COUNTERTERRORISM FUTURES

A WHOLE-OF-SOCIETY APPROACH

17 OCTOBER 2019

2019
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

TEAM MEMBERS

Team Champions: Abigail Kohn, Office of the Director of National Intelligence
Lora Loethen, Joint Counterterrorism Assessment Team

Johnna Bardell, National Cyber-Forensics and Training Alliance
Shaheen Ghori, United States Government
Mary Hackman, Visa Inc.
Barry Koch, Benjamin N. Cardozo School of Law
Kaivan Rahbari, FIS
Audra Richards, The Boeing Company
Samson Sampson, NC4
Joseph White, Defense Intelligence Agency, Defense Combating Terrorism Center
Kendyl Work, National Counterterrorism Center

Disclaimer Statement: This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Public-Private Analytic Exchange Program participants and may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and are the product of joint public and private sector efforts.

ACKNOWLEDGEMENTS

We would like to express our gratitude to the Office of the Director of National Intelligence (ODNI), the Department of Homeland Security (DHS), and our Team Champions, Abby and Lori, for their support and guidance throughout the duration of the 2019 Public-Private Analytic Exchange Program. Abby and Lori helped turn our ideas into an actionable product.

We would also like to express our sincere appreciation to the following law enforcement and industry organizations who contributed their time, expertise, and valuable insights on the future of counterterrorism, terrorism financing, and the need for better collaboration between public-private partnerships: Aite Group, Barclaycard U.S., Capital One, Citibank, Ephraim McDowell Health, Federal Bureau of Investigation (FBI) Headquarters and New York, Joint Terrorism Task Force (JTTF) New York, The McChrystal Group, National Cyber-Forensics and Training Alliance (NCFTA), National Counterterrorism Center (NCTC), New York City Police Department (NYPD) Counterterrorism Bureau, Office of the Director of National Intelligence (ODNI), PNC Bank, Standard Chartered Bank, Synchrony, and Turnkey Risk Solutions.

Each team member devoted many hours to organizing, researching, and writing this deliverable – as well as dedicating time for weekly team calls, a research trip to New York City, and several in-person team collaboration meetings in the Washington, DC, area. The team formulated its recommendations through extensive qualitative and quantitative research. We take responsibility for our conclusions and note that they are ours alone and not necessarily those of the U.S. government or the private sector.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The weakening of the Islamic State's caliphate in Iraq and Syria (hereinafter referred to as ISIS), coupled with a decline in the frequency and lethality of attacks in recent years, has contributed to a perception that the threat of Islamic terrorism is easing. Indeed, there are observable signs that conventional terrorism is receiving lower priority, including within the United States Government (USG). Resources for counterterrorism (CT)-related programs are being curtailed and, for the first time in several years, terrorism has been supplanted from atop the Department of Defense's (DoD) National Defense Strategy. Yet, while so-called "interstate strategic competition" with Russia and China should certainly be a component of the country's national security strategy, the terrorist threat landscape remains dynamic and ever-changing. Thus, it is the contention of the Public-Private Analytic Exchange Program (AEP) team examining "Counterterrorism Futures" that proliferation and advancements in technology, as well as enduring jihadist and other violent ideologies, all but ensure that the threat of terrorism will persist for the foreseeable future.

This report seeks to identify potential terrorist threats facing the U.S. amid rising political and societal polarization that threatens to ignite greater levels of civil unrest and contribute to extremism. In particular, this paper focuses on terrorists' exploitation of non-traditional mechanisms, technologies, and targets as a means of funding their operations. Through extensive research and a series of in-person meetings with government agencies and industry experts on the frontlines, our team has assessed that synthetic identity fraud, human trafficking, and cyber threats against the healthcare industry could increasingly become sources of financing or attack vectors for terrorists in the next five years. This article presents three case studies using near-term trends to identify potential vulnerabilities in this regard and provide an overview of how the public and private sectors are currently positioned to mitigate these threats. Our team also proposes several potential solutions that the USG and private sector partners should consider to better address these vulnerabilities.

Finally, because increased awareness and active collaboration are integral to any effective CT strategy, this document discusses several public-private partnerships that are already undertaking joint activities in the above topic areas. This includes identifying challenges presently facing these initiatives as well as successful models that could be replicated across all homeland security mission areas. One such entity that was consistently referred to and complimented over the course of our research was the National Cyber-Forensics & Training Alliance (NCFTA). This non-profit organization is focused on neutralizing cyber-crime via collaboration between subject matter experts (SMEs) from the public, private, and academic sectors, and illustrates how robust information-sharing among various stakeholders can produce tangible results. Citing the NCFTA and similar fusion center-style entities with broader information-sharing parameters, our team presents opportunities to facilitate more collaborative partnerships between members of the public and private sectors. It is only through active participation in information-sharing and other collaborative efforts that the country will be able to sustain future CT initiatives, especially in an environment of declining public resources. A primary objective of this paper is to stress the importance of this to policy- and decision-makers and provide some strategies and incentives to promote successful, long-lasting engagement between the government and the private sector.

SCOPE

This paper reflects the results of the Counterterrorism Futures team of the DHS-sponsored Analytic Exchange Program, which conducted a wide-ranging, six-month study of emerging terrorism risks projected through the next five years. Information from the study was derived from a variety of sources, including interviews with private and public sector subject matter experts, various open-source articles, and field research conducted in New York City. The team met with representatives of Citibank, the Federal Bureau of Investigation NY, the Joint Terrorism Task Force-NY, The McChrystal Group, the National Cyber-Forensic Training Alliance, the New York City Police Department, and Standard Chartered Bank to obtain firsthand knowledge and insight from their respective industries. We are grateful for the unique and diverse perspectives that they shared with us on our study topic.

Our team decided to focus on non-state Sunni terrorist groups, such as ISIS and al-Qa'ida, and their sympathizers, for this paper, and chose to exclude domestic or state-sponsored groups. Based on our research and meetings, we also decided to narrow the scope of future threats discussed to three specific types that will likely shape the threat landscape: Synthetic Identity Fraud, Human Trafficking, and Cyber Threats Against the Healthcare Industry. These three topics were selected as areas of increasing concern because we perceived a need for increased awareness and research on these methods contributing to terrorism. Further, while synthetic identity fraud and human trafficking are methods currently used by terrorists, we have not observed terrorists conducting cyber-attacks against the healthcare industry, and we believe for reasons stated herein that this is potentially a significant vulnerability.

This paper assumes, given its forward-looking focus, that government resources toward counterterrorism will continue to decline in the next five years in deference to shifting priorities, putting pressure on public and private sector cooperation to maintain counterterrorism efforts. We begin the paper by highlighting our assumptions surrounding this future landscape, many of which were derived from a "red teaming" exercise we conducted in New York City facilitated by The McChrystal Group and attended by private sector representatives, in addition to our team. The final section – recommendations to enhance future public-private partnerships to more effectively mitigate terror threats – was also in part derived from this exercise (along with our meetings and research).

FUTURE LANDSCAPES: STATE OF THE WORLD

SOCIETAL TRENDS

In the next five years, increasing political and societal polarization will likely shape the domestic landscape, creating heightened levels of civil unrest, more pervasive extremist organizations, and new challenges for public and private sector partnerships working to counter terrorism.[1] Polarization – which experts believe has steadily risen in the U.S. since the 1970s – may dampen public-private collaboration due to partisanship, or have the effect of energizing younger workforce leaders toward aims that reverse the trend.[2] Climate change is also likely to impact the future landscape, as resource scarcity becomes an intensifying global issue that leads to significant food and water shortages, severe weather events, major migrations of people, and political and social destabilization that may drive conflict, and subsequently, provide a fertile recruiting ground for terrorist organizations.[3]

Further, privacy regulations and how they are implemented between technology companies and the USG are likely to continue to cause challenges to information-sharing.[4] In the private sector, technological advances and their rapid pace may also make it increasingly difficult for the government to adjust.[5] For example, increasing anonymity of certain applications will likely make it harder for U.S. government agencies to conduct investigations.[6]

THREAT ACTORS

Social and political factors are also likely to have an effect on the terror actor landscape. We expect that the terrorists of the future will be younger, reliant on technology and social media, and subject to the same societal challenges faced by many of their peers. The National Institute of Justice released a report last year that examined potential risk factors and indicators associated with lone actor or small group radicalization to terrorism in the U.S., and they include having a sporadic work history or being unemployed; having trouble in both platonic and romantic relationships; having a lower socioeconomic status; and failing to achieve one's aspirations.[7]

Additionally, future terror actors are more likely to be diverse in ethnic background, gender, and country of origin, including more likely being born in the US.[8] Attacks by so-called "lone-wolves" – or those by small, less centrally directed groups – inspired by ISIS or like-minded jihadist ideology will likely be the most frequent form of terrorism in the United States. The majority of these plots will likely be self-financed and involve the use of rudimentary weapons, such as knives, firearms, vehicles, and fires.[9] Incidents of this sort are designed to be "low-cost, low-tech, and high-impact" in order to inflict casualties and damage without creating hurdles for aspiring attackers devoid of training, resources, and logistical support.[10] Additionally, they dramatically reduce a terrorist's "flash-to-bang" time—the period between radicalization and an attack—making plots much harder to detect and disrupt.

Future actors are also potentially more likely to have "blended" identities – meaning they could identify with transnational terror ideology as well as right-wing, racially motivated extremism.[11] They also have increasingly taken on the role of both criminal and/or terrorist actors intermittently, combining criminal skills and connections and terror activity facilitation, depending on the day and need. The proliferation of illegal activity on the darknet – which renders it anonymous – today has made the challenge of tracing criminal activity that could be funding terrorism or directly used in planning attacks even harder.[12] It also means criminal actors may be facilitating terror actors unwittingly.

TERROR FUNDING SOURCES

Illicit trafficking, fraud-based schemes, electronic currency exploitation, criminal services, and traditional hawala systems will likely continue to be sources of income for terror actors in the next five years. Physical and digital markets for illicit activities will likely continue to thrive and be facilitated by encrypted messaging platforms such as Telegram. We could also see certain criminal methods of raising funds – such as through ransomware – be taken on by terror actors as a method for fund-generation.

The trends and trajectory of these types of funding sources – with limited-to-no paper trails and covering small enough transactions so as not to raise red flags with financial institutions – will continue to represent significant challenges to institutions and authorities trying to counter them over the next five years.

FUTURE VULNERABILITIES

We have discussed future terror actors increasingly using low-sophistication methods to conduct physical attacks. In the future, we also assess there to be a likelihood of increasing cyber capabilities for attacks and disruption. Due to increasing usability and accessibility of hacking tools, terror actors with relatively low-level cyber capability (to date this has manifested primarily in defacing websites with poor security and publishing lists of personally identifiable information compiled through open source research) terror actors will be able to increase their sophistication.[13]

Today, pre-packaged hacking kits, such as Kali Linux and Metasploit, are among the most popular, as they have a multitude of built-in features and are free to download. Custom hacking tools for more specific applications are also available through websites such as GitHub, allowing access to more streamlined and user-friendly tools that can be used for nefarious purposes.

Thus, as individual or small-group actors of the future are likely to be self-radicalized, with relatively low levels of sophistication, these types of readily-available criminal tools for financing and conducting operations will likely be increasingly attractive. The tools' relative anonymity, as well as their anticipated low-level nature, means that the terrorists' activities may be harder to detect and counter.

FUTURE THREATS: CASE STUDIES

To illustrate how these future threats may play out, and the challenges faced by the USG and private sector in countering them, we have chosen three case studies. The first discusses the threat of synthetic identify fraud, showcases how the threat manifests, describes public-private partnerships currently in place to share information, and offers recommendations to address the threat. The second case study identifies a gap in the current understanding of the threat of human trafficking: namely that it is being approached primarily as a criminal issue and not also as one used to fund terror activities. We present opportunities to break down silos in how the threat is addressed and how law enforcement and the private sector can reduce the risk that it will continue to be exploited by terror groups. We then offer recommendations for expanded partnerships to combat the threat. Our third case study takes a relatively unstudied threat – terror exploitation of our current healthcare system – and identifies associated vulnerabilities that public-private partnerships could position themselves now to better mitigate. The recommendations we selected for all three cases are then used as a foundation for our final section, which delves more broadly into current gaps – and opportunities – in public-private partnerships related to counterterrorism, and how these could be enhanced in the future.

CASE STUDY 1: SYNTHETIC IDENTITY FRAUD AND TERROR FINANCING

Cybercrime continues to be a large threat across the globe, and is expected to have a $6 trillion impact by 2021.[14] Crimes involving ransomware and data breaches almost always gain more public attention, but financial crimes, such as identity theft, have become a large problem in the United States, with more than 14.4 million victims in 2018.[15] A lesser known cyber-enabled financial crime that can be equally as damaging as identity theft is synthetic identity fraud. Synthetic identity fraud is a crime in which perpetrators combine real and fictitious information, or entirely fictitious information, to create new identities with which they defraud financial institutions, lenders, government agencies, and individuals.[16]

For example, criminals may create synthetic identities using fictitious names, dates of birth, and stolen social security numbers in order to open fraudulent bank, auto loan, and mortgage loan accounts. In such cases, the stolen social security numbers often belong to children, the elderly, or the homeless, and cases involving children can go undetected for many years. Conversely, in cases where criminals create synthetic identities using entirely fictitious information, the lenders and financial institutions themselves are considered the victims. While synthetic identity fraud emerged years ago, activity continues to increase throughout the United States, with detection difficult because individual victims are almost always non-existent and therefore there is no one to notify financial institutions of fraudulent activity.

Terror organizations, like large criminal networks, often exploit the use of synthetic identities through various fraud schemes because they not only provide an avenue to launder money, but also to obtain and produce valuable goods and services, such as cell phones, airline tickets, and false identification documents needed to acquire passports. A panel of experts interviewed by the Government Accountability Office in 2017 expressed concern with national security programs that rely on verifying a purported identity against a list of suspected bad actors or terrorists.[17] They noted that terrorists, and any other type of criminal, can turn to synthetic identities to enter or move around the United States undetected.[18]

For example, according to a white paper written by ID Analytics, in May 2014, CBC News in Canada reported that Canadian officials discovered that terrorists on the No Fly List used synthetic identities to purchase airline tickets between New York, Toronto, and Pakistan.[19] The scheme included the use of fake names to obtain passports for a notorious murder suspect and major drug trafficking groups.[20] In the same CBC News article, Dr. Kalyani Munshani, a New York attorney and financial crime expert, said that "using synthetic identities, safe houses can be established, cars can be rented, heavy vehicles can be bought, international travel can be facilitated, restricted goods can be bought without any flags being raised. This is not a conventional crime. This is more towards terrorism, I believe, not just merely revenue generation."[21] She stressed that synthetic identity fraud, as a means to fund terrorism, is a "game-changer" that "requires immediate attention" and "is extremely serious, and it's been ignored for way too long."[22]

Toronto Police Detective Constable, Mike Kelly, stated, "Think of the potential of having an apartment and a vehicle and a phone, all registered in different names. That you can come and go as you please. You have the ability to open businesses and transport large volumes of materials in trucks with appropriate permits and license designations."[23] He further stated, "There's literally no limit to the types of things, the amounts of things, the amount of damage that can be caused to each sector that you can possibly think of — banks, government bureaucracies, police agencies, insurance, car lenders. Everybody."[24]

Fictional Case Study: Synthetic ID Fraud in Action

Consider the following scenario, some of which is based on actual cases.

A foreign national was living in the New York City area with his spouse and two children from 2009 to 2014 before he was deported from the United States after falsifying information on his immigration documents. His (now) ex-spouse is also a foreign national, but his children, ages seven and nine, obtained birthright citizenship. His ex-spouse and children still live in the United States. They also have family members who live in New York as well as other parts of the country.

The individual began applying for credit, while in the United States, in 2010 using credit privacy numbers (CPNs) in place of social security numbers because he was not a US citizen.[i] When initially applying for credit, he used his real name, date of birth, and apartment address with a random nine-digit CPN. Although he was initially declined due to lack of credit, a credit profile was created with the credit

[i] Credit privacy numbers (CPNs) are nine-digit non-government issued identification numbers that can allegedly be used to open lines of credit in place of using social security numbers. According to ID Analytics, CPNs are marketed by credit repair agencies as a way for consumers to "refresh" their credit history. However, the Federal Trade Commission warns that these numbers do not truly exist, and the Social Security Administration warns that the use of CPNs is illegal.

reporting agencies (or credit bureaus). He reapplied 30 days later and was immediately approved for low-dollar limits by three financial institutions. Once he received his credit cards, he "seasoned" the accounts over several years by creating a normal pattern of usage and repayment, thus, increasing his credit limit and adding tradelines – this type of scheme is often observed in cases associated with bust-out fraud.[ii]

Over time, he began creating synthetic identities in various ways: he used spelling variations of family member names and paired them with different dates of birth, CPNs, his children's SSNs, and even J-1 visa holder information.[iii] The initial synthetic identities he created were used to apply for credit accounts and auto loans. After these identities obtained well-established lines of credit, he started adding authorized users, which were also synthetic identities, to the accounts so that they could automatically inherit the primary cardholders' "good" credit after about three months. Adding numerous authorized users to a primary cardholder account (also called a pollinator account) is referred as "pollination" or "credit piggybacking."[iv] Once the synthetic authorized users established credit from the synthetic primary accounts, he removed them and then added new synthetic authorized users to the same primary accounts. The authorized users with newly established credit were then able to apply for their "own" lines of credit and add new synthetic authorized to their accounts – a truly viscious cycle. Most of the addresses associated with the synthetic identities were mail drop locations.

In addition to applying for credit cards and auto loans, the synthetic identities were also used to create shell merchants – jewelry stores, in particular – and produce false documents such as social security cards, drivers' licenses, pay stubs, and tax returns. The shell merchants were used to process fraudulent terminal transactions and move money between different accounts via Automated Clearinghouse (ACH), wires, and electronic checks. The relatively low-dollar transactions, all under $2,000, flew under the radar at many of the financial institutions because it was below their fraud threshold.

The individual also used the synthetic accounts to purchase airline tickets for himself and family members who were in the United States and overseas, one of whom was on the No Fly List, but because the tickets had been purchased using a synthetic identity (and she produced additional synthetic documentation), the family member was able to fly in and out of the United States without detection.

In addition to purchasing airline tickets and other miscellaneous items, he also used the synthetic accounts to purchase hundreds of thousands of dollars in high-end electronics, such as laptops, iPads, and iPhones. He would then ship the products overseas to be sold on the black market.

The individual continued to create synthetic identities after he was deported from the United States in 2014. He used variations of the same synthetic names and the same drop addresses, but the IP addresses associated with new credit applications and account activity resolved to a foreign country. Once these

[ii] Tradelines are the credit industry's term for the accounts listed on your credit report.; Bust-out fraud is a form of first-party credit card fraud in which a criminal applies for credit and "seasons" the account with normal pattern usage and repayment in order to build their line of credit. Once the desired line of credit is built, the criminal uses all available credit, with no intent to repay, and then disappears.

[iii] According to the U.S. Citizenship and Immigration Services, a J-1 visa is a nonimmigrant visa issued by the Department of State to exchange visitors "who intend to participate in an approved program for the purpose of teaching, instructing or lecturing, studying, observing, conducting research, consulting, demonstrating special skills, receiving training, or to receive graduate medical education or training." Terrorism financing organizations can bring people to the United States under the guise of employment, willingly or for payment, to one of their shell companies. J-1 tax IDs are an endless supply of SSA-issued visas for people seeking temporary work or education in the U.S. Financial institutions have no way of knowing if people using J-1s are still in the country without the assistance of law enforcement.

[iv] A pollinator is a primary cardholder who continually adds authorized users that are associated with fraudulent activity to their account. The authorized users are often synthetic identities.; Credit piggybacking occurs when an authorized user is added to a primary cardholder account in order to inherit the cardholder's (presumably good) credit history. The primary cardholder's entire credit history (on that card) appears on the authorized user's credit report and is included in their credit score. Credit piggybacking enables authorized users, real or synthetic, to be approved for accounts and loans they would not have been approved for, otherwise.

identities were approved for credit, the cards were sent to the drop locations (the addresses he had on the credit applications), where another individual – usually a family member – would ship them to him overseas. The credit cards were tied to suspicious transactions and patterns of activity conducted overseas.

A financial institution began noticing the suspicious IP/account activity and initiated an investigation. Their analysis revealed that he had created nearly 600 synthetic identities that were linked to roughly $2.5 million in bust-out fraud that had been written off as credit loss. The bank investigator alerted an intelligence analyst at a partner organization, where the analyst sent the suspect's information, and his shell businesses, to a Financial Fraud Working Group, which consisted of members from law enforcement and industry organizations. Within two days, six other financial institutions reported similar activity and losses totaling $8 million – all of which was laundered overseas and suspected to have funded other illicit activity, including terrorism. The intelligence was collected, analyzed, and created into a targeting package for a law enforcement case initiation.

One such case with several of the above attributes, prosecuted by federal authorities in New Jersey, involved the use of 7,000 fake identities, 1,800 phony mailing addresses, 25,000 fraudulent credit cards, and over $200 million in losses. Some of the stolen funds were allegedly used to fund trips to Yemen and attend paramilitary training camps.[25]

Challenges and Recommendations

Synthetic identity fraud is the fastest growing financial fraud and presents many challenges for both law enforcement and the financial services industry, primarily due to the inability of financial institutions to verify with certainty that an SSN or Taxpayer Identification Number was validly issued to a specific individual. This said, efforts at raising awareness through training and collaboration between the public and private sectors to identify and combat synthetic identity fraud have made significant progress over the past few years. In addition to current collaboration efforts, additional enhancements could include:

(i) Expanding law enforcement and industry training on synthetic identity fraud as a typology for money laundering and terror financing.

(ii) Creating a universal "synthetic identity" definition for law enforcement, industry and prosecutors.

(iii) Increasing collaboration and information-sharing among the financial institutions, lenders, and law enforcement, particularly with sharing strategically relevant personally identifiable information (consistent with privacy laws), thereby aiding more effective identity verification at the account opening stage.

(iv) Sharing detection and mitigation strategies among the financial industry.

(v) Enacting legislation that would direct the Social Security Administration to develop a database or other automated mechanism to facilitate the verification of consumer information upon request by a certified financial institution.

CASE STUDY 2: HUMAN TRAFFICKING AND TERROR FINANCING

Human trafficking for forced labor and sexual exploitation, one of the fastest growing forms of international crime, is estimated by the International Labor Organization to generate $150.2 billion per year, and includes potential involvement by opportunistic terror organizations.[26] In the U.S. and elsewhere, human trafficking is a predicate offense for the crime of money laundering, and financial institutions are required to report to the government financial transactions that may be designed to disguise or conceal (i.e., to launder) these criminally derived proceeds.

Despite increasing awareness of the global scope of human trafficking from a law enforcement and anti-money laundering perspective, less attention has been paid to the link between human trafficking and its value as a funding source for terrorist organizations. In fact, there are documented reports that terrorist groups such as ISIS, Boko Haram, and al-Shabaab have used human trafficking as a way to raise funds and provide material support to their organizations and activities.[27] These efforts have included holding "slave auctions" (including via the Internet) of kidnapped women, demanding ransom payments for enslaved women and young girls, and forced begging by children captured in conflict areas.

The United Nations Security Council has issued a compelling publication which explores and describes the nexus between human trafficking, terrorism, and terror financing.[28] According to the report, "[t]errorists' systematic use of acts of violence associated with human trafficking clearly demonstrates that such practices are a highly effective means to achieve strategic objectives. Military setback and loss of control over significant parts of territory have not deterred certain terrorist groups from using abduction, rape, sexual slavery, enslavement and other such acts to subjugate populations and advance their ideologies." [29]

In the case of ISIS in particular, we question whether the reduction of oil revenues following the physical decline of the caliphate, coupled with increased international efforts to crack down on traditional methods of terrorist financing in general, will increasingly lead terrorists to seek alternative tactics in the future, especially in failed or failing states with broken economies.

Anti-Trafficking Efforts

The USG has undertaken a number of anti-trafficking initiatives with both domestic and foreign partners, including the creation of various offices and task forces tasked with advancing the so-called "3Ps" approach: prosecution, protection, and prevention, in furtherance of its treaty obligations under the United Nations Convention Against Transnational Organized Crime (and the Palermo Protocol) and in accordance with the approach articulated in the United States' Trafficking Victims Protection Act (TVPA) of 2000.[30] Yet, many survivors and victims' advocates contend that the government's prioritization of, and response to, human trafficking has been insufficient.

For instance, although it has risen in recent years, the overall number of federal human trafficking prosecutions remains relatively low despite Justice Department data indicating conviction rates of nearly 80 percent under the TVPA.[31] The fact that state prosecutors lag behind their federal counterparts in obtaining convictions of human traffickers is also troubling. Together, these factors suggest that, despite several high-profile cases involving prominent public figures having raised the profile of human trafficking in recent years, the public sector's approach has failed to produce significant strides in addressing the issue.

For its part, considerations of disruptions to supply chains and business operations – in addition to brand reputation and threat of civil and criminal penalties – have prompted many private sector entities to increase their commitment to countering human trafficking. In particular, firms in industries that are at a greater risk of labor and sex trafficking are well-positioned to offer specialized expertise, pioneering tools, and resources potentially able to address the issue. Banks and other regulated financial institutions are required, under certain circumstances, to share customer and transactional information with law enforcement when the institution knows or has reason to believe that financial transactions may be related to, or derive from, the crime of trafficking. Financial institutions invest heavily in automated tools to identify patterns of suspicious financial transactions and those that may be indicative of any number of crimes.

These types of capabilities are also developed at a faster pace in the private sector than the public sector, underscoring the benefits for closer cooperation and increased collaboration. Thus partnership—a fourth "P" in addition to the statutory trio above—between the federal government and the private sector could facilitate a more informed and holistic approach to human trafficking that detects, warns, and mitigates potential threats more efficiently.

Recommendations

The public sector—federal, state and local law enforcement, among others—is best positioned to lead the fight against human trafficking. The federal government should remain committed to combatting human trafficking, and should continue to develop and implement new and innovative approaches to prevent, detect and prosecute these crimes. At the same time, the private sector, especially the financial sector, is an increasingly important and active partner in addressing trafficking.

A sophisticated infrastructure already exists in the U.S., whereby regulated financial institutions share certain transactional information about various crimes with law enforcement authorities. This information-sharing could be enhanced in the following ways:

(i) Providing additional training for law enforcement on terror financing money flows (related to the underlying crime of human trafficking). There are many substantive training partnerships currently in place between the financial sector and law enforcement, which could easily be expanded.

(ii) Providing additional training and shared indicators on identifying potential victims, trafficking trends, and supply chain due diligence, conducted with first responders, public institutions such as hospitals and schools, and financial and other private sector institutions in a position to identify trafficking activity. Social media and public awareness campaigns related to identifying trafficking activity, already underway by numerous organizations, should also be expanded.

(iii) Requiring public sector studies, including national money laundering and terror financing risk assessments and strategies, to examine the link between human trafficking and terror financing, and the subsequent dissemination of the studies' findings.[v]

(iv) Requiring financial institutions to include in their annual money laundering risk assessments an analysis of human trafficking as a potential funding source for terror groups.

[v] According to the FATF Report, "…of the 28 national anti-money laundering/countering the financing of terrorism (AML/CFT) risk assessments considered for th[e] report [including the U.S. report]…none identified human trafficking as a terrorist financing risk." See, Financial Flows from Human Trafficking, ¶ 43. Similarly, neither the United States *National Terrorist Financing Risk Assessment* nor the *National Strategy for Combatting Terrorist Financing and Other Illicit Financing* identifies human trafficking as a funding source for terrorist groups or terrorist activity.

(v) Increasing information-sharing, consistent with privacy laws, by national authorities.

(vi) Improving coordination among law enforcement authorities investigating trafficking cases from the money laundering and terror financing perspectives.

(vii) Identifying new opportunities to provide technical assistance to law enforcement and the financial sector in other jurisdictions.

(viii) Considering appropriate participation from the financial sector in government Money Laundering and Terrorist Financing studies (risk assessments, strategies, etc.). Many financial crimes investigators in the financial sector are former law enforcement personnel, and others have existing security clearances from a variety of agencies, so the occasional constraints involved when dealing with classified information can be managed appropriately.[32]

CASE STUDY 3: CYBER-ATTACKS AGAINST HEALTHCARE

Terror actor use of ransomware, while not observed to date, is a possible future vulnerability, particularly for hospitals and the healthcare sector. To date, one ISIS-linked hacking group has targeted the United Kingdom's National Health Service websites to spread violent images from the war in Syria, but did not access patient data nor affect any records.[33] That said, given terror organizations' goals of widespread media coverage, enhanced funding sources, and mass casualty events, ransomware targeting a hospital that could create a life safety threat while also garnering funds presents an attractive opportunity.

Further, ransomware does not require in-depth hacking knowledge to successfully target already vulnerable systems and populations, and it is a tactic that is already shown to have affected hospitals.[vi] Healthcare was the leading industry for cyber-attacks in 2018, and has reported more data breaches per year than any other industry since 2009, with much of the compromised medical data resulting in medical identity theft or instances of blackmail and reprisal.[34] Almost half of all reported ransomware incidents in 2017 and 2018 involved healthcare institutions, according to industry reporting.[35]

Current Healthcare Cybersecurity Efforts

While cybersecurity awareness has increased over the past several years, the healthcare industry, especially hospitals, is still plagued by limited resources, IT staffing shortages, and legacy software that makes major improvements to its overall cyber posture difficult.[36] Additionally, ransomware is not difficult to obtain, as there are malware samples available on GitHub and malware collection sites, users on popular blog sites willing to share samples, and malicious actors willing to sell the malware for profit.

The importance of protecting the healthcare industry from cyber-attacks is not a new concept, and numerous entities have come together over the years to set up information-sharing arrangements and mitigation strategies. The Health Information Sharing and Analysis Center (H-ISAC) serves as a global member-driven organization focused on coordinating and sharing physical and cyber threat intelligence

[vi] According to a *CBS News* article published on 18 August 2017: "The medical industry is the new number one target for hackers. Almost all U.S. healthcare organizations have reported at least one cyber attack…On average, hackers can sell credit card numbers for 10 to 15 cents each, but a medical record could be worth anywhere between $30 and $500."

and best practices among healthcare stakeholders.[37] The Department of Health and Human Services has led public-private partnerships to enhance the security and resilience of the U.S. healthcare sector through actions such as releasing publications on voluntary cybersecurity practices for a range of healthcare entities.[38]

Despite productive information-sharing initiatives already in place, we assess that the healthcare sector will likely be challenged as hospitals and other stakeholders face a confluence of increasingly sophisticated and unexpected threats, and insufficient security resources. Although regulating agencies issue voluntary guidance for healthcare cyber security, many facilities struggle to align security operations with their business goals.[39] Many clinicians and decision-makers in hospitals are generally unaware of threats or not trained in cybersecurity, leaving them vulnerable to less sophisticated attacks and unable to identify different attack types.[40] Financial constraints and lack of awareness are further compounded when dealing with future threats, such as terrorism, as forward-looking, futurist vulnerabilities can be sidelined for the most pressing current issues.

Recommendations

We offer several recommendations to improve public-private partnerships within the healthcare industry in order to anticipate and preempt challenges moving forward:

(i) Educating medical professionals on healthcare cyber threats, including anticipated threats over the next five years, could likely increase their awareness and engagement, while also helping prevent less sophisticated methods of deploying ransomware. Extending this education to medical or nursing school curricula might help foster a more security-conscious workforce moving forward.

(ii) Enforcing the inclusion of future threat analysis in information-sharing, to include actors who can quickly escalate their capabilities in several years, such as terrorist organizations. Representation from organizations such as the National Counterterrorism Center and think tanks in information-sharing agreements might aid this process.

PUBLIC-PRIVATE PARTNERSHIP MITIGATION AND COLLABORATION

The final section of our paper delves into the most critical piece of mitigating terror threats in the future, and that is strong, inclusive public-private partnerships. During our research trip to New York – which aimed to develop a more comprehensive understanding of certain vulnerabilities – we discovered that more important than the topic of *what* the threats were was the topic of *how* the often widely varied institutions aiming to counter them were working together. In general, we found that mitigation efforts varied from organization to organization – even those looking at the same threats – rather than having a consistent multi-disciplinary approach. Mitigation was also affected by organizational culture, lack of understanding of privacy laws and the regulatory environment surrounding what is possible to be shared, and was often based on personal relationships rather than institutionalized reporting streams.

Using findings from a public-private partnership red teaming exercise we conducted in New York City with Dr. Micah Zenko, an expert in the field, as well as the recommendations we extracted from the scenarios included above, this section: provides an analysis of strong public-private partnerships that could be models for others going forward; discusses gaps in our current models, and certain challenges that exist in these partnerships today (such as privacy regulations); and, offers opportunities/suggestions that could make these partnerships more effective in the future.

Public-Private Partnerships: Current Models of Success

As discussed in our study on synthetic identity fraud, the National Cyber Forensics and Training Alliance (NCFTA) is a useful model to showcase best practices and benefits of robust information-sharing among multiple sectors. NCFTA is “a non-profit partnership between private industry, government and academia for the sole purpose of providing a neutral, trusted environment that enables two-way collaboration and cooperation to identify, mitigate and disrupt cybercrime.”[i] The NCFTA has “enabled its community of trusted partners to prevent [nearly $2 billion] in potential losses while also helping to identify critical threats impacting private industry and supporting global law enforcement by helping to identify current threats most impactful to industry.”[i]

The NCFTA is just one model of a “fusion center” that brings multiple agencies together – with key stakeholders and decision-makers together in the same room – to share information in real time and resolve fraud and other financial crime cases of mutual interest. Other models of this type of sharing include Joint Terrorism Task Forces (including New York’s JTTF, with whom we met), and the National Capital Region Threat Intelligence Consortium (NTIC), which is one of a national network of fusion centers set up by the Department of Homeland Security for the purpose of sharing information across various threat types and critical infrastructure sectors.

Improving information-sharing among relevant stakeholders is critical to supporting an effective counterterrorism strategy, as this promotes a shared understanding of relevant data, trends, roles, and available resources. Public and private sector groups working together also allows for the creation of a common list of behavioral and transactional indicators for threats – be they human trafficking, fraud, or others.[i] Benefits include more positive and effective interactions with law enforcement, presumably leading to more investigations and successful prosecutions.

Fusion center information-sharing models have also set precedents for providing training to those who are most likely to encounter threats. For example, NTIC, a local fusion center, provides “Human Trafficking 101” indicator seminars to critical infrastructure sectors, hotels, school resource officers, and others in order to encourage them to recognize and report suspicious behavior.

Another example is California’s Terrorism Liaison Officer program, in which participants are trained to report suspicious activity that may be encountered during the course of their normal occupation. It links local law enforcement, paramedics, utility workers, railroad workers, and others to State Fusion Centers and the Office of Homeland Security. These fusion centers also promote information-sharing at a federal level between the FBI, DHS, Department of Justice, and State/Local/Tribal/Territorial Partners by managing the flow of information and intelligence across sectors of government – and then analyzing and integrating that information.

Public-Private Partnership Challenges

While there are good examples of groups, both public and private, that exist to share information (e.g., the non-profit DeliverFund that runs a database provided to law enforcement for human trafficking cases, or the FBI’s Domestic Security Alliance Council, which is a public-private information-sharing partnership), not all of these groups represent an equal flow of information from one side to the other. While one group may exist to push out security-related information *to* the private sector, it may not be receiving specific reporting *from* the private sector about actual incidents they face. Similarly, while the private sector may contact government authorities when red flags occur for potential security threats, once a government investigation is opened, the private firm may not hear back due to legal constraints, which can frustrate the reporting organizations looking to expand their security protocols based on these specific incidents.

While our findings led us to the conclusion that fusion center models are a good "jumping-off" point for efforts to enhance the value of public-private partnerships, they also are not without challenges that all information-sharing initiatives face. These include, but are not limited to:

- **Privacy regulations** surrounding the sharing of personally identifiable information (PII), which can hinder detailed collaboration on specific cases as well as lead to potential red flags being missed as multiple organizations may not realize they are all looking at the same threat.

- **Internal and external silos within and among organizations** that hinder information-sharing – whether it is a silo between cyber/fraud/physical security teams within an organization, silos between local, state, and federal agencies, silos between agencies with different mandates (such as anti-crime bodies and counter-terrorism bodies), silos between the public and private sectors that exist due to mistrust over sharing, or silos between the U.S. and other countries' agencies, all of them can degrade a whole-of-society approach to counterterrorism.

- A **wide variety of organizations – to include public and private – in the space with similar missions and no clear leader** for all, leading to confusion over whom to contact to share potential concerns, and a still too-heavy reliance on personal relationships to share the most sensitive information.

We also note that, as described above, terror actors have become less directed by a central core, more self-radicalized, and more likely to have multiple co-existent threats – for example, a lone-wolf terror actor could be experiencing mental health issues, be involved in criminal activities, and also be radicalizing via the Internet or associating with known terror actors simultaneously. With siloed organizations impeded by information-sharing authorities, this may mean that one actor who has been flagged for domestic violence by one agency, credit card fraud for another, and terror activity by another may slip through the cracks because these agencies are unable to share this varied reporting with one another or into a more holistic reporting stream for suspicious activity.

Future Opportunities

While the above point to some of the difficulties currently faced by public-private partnerships, they also open the door to a wide variety of opportunities to improve them in the future and better position counterterrorism mitigation efforts going forward.

The options below were derived from our meetings in New York, the red teaming exercise, research for the case studies, and our team's expertise. They include:

(i) Facilitate NCFTA's efforts with relevant parties to provide ongoing guidance to private industry as to what can be shared, how, and with whom. DHS's Cybersecurity and Infrastructure Security Agency (CISA) offers a useful model to look toward, as it provides compelling permissions to share, including PII that is relevant to an incident or threat.

(ii) Create a “safe harbor” initiative to be implemented in the event of a narrowly defined crisis to enable appropriate stakeholders to share/receive critical information. This is occurring now with CISA when threats warrant, and could be expanded more widely.

(iii) Encourage the use of multi-agency task forces to investigate and prosecute appropriate cases, and to share relevant typology information with the private sector. Here again, the NCFTA is an excellent model to follow.

(iv) Evaluate how best to include additional, relevant entities in JTTFs or other fusion center models that have typically been unrepresented, such as Cyber or Counterintelligence agencies.

(v) Create a central authority to bring public sector analysts (FBI, CIA, NCTC, etc.) together with private sector analysts from all critical infrastructure/key resource and major emerging technology companies to enhance information-sharing for counterterrorism purposes, with as much sharing as possible. Other private sector non-profits, such as DeliverFund, that support law enforcement with data on key threats, would also be valuable partners. This body would best be run on a fusion center model, as described above.

(vi) Barring the above, or potentially in addition to it, create a central authority and/or directory of complementary public and private sector entities that exist to share information, with contact information (generic email groups) and specific roles delineated, to reduce confusion on how and with whom to share information. Preferably, this directory would be maintained, with some small amount of resources dedicated to answering questions of those needing assistance and ensuring inclusion of new entities.

(vii) Continue and expand trainings provided by fusion centers and other entities that reach frontline first responders and potential suspicious activity reporters.

(viii) Continue and expand trainings by fusion centers on what information may and may not be shared. Further information and training in this space could go far toward increasing the scope and value of what is shared. This should occur with new members joining, but also regularly enough so that all members can stay apprised of changing regulations and what this means for them.

(ix) Consider red teaming as an option for relevant organizations with a role to play in counterterrorism mitigation in the future. As a group, we found that the exercise we conducted to red team future vulnerabilities and the public-private response to them was instructive at quickly identifying and prioritizing higher-risk areas. Sharing the results of these red-teaming exercises, and potentially conducting joint exercises within their fusion centers, could be beneficial.

Red Teaming Event Management

One example we heard from our research concerned planning for a major sporting event in a large city. By bringing together – well in advance of the event – city officials, emergency responders, event organizers and sponsors, vendors, law enforcement, utility workers, and others, all were able successfully to play out certain vulnerabilities and discover immediately which entity was best positioned to take action. By doing these types of exercises regularly within organizations, as well as conducting multi-agency exercises – all parties may see threats, connections, and responses in a new light.

CONCLUSION

By prioritizing and taking a more targeted approach (as opposed to trying to consider a larger threat universe), we have been able to highlight certain future vulnerabilities in closer detail, and offer specific recommendations to improve our abilities to counter them collaboratively. We also have been able to extract some critically important lessons from these three studies that are relevant to a wider range of future threats and the public and private entities tasked with fighting them. By recognizing the key challenges that currently exist in our public-private partnership models, offering examples of certain models that are working well today, and providing possible recommendations for enhancing them in the future, we believe that we – the U.S. government and private sector working together – will be better able to overcome the resource, technology, societal, and information-sharing challenges that may await in the near future.

[1] Jilani, Zaid and Smith, Jeremy (04 March 2019). What Is the True Cost of Polarization in America? *Greater Good Magazine*. https://greatergood.berkeley.edu/article/item/what_is_the_true_cost_of_polarization_in_america

[2] Parker, Kristen (01 October 2018). U.S. political division is only going to get worse. *Michigan State University*. https://www.futurity.org/political-parties-division-1878742/; Cilluffo, Anthony and Cohn, D'Vera (11 April 2019). 6 demographic trends shaping the U.S. and the world in 2019. *Pew Research Center*. https://www.pewresearch.org/fact-tank/2019/04/11/6-demographic-trends-shaping-the-u-s-and-the-world-in-2019/

[3] Information retrieved from https://19january2017snapshot.epa.gov/climate-impacts/climate-impacts-society_.html; Morisetti, Neil, Koenders, Bert, and Ruttinger, Lukas (unknown date). Climate change and terrorist groups - explaining the links. *Climate Diplomacy*. https://www.climate-diplomacy.org/videos/climate-change-and-terrorist-groups-explaining-links

[4] Michaels, Jon D (10 August 2018). Tech giants at the crossroads: A modest proposal. *National Security, Technology and Law Working Group, Hoover Institution, Stanford University, Series Paper No. 1809.*

[5] *Ibid*

[6] *Ibid*

[7] Smith, Allison G. (June 2018). Risk factors and indicators associated with radicalization to terrorism in the United States: What research sponsored by the National Institute of Justice tells us. *National Institute of Justice 251789.*; Fitzpatrick, Thomas M. (September 2018). Global radicalization and the San Bernardino attack- Evolving extremist U.S. domestic threat. *International Relations and Diplomacy, 6(9).*; AEP Team Interview with FBI Counterterrorism Division and New York Joint Terrorism Task Force Official, June 19, 2019.

[8] Williams, Heather J., Nathan Chandler, and Eric Robinson (2018). Trends in the Draw of Americans to Foreign Terrorist Organizations from 9/11 to Today. *RAND Corporation*. https://www.rand.org/pubs/research_reports/RR2545.html.

[9] AEP Team Interview with NYPD Counterterrorism Bureau Official, June 19, 2019.

[10] AEP Team Interview with FBI Counterterrorism Division and New York Joint Terrorism Task Force Official, June 19, 2019.

[11] AEP Team Interview with NYPD Counterterrorism Bureau Official, June 19, 2019.

[12] Malik, Nikita (15 January 2019). How the Darknet Can Be Used by Terrorists to Obtain Weapons. *Forbes*. https://www.forbes.com/sites/nikitamalik/2019/01/15/how-the-darknet-can-be-used-by-terrorists-to-obtain-weapons/#6b4a8df662cd

[13] Alexander, Audrey and Clifford, Bennett (April 2019). Doxing and Defacements: Examining the Islamic State's Hacking Capabilities. *Combating Terrorism Center*. https://ctc.usma.edu/doxing-defacements-examining-islamic-states-hacking-capabilities/

[14] Unknown Author (21 March 2019). Cyber Security Statistics for 2019. *Cyber Defense Magazine*. https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/

[15] Cook, Sam (20 June 2019). Identity theft stats & facts: 2018 – 2019. *CompariTech*. https://www.comparitech.com/identity-theft-protection/identity-theft-statistics/

[16] U.S. Government Accountability Office (July 2017). Highlights of a Forum: Combating Synthetic Identity Fraud. *GAO-17-708SP*. www.gao.gov/2Fassets/2F690/2F686134.pdf

[17] *Ibid*. ¶ 14.

[18] *Ibid*. ¶ 14.

[19] Unknown Author (October 2014). The Long Con: An Analysis of Synthetic Identities. *ID Analytics.* http://hub.idanalytics.com/synthetic-identity-white-paper; MacInnes-Rae, Rick (04 March 2014). Suspected terrorist links to synthetic ID fraud are being 'ignored'. *CBC*. https://www.cbc.ca/news/canada/suspected-terrorist-links-to-synthetic-id-fraud-are-being-ignored-1.2557677

[20] Seglins, Dave and Nicol, John (15 May 2014). RCMP bust passport fraud scheme tied to Canada's 'most wanted'. *CBC*. https://www.cbc.ca/news/canada/rcmp-bust-passport-fraud-scheme-tied-to-canada-s-most-wanted-1.2642559

[21] MacInnes-Rae, Rick (04 March 2014). Suspected terrorist links to synthetic ID fraud are being 'ignored'. *CBC*. https://www.cbc.ca/news/canada/suspected-terrorist-links-to-synthetic-id-fraud-are-being-ignored-1.2557677

[22] *Ibid*.

[23] *Ibid*.

[24] MacInnes-Rae, Rick and Gollom, Mark (03 March 2014). How 'synthetic' identity fraud costs Canada $1B a year. *CBC*. https://www.cbc.ca/news/canada/how-synthetic-identity-fraud-costs-canada-1b-a-year-1.2554429

[25] Federal Bureau of Investigation (05 February 2013). U.S. Attorney's Office. District of New Jersey. *Eighteen People Charged in International $200 Million Credit Card Fraud Scam.* https://archives.fbi.gov/archives/newark/press-releases/2013/eighteen-people-charged-in-international-200-million-credit-card-fraud-scam

[26] Financial Action Task Force (July 2018). Financial Flows From Human Trafficking. www.fatf-gafi.org/2Fmedia/2Ffatf/2Fcontent/2Fimages/2FHuman-Trafficking-2018.pdf

[27] *Ibid*, ¶ 39.

[28] Counter-Terrorism Committee Executive Directorate (February 2019). Identifying and Exploring the Nexus between Human Trafficking, Terrorism, and Terrorism Financing. *United Nations Security Council*. https://www.un.org/sc/ctc/wp-content/uploads/2019/02/HT-terrorism-nexus-CTED-report.pdf

[29] *Ibid.* ¶ 34

[30] Information retrieved from https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12-a&chapter=18&lang=en; Information retrieved from *Victims of Trafficking and Violence Protection Act of 2000*, 114 STAT. 1464, Public Law 106-386. 28 October 2000 (and subsequent reauthorizations).

[31] Marcelo, Philip (26 May 2019). State Prosecutors Struggle with Human Trafficking Cases. *Associated Press*. https://apnews.com/a27f0cb72b4a48ca96f9b8249480d579

[32] Information retrieved from https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf; https://home.treasury.gov/system/files/136/nationalstrategyforcombatingterroristandotherillicitfinancing.pdf

[33] Sengupta, Kim (08 February 2017). Isis Carried out Cyber-Attack on NHS Sites. *The Independent*. https://www.independent.co.uk/news/uk/crime/isis-islamist-hackers-nhs-websites-cyber-attack-syrian-civil-war-images-islamic-state-a7567236.html

[34] Donovan, Fred (02 April 2019). Healthcare Hardest Hit by Cyberattacks, Data Breaches in 2018. *HITInfrastructure*. https://hitinfrastructure.com/news/healthcare-hardest-hit-by-cyberattacks-data-breaches-in-2018; Information retrieved from www.hipaajournal.com/healthcare-data-breach-statistics/; Davis, Jessica (08 August 2019). Healthcare Data Hacking the New 'Space Race," Leaders Tell Senate. *HealthITSecurity*, https://healthitsecurity.com/news/healthcare-data-hacking-the-new-space-race-leaders-tell-senate

[35] C. , Eric (28 October 2018). Ransomware Facts, Trends and Statistics for 2019. *Safety Detective*. www.safetydetectives.com/blog/ransomware-statistics/; Dobran, Bojana (18 April 2019). 27 Shocking Ransomware Statistics That Every IT Pro Needs To Know. *PhoenixNAP Global IT Services*. http://phoenixnap.com/blog/ransomware-statistics-facts

[36] Davis, Jessica (06 August 2019). Has Medical Device Security, Awareness Improved in Healthcare? *HealthITSecurity*. http://healthitsecurity.com/news/has-medical-device-security-awareness-improved-in-healthcare

[37] Information retrieved from https://h-isac.org/

[38] U.S. Department of Health and Human Services (28 December 2018). HHS, in Partnership with Industry, Releases Voluntary Cybersecurity Practices for the Health Industry. *HHS.gov*. https://www.hhs.gov/about/news/2018/12/28/hhs-in-partnership-with-industry-releases-voluntary-cybersecurity-practices-for-the-health-industry.html

[39] Drinkwater, Doug (20 April 2016). These CISOs Explain Why They Got Fired. *CIO.* https://www.cio.com/article/3058726/these-cisos-explain-why-they-got-fired.html

[40] Snell, Elizabeth (25 June 2019). Weak Healthcare Cybersecurity Employee Training Affects IT Security. *HealthITSecurity*. https://healthitsecurity.com/news/weak-healthcare-cybersecurity-employee-training-affects-it-security; Lagasse, Jeff (20 August 2019). Close to One-Third of Healthcare Employees Have Never Received Cybersecurity Training, Report Shows. *Healthcare Finance News*. https://www.healthcarefinancenews.com/node/139082