AGILEPQ

Consequences and Risks of Security Breaches from Internet of Things (IoT) Devices

August 29, 2019

INTRODUCTION:

The world is currently experiencing a period of unprecedented technological advance. Technology is getting smaller and the world is getting smarter. Every day smart devices enter a new area of our lives. From pacemakers to coffeemakers and industrial sensors, IoT devices are now present in more areas than most even realize. The advancements achieved through the proliferation of the Internet of Things (IoT) have not come without accompanying risks. These devices become more prevalent every day, and with them come additional dangers.

Despite these major security concerns, many in corporate boardrooms and the IoT industry are seemingly unaware of the severity and magnitude of the IoT security deficit. Many IoT device and platform manufacturers rationalize the implementation of inadequate security by downplaying the significant role these devices play and the potential dangers they represent when they are compromised. Some of these dangerous misconceptions include:

1. Constrained IoT devices do not pose a threat to firewalls upstream.
2. Time to market, cost of goods sold, and feature-sets take priority over security measures.
3. Small devices do not transmit or receive important data, perform important functions, or provide direct access to corporate data.
4. Authentication/Authorization of IoT devices is sufficient to secure an IoT device.
5. Threat detection works because it notifies when attacks are occurring, and devices can rebooted.
6. IoT devices are not an entry point for bad actors to gain access to a server.
7. Even if someone accesses an IoT device and obtains the data, there is little liability.

These misconceptions have led and will lead to catastrophic results. In recent years, breaches in IoT security have caused significant damage across several industries and market segments. Below are examples of the hazards, damages, and liabilities of neglecting proper security implementation on all IoT devices—now and in the future. Data from recent breaches elucidates threats and ongoing risks.

KEY FINDINGS:

- There is a substantial and growing unrecognized risk associated with billions of connected IoT devices sold each year.
- IoT devices are often void of or sorely lacking in security features. These systems are now one of the most attractive targets to malicious actors.

- A recent Security Innovation Europe study concluded that cyber-attacks now account for 35% of all internet traffic.
- A study from the Ponemon Institute showed a “dramatic increase” in IoT related hacks with IoT representing over a quarter of all data breaches. Additionally, these breaches cause significant harm, with the average data breach in the United States costing $8.2 million.
- Breaches in IoT security have caused significant damage across several industries and entities and will continue to do so unless protective cybersecurity measures are taken.
- Many device manufacturers overlook the risk associated with IoT by prioritizing time to market, cost of goods sold, and feature-sets above security measures.
- IoT data breaches have already caused billions in damages and have exposed companies to innumerable risks. Companies currently stand to lose billions of additional dollars, and in some cases these vulnerabilities may be endangering human lives.
- The lesson these breaches teach us is clear: corporate executives and policymakers around the world can no longer afford to ignore securing all elements of the Internet of Things. The time is now to take the necessary steps to secure IoT networks.

LARGE BREACHES FROM SMALL DEVICES

Target Stores

Among the most prevalent of common misconceptions is the idea that constrained devices do not pose a threat with firewalls upstream, and that IoT devices are not an entry point for bad actors to gain access to a server. Both statements have been proven false.

In November of 2013, Target learned they had experienced a massive data breach. This breach compromised 70 million records, including customer credit card information. The hackers were able to gain initial access to Target’s vendor portal by first compromising an unprotected device on their network—an HVAC machine. Once they gained deeper access into Target’s systems, they were able to extract 11 GB worth of data containing the customer records.[1] Target initially stated in their 2013 10-K that they would incur $61 million in expenses related to the data Breach. After a few years and over 140 lawsuits later their 2016 10-K stated, “since the Data Breach, we have incurred $292 million of cumulative expenses, partially offset by insurance recoveries of $90

[1] https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/#4976ee3e7954

million, for net cumulative expenses of $202 million."[2] The costs detailed by Target in their annual reports are just a fraction of the complete cost for their massive data breach. Target actually incurred costs ranging from 1.76 Billion to 2.50 Billion, 2.4% - 3.4% of their total revenue and 89% - 127% of net income in 2013.

Total Cost Incurred ($)	Best Case	Worst Case
Data-Breach Related Expenses	292,000,000	292,000,000
Q4 2013 Decline in Rev.	1,319,448,088	1,709,762,362
Q1 2014 Decline in Rev.	208,000,000	411,868,140
Cost of Losing CEO	25,800,000	82,400,000
Cost of Losing CIO	2,000,000	4,000,000
Total (with insurance)	**1,757,248,088**	2,410,030,501
Total (without insurance)	1,847,248,088	**2,500,030,501**

Target stated, "We know our guests' confidence in Target and the broader U.S. payment system has been shaken."[3] The impact of the loss in confidence resulted in a decline of 1.5-2.1 billion in revenue during Q4 (2013) and Q1 (2014). Moreover, the board of directors decided to remove their current CEO and CIO resulting in a projected cost of replacement of 200-400% of their annual salaries. This resulted in a cost range of 27.8-86.4 million to adequately replace these C-suite executives.

Fiat Chrysler

Fiat Chrysler has also experienced the impact of a small device being compromised. In 2015, hackers found a vulnerability in the key fob that gave them the capability of taking control of over 1.4 million vehicles.[4] Through the unprotected device hackers could control the steering wheel, brakes, and transmission. They would even able to turn the steering wheel 90 degrees at high rates of speed. Fortunately, the hackers chose to report the vulnerability to Fiat Chrysler instead of using it for nefarious purposes. This demonstration of moral character did not, however, prevent Fiat Chrysler from incurring large damages. The average cost of recalling a vehicle for a critical safety repair is $416 dollars per vehicle.[5] With 1.4 Million cars being recalled, the cost of this recall was approximately $582 million dollars.

However, this is not the only cost involved with the breach. As the media reported the breach, consumer trust was severely shaken by the event, and Fiat Chrysler incurring a loss of approximately 330 million in net income in Q3 2015.[6] Fiat Chrysler is also facing a large class action lawsuit by several owners of their vehicles. 200,000 class members

[2] Target 10-K 2016

[3] Target 10-K 2013

[4] https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

[5] 2016 Automotive Recall Information (National Highway Safety Administration)

[6] https://www.macrotrends.net/stocks/charts/FCAU/fiat-chrysler-automobiles/net-income

are seeking $50,000 each, representing a potential loss of $10 billion. This lawsuit was filed in spite of the fact that none of the class members actually had their vehicles compromised. The U.S. Supreme court recently overruled a motion to dismiss filed by Fiat Chrysler wherein the corporation asserted that the company had addressed the issue before any customer's vehicles were actually compromised.[7] This case illustrates the magnitude of liability that companies are exposing themselves to when neglecting device security.

ESSENTIAL FUNCTIONS AND RECORDS LEFT VULNERABLE

Another common fallacy related to IoT security is that Small devices do not contain data or perform functions important enough to cause significant damage if compromised. Medical devices are perhaps the most obvious examples of small devices that serve a purpose tied directly to human life and quality of life. When consumers have medical devices implanted or attached to monitor or control human functions, or even to collect critical health data, the consumer assumes that these devices are secure given the life or death nature of their functions. Unfortunately, this is often not the case.

Dr. Ken Dick, a professor of IT innovation and informatics at the University of Nebraska Omaha recently documented a harrowing experience regarding medical device vulnerabilities. Dr. Dick described an incident when one of his undergraduate students hacked her own pacemaker. She confided to the class that she could hack it and that the data stream was easy to decipher. At the close of class Dr. Dick suggested to her that she should exercise caution in dealing with a life-impacting device such as her pacemaker. Her response was “well I was just curious.” This incident is one of many examples of potentially life-threatening breaches in the medical device industry.

Besides the obvious tragedy that accompanies the loss of a human life due to a security breach, a death would represent a major liability for the device manufacturer. In the case of a lethal breach, businesses would be liable for approximately $7.8 million dollars per fatality[8]. This statistic is a universal average of several organization's estimates of the liability associated with losing a human life, and therefore can be applied to industries other than medical as well. In addition to this liability, a breach in the medical device industry would present significant risks even if there were no fatalities involved. Medical records are the most expensive type of record when data loss occurs with each record costing the party at fault $429 and the average breach in the industry costing $6.45 million.[9] These costs do not account for the potential fines associated with violating HIPAA laws, with HIPPA violations historically assessed at up to $16 million dollars.[10] The Blue Cross incurred this cost as part of their larger $131

[7] https://www.reuters.com/article/us-usa-court-fiat-chrysler/u-s-top-court-declines-to-take-up-fiat-chrysler-hacking-case-idUSKCN1P11FZ

[8] https://www.theglobalist.com/the-cost-of-a-human-life-statistically-speaking/

[9] IBM Cost of a Data Breach Report 2019

[10] https://www.healthleadersmedia.com/anthem-pay-biggest-hipaa-settlement-history

million breach in 2015.[11] These incidents illustrate both how devastating the breach of a small device has been and will be.

SHORT-TERM THINKING LEADS TO LONG-TERM DISASTER

Many device manufacturers also overlook the risk associated with IoT by prioritizing time to market, cost of goods sold, and feature-sets above security measures. The Department of Homeland Security addressed this issue with IoT devices in a report to the President saying,

> Unfortunately, IoT devices are often sorely lacking in security-focused features. These systems now offer the most attractive target to malicious actors and are an increasingly large percentage of the devices in the ecosystem. In fact, the November 2016 Ericsson Mobility Report predicted that IoT devices will surpass mobile phones as the largest category of connected devices in 2018. Given the level of security on IoT devices, that is a daunting prediction. . . Market incentives appear to exacerbate the problem. Product developers prioritize time to market and innovative functionality over security and resilience. Security features are not easily understood or communicated to the consumer, which makes it difficult to generate demand.[12]

This approach has already cost some device makers dearly. In 2016 SimpliSafe, a smart-home security company, had over 300,000 of their devices breached. Hackers disarmed the systems and even accessed camera feeds from within customers' homes.[13] Due to the lack of foresight, an over-the-air patch was impossible, and the company had to offer enormous discounts on new systems for clients with compromised products. SimpliSafe is not alone in physical facilities breaches through IoT devices with the system.

The risk for companies is now moving from damages for actual attacks to damages for being negligent in design. ADT, the market leader in home security, recently paid $16 million in settlements in five separate class action lawsuits for not being honest in their marketing about how easily their systems could be hacked.[14] This is a significant development. The proliferation of damages from clandestine cyber attacks is reaching a scale that this lawsuit sought redress for potential future attacks.

Data collection, storage and analysis is ever-increasingly becoming more important for companies. As a result, corporations are extremely protective of their sensitive

[11] Anthem Inc. 10-K 2014 and 2015

[12] Department of Homeland Security & Department of Commerce, "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats."

[13] https://www.forbes.com/sites/thomasbrewster/2016/02/17/simplisafe-alarm-attacks/#783194b13b00

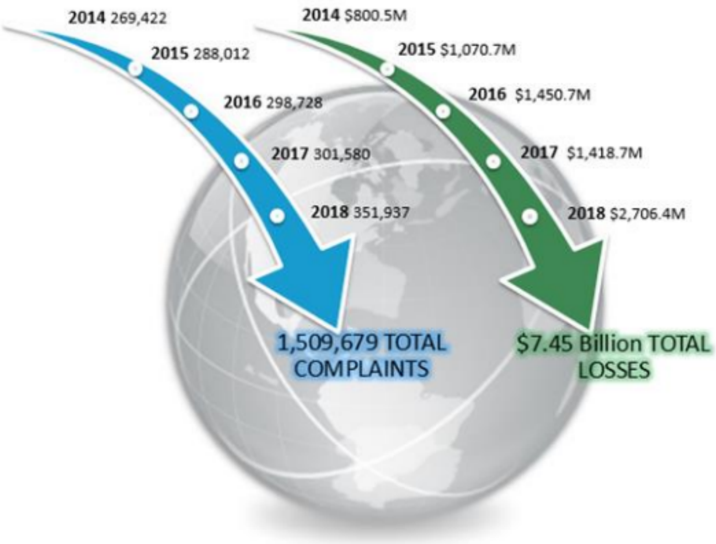
[14] https://www.securityinfowatch.com/residential-technologies/article/12335708/baker-vs-adt-resolved

information such as financial records, HR documents, intellectual property, business plans, and legal documentation. Companies understand the loss of these records is catastrophic, with financial records costing an average of $210 per record lost and the exposure of other documents such as technical write-ups, intellectual property, and managerial financial information potentially compromising an organization's entire operation.[15]

Additionally, the breach of IoT devices can also pose a significant threat to the general population through the use of compromised devices in Botnets and other distributed attacks (DDoS). While there is little evidence of litigation for these events, it is likely that such suits will come in the near future—with the owner of the infected device potentially responsible for damages if negligent in ensuring they are operating a secure network down to the smallest of devices.

CONCLUSION

Attacks are increasing at a rate higher that the development of new IoT devices and systems with catastrophic results.



Source: 2018 FBI Internet Crime Report

The financial losses from cyber theft of data is now compounding to and will reach a point that the fallout will be an unrecoverable event. Breaches caused by a malicious attack were **27%** more costly than breaches caused by human error. . . and **37%** more costly than a breach caused by system glitches (*IBM cost of a data breach).*

[15] IBM Cost of a Data Breach Report 2019

Widespread misconceptions concerning the urgency of securing all elements of the Internet of Things have already extracted large costs. These ideas and practices will continue to lead to catastrophic results if they continue to be accepted as the norm. Cyber-attacks are on the rise with 51% of data breaches resulting from malicious attacks[16] coming from IoT devices, which are frequently named as the weak link.

A study from the Ponemon Institute showed a “dramatic increase” in IoT-related hacks with IoT representing over a quarter of all data breaches.[17] These breaches are significant events with the average data breach in the United States costing $8.2 million.[18] The aggregate damage wrought by these breaches is difficult to quantify due to its sheer immensity. However, the lesson these breaches teach us is clear. Industry leaders can no longer afford to ignore securing all elements of their networks, including IoT devices. Rationalizations for inadequate device security may seem sufficient but will inevitably lead to paying a greater price in the long run. The price of inaction could reach billions of dollars and can risk lives. Corporate boards, executives, and management of commercial, civic and government entities must choose to act now to protect their clients and organizations, but also the entire global cyber ecosystem.

[16] IBM Cost of a Data Breach Report 2019

[17] Ponemon Institute: Third Annual Party IoT Risk: Companies Don’t Know What They Don’t Know" report

[18] IBM Cost of a Data Breach Report 2019