems
Water and Wastewater Systems

Information Governance – the Foundation for Information Security

Deborah Juhnke[1]

Abstract:

Reducing the amount of data under management is appropriate and necessary to help improve an organization's security posture. The identification, classification, and segregation of information, coupled with routine disposition of detritus, will yield less information requiring protection and a better ability to apply tiered safeguards. The solution is not simply technical, however, and requires legally-defensible guidance, executive mandate, and changes to culture. We explore a data management model based on Information Governance principles and propose a triage process that focuses on the elimination of ROT (redundant, obsolete, and trivial data) using legally-validated retention schedules and policy guidance. We review various information security standards that support the inventory and management of information assets, with an eye toward practical applications.

DARK DATA IS BECOMING an information governance nightmare (Shetty 2017). Unstructured and uncontrolled for decades, "[e]mail, instant messages, documents, ZIP files, log files, archived web content, partially developed and then abandoned applications, [and] code snippets" (Shetty) not only impact costs, but also the ability to apply effective security controls. A recent survey suggests that fifty-four percent of data in organizations is stale, and that seventy-four percent of organizations have over one thousand stale sensitive files (Varonis 2018, 11).

This paper offers a roadmap on how to solve this problem. It explores an information management model based on the Information Governance principles of Structure, Direction, Resources, and Accountability, and proposes a triage process that focuses on the elimination of unnecessary information using legally-validated retention schedules and policy guidance.

[1] Senior Consultant, Information Governance Group, LLC. djuhnke@infogovgroup.com. 4324 Belleview, Suite 201, Kansas City, MO 64111

Better information governance yields better information security.

By reducing the volume of unstructured data under management to a fraction of its current information inventory, an organization will free up storage, reduce licensing costs, shorten backup cycles, and drastically cut e-discovery preservation costs. More importantly, a reduction will diminish the footprint for potential compromises. Less, better-categorized data offers a smaller attack surface and limits vulnerabilities arising from redundant, orphaned, obsolete, forgotten, transitory, and hidden data stores (ROT, or **r**edundant, **o**bsolete, and **t**rivial data). The availability of ROT in systems opens the door for external penetration, exploitation, and internal compromise.

Insider threats—both intentional and inadvertent—are responsible for a significant number of data breaches. This has justifiably led to more training regarding password management and recognition of phishing attacks. Overlooked, however, is the fact that the ROT that lies dormant in unstructured systems, and that is *created* by insiders, offers up a cornucopia of treats for hackers: files containing business confidential information, credentials in plain text files, Intellectual Property (IP), sensitive Protected Health Information (PHI) and Personally Identifiable Information (PII), and more. A focus on eliminating ROT through retention and rule enforcement will mitigate many of the vulnerabilities that come from excess and unmanaged data. Insiders are the soft underbelly of information security, especially given the vast amount of unprotected, unstructured data that exists in most organizations.

Reducing the amount of ROT under management is appropriate and necessary for businesses generally, but particularly for all critical infrastructure sectors, and begins with a simple proposition:

> ***Identification, classification, and segregation of information + routine disposal of detritus = less to protect + better ability to apply tiered protection***

The solution, however, is not simply a technical one. It requires engagement of senior management and end users and will benefit greatly from the support of an organization's legal, risk, compliance, privacy, and audit functions. Such groups may be engaged to identify common goals and to leverage budgets and bandwidth. These siloed groups have similar concerns, yet often struggle to make an isolated business case for change. Like puzzle pieces, aggregating these concerns creates a complete picture, most often with enough clarity and unified purpose to get an executive commitment and budget for change.

Current State of Information Governance

According to the Compliance, Governance and Oversight Council's Information Governance Benchmark Survey of 2018, even though there is evidence showing that information governance (IG) programs have increased support, there continues to be a lack of measurable progress (CGOC 2018, 6). Although roughly seventy-five percent of respondents report progress in their IG programs and have an appropriate level of executive sponsorship and leadership, only a third have an automated defensible disposition program in place (even though in 2010 ninety-eight percent of respondents identified defensible disposal of information as a desired benefit).

The CGOC report suggests that problems and barriers include a lack of data classification, data silos that make it difficult to link retention schedules to data, and the fact that retention, preservation, and disposal are often not considered prior to provisioning new systems. External pressures also play a role. Vendors of IT storage and cloud solutions promote sales to their clients of unlimited space for email and documents because it increases their revenue, with little

consideration for the risks their clients will face from over-retention. More storage is the short term, easy answer to rampant data growth, but not a good one. More storage and unlimited email repositories only exacerbate the problem.

The Association for Information and Image Management, an information governance industry association, recently published The State of Intelligent Information Management: Getting Ahead of the Digital Transformation Curve (AIIM 2018). The survey found that on average forty percent of respondents reported that organization of their Office documents, email, scanned documents, design files, and intellectual property assets was "chaotic" or "somewhat unmanaged" (AIIM 2018, 10). The same was true for over fifty percent of web content, social media, photos, and instant messaging. Nearly half of respondents also rated the effectiveness of their organization in managing, controlling, and utilizing electronic information as toward the "terrible" end of the scale, as opposed to "excellent." Most telling is that the needle has barely budged toward "excellent" for the same survey question in the last ten years. Recognition that something needs to change to modernize information management strategies is strong, however, at ninety-two percent.

The CGOC survey shows that there is a fundamental disconnect between desired outcomes and true progress, as respondents still report after eight years that *sixty percent of all stored data has no business, legal, or regulatory value* (CGOC 2018, 8). Shifting the focus to improved information security is a way to bridge this gap.

Data Lakes Are Not the Answer

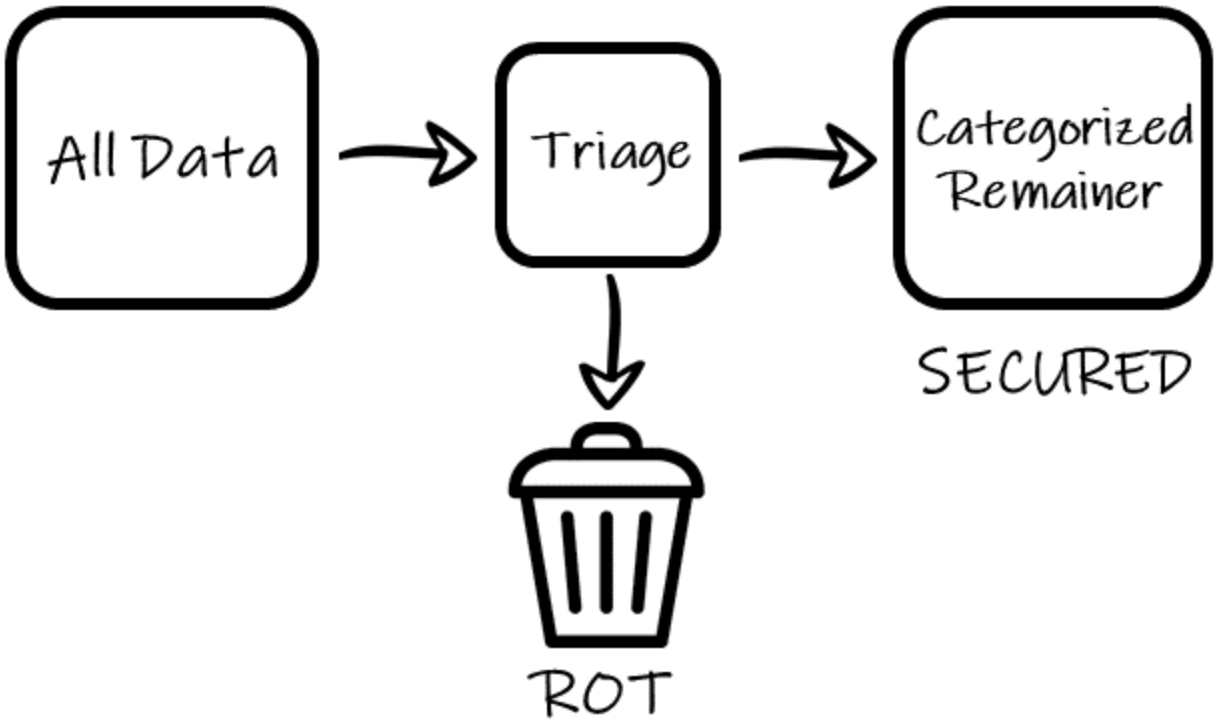
Although it may be tempting to create larger pools of unrelated data to simplify application of security controls, data lakes do not solve the problem of too much data. Simply aggregating poor quality, irrelevant, or obsolete data diminishes the value that may be gained from targeted data mining of curated information. Routinely cleaning out the chaff makes the remaining data more valuable—just one of many benefits of good governance.

Unstructured data also commonly holds highly sensitive information that, if exploited, can yield everything from unencrypted passwords to sensitive business and industrial system information. In addition, unnecessary storage of seemingly inconsequential information can enable inference attacks by allowing access to files from which more robust information about sensitive databases may be inferred, leading to unauthorized access and exfiltration.

Maintaining less data can limit entry points, limit the scope of a breach, limit the exposure of sensitive information such as IP, PHI and PII, and significantly minimize e-discovery costs in the event of litigation or regulatory investigation. Perimeter security is useful, but once breached, a far greater amount of aggregated data becomes exposed than would be if culled and sequestered in appropriately protected tiered systems.

Proposed Model

Below is a simplified diagram illustrating an improved information governance approach.



The **All Data** box represents the entire body of an organization's information, including structured and unstructured data, archives, and local and cloud-based storage. More than half of this data may commonly be classified as ROT—redundant, orphaned, obsolete, forgotten, transitory, and hidden data. But "All Data" also includes business critical information, IP, PHI, PII, and information required to be retained pursuant to regulation or statute. The goal is to eliminate the ROT permanently while ensuring that the remainder are identified, segregated, protected, and retained appropriately.

Triage occurs through a series of processes designed to identify, classify, and apply rules. Identification of information assets may sound like an obvious task and one that many would assume has been done. In fact, most organizations do not have a firm grasp of what information they hold and where it is. Creating a basic inventory of both systems and data is the first step. The inventory should include not only active data, but also data held in archives and off-line storage.

The rules to apply take the form of policies (such as for data classification, records retention, and legal holds), a retention schedule, and guidance documents regarding segregation and storage of sensitive information.

Applying these rules will enable organizations to cull **ROT**, and the methods used can vary. For example, large scale culling may sometimes be applied to known data sets such as unstructured files of terminated employees, ad hoc backups of data, redundant "just in case" archives, and transitory data. In some cases, a more refined approach must be taken (particularly in regulated industries that have rigorous retention requirements), but in no instance should anyone, including users, be required to sift through files one-by-one. There are numerous software products that support the inventory, categorization, review, and triage of unstructured data stores, most of which also provide for migration or disposition of data.

During the triage process, **Categories** of data will emerge, some of which will require one or more levels of security controls, and others of which will not. Key to efficient categorization is

limiting the options to no more than three or four. For example, based on the sensitivity of the information, the categories to use might include Public, Business Confidential, and Restricted.

Once categorized and culled, information may be segregated to **Secure** and **Other** locations, where appropriate security controls are applied. The "crown jewels" will warrant having the most layered and stringent controls, while Public data may have fewer and less-sophisticated controls. Segregation is the operative word, ensuring that any eventual compromise is contained.

Beyond the expected compliance and security benefits, following the above process gives great visibility into an organization's information assets, and can uncover additional opportunities for streamlining workflows and eliminating unnecessary creation or duplication of information. Information governance, however, is not a one-time project. It is evergreen and demands periodic, (e.g., at least bi-annually), refreshing of regulatory, statutory, and business-need retention requirements, as well as internal audits to ensure adherence to policy.

Legal & Compliance Support for Information Governance

Because the Information Security function cannot decide in a vacuum what to manage and what to dispose of, the Legal department can be a great ally and facilitator of change. Most unstructured information that exists in file shares, SharePoint sites, dormant databases, archives, and email systems is at best redundant, and at worst obsolete. "Last accessed" dates offer a simple measure of the volume of ROT, though they may not always be available or reliable enough alone to trigger disposition. A "last accessed" date may, however, be a useful metadata element as part of a more nuanced set of review criteria such as "last modified" and file extension. Lawyers understand that *some* information must be retained according to various statutes and regulations and that *some* information has business value beyond retention requirements. They also understand that the remainder falls under the categories of convenience copies or duplicates, non-business data, and obsolete copies of what were once *bona fide* records. The reality is that as much as eighty percent or more of most organizations' information falls into these latter categories. One caveat: In the case of an impending or existing lawsuit or investigation, data that is not otherwise required to be kept, but which is pertinent to the matter, must be *preserved* until the matter is finally resolved.

Appropriate use of terminology here is an important and critical distinction. *Retention* is applied to data in the normal course of business. *Preservation* is applied to data pertinent to a lawsuit or investigation, regardless of its value or retention requirements, and supersedes any disposition mandate. This preservation duty is commonly effected through a "legal hold" issued by an organization's internal or outside legal counsel. Legal holds remain in effect until formally lifted by legal counsel. Consequently, inventory and triage efforts *must* consider any existing legal holds when designating data for disposition.

There are also regulatory authorities in virtually every critical infrastructure industry for recordkeeping and other compliance requirements. A thorough legal review and summary of these authorities will yield a records retention schedule—the roadmap to compliant disposal of data. It is the primary basis for decision-making regarding what to keep and what to toss and, if well crafted, will be an authoritative source of guidance for defensible disposition.

Lawyers know the value of enforcing disposition of ROT: improved compliance, reduced risk, improved security, and cost savings. They also know how to draft policies and gather executive support for information governance initiatives.

Building Blocks to Improved Security

Before controls may be applied, good information security requires: (1) knowledge of what information exists, (2) where it is, and (3) the legal and compliance requirements for its retention, all to enable compliant disposition. This information will help dictate what policies to put in place, what tools to acquire, what training to provide, and what other technical, administrative, physical, and operational controls to apply.

Foundational elements of information governance include:

- **Structure**
- **Direction**
- **Resources**
- **Accountability**

Structure supports the understanding of what information exists, where it is and in what form, how long to retain it, and when and how to dispose of it. A **Record** is defined as, "[r]ecorded information, regardless of medium or characteristics, made or received by an organization that is evidence of its operations, and has value requiring its retention for a specific period of time." It is common to consider only record-worthy information when performing a data inventory, but to be effective, *all information* must be identified and classified. Record retention is as much about segregating and managing the lifecycle of non-record information as it is about retaining information required by law.

An actionable, current, and legally-validated records retention schedule codifies not only legal requirements, but also business needs for retention and disposition. Note that a retention schedule is not simply a policy. It is a detailed, legally annotated framework that identifies bundles of information and record types and how long to retain them. File plans capture further detail about the specific types and locations of business records, typically on a departmental basis, and can enhance the framework for classification and segregation of sensitive information.

Direction comes from policies and processes that enable employees to comply with information governance requirements. Email and computer use policies, records management policies, and privacy and security policies all inform employees of what they should do. Processes, such as document creation guidance, storage guidance, and periodic clean-up days, tell employees how they should do it.

Identifying the right **Resources** is an indispensable aspect of good information governance. The right people, training, and technology all play a role. Because security is not simply an IT issue, it is important to engage personnel at many levels, including executive mandate and oversight, departmental liaisons, end users, internal subject matter experts, and those in the legal, compliance, privacy, risk, and audit functions. The necessary cultural change required to accept and effectuate policy, discussed further below, is achieved in part through training both in new or improved processes, and training to support behavioral change generally. The range of technology tools available to support information governance and security is vast, but certain classes of tools are particularly useful. These include content management systems, auto-classification tools, and data identification and culling tools.

Without **Accountability**, efforts to improve information governance usually fall short. There must be a clear executive mandate and a strong audit function. Individual accountability must be driven by a combination of policy and cultural change. Workers may only be held accountable, though, if they are informed, trained, and supported. Organizations must work to

instill and support the self-discipline required to rein in the indiscriminate creation and retention of information.

Making the Cultural Leap

Controls for the creation, management, retention, and disposition of data have not kept pace with the ability to create and store it, opening the door for compromise of critical infrastructure systems through unmanaged unstructured data. Because employees have for decades been left to create and store data indiscriminately, a culture and practice of data hording proliferates. Yet most data that is not otherwise required to be kept loses its value in a relatively short time—as soon as one to two years (CGOC, 2013). Further, storing excess data can compromise the ability to find the most current and accurate version. Still, users often keep data "just in case" by default.

To be successful beyond the scope of a one-and-done information clean-up project, it is imperative that executive management lead the way to cultural change and lead by example. This means that not only must they set out expectations and guidance, they must themselves subscribe to the change, particularly since compromise of executive information poses the greatest risk.

Security Standards Support for Information Governance

Various security standards support the concept of information asset management as a key component of information security. Among these are the National Institute for Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, Ver. 1.1 (NIST 2018); International Organization for Standardization 27001:2013, Information technology — Security techniques — Information security management systems — Requirements (ISO 2013); NIST Special Publication 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organization (NIST 2015); and NIST Special Publication 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (NIST 2018).

In the **NIST Framework for Improving Critical Infrastructure Cybersecurity**, **Ver. 1.1**, Asset Management is the first component in the Identify section: ID.AM. "The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy" (NIST 2018, 24), with references to Control Objectives for Information and Related Technologies (COBIT) and ISO 27001:2013, among others.

ISO 27001:2013 emphasizes the importance of information asset management. Among the 114 controls in Annex A is a section dedicated to Asset Management (A.8), and another focusing on Compliance (A.18). These sections address the orderly and compliant management of information assets throughout their lifecycle.

NIST SP 800-53, Rev. 4, speaks to security categorization: "The organization… [c]ategorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance" (NIST 2015, F-151). This process "facilitate[s] the development of inventories of information assets, and along with CM-8 [Information System Component Inventory], mappings to specific information system components where information is processed, stored, or transmitted" (NIST 2015, F-152).

The recently released revision of **NIST SP 800-37, Rev. 2** importantly recognizes need to prepare. Among other things, it promotes the need to:

- "Maximize the use of automated tools to manage security categorization; control selection, assessment, and monitoring; and the authorization process; …
- "Decrease the level of effort and resource expenditures for low-impact systems if those systems cannot adversely affect higher-impact systems through system connections; … and
- "Reduce the complexity of the IT/OT infrastructure by eliminating unnecessary systems, system components, and services — employing the least functionality principle" (NIST 2018, vii).

It further states that,

> "Recognizing that the preparation for RMF [Risk Management Framework] execution may vary from organization to organization, achieving the above objectives can reduce the overall IT/OT footprint and attack surface of organizations, promote IT modernization objectives, conserve resources, prioritize security activities to focus protection strategies on the most critical assets and systems, and promote privacy protections for individuals" (NIST 2018, vii)

This guidance is highly consistent with good recordkeeping and information governance practices, as discussed above. Several sub-sections of NIST 800-37 speak directly to the issue:

Asset Identification

Task P-10 requires *identification of assets that require protection*. Assets are defined as "tangible and intangible items that are of value to achievement of mission or business objectives," and include "mission and business processes, functions, digital information and data, firmware, software, and services. Information assets can be tangible or intangible assets and can include the information needed to carry out missions or business functions, to deliver services, and for system management/operation; controlled unclassified information and classified information; and all forms of documentation associated with the information system" (NIST 2018, 38).

Information Types

Task P-12 requires *identification of the types of information* to be processed, stored, and transmitted by the system. "Identifying the types of information needed to support organizational missions, business functions, and mission/business processes is an important step in developing security and privacy plans for the system and a precondition for determining the security categorization. NARA [National Archives & Records Administration] CUI defines the information types that require protection as part of its Controlled Unclassified Information (CUI) program, in accordance with laws, regulations, or governmentwide policies" ((NIST 2018, 39).

Information Life Cycle

Task P-13 requires *identification and understanding* of "all stages of the information life cycle for each information type processed, stored, or transmitted by the system . . . , typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion [OMB A-130]. Identifying and understanding how each

information type is processed during all stages of the life cycle helps organizations identify considerations for protecting the information, informs the organization's security and privacy risk assessments, and informs the selection and implementation of controls. Identification and understanding of the information life cycle facilitates the employment of practices to help ensure, for example, that organizations have the authority to collect or create information, develop rules related to the processing of information in accordance with its impact level, create agreements for information sharing, and follow retention schedules for the storage and disposition of information.

"Using tools such as a data map enables organizations to understand how information is being processed so that organizations can better assess where security and privacy risks could arise and where controls could be applied most effectively" (NIST 2018, 40).

Categorize

"The purpose of the ***Categorize*** step is to inform organizational risk management processes and tasks by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the Nation with respect to the loss of confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems" (NIST 2018, 46). "The RMF *Categorize* step is a precondition for the selection of security controls" (NIST).

Task C-2 requires that systems be categorized regarding impacts to organizational operations, organizational assets, individuals, other organizations, and the Nation, as well as the security objectives of confidentiality, integrity, and availability (NIST 2018, 48). Suggested categories include high, medium, and low impact systems, and the task suggests that further refinement is possible through prioritization of systems within the same impact level.

In the context of this discussion, categorization should extend beyond systems to include classes and groups of information, not only the systems on which they are stored. For example, a network share may be classified as low or medium impact for most data housed there, but there may, in fact, be highly sensitive or protected information co-mingled in that location. An important outcome of following the model above is to ferret out sensitive data that has been stored in open systems and either move it to more highly secured locations or dispose of it, leaving low impact data on low impact systems. If information is properly classified, technical controls may also be applied to enforce storage requirements.

System Disposal

Task M-7 requires that a system disposal strategy be implemented, to include execution of required actions when a system is removed from operation. Here, as above, the disposal task should be expanded to include disposal of data from systems that remain in operation. Certainly, when a system is removed from operation "[o]rganizations [should] ensure that controls addressing system disposal are implemented. Examples include media sanitization; configuration management and control; component authenticity; and *record retention* (NIST 2018, 83). *(Emphasis added.)*

It is evident that identification, categorization, and compliant disposal of information are important features of the risk management framework in NIST 800-37, as well as other standards referenced above. The most compelling arguments in favor of pursuing these tasks lie in the ability to mitigate risk associated with system ROT, to control costs, and to ensure information lifecycle management. There is an added benefit from operational efficiency gained in the ability to access

the correct and most current information, as opposed to sifting through years of redundant or superseded records.

How to Get Started

1. Create rules for tools. Develop a legally-valid retention schedule to apply against information assets and understand the difference between legally-required retention and preservation for litigation. These concepts, though related, are different (see discussion above.) Be sure policies and procedures reflect the reality of data management requirements and that they are enforceable. Plan for "security by design" when considering new technology acquisitions by building in retention rules before data are created.
2. Address the human element. Training for information governance and security is critical, but its quality and impact must also be measured to be effective. Cultural "will" and the "tone from the top" will drive the success of IG initiatives. Be sure to secure executive support and consider offering periodic training.
3. Reach out to peers in other functions to find out what issues and challenges they face because of information glut. Look for synergies to gain a critical mass behind a request for change.
4. Look for opportunities to leverage triggers. It's hard to get started without a compelling argument. Look for that argument in litigation/e-discovery spend, regulatory audit findings, Board of Directors inquiries, and budget requests.
5. Resist the temptation to allocate budget for more unstructured storage. Instead, work with the legal, compliance, privacy, audit, and risk functions to establish and enforce the classification, retention, and disposition of information.

Conclusions

Organizations have for decades allowed data to proliferate unmanaged. The accumulation of ROT not only carries with it the cost of storage, but also creates tremendous security risks by increasing the footprint for compromise by both internal and external players. This paper offers a rationale and process by which ROT may be eliminated through a triage and disposition process that applies legally-validated retention rules, so that the remaining information may be categorized and stored using appropriately tiered controls.

The goal is to diminish the attack surface, while at the same time achieving improved regulatory retention compliance and reducing storage costs. The ultimate success of this approach is dependent, however, on a commitment to cultural change and on participation by all invested stakeholders, including executive management, legal, compliance, IT, privacy, risk, and audit.

Effective information governance will most certainly reduce security risk, enhance compliance, and minimize costs. Take the first step by building the right foundation.

References

AIIM, 2018. State of Intelligent Information Management: Getting Ahead of the Digital Transformation Curve. https://www.aiim.org/Resources/Research/Industry-Watches/2018/2018_May_2018-State-of-Intelligent-Information-Management.

CGOC, 2018. Information Governance Benchmark Survey 2018. https://www.cgoc.com/information-governance-benchmark-survey-2018/.

ISO, 2013. ISO 27001:2013, Information technology — Security techniques — Information security management systems — Requirements.

NIST, 2015. Special Publication 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organization.

NIST, 2018. Framework for Improving Critical Infrastructure Cybersecurity, Ver. 1.1.

NIST, 2018. Special Publication 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.

Saffady, William. 2004. Records and Information Management: Fundamentals of Professional Practice. ARMA International.

Shetty, S. 2017. How to Tackle Dark Data. https://www.gartner.com/smarterwithgartner/how-to-tackle-dark-data/.

Varonis, 2018. Data Under Attack: 2018 Global Data Risk Report From the Varonis Data Lab. https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf.

Weaponized Letter and Package Attacks Against Public and Private Sector Targets: Key Takeaways for Security Practitioners

Joshua Sinai[1]

Abstract:

This article assesses the risk posed by the ability of a variety of threat actors to send weaponized letters and packages, usually via a country's mail system, against a spectrum of public and private sector targets in the U.S. and globally. A chronological listing of significant past attacks provides an empirical basis to assess the nature and severity of these incidents. The types of perpetrators involved in such attacks, their motivations, their weapons and devices (including hoaxes) used in the attacks, and targeting categories of the attacks are analyzed in this article. Best practices to prevent and mitigate the impacts of such attacks, including some of the techniques used by law enforcement and counterparts in the mail and package services to identify and apprehend the perpetrators, are reviewed.

THIS ARTICLE ASSESSES THE NATURE AND IMPLICATIONS of the risk posed by weaponized letter and package attacks, primarily via a country's mail system, against a spectrum of public and private sector targets. In order to better contextualize this issue, this article presents a chronological listing of significant past attacks in the United States and internationally. The types of perpetrators involved in such attacks, their motivations, the types of weapons and devices (including hoaxes) used in the attacks, and the targets are analyzed in this article. As demonstrated by a listing of 27 incidents, a majority of the perpetrators (18) are considered politically-motivated terrorists, while a minority of perpetrators (9) had non-political motives, such as seeking personal revenge against former employers. Most incendiary weaponized letter and package attacks consist of improvised explosive devices (IEDs). A minority of attacks employ non-IED devices, such as chemical agents (e.g. anthrax or ricin), and a considerable number also involve hoaxes intended to intimidate the intended recipient(s). Best practices to prevent and mitigate the impacts of such attacks, including some of the techniques used by law enforcement and counterparts in the mail and package services industry to identify and apprehend the perpetrators, are reviewed.

Weaponized letter and package attacks make up only a small portion of the overall tactics and weapons employed in domestic and foreign terrorist operations against their adversaries.[2]

[1] PhD and Consultant, TorchStone Global, Joshua.sinai@comcast.net. 1707 Pasture Brook Way, Potomac, MD 20854

[2] According to this research note, the majority of weapons used in 2,817 terrorist attacks between 2002 and 2016 in the United States, Canada, Western Europe, Australia and New Zealand employed explosives (49.0%), incendiary devices (33.3%), firearms (9.2%), vehicles (5.4%), and miscellaneous (3.1%). Although authoritative figures are not

However, they present a significant threat and are likely to persist because of the relative simplicity of acquiring and assembling such devices, the ease of sending them undetected via mail and parcel services, and the potential to generate widespread public anxiety and fear among their target(s), even if it is a hoax or the payload does not detonate. Given the perceived anonymity of putting a weaponized letter or package in the mail, whether at a postal office or in a postal box, a perpetrator may believe they will not be caught. New detection technologies are being built to better assist law enforcement services in identifying problematic letters and packages, the individuals that sent them, and apprehending such perpetrators – even if it can take some time to "connect the dots". However, new innovations in weaponizing letters and packages can be expected in this "cat-and-mouse" game in which perpetrators and security service providers are currently engaged.

Chronology of Incidents

The tactic of weaponizing letters and packages by various types of perpetrators to terrorize or eliminate rivals has occurred in the United States and internationally since the 18th century. For example, the first recorded incident occurred in Denmark in January 1764 when a parcel bomb was sent to a 'Colonel Poulson' – 11 years prior to the formation of the U.S. Postal System by the Second Continental Congress in 1775.[3] In a notable spate of such attacks in the United States, anti-government anarchists sent a series of mail bomb packages throughout 1919 that targeted politicians, including Supreme Court Justice Oliver Wendell Holmes, and powerful Wall Street figures like J.P. Morgan and John D. Rockefeller.[4] This chronology of incidents spans events since the early 1970s to the present day, organized by incidents in the United States and international incidents.

Incidents – United States

May 25, 1978 to April 24, 1995: Beginning on May 25 1978 and ending on April 24, 1995, Theodore Kaczynski, 36, (known as the "Unabomber"), killed three persons and injured 23 others with a series of package bombs delivered via the mail service that targeted universities, airlines, and newspapers.[5] He used the mail system to deliver nine of his 16 known devices.[6] Kaczynski was a former university professor of mathematics turned environmentalist anarchist and domestic terrorist, who believed that his bombings were necessary to call attention to how modern technologies and scientific research have destabilized society, increased psychological suffering, and eroded human freedom. While still on the loose, a break in the case occurred when, in cooperation with authorities, the *New York Times* and *Washington Post* published Kaczynski's diatribe against technological advancement (known as the "Unabomber Manifesto") on September

available, it can be assumed, based on the 7 U.S. domestic and international incidents listed in this article during this timeframe that weaponized letters and packages constituted a small percentage of the overall use of explosive and incendiary devices used in this database's listing of terrorist attacks. https://www.researchgate.net/publication/320260053_Use_of_Firearms_in_Terrorist_Attacks_Differences_Between_the_United_States_Canada_Europe_Australia_and_New_Zealand.

[3] https://www.economist.com/international/2010/11/04/going-postal.

[4] https://www.nydailynews.com/news/crime/1919-day-bomb-plot-helped-spur-1920-deadly-wall-st-blast-article-1.145630.

[5] For an account of Ted Kaczynski's bombing activities, see Jim Freeman, Terry Turchie, Donald Max Noel, Unabomber: How the FBI Broke Its Own Rules to Capture the Terrorist Ted Kaczynski (History Publishing Company, 2014).

[6] https://postalmuseum.si.edu/behindthebadge/unabomber.html.

19, 1995, in exchange for an end to his violence. It was at that time that David Kaczynski recognized the manifesto as his brother's writing and notified law enforcement authorities. This led to the FBI-ATF task force's eventual identification of his cabin in Montana, leading to his arrest on April 3, 1996.[7] On January 22, 1996 Kaczynski accepted a plea agreement sentencing him to life imprisonment without parole.

February 13, 1987: John Buettner-Janusch, 64, was a physical anthropologist and former university professor, who had previously been convicted in 1980 on several counts of harboring an illegal drug operation in his university laboratory.[8] Buettner-Janusch sought revenge for the drug conviction and anonymously mailed poisoned Valentine's Day chocolates, which arrived at the home of U.S. District Court Judge Charles Brieant, Jr. on February 13, 1987, nearly killing his wife, who had assumed they were intended for her. The chocolates contained atropine and sparteine. DNA tests proved that Buettner-Janusch, whom the judge had convicted several years earlier, was his would-be assassin. Buettner-Janusch also sent similar boxes of poisonous chocolates to several of his former colleagues. He pleaded guilty in 1988 and was sentenced to 20 years, but died in prison four years later.

December 16, 1989: Walter Leroy Moody, Jr., 55, sent a mail bomb to U.S. Federal Judge Robert Smith Vance, killing him upon opening the parcel in his home in Birmingham, Alabama.[9] His wife was also seriously injured. Moody also sent a mail bomb to Atlanta, Georgia attorney, Robert Robertson, who was killed by the explosion. Moody was motivated by his resentment of the court system ever since he was convicted in the 1970s of possessing a bomb that had hurt his wife when it detonated and subsequent interactions with Vance. In 1997 he was sentenced to death by execution, which took place on April 19, 2018.

September 18 – October 15, 2001: In the immediate aftermath of al Qaida's 9/11 attacks, a batch of several letters containing anthrax bacterial spores were dropped at a mailbox in Trenton, New Jersey. Two letters, which reportedly contained a more potent form of anthrax, arrived at the offices of Senator Tom Daschle and Patrick Leahy on October 15.[10] Letters were also sent to the offices of news organizations and U.S. Congressional lawmakers. The attacks killed five people and injured 17 others.[11] Several copycat hoax letters were reportedly sent by others. During the course of a seven-year investigation, Bruce Edwards Ivins, a senior biodefense researcher who had worked with anthrax at the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) in Frederick, Maryland, was suspected of mailing the letters, but no definitive conclusion had been reached at the time.[12] The motive for the letter attacks has also not been conclusively proven, with one possibility being Ivins may have viewed the letters' impact as an opportunity to rejuvenate interest in his anthrax vaccine program that was facing closure. He committed suicide in July of 2008.

---

[7] Ibid.
[8] For an account of John Buettner Janusch's attack, see https://www.nytimes.com/1992/07/04/nyregion/john-buettner-janusch-67-dies-nyu-professor-poisoned-candy.html.
[9] https://www.nytimes.com/2018/04/19/us/alabama-execution-walter-leroy-moody.html.
[10] https://www.cfr.org/backgrounder/anthrax-letters.
[11] https://www.smithsonianmag.com/smithsonian-institution/anthrax-letters-terrorized-nation-now-decontaminated-public-view-180960407/.
[12] For an account of Ivins, see https://www.nytimes.com/2009/01/04/us/04anthrax.html.

January 2007: John Patrick Tomkins, 42, a machinist in Dubuque, Iowa, who called himself "The Bishop" sent several threatening letters to investment firms and advisors between 2005 and early 2007. In January 2007, he mailed an unassembled bomb package to two financial firms in the United States. He was reportedly motivated by his worsening financial situation thinking that attacking financial institutions would lower their share prices, thereby increasing the value of his speculative bets against them. He was arrested on April 25, 2007 and received a 37-year sentence.[13]

April 15-17, 2013: James Everett Dutschke, 41, of Aberdeen, Mississippi, a martial arts instructor with an unstable work history, mailed ricin-laced letters to then-President Barack Obama, Senator Roger Wicker of Mississippi, and Mississippi judge Sadie Holland. Reportedly, he had sent the letters in order to frame his personal rival.[14] In May 2014 he was sentenced to 25 years in prison.

May 2013: Shannon Guess Richardson, age 40-41, a Texas actress, was arrested for sending ricin-laced letters to then-President Barack Obama, then-New York Mayor Michael Bloomberg, and Mark Glaze, the Director of Mayors Against Illegal Guns.[15] Her motivation was reportedly to frame her husband for the attacks while going through their divorce. In July 2014, she was convicted and sentenced to 18 years' imprisonment.

March 2018: Daniel Frisiello, 25, of Beverly, Massachusetts sent several letters containing a white powder to Donald Trump Jr.[16] The letter was opened by Trump Jr.'s then-wife, Vanessa Trump, inside their Manhattan, New York apartment. This was not the first time Frisiello had sent white-powder letters, as he had reportedly sent a white-powder letter to family members of then-presidential candidate, Donald Trump during the 2016 presidential campaign, threatening that if Trump did not drop out the next letter would not be fake. In September 2018, Frisiello pleaded guilty to 13 counts of mailing a threat to injure a person of another and six counts of false information and hoaxes.

March 2018: Mark Anthony Conditt, 23, of Pflugerville, Texas, was unemployed at the time he began his campaign of mailing IED-laden packages to several homes in Austin, Texas, including leaving several packages on front porches.[17] Two persons were killed and five were injured. Five months later, on August 28, he blew himself up when he realized police were closing in on him. Conditt left a video confession and reportedly did not have any terror- or hate-related references in the confession. His exact motivation remains undetermined.

October 1, 2018: William Clyde Allen III, 39, of Logan, Utah, a U.S. Navy veteran, had sent letters containing ricin to high officials in President Trump's Administration. On October 3, he

---

[13] See, https://www.justice.gov/usao-ndil/pr/iowa-man-sentenced-37-years-prison-mailing-pipe-bombs-and-threats-investment-firms-bid

[14] https://www.politico.com/story/2014/05/james-everett-dutschke-ricin-barack-obama-106840.

[15] https://www.independent.co.uk/news/world/americas/shannon-guess-richardson-actress-jailed-for-18-years-after-mailing-ricin-spiked-letters-to-us-9611491.html.

[16] https://www.nbcnews.com/news/us-news/man-who-sent-powder-trump-sons-others-gets-5-years-n996646.

[17] https://www.cnn.com/2018/03/21/us/austin-explosions/index.html.

was charged with seven counts for sending the letters.[18] The motivation for his letter attacks was unknown at the time, but he reportedly had previous encounters with the court system.

October 2018: Cesar Sayoc, Jr., 56, of Aventura, Florida, embarked on a several weeks long mailing of 16 explosive-laden packages against two former presidents, public figures, and media organizations such as CNN. He reportedly had a long criminal history. On October 26, he was arrested and charged with federal crimes, including interstate transportation of an explosive.[19]

Incidents - International

August 17, 1982: The South African government reportedly mailed a parcel bomb to the Mozambique home of Ruth First, a leading anti-apartheid activist in South Africa, who was living in exile at the time.[20] The parcel bomb killed her.

August 1985: David Sticovich, Rotorua, New Zealand, an estranged husband, sent a parcel containing sticks of gelignite to the home of Michele Sticovich, his wife, killing her, while a friend standing nearby was seriously injured. He was arrested and ultimately pleaded guilty to her murder.[21]

October 19, 1986: Nigeria's former leader, General Ibrahim Babangida, reportedly was responsible for sending a package bomb to Dele Giwa, a Nigerian journalist and editor of the *Newswatch* magazine, killing him.[22]

April 1990: The South African government's Civil Cooperation Bureau allegedly sent a letter bomb, that was hidden inside two religious magazines, to Michael Lapsley, a priest, severely injuring him.[23]

December 1993 - December 1995: During a two-year period, Franz Fuchs, 40, of Graz, Austria, mailed a total of 24 IED-laden letter bombs to Austrian politicians, including the mayor of Vienna, and others, killing four persons and injuring 15. Fuchs was reportedly a xenophobic activist. At his trial on March 10, 1999 he was sentenced to life in prison. On February 26, 2000, he committed suicide in his prison cell.[24]

September 12, 1996: Ricardo López, 21, an Uruguayan-American pest control worker, based in Hollywood, Florida, sent a letter bomb, containing explosives and sulfuric acid, to the London, England home of Björk, an internationally famous Icelandic singer. The bomb did not reach her as it was intercepted by London Police. López was reportedly an obsessed fan of Bjork who

[18] https://www.justice.gov/usao-ut/pr/allen-charged-seven-count-federal-indictment-threat-use-biological-toxin-weapon.
[19] https://www.nytimes.com/2019/03/15/nyregion/mail-bomber-cesar-sayoc.html.
[20] https://www.sahistory.org.za/dated-event/ruth-first-assassinated-mozambique.
[21] https://www.newshub.co.nz/nznews/former-top-roturua-cop-dies--2009112219.
[22] https://www.pulse.ng/news/local/dele-giwa-and-the-32-yr-old-haunting-mystery/djkryk7.
[23] https://www.sahistory.org.za/dated-event/father-michael-lapsley-anglican-priest-injured-letter-bomb.
[24] http://murderpedia.org/male.F/f/fuchs-franz.htm.

became angry over her relationship with another musician. López died by suicide before the police could apprehend him.[25]

January – February 2007: Over a three-week period, Miles Cooper, 27, of Cherry Hinton, near Cambridge, England, a primary school caretaker, sent seven letter bombs to public institutions and private companies he believed were involved in creating a 'surveillance society.' Nine people were injured by the letter bombs. On February 23, 2007 Cooper was arrested and in late September of that year was sentenced to prison.[26]

August 11, 2007: Adel Arnaout, 27, a Lebanese immigrant, of Ontario, Canada, sent three letter bombs to several individuals with whom he had legal entanglements, with the first letter bomb arriving on August 11. Reportedly, he aspired to become an actor, which was a dream he believed those individuals had deliberately sabotaged. He had also sent four cases of poisoned water to talent agencies, a bank, and a judge. On August 30, 2007, he was arrested and on March 7, 2012 was sentenced to prison.[27]

March 1 – April 15, 2011: Trevor Muirhead, 42, and Neil McKenzie, 43, from Ayrshire, Scotland, allegedly sent parcel bombs to Paul McBride, an attorney; Neil Lennon, a Celtic football club manager; and Trish Godman, a former Labour Party Member of Parliament. Both men were reportedly hardline Protestant loyalists and anti-Celtic Football Club (and anti-Catholic) extremists. They were arrested in May 2011 and convicted at the High Court in Glasgow, Scotland and on March 30, 2012, were sentenced to imprisonment.[28]

February 2014: Seven letter bombs were allegedly sent by the Northern Ireland-based the 'Real IRA' dissident splinter faction to British Armed Forces recruitment offices in England. the United Kingdom.[29] No other information was available about the senders' identities or their motivation.

September 2015: At least six people were killed and dozens injured in explosions at 15 locations in Liucheng County in China's Guangxi Zhuang Autonomous Region. The explosives were concealed inside express delivery packages.[30] No other information was available about the senders' identities or their motivation.

March 15, 2017: A package with an explosive mechanism that was mailed from Greece and addressed to Wolfgang Schäuble, a German government minister, was intercepted by German authorities. On the package, the name of a prominent German politician was written as the "sender." "The Conspiracy of Cells of Fire," an extremist anarchist organization claimed responsibility of the attack.[31] No other information was available about the senders' identities or their motivation, as well as the name of the "politician" whose name was listed as the sender.

---

[25] https://en.wikipedia.org/wiki/Ricardo_L%C3%B3pez_(stalker).
[26] https://www.theguardian.com/uk/2007/sep/27/ukcrime.davidbatty.
[27] https://www.thestar.com/news/crime/2012/03/07/toronto_judge_declares_letter_bomber_adel_arnaout_a_dangerous_offender.html.
[28] https://www.bbc.com/news/uk-scotland-glasgow-west-17869217.
[29] https://www.theguardian.com/uk-news/2014/feb/17/new-ira-sent-bombs-army-recruitment-centres-britain.
[30] https://www.rt.com/news/317030-china-massive-blasts-liuzhou/.
[31] https://www.thenationalherald.com/154689/parcel-explosives-sent-schaeuble-cited-nd-vp-georgiadis-sender/.

March 16, 2017: An explosive mechanism-laden package that had been sent from Greece arrived at the International Monetary Fund (IMF) offices in Paris. It exploded, injuring an employee. It was reportedly intended for the IMF's Director. The name of another prominent German politician was written on the package as "sender."[32] No other information was available about the senders' identities or their motivation, as well as the name of the "politician" whose name was listed as the sender.

May 25, 2017: A letter bomb exploded inside the car of Lucas Papademos, a former Prime Minister of Greece, injuring Papademos, his driver, and another passenger. The explosive device was placed inside the envelope, which was in Papademos's possession, and had detonated while the car was driving in Athens.[33] No other information was available about the senders' identities or their motivation.

January 2019: Envelopes containing threatening letters and a powder, believed to be potassium cyanide, were sent to more than a dozen Japanese companies. One of the letters had threatened to distribute drugs laced with potassium cyanide, unless a ransom was paid in Bitcoin. The targets included the Asahi and Mainichi newspapers and pharmaceutical companies. A food company in the northern city of Sapporo was also targeted. The names on the envelopes were former leaders of the Aum Shinrikyo who had been executed the previous year for their 1995 sarin gas attack on the Tokyo subway.[34] No other information was available about the senders' identities or their motivation.

March 5, 2019: Three suspicious packages that contained homemade bombs capable of igniting a small fire were found in and around transport hubs in London, England. These included Heathrow Airport, a mail room at Waterloo Station on Cab Road, and the City Aviation House near London City Airport (LCY). A fourth explosive device was discovered at the University of Glasgow. The three packages were described as similar: all midsize white envelopes with padded manila envelopes inside. These attacks were followed by another suspect package that arrived on March 22 at a mail sorting center in Limerick, Ireland.[35] Though still under investigation, it was suspected that NIRA, an IRA dissident splinter faction, may have been responsible for the letter bombs.

Tactics and Weapons

It should be noted that the likelihood of an organization or individual receiving a weaponized letter or package is extremely rare. As an illustration, although a timeframe is not provided, according to the U.S. Postal Service, it had investigated "an average of 16 mail bombs [annually] over the last few years," while it had "processed over 170 billion pieces of mail," so "the chances that a piece of mail actually contains a bomb average far less than one in 10 billion!"[36]

---

[32] https://www.nytimes.com/2017/03/16/world/europe/paris-imf-bomb.html.
[33] https://www.nbcnews.com/news/world/former-greek-prime-minister-lucas-papademos-injured-explosion-car-n764651.
[34] https://www.reuters.com/article/us-japan-crime/suspected-potassium-cyanide-sent-to-japanese-newspapers-drug-and-food-companies-media-idUSKCN1PN08U.
[35] https://www.nytimes.com/2019/03/05/world/europe/london-transit-bombs.html.
[36] https://postalinspectors.uspis.gov/raddocs/bombs.htm.

A perpetrator deciding to weaponize a letter or package makes a variety of decisions that are involved in selecting the tactics for an attack. These include:

- Delivery mechanism. Should an envelope or a package be used? A letter is usually a standard No. 10 envelope, and is designed to contain a flat object, such as folded sheets of paper. A package is the size of a parcel or a box.
- Delivery method. Should the letter or package be sent via mailbox or hand-delivered to a post office? Using a mailbox facilitates anonymous delivery, whereas at a post office the sender would have to interact with a window clerk.
- Payload. A letter bomb may be designed to explode immediately on opening or damage could be inflicted by the recipient making contact with its contents, such as a letter containing a poisonous chemical or biological agent. If a hoax is intended, perhaps just material that represents something more malicious, such as talcum powder, could be used.
- Detonation. Should a package containing an IED be employed, such as a pipe bomb, what triggering mechanism should be used that sets it to explode upon opening?

Based on the U.S. and international incidents listed in this article's chronology, it appears that almost an equal number of attacks involved sending either weaponized letters or packages to their intended victims. As demonstrated by Table 1 (below), in the 11 U.S. domestic attacks, four letters used anthrax or ricin, one letter contained a hoax powder, while of the 6 weaponized package attacks, five contained bombs, while one contained a non-IED poison consisting of poisonous chocolates. In one of the package bomb attacks, in addition to mailing some of them, a few of the packages were left at their intended victims' porches or mailboxes and intended to look as though they were dropped off by a parcel delivery service. Internationally, of the 16 attacks, seven of the attacks featured letter bombs, one featured potassium cyanide, while eight were bomb-laden packages. Of the eight package bombs, two were allegedly sent by the then-Apartheid-dominated South African government, while one was allegedly sent by a former government leader in Nigeria. Finally, five of the attacks involved cross-country letter- and package-laden bomb explosives.

	Domestic	International
Total Incidents	11	16
Weaponized Letters		
Anthrax/Ricin	4	0
Hoax Powder	1	0
Potassium Cyanide	0	1
Bombs	0	7
Total	5	8
Weaponized Packages		
Bombs	5	8
Non-IED Poison	1	0
Total	6	8
Alternate Delivery Methods		
Impersonating Mail	1	0
Cross-Country	0	5

Table 1

Overall, the delivery advantage for an attacker is to write an address on an "innocent looking" envelope or a package and expect it to arrive days later at the specified address of the intended individual or organization, anywhere domestically or internationally, where it is set to cause terror or actual harm through chemical agents or explosive devices once opened or interacted with. This mode of attack has transformed a country's postal service and private package delivery companies into unwitting vectors for the perpetrators' violence.

Motivation

Several motivation types drive perpetrators to employ weaponized letters and packages in their attacks. One of the first motivations to be examined is whether it is perpetrators' intent to "send a terrorizing message," whether politically driven or of a non-political nature, or to inflict physical and emotional casualties on their intended targets? Thus, of the 11 attacks in the U.S., 10 were intended to inflict casualties and one was a hoax, while internationally, all 16 of the attacks consisted of weaponized letters or packages.

Another motivation for employing the postal service to deliver an attack is anonymity. This might be due to the relative ease of acquiring and assembling weaponized letters and packages, and what they might perceive to be the relative low risk of being identified as the sender(s) since it is difficult for law enforcement authorities to trace such perpetrators. This method may also enable the sender to circumvent other defenses like security gates and locked doors, since mail is generally implicitly trusted and delivered straight to the target. This was the case with several of the international incidents listed above, such as in Greece and Britain, where the perpetrators had reportedly not been apprehended. In the case of Ted Kaczynski, it took almost 18 years for the U.S. authorities to apprehend him.

A spectrum of radical ideologies is another motivation, whether far-right-wing, far-left-wing, or single-issue philosophies, such as environmental extremism such as Theodore Kaczynski (late 1970s until 1996). Even though many extremist ideologies contain conspiracy theories, there are other cases where the perpetrators' conspiratorial theories are just too confusing to be categorized. Examples of such far-right-wing perpetrators include William Clyde Allen III (October 1, 2018).

Some perpetrators are motivated not by extremist political beliefs but by personal vengeance. Jilted spouses or lovers, or terminated employees, might seek revenge against their perceived "wrongdoers." Judges might also be targeted by defendants seeking revenge for their perceived wrongdoing of their court decisions. Examples include John Buettner-Janusch (February 13, 1987) and Walter Leroy Moody, Jr. (December 16, 1989).

Widespread media coverage of their attacks is a considerable motivator for many perpetrators, eager for the attention that the use of such tactics and weaponry can generate, thereby amplifying their "message" to a large audience. Terrorism, caused by widespread panic and anxiety beyond the localized incident, is the goal. This was the case with all the incidents listed in this sample, particularly the post 9/11 anthrax letter attacks, as well as the October 2018 bomb-laden package attacks, with the wider audience believing that if they cannot safety open their mail, they cannot feel safe anywhere.

A final motivation is the desire to extort ransom from their intended victims. This was the case with the January 2019 letter threats in Japan by remnants of the Aum Shinrikyo cult that included a demand for ransom to be paid in Bitcoin.

Categories of Attackers

Several types of attackers employ the tactic of weaponized letters and packages. Domestically, they tend to be lone actor attackers, as opposed to centrally organized groups or loosely affiliated local networks of foreign terrorist groups. Overall, from the early 1990s to around 2015, lone actors accounted for six percent of all terrorists in the U.S. — but they were responsible for 25 percent of all U.S. terrorist attacks.[37] Social isolation may be why lone actors are typically able to evade arrest for longer periods of time than terrorists who act in groups—they tend to draw less attention. An example of such a lone actor terrorist includes Cesar Altieri Sayoc (October 2018). Internationally, however, of the 17 incidents, nearly half were likely carried out by individuals belonging to terrorist groups in attacks in China, Greece, and Northern Ireland.

Financial Impact on Organizations

Being targeted by weaponized letters and packages is disruptive and costly for affected organizations, whether in the public or private sectors. Of the 11 U.S. attacks, with eight targeting public sector organizations or individuals and three targeting private sector organizations or individuals, the associated actuarial insurance and other liability-based costs of such attacks are an important consideration for a private organization's human resources, legal, and security departments. In other cost estimations, for example, the U.S. Postal Service refused to accept packages or letters bigger than 12 ounces for about six days at the beginning of Ted Kaczynski's campaign.[38] In late 2001, with the U.S. already on edge after the 9/11 attacks, the envelopes containing anthrax spores that arrived at media companies and Congressional offices resulted in high public and private costs associated with their decontamination, which were estimated at about $320 million.[39] In addition, this campaign also set off a trend of copycat attacks, with envelopes stuffed with talcum powder and baking soda generating additional costs in ensuring their safety. Although it was too early to formulate an accurate estimate, it is likely the Cesar Sayoc attacks in October 2018 cost several million dollars for the responding organizations.

Mitigation Methods

Several mitigation methods are employed to identify suspicious weaponized letters and packages. In the U.S., major innovations were instituted in the aftermath of Ted Kaczynski's almost 18-year long mail attack, including the development of new detection technologies to identify and safeguard the country's mail system.

An example of protection at the post office level is the U.S. Postal Inspection Service's National Forensic Laboratory, which is staffed with forensic scientists and technical specialists who investigate the identities and locations of such senders. They perform investigations such as handwriting, paper type, and fingerprint analyses to uncover a sender's unique signature. For example, it is reported that Sayoc's social media postings had included some of the same misspellings that were noticed on the packages he had sent. The postal service's laboratory can also conduct physical and chemical tests on bomb debris that might lead to larger discoveries that enable them to identify possible suspects. Private sector delivery services also deploy in-house security units to investigate weaponized letters and packages.

Also examined is the identity of potential individuals who might be involved in delivering the packages. For instance, they may try to track down the courier in order to identify possible

[37] https://fivethirtyeight.com/features/pipe-bomb-lone-wolf-terrorism/.
[38] https://www.theatlantic.com/technology/archive/2018/03/mail-postal-service-bombs/555440/.
[39] https://www.liebertpub.com/doi/abs/10.1089/bsp.2010.0053?src=recsys&mobileUi=0&journalCode=bsp.

linkages to their original senders. At the postal sorting facilities where such mail may have been sent, advanced technology surveillance cameras might also catch the individual dropping off a suspicious letter or package. This was the case with the Austin bomber who was identified when he dropped off one of his package bombs on March 20, 2018.

Related technological advances in biometric fingerprint and DNA detection of such senders, including the automated capability to digitally reverse engineer the transport movement of mailed packages, and make it possible for law enforcement authorities to quickly identify and apprehend such threat actors. This was the case with Sayoc, who was identified as a potential suspect within days of the IED packages' detection, leading to his arrest.

Mitigating the Impact for Potential Private Sector Recipients

With the U.S. Government's weaponized letter and package mitigation program well-developed, and the U.S Postal Service's investigative arm (as well as other government investigative services, such as the U.S. Secret Service and the FBI) working with the private sector, it is still up to private sector to implement their own protective programs. There are several measures for the private sector to mitigate the risk of weaponized letters and packages that might threaten their employees and facilities.

First, if a prominent person or organization fits the profile of being a possible recipient of weaponized letters or packages, those individuals and organizations should be trained to not open packages that are unexpected, that appear suspicious, or come from an unknown sender. Ensure that colleagues are also instructed on how to identify and physically handle such suspicious letters and packages.

Some suspicious indicators include the following:[40]

- A missing return address
- An item from an unknown or unusual location
- A misspelling of an address
- A return address that is different from the location from which it was mailed
- A package that is taped excessively
- A wire protruding from a package
- A package that emits a suspicious odor due to the presence of chemicals
- A letter or package that does not feel "normal", such as containing unusual plastic or metallic components as opposed to typical paper or bubble stuffing
- Unusual sounds emanating from the package, such as a buzzing or ticking noise

Second, an organization's internal mail screening/handling and package delivery acceptance procedures should be reviewed to ensure consistency and efficient response measures for suspicious mail/package incidents. Updates to security awareness training should include safe handling and notification procedures if a suspicious package/envelope arrives. Security precautions should also be aligned to heightened national/local threat environments, including industry sector specific recommendations. Thus, for example, if certain sectors, such as media communications or financial institutions, are being targeted by a wave of weaponized letters and packages, then the organizations and companies in those sectors should take special precautions to protect themselves as well.

[40] This listing of suspicious indicators is based on https://www.wrc.noaa.gov/wrso/security_guide/mailbomb.htm.

Third, companies and organizations need to establish an interdisciplinary threat assessment team to identify, assess, and manage potential threats against them by individuals who might harbor a grievance against them – or their general sector – that could lead to a weaponized letter/package attack.

Finally, there should be well-established processes in organizations and companies for responding to suspicious letters and packages, whether they are sent to employees' offices or homes. These include establishing cooperative relationships with appropriate public safety authorities, such as an organization's security department, local police, a local postal inspector, or other relevant investigatory agencies so that if an incident occurs, established procedures are in place for a quick mitigation response.

Conclusions

The frequency of weaponized letter and package attacks is rare relative to other forms of violence (only eight of the 2,817 terrorist attacks reported between 2002 and 2016 were identified as being a weaponized letter or package attack; see footnote #1), but they continue to occur. Because they are a low probability, but high consequence risk, public and private sector organizations and companies need to anticipate the full spectrum of potential threats that might challenge them, and to effectively protect their employees and facilities from such "postal" threats. To do so effectively, they need to allocate appropriate budgets for mailroom security, conduct risk assessments against a spectrum of such threats that might challenge them, implement appropriate security programs, exercise them regularly, and thereby minimize the potential impact to their employees and facilities if a weaponized letter or package attack occurs.

The Anti-Vaxxers Movement and National Security

Mark Jarrett and Christine Sublett[1]

Abstract:

The article reviews the national security implications of the anti-vaccine movement ("Anti-Vaxxers") in the United States. In addition to reviewing the background and psychology of the Anti-Vaxxers movement, the national security implications of both naturally-occuring pandemics and bioterrorism are considered.

VACCINES ARE AMONG THE STRONGEST TOOLS in the medical armamentarium against infectious diseases (Immunization Action Coalition, 2018). Despite the cultural advances in sanitation, clean water and personal hygiene, vaccines play a major role in decreasing morbidity and mortality of infections. If one compares morbidity figures for the early 20th century with 2016, one sees that measles has decreased from over 500,000 cases to 69, smallpox from 29,000 to zero, and rubella from 47,000 to 5 (CDC 2019b; CDC 2016). These remarkable results can be attributed to the effectiveness of the vaccines and herd immunity. Vaccines are not 100 percent effective, but the concept of herd immunity prevents the spread of an infectious vector even if the population is not totally protected. The recent outbreaks of measles, a highly infectious and potentially fatal disease, in the United States underscores the risk to the public health of significantly large groups of people deciding not to vaccinate their children, as well as waning immunity in the adult

[1] MD, MBA, MS, Chief Quality Officer, SVP & Associate Chief Medical Officer, Northwell Health, New Hyde Park, NY, mjarrett@northwell.edu (Jarrett) and M.A., CISSP, CIPT, CRISC, CGEIT, Sublett Consulting, LLC, San Mateo, CA, csublett@sublettconsulting.com (Sublett).

population. This has dangerous implications for public health for both natural and purposeful future pandemics.

There are serious public health ramifications and national security issues if there was a naturally occurring pandemic with a novel organism or an infectious disease outbreak due to bioterrorism. Disease transmission is now a global phenomenon because of air travel and open borders. Increasing drug resistance is also another threat (WHO 2018). In addition, the relative ease of "bad actors," such as nation states or terrorists, to weaponize infectious agents has increased the vulnerability of the population. Reduction in mortality and morbidity by halting the spread of the organism will require both social isolation and mass vaccination. In the Ebola outbreak of 2014–2016 only a small number of possible contacts were placed in isolation within the United States, but despite the press coverage, some still went out into the public, including one physician television correspondent (McCoy 2015). The economic burden from the 2014–2016 Ebola outbreak on the United States was $2.4 billion (CDC 2019a) and $53 billion worldwide (Miles 2018). The CDC in 2017 updated guidelines on social distancing and isolation (Qualls et al. 2017). Clearly, social isolation will be one component of preventing the spread of a potential pandemic. A critical strategy will be the use of a vaccine, if available, to control outbreaks. Historically, the complexities of manufacturing vaccines and distributing them to entire populations were the main difficulties in managing outbreaks, but this has changed. Today, the biggest threat in controlling an outbreak comes from those who categorically reject vaccination.

This poses specific risks for bioterrorism events where lack of trust in government, coupled with a fear of vaccinations, will produce gaps in our ability to achieve herd immunity. This can be magnified by nefarious use of social media, such as Russian trolls spreading vaccination fears, making it much more difficult to achieve compliance. As stated before, since vaccines are not always 100 percent effective, spread of the disease will continue, especially to the most vulnerable — the very young, those with compromised immune systems, and the elderly. This is compounded by our mobile society that will allow further spread even with social isolation. Severe government restrictions on travel may need to be put in place, but the impact of such restrictions on both the economy as well as the supply chain for food, medications, and other essentials will have more impact than would otherwise be necessary. The SARS coronavirus outbreak of 2003 resulted in only 800 deaths worldwide, but the cost to the world economy was estimated to be $40 billion (Lee and McKibbin 2004). Finally, the human toll of suffering due to the disease will be much greater than was necessary.

Vaccines work by helping the body develop immunity to an infectious agent that it has never been exposed to naturally. They imitate a naturally occurring infection by stimulating the immune system to produce both cells and antibodies that will fight the infection, often preventing or minimizing symptoms. Since this process may take several weeks, there is a window after vaccination where the infection can still produce illness. Also, the elderly and people with weakened immune systems may not respond to vaccines. There are five types of vaccines: Inactivated vaccines, live-attenuated vaccines, toxoid vaccines, subunit vaccines, and conjugate vaccines (CDC 2018). In order to deliver long-lasting immunity, some vaccines require multiple doses, and some require boosters, such as a tetanus booster every 10 years. For one example, smallpox was eradicated worldwide, which allowed the discontinuation of the vaccine. Following 9/11, fear of weaponized smallpox prompted the New York State Department of Health to start a program of volunteer clinicians who would be revaccinated and trained on giving the vaccine if needed.

The percentage of the population that needs to be immunized in order to provide herd immunity varies based on the infectious agent. This threshold, called "basic reproduction number," is often referred to as "R0." This number represents how many people in an unprotected population one infected person could pass the disease along to. For example, R0 for measles is between 12 and 18, whereas for polio, it is between 5 and 7. The higher this number is, the higher the immunity threshold must be to protect the community. Because measles is extremely contagious and can spread through the air, for example, the immunity threshold needed to protect a community is high, at 95%. Diseases like polio, which are somewhat less contagious, have a lower threshold—80% to 85%.4 (Funk 2017).

There are many reasons people choose to not vaccinate their children or themselves. These reasons range from personal and religious beliefs, to medical reasons such as allergies, to distrust of vaccine ingredients. State laws establish vaccination requirements for school children, and these laws often apply to children attending not only public schools but also private schools and day care facilities. All states provide medical exemptions, and some states also offer exemptions for religious and/or philosophical reasons. State laws also establish mechanisms for enforcement of school vaccination requirements and exemptions. In response to the current measles outbreak, Washington state passed a new law limiting the use of parents' personal and philosophical objections to refuse vaccinations for their children (Lee 2019), and the California legislature has also proposed a bill to close the personal and philosophical objection loophole (Liss 2019).

The modern anti-vaxxer movement, composed of people who falsely believe that vaccines are dangerous, started with the publication 20 years ago of a now-retracted study by David Wakefield that erroneously linked the measles, mumps and rubella vaccine (MMR) to autism (McCoy 2015). And while the Centers for Disease Control (CDC) has released studies that show no link between autism and vaccines or that an aggressive vaccination schedule for children causes autism, many people still believe that there is a connection and refuse to vaccinate their children. There has also been a rejection of scientific evidence in many communities that vaccines protect against disease, predating widespread use of the Internet and social media. Worldwide, there are many cases of leaders lying to their citizens about vaccine efficacy in populist movements, including by Italy's Five Star Movement, which is now a part of that country's government, and among the Taliban in Afghanistan. Healthcare workers involved in intelligence operations in locales including Pakistan has led to distrust of the services offered, including vaccines against deadly diseases like polio and measles (McNeil, Jr. 2012).

While the anti-vaxxer movement is not new, a 2019 report issued by the World Health Organization (WHO) named "vaccine hesitancy" one of the top 10 threats to global health (WHO 2019). Vaccine hesitancy is defined as the belief that vaccines are not important, safe or effective. It is not just the United States that is experiencing a surge in measles cases; several western countries including the United Kingdom, Australia, New Zealand and Italy have experienced recent measles outbreaks. The World Health Organization recently issued a report that estimated there were 6.7 million cases of measles worldwide in 2017, an increase of 30 percent over 2016 numbers. In addition, Washington, Oregon and New York are in the midst of a widespread measles outbreak, with most cases in Washington involving children under 10 who were not vaccinated (Floccus 2019). In April 2019, nearly 700 students and staff were quarantined at the University of California, Los Angeles (UCLA), and California State University, Los Angeles (CSULA) after possible exposure to a person with measles (Mele 2019).

There have been several disease outbreaks in the U.S. in recent years including a 2015 measles outbreak originating at Disneyland that proceeded to infect 70 people in six states. And

it's not just measles; many other diseases that had been all but eradicated by modern medicine are candidates for or have experienced outbreaks, including whooping cough, polio, mumps and more.

In addition to the retracted study by Wakefield, there are several other factors driving the anti-vaxxer movement. These include alignment with other conspiracy movements including the far right (Weill 2019), and social media misinformation and propaganda campaigns by many foreign and domestic actors. Included among these actors is the Internet Research Agency (IRA), the Russian government–aligned organization that has been identified as responsible for interfering in the 2016 U.S. presidential election. Russia's disinformation campaigns are not limited to the United States; they continue to play a role in anti-vaxxer initiatives in many western countries including Italy, Australia and the United Kingdom. Russia's ultimate goal is to sow discontent and distrust in topics and initiatives that serve U.S. interests (Kirk 2019).

Social media continues to play a significant role in propagating false and misleading information about vaccines. In March of this year, Ethan Lindenberger, a teen who had himself vaccinated against his mother's wishes, testified in front of a Senate committee and attributed his mother's anti-vaccine ideology to misinformation she read on Facebook (Doubek 2019). Facebook has acknowledged that their algorithms have targeted anti-vaccination materials and advertisements toward women (since mothers are still primary caregivers for most children) in areas with high numbers of measles reports and have agreed that they need to reduce the distribution of health and vaccine–related misinformation.

A 2018 study (Broniatowski et al. 2018) found that the Internet Research Agency has used both trolls (individuals who misrepresent their identities with the intention of promoting discord) and bots (accounts that automate content promotion) to amplify anti-vaxxer positions on the Internet. These trolls were Russian users connected to the Internet Research Agency; their goal was to present both pro- and anti-vaccination information in the form of posts that would sow division, act as a political wedge issue and exploit discord. Twitter bots distributed spam and malware impersonating human users to distribute anti-vaccine messages. In many cases, tweets and posts by the Internet Research Agency bots and trolls were identified with the hashtag #VaccinateUS. The authors tied both anti- and pro-vaccine messages to U.S. politics and often referenced conspiracy theories focused on the U.S. government. These messages often cited arguments and opinions designed to heighten ethnic and racial tensions. Standard anti-vaccine messages not tied to Russian trolls and bots did not generally target socioeconomic or racial tensions that exist in the U.S.; rather, they generally characterized vaccines as unsafe for all people.

In April 1947 millions in New York City received smallpox vaccinations after a businessman contracted the disease from his travels and returned to New York. Ring vaccination, in which anyone who had contact with infected individuals were immunized, halted the spread of the disease, but almost all New Yorkers were immunized by the end of the month (Sepkowitz 2004). Pictures from that time show people waiting politely on lines blocks long for their immunization. Unfortunately, based on the anti-vax movement fueled by false information spread by social media, this type of public response seems unlikely today.

Both natural and intentional epidemics pose a serious risk for the United States and the world. The direct effect of such an epidemic in terms of morbidity and mortality is clear, but the toll on the infrastructure can be just as devastating. Social distancing and isolation have impacts that include loss of manufactured goods, reduced food supply, and other disruptions to the supply chain. We live in a "just in time" culture where supplies will be quickly consumed and not replaced. This was underscored by Hurricane Maria, which caused widespread damage in Puerto Rico and halted the production of drugs and medical supplies manufactured there (Aton 2017).

Conclusion

What can we do to prevent this scenario? We need to have bipartisan leadership support the scientific evidence. In addition, clinicians, health educators, community and religious leaders, and physicians must be part of a campaign to refute the anti-vaxxers and need to specifically reach out to communities with a high prevalence of vaccine hesitancy. We also need social media companies to continue to refine the algorithms that power their services to better distinguish quality information from deceptions or otherwise misleading information. Unfortunately, there is no guarantee that these approaches will be successful. Therefore, public health and emergency planners must now prepare for possible scenarios where herd immunity will not be a tool to control a pandemic.

References

Aton, Adam. 2017. "Hurricane Maria Takes a Toll on Global Medical Supplies." *Scientific American*, October 25, 2017. https://www.scientificamerican.com/article/hurricane-maria-takes-a-toll-on-global-medical-supplies/

Broniatowski , David A., Amelia M. Jamison, SiHua Qi, Lulwah AlKulaib, Tao Chen, Adrian Benton, Sandra C. Quinn, and Mark Dredze. 2018. "Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate," *American Journal of Public Health* 108, October 2018: 1378–1384. doi: https://ajph.aphapublications.org/doi/10.2105/AJPH.2018.304567

CDC (Centers for Disease Control). 2016. The Spread and Eradication of Smallpox. Last modified August 30, 2016. https://www.cdc.gov/smallpox/history/smallpox-origin.html

CDC (Centers for Disease Control). 2018. Understanding How Vaccines Work. Last modified July 2018. https://www.cdc.gov/vaccines/hcp/conversations/downloads/vacsafe-understand-color-office.pdf

CDC (Centers for Disease Control). 2019a. The Cost of the Ebola Epidemic. Last modified March 8, 2019. https://www.cdc.gov/vhf/ebola/history/2014-2016-outbreak/cost-of-ebola.html

CDC (Centers for Disease Control). 2019b. Measles. Last modified May 13, 2019. https://www.cdc.gov/measles/index.html

Doubek, James. 2019. "18-Year-Old Testifies About Getting Vaccinated Despite Mother's Anti-Vaccine Beliefs." National Public Radio, March 6, 2019. https://www.npr.org/2019/03/06/700617424/18-year-old-testifies-about-getting-vaccinated-despite-mothers-anti-vaccine-beli

Floccus, Gillian. 2019. "Measles Outbreak in Pacific Northwest about Half of U.S. Cases." *The Associated Press*, March 1, 2019. https://www.apnews.com/5ba32e2d9dab42c7a7a80ff83a0bdfbe

Funk, Sebastian. 2017. "Critical Immunity Thresholds for Measles Elimination." Centre for the Mathematical Modelling of Infectious Diseases, London School of Hygiene & Tropical Medicine, October 19, 2017. https://www.who.int/immunization/sage/meetings/2017/october/2._target_immunity_levels_FUNK.pdf

Immunization Action Coalition. May 11, 2018. Vaccine Basics – Importance of Vaccines. http://www.vaccineinformation.org/vaccines-save-lives/

Kirk, Katherine. 2019. "How Russia Sows Confusion in the U.S. Vaccine Debate." *Foreign Policy*, April 9, 2019. https://foreignpolicy.com/2019/04/09/in-the-united-states-russian-trolls-are-peddling-measles-disinformation-on-twitter/

Lee, Bruce Y. 2019. "With Measles Crisis, Washington State Now Limits Vaccine Exemptions." *Forbes*, May 12, 2019. https://www.forbes.com/sites/brucelee/2019/05/12/with-measles-crisis-washington-state-now-limits-vaccine-exemptions/

Lee, Jong-Wha, and Warwick J. McKibbin. 2004. *Estimating the Global Impact of SARS, Learning from SARS: Preparing for the Next Disease Outbreak: Workshop Summary, Institute of Medicine (US) Forum on Microbial Threats*, edited by Knobler S, Mahmoud A, Lemon S, et al. Washington (DC): National Academies Press (US); 2004. https://www.ncbi.nlm.nih.gov/books/NBK92473/

Liss, Julie Patel. 2019. "A 'Booster Shot' for California's Vaccine Law?" *EdSource*, April 23, 2019. https://edsource.org/2019/a-booster-shot-for-californias-vaccine-law/611447

McCoy, Terrence. 2015. "The Disneyland Measles Outbreak and the Disgraced Doctor Who Whipped Up Vaccination Fear." *The Washington Post*, January 23, 2015. http://www.washingtonpost.com/news/morning-mix/wp/2015/01/23/the-disneyland-measles-outbreak-and-the-disgraced-doctor-who-whipped-up-fear-about-vaccinations/

McNeil, Jr., Donald G. 2012. "C.I.A. Vaccine Ruse May Have Harmed the War on Polio." *New York Times*, July 9, 2012. https://www.nytimes.com/2012/07/10/health/cia-vaccine-ruse-in-pakistan-may-have-harmed-polio-fight.html

Mele, Christopher. 2019. "More Than 700 at 2 California Universities Under Quarantine Amid Measles Outbreak." *New York Times*, April 26, 2019. https://www.nytimes.com/2019/04/26/us/measles-outbreak-los-angeles-quarantine.html

Miles, Tom. 2018. "West Africa's Ebola Outbreak Cost $53 Billion — Study." *Reuters*, October 24, 2018. https://www.reuters.com/article/us-health-ebola-cost/west-africas-ebola-outbreak-cost-53-billion-study-idUSKCN1MY2F8

Qualls, Noreen, Alexandra Levitt, Neha Kanade, Narue Wright-Jegede, Stephanie Dopson, Matthew Biggerstaff, Carrie Reed, and Amra Uzicanin. 2017. Community Mitigation Guidelines to Prevent Pandemic Influenza — United States, 2017. MMWR Recomm Rep 2017;66(No. RR-1):1–34. http://dx.doi.org/10.15585/mmwr.rr6601a1

Sepkowitz, Kent A. 2004. The 1947 Smallpox Vaccination Campaign in New York City, Revisited. *Emerging Infectious Diseases*, 2004 May; 10(5): 960–961. https://wwwnc.cdc.gov/eid/article/10/5/03-0973_article

Weill, Kelly. 2019. "Anti-Vaxxers Are Cozying Up to the Far Right Online." *The Daily Beast*, March 1, 2019. https://www.thedailybeast.com/anti-vaxxers-are-cozying-up-to-the-far-right-online

WHO (World Health Organization). 2018. Antibiotic Resistance. Last modified February 5, 2018. https://www.who.int/news-room/fact-sheets/detail/antibiotic-resistance

WHO (World Health Organization). 2019. Ten Threats to Global Health in 2019. https://www.who.int/emergencies/ten-threats-to-global-health-in-2019

The State of Medical Device Cybersecurity

Vidya Murthy and Mike Kijewski[1]

Abstract:

Beginning with breaking down why cybersecurity matters, we discuss the evolution from privacy to patient safety. Considering the regulatory evolution specific to medical device cybersecurity posture over time, we investigate the difference between mandated behavior and better practices portrayed by device vendors. Through an empirical review of healthcare hack events, we explore trends in the types of device vulnerabilities that have led to cyber-events and those which have been researched to have an impact on patient safety. Lastly, we will consider the healthcare community as a whole and reflect on the roles medical device vendors, security researchers, health delivery organizations and service providers play in increasing our collective maturity as well as challenges each function faces.

MEDICAL DEVICE CYBERSECURITY has hyperbolically been portrayed in a Homeland episode where the fictional vice-president's pacemaker is hacked and a Grey's Anatomy episode where the hospital is shut down by a hacker. In reality, the state of cybersecurity in medical devices as part of the healthcare ecosystem is something to be understood in the context of patient care.

The healthcare industry is a complex web of payers, providers, medical device manufacturers, third-party vendors, and (perhaps most importantly) patients. Over the last decade, technology has played a central role in advancing quality of care, creating new delivery mediums and changing access for patients, in large part due to the development of new connected medical devices. The lesser-discussed innovation has been in viewing healthcare cybersecurity as a HIPAA compliance mitigation instead of a patient safety mechanism.

Cybersecurity and patient safety

Frequently perceived as *the* regulatory burden for Healthcare Delivery Organizations (HDOs), device vendors and clinicians, the Health Insurance Portability and Accountability Act

[1] VP of Operations at MedCrypt, vidya@medcrypt.co, 125 South Hwy 101, Suite 101, Solana Beach, CA 92075 (Murthy) and CEO/co-founder of MedCrypt, mike@medcrypt.co, 125 South Hwy 101, Suite 101, Solana Beach, CA 92075 (Kijewski).

(HIPAA) has had an indelible impact on our healthcare system. An average of 35 HIPAA violation complaints (HHS Office of the Secretary, Office for Civil Rights. (2019, May 16) are made on a daily basis with estimates that 59% of the U.S. population has had its health records breached/exposed (HIPAA Journal, n.d.). Since the mandated compliance date of April 2003, the challenge of complying with HIPAA rules has created various cybersecurity programs to control the flow of personal health information.

The introduction of connected medical devices not only expands the scope of HIPAA management, but also introduces patient safety considerations. What if a glucose monitor is manipulated and the attached insulin pump provides an injection that a patient doesn't need? What if a critical calculation in radiation therapy is manipulated? (Chen, Xiao, and Li, 2014). Although Homeland showed a pacemaker vulnerability exploited in an assassination, this is not a common scenario that HDOs and patients face (Homeland, 2018).

A possible attack may include a hacker gaining control of an HDO via a medical device that is compromised. For example, a hacker may access an HDO's network, and inhibit its ability to update electronic health records and use devices that rely on connectivity for delivering care (such as devices used in radiation oncology and sophisticated surgical robots).

While a possible solution may be to revert to pencil and paper during a ransomware attack and rescheduling any elective procedures, delayed operational capabilities can also result in a re-routing of patients who have emergent needs. Extant research documents a 13.3% higher mortality rate for patients experiencing a cardiac arrest who received a delay in care of four minutes (Jena, Mann, Wedlund, and Olenski, 2017). When applying this finding to a delay in care due to a network takeover by hackers, one can imagine an increase in mortality rates far greater than 13.3%.

Regulatory requirements - today and looking forward

Issuing their first guidance document in January 2005, the Food and Drug Administration (FDA) has actively worked to build a collaborative cybersecurity community including clinicians, hackers, device manufactures and HDOs. Most recently the PreMarket and PostMarket Management of Cybersecurity in Medical Device documents have created a clear roadmap and goals for the industry to work towards.

PreMarket Guidance (Food and Drug Administration, 2018) -

While this guidance remains in draft form after its initial released in October 2018, there are a few areas of focus that it will endorse once finalized (expected sometime in 2020):

- Devices should make extensive use of encryption to keep data private.
- Digital signatures should be used to verify authenticity of devices, data and instructions.
- Devices should be designed in a way that anticipates regular, routine cybersecurity patches.
- User authentication needs to be secure and robust.
- Devices should be able to alert users when a cybersecurity breach occurs.

PostMarket Guidance Food and Drug Administration, 2016) -
Released in 2016, this guidance includes a combination of process and procedural requirements for both medical device manufacturers (MDMs) and HDOs. These requirements include:

- Understanding, assessing and monitoring vulnerabilities and risks.
- Implementing robust software lifecycle processes that including having a process for ongoing updates and patches.
- Threat modeling cybersecurity risks around a medical device.
- Participating in a coordinated vulnerability disclosure policy.

The FDA has made it clear that MDMs and HDOs must collaborate to successfully build a robust security program.

Threat sharing as a view to cybersecurity trends

One of the recommendations in the post-market guidance is for device vendors to participate in "threat sharing," in which information about security vulnerabilities is shared with the medical device community via Information Sharing Analysis Organizations (ISAO).

Two of the presumed benefits of threat sharing are that 1) industry stakeholders have the information necessary to minimize their cybersecurity risk and 2) other medical device vendors can use this information to prevent their products from having the same or similar vulnerabilities.

The ICS-CERT Advisory Database plays a critical role in bringing visibility to emerging threats by building a repository for medical device vendors to communicate with each other and customers. Assessing these advisories offers insight into cybersecurity practices in place at various medical device manufacturers. In total, 61 medical device advisories were released between 2013 and February 28, 2019, consisting of a total of 144 cybersecurity vulnerabilities.[2]

Frequency is Increasing

Prior to the Postmarket Guidance (December 2016), advisories were issued at a rate of 0.95 vulnerabilities / month, but subsequent to the guidance release it increased 432% to a rate of 4.11 vulnerabilities / month. A hypothesis presents itself here - has there been an increase in the number of vulnerabilities in devices, or has the FDA guidance which encourages "threat sharing" helped the industry move up the cybersecurity maturity curve?

It is possible that medical device vendors face a perceived stigma when issuing information about security vulnerabilities, and this inhibits participation in this process. Media has certainly picked up advisories and cherry picked attributes from disclosures to highlight security shortcomings. In reality**, disclosing security vulnerabilities indicates a strong and operational security program.** Security is constantly and rapidly evolving. It is not a 'one and done' activity, but instead must be doggedly managed, which means ongoing vulnerability identification, disclosure and remediation. As other device vendors mature their programs, another 4x increase in the rate of disclosure can be anticipated.

[2] Raw data available at https://docs.google.com/spreadsheets/d/1GDIN_BAdHndK3TvzbWZUCnC09xqJrqe-uxEoCxBVc5U/edit?usp=sharing.

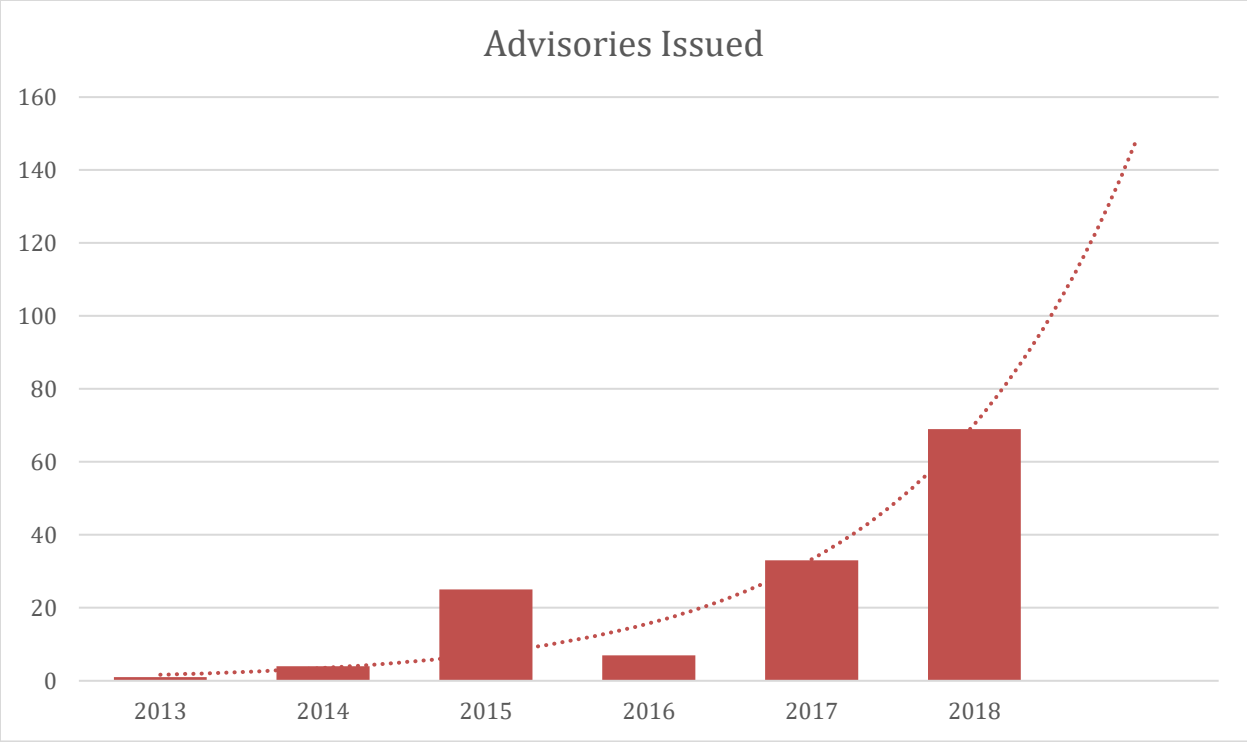


Figure 1

Some Companies Have Yet to Issue an Advisory

A comparison of the list of companies who have made disclosures, against a list of connected-device vendors ranked by market cap, shows that only ten (10) of the top twenty nine (29) medical device vendors have ever made a vulnerability disclosure through ICS-CERT. That leaves 19 top medical technology vendors that have never made a disclosure. It is highly unlikely that there are no security vulnerabilities in any of the devices they currently sell.

There are two valid reasons a medical device vendor would never have made a disclosure.

1) Their devices have no vulnerabilities.
2) They have never been made aware of or discovered a vulnerability.

Vendors who have not issued an advisory should continue to ensure their product development lifecycle aligns with the requirements outlined in the FDA pre- and post- market guidance. These vendors should also consider partnering with the security community, perhaps in the form of a bug bounty program, to ensure rigorous security practices (Bugcrowd, 2019).

Noting that 36.84% of all advisories were disclosed by two companies (Phillips and Becton, Dickinson), there is perhaps a hypothesis here between size or organization and frequency of disclosure. The FDA draft pre-market guidance (October 2018) proposes a tiered structure to align security requirements with impact on patient safety, but does not change requirements based on the size of company.

Certain Classes of Devices are Under-represented

There are certain classes of medical devices that are absent from ICS-CERT advisories. One expects a uniform cross section of the networked medical device market, yet the advisories

tend to focus on specific device classes, like pacemakers, insulin and infusion pumps, and imaging systems.

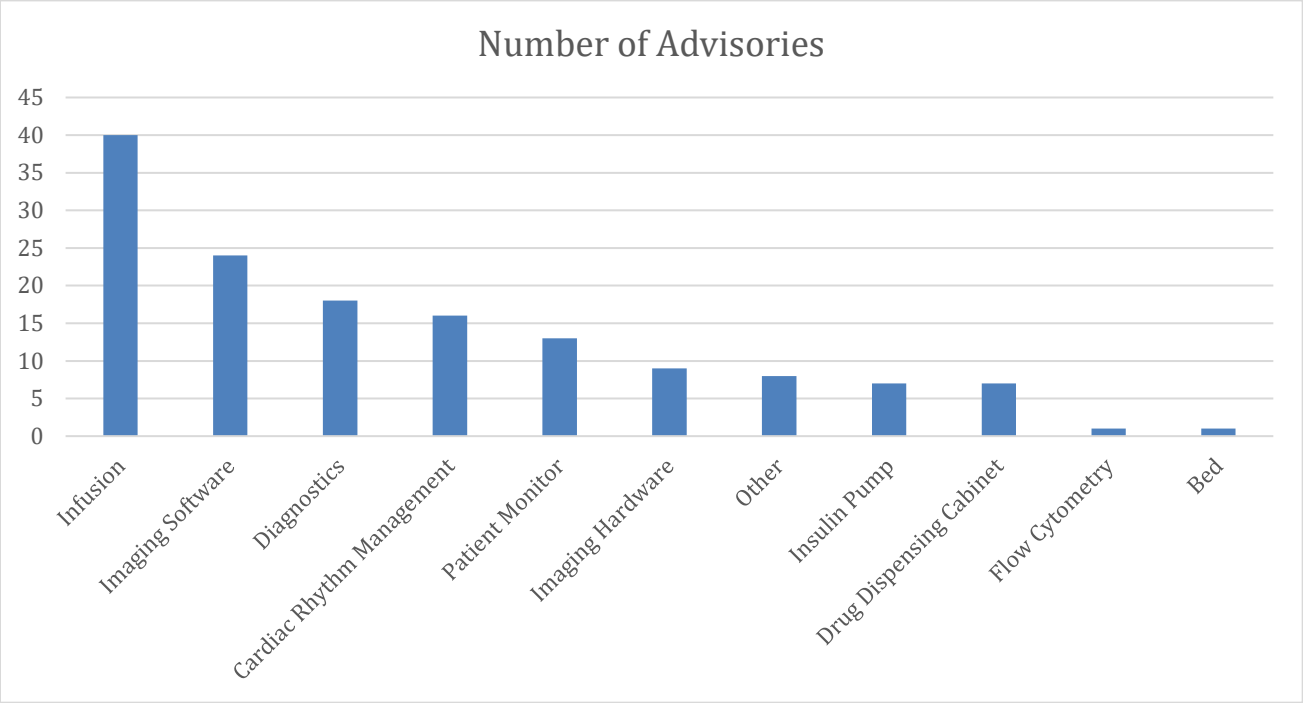


Figure 2

It seems unlikely that a certain class of device is any more or less vulnerable than another class of device. Cybersecurity researchers are directly cited in 43% of all vulnerabilities to date – and noticeably absent from any of the imaging software advisories. Could it be the device classes with advisories are attributed to these devices being more accessible to security researchers?

Issues with User Authentication is a Common Problem

Vulnerabilities attributed to user authentication and code defects covered 66% of all vulnerabilities. Is it possible that user authentication is the most commonly reported on because it is the first thing a penetration tester would interact with? If that is true, future advisories are likely to focus on deeper "layers" of the technology stack as medical device cybersecurity matures. In comparison, advisories from the more cyber-mature industrial control systems (ICS) industry demonstrate a variety of custom developed attacks and multi-pronged strategies that have to work together to successfully a vulnerability.

Patient Impact

A common rebuttal targeting the efficacy of cybersecurity efforts in medical devices is the absence of a death attributed to a cybersecurity event. Perhaps the question to be asked is why is it so difficult to track this statistic. Attributing a medical device cybersecurity incident to the loss of a life is incredibly difficult due to the limited logging capability of devices, missing attribution data and a lack of historical regulatory requirement.

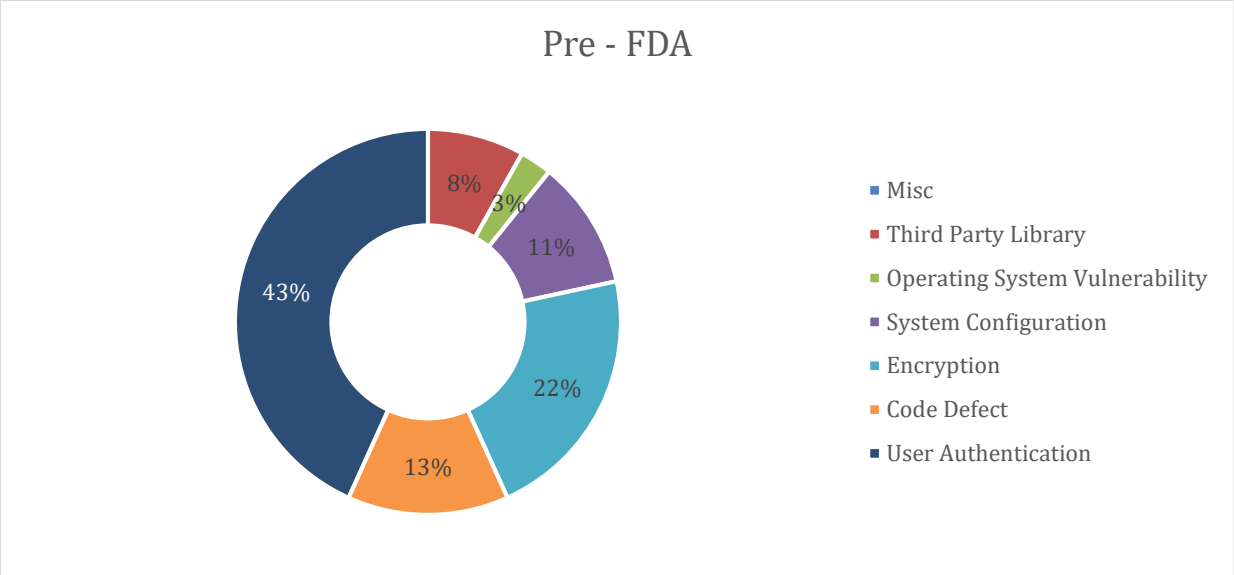


Figure 3

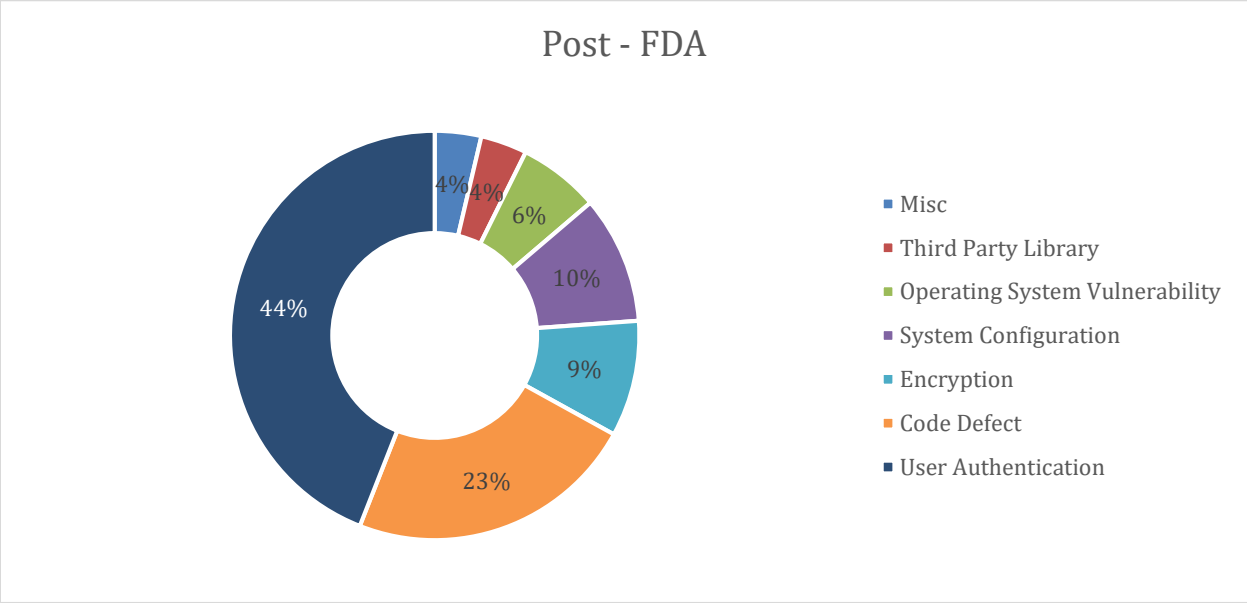


Figure 4

In 2016 when the FDA released their post-market cybersecurity guidance, it mandated device log management and analysis. This indicates that at a future date, we should have technical insight to assess the impact of device information integrity on clinical outcomes. It also indicates that at this time, many 'live' devices were never designed to capture log data.

Attempting to capture data that is currently available, the Safe Medical Devices Act of 1990 created the Manufacturer and User Facility Device Experience (MAUDE) database to capture device-related fatalities and adverse events for both device manufacturers and the FDA. Manufacturers are mandated to report any adverse event communicated to them.

The table below captures the problem types determined to possibly originate from a cybersecurity problem, with the related number of reports.[3]

Problem Type	**Number of Reports**
Application Program Version or Upgrade Problem	95
Application Security Problem	1
Computer System Security Problem	13
Patient Data Problem	788
Problem with Software Installation	259
Unauthorized Access to computer system	37

Table 1

In total, 1,193 unique MAUDE entries from January 2010 - February 28, 2019 were found for the selected problem types.

An additional search for 'cybersecurity' in the "advanced search" interface identified 244 reports. However, this was across only three companies: Roche, Siemens and St. Jude. With 229 of the MAUDE entries coming from St. Jude, the absence of diversity in vendors makes it difficult to conclude about trends in reporting, but does validate the challenge in obtaining data from events that result in physical harm (or even death) due to cybersecurity vulnerabilities.

In reviewing these MAUDE entries, there is an absence of technical data, making it difficult to assess incidents from a technical perspective and determine how a cyber threat resulted in a problem that caused a loss of life.

Looking Ahead

The lack of details that are captured when issues arise is the result of log retrieval not being architected into a device. The lack of this fundamental security feature could be the result of several factors, including:

- The high volume and variety of devices deployed means the type of information retrieved can vary significantly in utility for forensic review.
- Since devices operate in a variety of settings, such as hospital networks or with limited wireless connectivity, accessibility to retrieve history can be unpredictable.
- Depending on the memory available on a medical device, there may be a limit on the history it retains.

Complicated hospital IT infrastructures can cause the device's interactive interface to only provide limited information to be available for review.

We think medical device vendors have been making lots of progress over the last few years and we have yet to see a case where the cybersecurity of a device outweighs its clinical benefit. With the FDA's encouragement the market is starting to understand that vulnerability disclosures are indicative of a working security program. We predict that with the perceived stigma associated with disclosures waning, additional device classes & companies to will start disclosing

[3] Raw data available at (requires a request for access):
https://drive.google.com/open?id=1fuxAhUStUeAv68JKH8SgnV9OfChBYMkdYl4wn4KmB9I

vulnerabilities. Further, we predict that the complexity of vulnerabilities disclosed will also increase. The 400% increase in disclosure frequency to date indicates more device vendors are prioritizing cybersecurity and have functioning security processes.

The FDA premarket guidance goes a long way to outline the roles that different community members will have to play to enhance the collective cybersecurity posture faced by healthcare . With a shared burden it is expected that HDOs will build a more robust practice that considers cybersecurity risk in device design and implementation, and medical device manufacturers will increasingly harden the security of the devices they provide in order to obtain their 510(k).

References

Anupam B. Jena, M.D., Ph.D., N. Clay Mann, Ph.D., Leia N. Wedlund, and Andrew Olenski, B.S (2017). "Delays in Emergency Care and Mortality during Major U.S. Marathons | NEJM." *New England Journal of Medicine* 376, 1441-1450.

"Broken Hearts (Homeland)." *Wikipedia*, Wikimedia Foundation, 9 Sept. 2018, en.wikipedia.org/wiki/Broken_Hearts_(Homeland).

"Bug Bounty List." *Bugcrowd*, www.bugcrowd.com/bug-bounty-list/.

Chen, W., Y. Xiao, and J. Li, 2014. Impact of dose calculation algorithm on radiation therapy, *World Journal of Radiology* 6, 874-880.

Food and Drug Administration. *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff*. Available at: www.fda.gov/media/119933/download. Accessed June 13, 2019.

Food and Drug Administration. *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. Available at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices. Accessed June 13, 2019.

Healthcare Data Breach Statistics. (n.d.). Retrieved from https://www.hipaajournal.com/healthcare-data-breach-statistics/

HHS Office of the Secretary, Office for Civil Rights. (2019, May 16). Enforcement Highlights - Current. Retrieved from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html