SCIENCES AND CONSULTING

JOHN WARD CYBERSECURITY BLOGS

YOUR ONLINE RESOURCE FOR TIMELY ANALYSIS, COMMENTARY AND RESOURCES TO KEEP YOU INFORMED ON THE EVER EVOLVING AND HIGHLY CRITICAL FIELD OF CYBERSECURITY

John Ward – Cyberblog January 2021

Topics covered in this issue:

- Privacy concerns of Covid vaccination patient data
- Employee cyber breach of home security systems
- Professionalization of ransomware

Privacy concerns of Covid vaccination patient data

The initial topic of this resource list pertains to the details of Israel's rollout of the COVID-19 vaccine supplied by Pfizer. The unique circumstances pertaining to the procurement, distribution and chronicling of Israel's vaccine rollout could have significant ramifications on medical data policy, not just in Israel but internationally. Furthermore, the relationship between Israel's government and the drug's manufacturer, Pfizer, and the unprecedented business deal that they have made could signal a new trend in how public and private entities interact in the medical community, and perhaps many other areas of critical infrastructure.

In an article appearing in The Washington Post titled Vaccines for Data: Israel's Pfizer Deal Drives Quick Rollout-And Privacy Worries, author Daniel Erstein reported that as of the article's publication date (January 27th, 2021), Israel had administered the COVID-19 vaccine to a higher percentage of their citizenry than any other country in the world. Israel is administering the Pfizer version of the vaccine. At the time of reporting, Israel had administered the first shot to approximately 1/3rd of the population, with approximately 17% of the population having received both shots (Erstein, 2021). Both of these figures are far and away the highest rates internationally (Erstein, 2021).

This success is not without controversy. Israel and Pfizer made a deal to in which Israel would provide medical data and medical statistics pertaining to the vaccine rollout to Pfizer-ostensibly to study "whether herd immunity is achieved after reaching a certain point of vaccination coverage in Israel" (Erstein, 2021). Pfizer has not made a similar deal with any other country (Erstein, 2021). According to an article written by Shira Rubin and Steve Hendrix for NPR entitled Israel Moves To Head of Vaccine Queue, Offering Pfizer Access to Country's Health-Care Database, Israel is also paying a premium price to Pfizer for the vaccine. It is believed that Israel is paying Pfizer approximately $50 per vaccine, which is roughly twice as much as European Union countries are paying (Rubin and Hendrix, 2021).

The benefits for this deal are obvious for both parties. For Israel, they have the opportunity to provide their populace with the vaccine to an international pandemic at a rate that far surpasses any other nation in the world. Furthermore, Israel's international prestige could be significantly enhanced by leading all national efforts in vaccination. In January, Prime Minister Netenyahu spoke at the Davos World Economic Forum and indicated that he believed that Israel could be a "world laboratory for herd immunity" (Rubin and Hendrix, 2021). For Pfizer, the combination of Israel's small population, technological interconnectivity, and advanced healthcare system provide an opportunity for the rapid and accurate tracking and chronicling of the vaccine rollout and its' successes and weak points, which can ostensibly be scaled up for a more effective rollout in larger nations (Rubin and Hendrix, 2021).

The terms of the deal were kept confidential from the public until January 17th, when the Israeli government published a redacted portion of the contract (Erstein, 2021). Israeli government officials insist that they are providing Pfizer solely with anonymous medical data that is already publicly available, such as statistics on confirmed cases of the virus and hospitalization (Erstein, 2021). Pfizer has stated that they are not going to be receiving any "identifiable health information", and indicated that they are only going to be receiving "aggregated epidemiological data" (Erstein, 2021). While this deal may sound innocuous, on the surface, there are significant concerns within Israel and without. The contract has a stipulation that either Pfizer or Israel can "provide input, make factual corrections, and delay publication of their studies of the vaccine's effectiveness" (Erstein, 2021). Essentially this means that either the Israeli government or Pfizer, both of whom have a significant interest in the successful rollout of the vaccine, have the option to decline or delay to publish any negative aspects of the vaccine roll-out. This is a troubling development, as it gives significant leeway to a hybrid public/private entity in the matter of information-sharing in the midst of a pandemic.

More troubling, specifically for the Israeli people, are privacy concerns relating to the medical data that is being shared by the Israeli government. Despite Israel and Pfizer both claiming that the data that is being shared is not identifiable nor intrusive, they have not defined exactly what the data will be outside of a vague definition, and significant portions of the contract which may clarify the matter are redacted or unpublished. Some Israeli citizens are comparing the deal to a "nationwide clinical trial" (Erstein, 2021), and claim that even if the Israeli government is only providing Pfizer with unidentifiable data, it can still be used to identify people by cross-referencing with other available data (Erstein, 2021).

John Ward – Cyberblog January 2021

The legality of the deal is also in question, as former deputy general of Israel Yoram Bar-Sela wrote an opinion piece in which he indicated that he did not believe the Israeli government, nor the HMOs who would be collecting and providing the medical data, have the legal authority to transfer citizen medical data to a foreign body unilaterally (Rubin and Hendrix, 2021). The Israeli government has already created privacy concerns for a portion of their citizenry during the coronavirus pandemic-in the early stages of the pandemic Shin Bet, the national security agency, tracked Israeli citizen's cell phones without their knowledge or consent in an effort to track infected individuals and notify those who may have come in to contact with them (Rubin and Hendrix, 2021). The program resulted in a number of individuals being wrongfully contacted and quarantining based on mistaken information, and the Israeli government admitted that the program had "limited effectiveness" (Rubin and Hendrix, 2021).

A successful rollout of the Pfizer coronavirus vaccine could play an important role in crafting an effective framework that could be used to vaccinate larger and less centralized nations. Does this mitigate the privacy concerns that come from a national government sharing it's citizen's medical data with a private corporation, especially one that is based in another country? Despite the claims of Israel and Pfizer that the specific data being shared is not identifiable, neither party is being transparent enough to verify that. It is difficult to argue with the success Israel has had vaccinating their citizenry, and the potential benefit to the international community, but a dangerous precedent could be set in this time of extreme circumstances that could have ramifications for governmental-corporate partnerships that disregard or minimize citizen privacy concerns. Finally, there are concerns regarding the protection of the data that is being given to Pfizer by Israel-Israel is a technologically-advanced nation with a robust cybersecurity policy that is the envy of a number of nations. They have prioritized cybersecurity and there exists and there exists a tangible security interest, as well as a responsibility to their citizens to protect them and their privacy and data (at least from external threats). Sharing that data with another entity that doesn't necessarily have the same concerns or responsibilities regarding the data raises concerns about how well the data will be protected.

John Ward – Cyberblog January 2021

Employee cyber breach of home security systems

The second topic of this report focuses on recent charges brought against a Texas man who exploited his employment position to digitally access security cameras in the homes of private citizens. On January 21st, 2021, the Department of Justice Northern District of Texas announced that Telesfloro Aviles, a Texas-based employee of ADT, pleaded guilty to computer fraud. The charges stemmed from the allegation that Mr. Aviles had accessed ADT-installed and maintained security cameras to unlawfully spy on ADT customers (DOJ, 2021). According to the investigation, Mr. Aviles added his personal e-mail address to the list of authorized users on customer's "ADT Pulse" accounts, granting him real-time access to the security cameras installed in their homes (DOJ, 2021). Mr. Avilles admitted that over a four-and-a-half year period, he had secretly accessed approximately 200 customer accounts over 9, 600 times (DOJ, 2021).

According to an April, 2020 statement on the ADT website, they reacted quickly when they were informed by a customer that there was an unauthorized e-mail on their Pulse account. An internal investigation revealed that Mr. Aviles was the culprit, and that he had accessed 220 other such accounts linked to his e-mail (ADT, 2020). ADT stated that they immediately contacted the police and had launched a review of all their processes, including engaging with "third-party experts" (ADT, 2020). In a separate section on their website, ADT indicated that they had implemented a new feature for their "ADT Pulse" service where customers will be notified when a new e-mail address is added to their access list, as well as implementing an automated process that helps to identify "abnormal account activity" which leads to an investigation by human beings (ADT 2020).

According to an article written for Buzzfeed by Salvador Hernandez titled A Home Security Tech Hacked Into Cameras To Watch People Undressing, And Having Sex, Prosecutors Say, ADT is currently facing three federal lawsuits in relation to the incident. One lawsuit claims that ADT "failed to implement adequate procedures that would prevent non-household members from adding non-household e-mail addresses" (Hernandez, 2021). Another lawsuit claims that ADT "failed to monitor consumer's accounts and promptly alert them any time a new e-mail was added to their accounts" (Hernandez, 2021). It is furthermore alleged in the lawsuits that ADT only discovered the breach by "luck and circumstance", and that a reporting customer was the catalyst for ADT discovering the unauthorized access, not any internal ADT protocols (Hernandez, 2021). At least one of the affected customers stated that ADT had attempted to get them to sign a confidentiality agreement in the initial aftermath of the disclosure, beginning with an offer of $2,500 and eventually offering $50,000 and credit for "services and equipment" (Hernandez, 2021).

John Ward – Cyberblog January 2021

This case is indicative of a number of aspects of modern cybersecurity, including many that appear to be self-evident, but are often overlooked. Although Mr. Hernandez's article states that ADT had a company policy against adding a technician adding their (or any other unauthorized user's e-mail) to a customer's pulse account, this was clearly not monitored nor enforced. Nor was there any sort of monitoring implemented that would have monitored irregularities regarding the access of these accounts once the inappropriate e-mail address was added, and only became aware of the situation when it was brought to their attention by a customer. In today's cybersecurity landscape, this is almost unconscionable. Furthermore, if the allegations regarding ADT's attempt to have affected customers sign confidentiality agreements is true, it is an indication that while ADT intended to notify all who were affected by this particular breach, they were not eager to publicize the matter, which could have been detrimental to other ADT customers who may have been similarly affected. Finally, the measures implemented by ADT following the breach indicate that they had previously not considered that such a breach could occur, and had not implemented these measures prior to being faced with an actual breach. Implementing these mitigation measures at any point prior to being faced with an actual breach could have significantly mitigated, if not avoided altogether, the damage.

The ADT breach also highlights that ultimately, a consumer must be an advocate of their own cybersecurity. While ADT did have a policy against the addition of unauthorized email addresses to customer's ADT accounts, it is clear that having a policy and effectively enforcing/monitoring that policy are two wildly different things. One should have a reasonable expectation that a major company which focuses on security would have prioritized effective cybersecurity, it is clear in this case and in many others that that is not always the case. As the FBI noted in the DOJ statement, "…we encourage everyone to practice cyber hygiene with their connected devices by reviewing authorized users and routinely changing passwords" (DOJ, 2021) before offering links to their own resources on cybersecurity. While it is unfortunate that lapses is policy and protocol on ADT's part led to the breach situation occurring and not being detected, the need for individual consumer cyber-hygiene is made clear by this situation, no matter the expectation of protection one has for a company based on their size, reputation, and history. The final lesson from this situation is that often, cybercrime and cybersecurity is perpetrated by opportunistic offenders who may not even need a significant amount of technical skill to be able to victimize someone. Mr. Aviles, due to his position and training, had access to ADT Pulse, as to presumably countless other individuals working for ADT and similar companies. This breach was not a "hack", in the sense that Mr. Aviles did not use advanced technical knowledge to trespass into digital areas that were unauthorized.

In reality, he exploited the access that he had and used minimal technical skill to affect the breach. Too often, cybersecurity is portrayed as international actors with significant resources, or highly-skilled and specialized criminals utilizing their advanced means to perform digitally sophisticated crime. This portrayal can have significant consequences on those who are eventually victimized and be detrimental to the practicing of good cyber-hygiene on their parts, as they expect that attacks would be overwhelmingly sophisticated to understand or precent, when in reality they are more likely to be simple and preventable.

Professionalization of ransomware

The final issue in this report deals with perhaps the most significant and direct threat to the cybersecurity of the medical device industry: Ransomware. Several previous reports composed by this author for Ward Sciences and Consulting LLC have highlighted the proliferation of ransomware attacks on critical industries in the previous two years, largely focusing on critical infrastructure targets and especially focusing on healthcare facilities which are accessed through vulnerable medical devices/networks. In an article for Wired titled Ransomware is Headed Down a Dire Path, author Lily Hay Newman provides a telling update on the ever-augmenting ransomware threat.

According to Ms. Newman, ransomware attacks have increased in severity in 2020, and many experts are predicting that that trend will continue moving forward. The antivirus firm Emisoft is quoted as saying that the average requested ransomware payment went from $5,000 in 2018 to approximately $200,000 in 2020. Municipal governments, healthcare facilities, school systems, and countless other entities are at severe risk for ransomware attack. The reasons for the proliferation of ransomware attacks have been explored in depth in previous reports by this author for Ward Sciences and Consulting LLC, including lack of cohesive deterrent policy, relative ease of procurement/use of ransomware tools by the perpetrator, and the proliferation of cryptocurrency allowing for a better guarantee of anonymity for the perpetrator. Ms. Newman highlights some further dangerous trends that paint a grim picture for the future of ransomware.

John Ward – Cyberblog January 2021

One of the major recent trends in ransomware is the "professionalization" of ransomware perpetrators (Newman, 2020). Underground resources available to a motivated offender are becoming more easily accessible, user-friendly and comprehensive (Newman, 2020). According to Ms. Newman, a motivated perpetrator preparing to launch a ransomware attack could, with relative ease, gain access to ransomware "consultants" or network security experts who could provide material or communicative assistance. Emisoft believes that the number of ransomware attacks has not significantly increased in 2020, but due to factors such as this one, ransomware attacks are becoming more effective (Newman, 2020).

Another troubling trend in ransomware is that perpetrators are becoming more discerning about who they victimize (Newman, 2020). In the past, the trend was largely that ransomware offenders would cast a wide net to a variety of "smaller" victims, in the hope of procuring a large amount of smaller ransom payments (Newman, 2020). That trend has now shifted to where the trend is that ransomware perpetrators are targeting larger potential victims in the hope of securing small amounts of "massive ransoms" (Newman, 2020). Furthermore, where encrypting proprietary files and denying access for ransom was once the endgame for these offenders, it is now merely being seen as the first step for particularly motivated offenders (Newman, 2020). In addition to blocking access to data/network systems, some offenders are also taking advantage of this access to "(exfiltrate) an organization's data and threatening to release it" (Newman, 2020). This augmentation of the original ransomware attack can serve to either drive up the initial ransom demand or force an organization into making two separate payments. In this author's opinion, this could also serve to dissuade an organization from being fully transparent and to take full advantage of cybersecurity resources available to them after a ransomware attack-in the modern cybersecurity environment it is understandable that an organization will be victimized by ransomware, but news that their data is being potentially held for blackmail could be a major consideration for how openly or discreetly an organization attempts to respond to the problem as they worry about shareholder/consumer/stakeholder response.

Finally, Ms. Newman indicates that ransomware perpetrators are becoming more sophisticated and discerning with the timing of their attacks. It is clear that more sophisticated offenders are timing their attacks on certain entities with real-world events that exacerbate that entities need for full and unfettered access to their files and networks.

John Ward – Cyberblog January 2021

COVID-19 has created a rich opportunity-laden landscape for victimization across a number of entities (Newman, 2020). The widespread digitization of education due to COVID-19 quarantine means that the digital infrastructure for most educational entities are more heavily-relied on than ever before (Newman, 2020). As such, August and September, the traditional start of most school years in the United States, saw heavy ransomware victimization among educational entities (Newman, 2020). Likewise with the COVID-19 vaccine rollout-such a highly complex, time-dependent and multi-faceted effort provides an enticing target to ransomware perpetrators.

The ransomware picture is not entirely bleak, however. The current trend of greater sophistication in ransomware attacks on smaller clusters of larger, often related targets, and greater focus on advantageously timing the attacks, could work in the favor of security experts. These factors may serve to create more predictable patterns, or more obvious targets, that can be more carefully monitored and protected (Newman, 2020). Also, a trend has been emerging where some ransomware attackers are laying the digital groundwork for their attacks well before the actual attack, infiltrating target networks in anticipation and lying dormant until the appropriate moment presents itself (Newman, 2020). While striking at the most opportune moment provides the perpetrator with the greatest chance of a successful ransomware operation, the preparation for such a precise attack appears to be that they risk earlier potential exposure and neutralization prior that opportune moment occurring.

Ms. Newman's article offers some hope for the immediate future in regards to the ransomware threat. Cybersecurity firm Mandiant said in the article that they believe 2020 will "be an important year in terms of law enforcement actions related to ransomware", including major steps in international law enforcement cooperation. While this statement is vague, it has long been argued that international cooperation and a strong, enforceable law enforcement policy towards ransomware would act as a major deterrent to cybersecurity threats, and in particular ransomware attacks, which rely on taking advantage of half-baked policies or policies that are not enforceable/at odds with each other due to the legal jurisdictions involved.

John Ward – Cyberblog January 2021

Finally, Ms. Newman's article makes note of the January, 2020 announcement of the formation of the Ransomware Task Force (RTF)-a group that was formed under the auspices of the Institute for Security and Technology (IST), an organization which attempts to combat cybersecurity threats with a multi-disciplinary, international approach involving several categories of stakeholders. The group includes 33 separate partners, several of which are organizations composed of several different entities (Newman, 2020). These partners include Microsoft and FireEye, whom have both proven to be tremendous cybersecurity assets in the detection and mitigation of the recent SolarWinds attack (Newman, 2020). The RTF also includes the Cleveland Clinic as a stakeholder, which bodes well for representation within the medical and medical device community (Newman, 2020). In a statement announcing the formation of the RTF, the IST described it as "a broad coalition of experts from disparate sectors dedicated to producing a roadmap for ransomware mitigation. The objective is not simply to put forward ideas but to provide actionable solutions that can be undertaken in the immediate and long-term" (IST, 2020). While it remains to be seen if the RTF has the capabilities, resources, and authority to affect a real change in the ransomware landscape, their stated mix of multi-disciplinary, international, action-instead-of-theory focus could provide an important step in the battle against ransomware. As of the writing of this report two weeks after the announcement of the formation of the RTF, there have been no reported developments with the organization.

John Ward – Cyberblog January 2021

REFERENCES CITED AND RELATED CYBER RESOURCES OF INTEREST

1. ADT technician pleads guilty to Hacking home security footage. (2021, January 21). Retrieved January 28, 2021, from https://www.justice.gov/usao-ndtx/pr/adt-technician-pleads-guilty-hacking-home-security-footage

2. Berg, L. (n.d.). Ransomware task force (rtf). Retrieved January 20, 2021, from https://securityandtechnology.org/ransomwaretaskforce/

3. Estrin, D. (2021, January 31). Vaccines for DATA: Israel's PFIZER Deal Drives Quick rollout - and privacy worries. Retrieved January 31, 2021, from https://www.npr.org/2021/01/31/960819083/vaccines-for-data-israels-pfizer-deal-drives-quick-rollout-and-privacy-worries

4. FAQs about ADT's response. (n.d.). Retrieved January 20, 2021, from https://www.adt.com/adt-privacy-notice/steps-we-took

5. Hernandez, S. (2021, January 21). A home security tech hacked into cameras to watch people undressing and having sex, prosecutors say. Retrieved January 28, 2021, from https://www.buzzfeednews.com/article/salvadorhernandez/home-security-camera-hacked-adt

6. Newman, L. (2021, December 29). Ransomware is headed down a dire path. Retrieved January 20, 2021, from https://www.wired.com/story/ransomware-2020-headed-down-dire-path/

7. Shira Rubin and Hendrix, Steve. (2021, January 28). Israel moves to head of vaccine queue, offering Pfizer access to Country's health-care database. Retrieved January 30, 2021, from https://www.washingtonpost.com/world/middle_east/israel-pfizer-coronavirus-vaccine-privacy/2021/01/27/b9773c80-5f4d-11eb-a177-7765f29a9524_story.html

8. Was my account accessed? (n.d.). Retrieved January 20, 2021, from https://www.adt.com/adt-privacy-notice/my-account

