CHAPTER 14

Advice to Cybersecurity Investors

Over $45 billion of private equity and public IPO (initial public offering) investment has been made in cybersecurity companies from 2003 to 2020, yet the mega-breaches have continued. This chapter covers where all this money has been going and what categories of defenses have been invested in thus far. We then go on to analyze what areas of cybersecurity are ripe for further investment. As an example, areas such as Internet of Things (IoT) security and privacy, among others, have received less investment as compared to, say, network security and probably warrant more investment going forward.

Data Sources

Most of the raw data on cybersecurity companies used to draw the conclusions in this chapter comes from Crunchbase. Crunchbase was founded in 2007 to initially track startups featured in TechCrunch articles, but has grown significantly over the years. The data in Crunchbase’s database comes from over 4,000 venture firms, accelerators, and incubators, in addition to data aggregated by an in-house data team and members of the Crunchbase community. Machine learning algorithms also scour the Web to add to the database.
The data from Crunchbase is not perfect, and I (Neil) fully expect that neither is my analysis based on their data. That said, while every category in the data set that is attributed to a security startup and every single figure on how much money the startup raised may not be 100% correct, I believe that the macro-trends that I derive from the data are highly likely to be directionally correct, even if not 100% technically accurate. For instance, if approximately $11 billion has been invested in network security over the 17-year period from 2003 to 2020, but less than $2 billion has been invested in IoT security, it is more likely than not that more investment is needed in IoT security, especially considering that billions of devices will be coming online, and we’ve only begun to see IoT attacks such as the Mirai botnet cripple some of the largest sites on the Internet, including Twitter, Netflix, Spotify, and many others back in 2016.

Security Startup Revolution

Since the commercialization of the Internet started in the mid-1990s, it has been a revolutionary time for cybersecurity. Approximately 4400 cybersecurity companies have started from 2003 to 2020, but the breaches continue on an all too frequent basis.

The number of cybersecurity companies that have been founded per year skyrocketed from under 200 per year in 2010 and prior to over 400 in 2014, as per Figure 14-1. After Target’s mega-breach in 2013, the number of new cybersecurity startups started increasing significantly up until 2017. However, the number of security companies founded from 2018 to 2019 significantly dropped as compared to previous years. The drop continued in 2020 with only about 90 cybersecurity companies founded in the first three quarters of the year. Although the immense drop in 2020 could be attributed to economic recession due to COVID-19, the number of new cybersecurity companies founded in 2018 and 2019 represented a significant decrease in cybersecurity startups. The market was likely getting flooded with cybersecurity companies in reaction to the number of big breaches taking place.
Given the economic climate as of 2020 with the COVID-19 pandemic, the growth of many companies was impacted. However, COVID-19 brought with it impact to information security, as it brought impact to many aspects of the world. Rising numbers of remote workers coming in from insecure, relatively unmanaged home routers and lack of VPN (virtual private network) bandwidth resulted in new cybersecurity challenges. Some companies, for instance, resorted to using split tunneling as a result of a lack of VPN bandwidth, and many CISOs have lost visibility. They were not having all corporate traffic fully tunneled and backhauled through all the enterprise defenses that they have invested in over the years. As the world continues to evolve, the cybersecurity landscape will continue to evolve with it.

As there are going to be more cybersecurity companies to come, the natural question that arises is: what should those companies be doing? The answer lies at the intersection of what big cybersecurity
needs the market has and what is already being covered relatively well by incumbent cybersecurity companies. We will first focus on the latter question by analyzing investments to date. Then, we’ll analyze areas where investments to date probably have not been sufficient.

**Investment Factors**

While many data breaches can be avoided by just getting the basics of information security right, there is a saying in our field: “Attacks only get better.” Organized cybercriminals and nation-state actors relentlessly continue to develop more sophisticated attacks, and we need to always be innovating and coming up with new and better defenses to proactively anticipate novel attacks.

There are a few key factors that need to be considered to understand which specific areas of cybersecurity need the most additional funding. They are

1) **Market size/need:** The cybersecurity market, overall, is a large market. Well-known industry analyst groups IDC and Gartner both estimated cybersecurity market spend to be more than $100 billion annually for 2019. IDC estimated $103 billion, while Gartner estimated $124 billion. One can look at breakdowns of the expected market size for sub-areas of security as an indicator of market need for those sub-areas. Although that might be useful to do for larger sub-areas of security, it may be harder to reliably use such statistics for growing areas of cybersecurity. Hence, while existing expected market need is one factor, we also look at expected future trends.
2) **Investments to date**: Even if there is a sizable existing market need for a particular area of security, further investment in that area may not be as critical as in other areas where there has been less historical investment. With this in mind, we look at the amount invested to date in a particular area.

3) **Root causes of breaches**: Although the existing security market may be heading in particular directions, future breaches may occur for reasons that may not be getting proportionately addressed by current directions. Also, understanding the root causes for past breaches and whether or not current market directions are addressing those root causes sufficiently can be important.

4) **Expected future trends**: While no one has a crystal ball, one can speculate about areas of cybersecurity that are likely to experience significant growth based on technological trends, market trends, and evolution of an attacker’s goals. I’ll comment on future trends throughout in the discussion that follows.

We now cover the preceding factors in detail and discuss what we can learn about which areas of cybersecurity need further investment, which may not, and why.

### Market Size/Need

Table 14-1 shows Gartner’s estimate of total market size broken down by category. Note that we will see that while Gartner uses some of the same category names that Crunchbase uses, their definitions of these categories
are unlikely to be an exact match. That said, it may nevertheless be interesting to see what we can learn from Gartner’s assessment of market need in an area and Crunchbase’s assessment of investment to date in a particular area, even if the category match may be “fuzzy.”

**Table 14-1. Gartner Market Size for Cybersecurity Areas,¹ in Millions of Dollars (2017–2019)**

| Market Segment                        | 2017  | 2018  | 2019  |
|---------------------------------------|-------|-------|-------|
| Application Security                  | 2434  | 2742  | 3003  |
| Cloud Security                        | 185   | 304   | 459   |
| Data Security                         | 2563  | 3063  | 3524  |
| Identity Access Management            | 8823  | 9768  | 10,578|
| Infrastructure Protection             | 12,583| 14,106| 15,337|
| Integrated Risk Management            | 3949  | 4347  | 4712  |
| Network Security Equipment            | 10,911| 12,427| 13,321|
| Other Information Security Software   | 1832  | 2079  | 2285  |
| Security Services                     | 52,315| 58,920| 64,237|
| Consumer Security Software            | 5948  | 6395  | 6661  |
| **Total**                             | 101,544| 114,152| 124,116|

From Gartner’s data, the largest areas of cybersecurity market size for 2019 are Security Services ($64 billion), Infrastructure Protection ($15 billion), and Identity and Access Management ($10 billion).

¹[www.forbes.com/sites/rogeraitken/2018/08/19/global-information-security-spending-to-exceed-124b-in-2019-privacy-concerns-driving-demand/#5d828e9f7112](http://www.forbes.com/sites/rogeraitken/2018/08/19/global-information-security-spending-to-exceed-124b-in-2019-privacy-concerns-driving-demand/#5d828e9f7112)
Investments to Date

From the cybersecurity companies that are in Crunchbase’s data set, Table 14-2 shows a list of 25 categories of interest that have received private equity and public IPO investment from 2003 to 2019. When a private equity investment takes place, a venture capital or private equity firm is given stock in the company, and the company is given capital to spend on growing its business. When an IPO (initial public offering) takes place, a company that was previously private allows the public to buy its stock in exchange for capital. Both private equity investments and IPOs result in more funding for a company, and both types of investment are reflected in the aggregate figures in Table 14-2.

Table 14-2. Cybersecurity Categories and Funding

| Category                                      | Funding (Billions, Rounded) |
|-----------------------------------------------|----------------------------|
| 1 Network Security                            | $11.3                      |
| 2 Cloud Security                              | $10.4                      |
| 3 Artificial Intelligence                     | $7.7                       |
| 4 Mobile Security                             | $7.0                       |
| 5 Blockchain                                  | $6.1                       |
| 6 Cryptocurrency                              | $5.9                       |
| 7 Analytics                                   | $4.0                       |
| 8 Identity Management                         | $3.2                       |
| 9 Big Data and Database Security              | $2.9                       |
| 10 Social Media and Online Advertising Security| $1.8                       |

(continued)
Note that in Crunchbase’s data set, categories are not mutually exclusive. That is, a single company can be assigned multiple categories, such as “Network Security” and “Artificial Intelligence.” When a company is assigned multiple categories, as was the case with the overwhelming majority (94%) of them, it is an indication that the amount of funding that went into the company is being invested in those category areas. However, since it is unclear as to how much a particular company might be focusing on, say, Network Security as compared to, say, Artificial Intelligence, I do not make an attempt to guess. As such, one should not expect that

Table 14-2. (continued)

| Category                                      | Funding (Billions, Rounded) |
|-----------------------------------------------|-----------------------------|
| 11 Privacy                                    | $1.6                        |
| 12 Fraud Detection                            | $1.6                        |
| 13 Manufacturing and Industrial Security      | $1.4                        |
| 14 IoT Security                               | $1.3                        |
| 15 Risk Management                            | $1.3                        |
| 16 Developer Platform Security                | $1.2                        |
| 17 Telecommunications Security                | $1.0                        |
| 18 Compliance                                 | $0.8                        |
| 19 Consumer                                   | $0.7                        |
| 20 Healthcare                                 | $0.6                        |
| 21 GovTech                                    | $0.6                        |
| 22 Consulting                                 | $0.5                        |
| 23 Penetration Testing                        | $0.4                        |
| 24 Automated Driving                          | $0.3                        |
| 25 Cyber Insurance                            | $0.3                        |
summing up all the dollar amounts invested in the categories will sum up to $45 billion, the total funding amount that has gone into all companies. Also, while I show 25 categories in Table 14-2, note that it is not strictly the top 25 categories that Crunchbase used. As some categories were superfluous or not useful (e.g., “Software”) for the analysis, they have been excluded from Table 14-2. Especially with regard to categories with under $1 billion of investment attributed to them thus far, I report on only a subset of such categories that I felt were most interesting. That said, I focused on a subset of the top 150 categories where there was at least $100M in funding to date in the area, and I felt there was something to be learned from the category and its level of funding to date. (There was a total of over 500 categories in the data set.)

**Network Security**

Network security (including intrusion detection) is the most highly invested category. Firewalls are an example of a network security technology that have been around for the longest time. While they are a necessary but not sufficient basic defense, every six to seven years there have been new challengers to the prior generation of firewalls. Some of the earliest firewall companies were Checkpoint and Netscreen. They gave way to Palo Alto Networks, ZScaler, and FireEye/Mandiant. Approximately $11.3 billion has been invested in network security technologies, including firewalls.

**Cloud Security**

As organizations have been moving more and more systems to the “cloud” in data centers run by Amazon, Microsoft, and Google, among other competitors, a generation of cybersecurity companies has started to help provide defenses for such systems. Some of these companies have been acquired by cloud providers, and it remains to be seen if there may perhaps be room for such companies to exist independently. That said, it
also remains to be seen if cloud providers can offer the full stack of security services required, ranging from the analog of on-premise firewalls to application layer defenses. Approximately $10.4 billion has been invested in cloud security, not including private investments made by the cloud providers themselves. As that amount is on par with the investments made into network security, it is possible that such level of investment could be sufficient to date.

**Mobile Security**

Mobile security is a category that has been attributed to $7 billion worth of investment. Such investment is more than half of the amount that has gone into network security. In the mid- to late 2000s, there was quite a bit of fanfare about the growth of the mobile device market and the looming security issues that mobile devices and mobile apps could cause. Mobile device management companies were all the rage, and various services that could scan mobile apps for security and privacy issues started to appear on the market.

Proactive adoption and deployment of mobile security technology have resulted in a world in which mobile devices and vulnerabilities due to them are not a major root cause of breaches. Apple and Google employ multiple forms of both manual and automated scanning of mobile apps on their corresponding app stores. Although their defenses are definitely not perfect and there have been various published works (some by yours truly\(^2\)) on their limitations, we have also seen that mobile security issues are certainly not among the top six technical root causes of breaches that we covered in Chapter 1. However, as mobile phones continue to become more prevalent as our “first screens,” more investment may be required going forward. Investment that was previously made in defenses that

---

\(^{2}\)Eisenhaur, G., Gagnon, M.N., Demir, T., & Daswani, N. (2011). Mobile Malware Madness and How to Cap the Mad Hatters: A Preliminary Look at Mitigating Mobile Malware.
protect desktop and laptop computers should likely be transitioned to mobile phone defenses. Phishing, malware, and other forms of attack are likely to impact mobile phone users more going forward (even if they have not specifically been as much of an issue in the past). As such, it is likely that mobile security is a “sufficiently invested” category to date but may need further investment in the future.

Table 14-3. Cloud and Mobile Security Investment

| Category          | Approx $ Invested | Comments                                                                                                                                 |
|-------------------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Cloud Security    | $10.4B            | There has been significant investment, but slightly less than network security ($11B), not including investments by major cloud computing providers Amazon, Microsoft, and Google themselves. |
| Mobile Security   | $7.0B             | Mobile security is not specifically one of the major root causes of breaches (yet) and seems sufficient compared to categories such as network security ($11B). As mobile phones continue to become more prevalent as our “first screens” though, more investment may be required going forward. |

Market Size vs. Investment to Date

For some of the largest areas of 2019 market size, I have shown the total invested from 2003 to 2019 in Table 14-4. The network security market is quite a mature market with $13.3 billion spent annually and $11.2 billion invested over a 16-year period. By comparison, the market size of cloud security seems very small at only $500 million annually. That figure is expected to grow quickly over the next few years, but still seems small compared to the $10.4 billion invested in companies that are either
working on cloud security or doing something tangential enough to the area to be attributed with a cloud security categorization. Competing industry analyst firm Forrester reports that cloud security spending is much larger for 2019, though, and could be expected to grow to $12 billion by 2023. Looking at the market size for cloud security annually, one might hypothesize that investment in cloud security may be sufficient to date or even possibly overinvested to date until the actual annual market size and demand for cloud security grows.

Table 14-4. Comparison of Forrester Market Size to Total Invested for Selected Categories

| Market Size, Billions $ (2019) | Total Invested, Billions $ (2003–2019) |
|-------------------------------|----------------------------------------|
| Network Security              | 13.3                                   |
|                              | 11.3                                   |
| Cloud Security                | 0.5                                    |
|                              | 10.4                                   |
| Identity and Access Management| 10.6                                   |
|                              | 3.2                                    |
| Risk Management               | 4.7                                    |
|                              | 1.3                                    |
| Consumer Security Software    | 6.6                                    |
|                              | 0.7                                    |

Identity and access management, like network security, is a large, stable sub-area of security with $10.6 billion spent in 2019. There has been a relatively small amount of $3.2 billion invested in the area over the 16-year period. Similarly, for Risk Management, there has been relatively a small amount invested compared to the annual spend, with an annual spend of $4.7 billion and only $1.3 billion invested. For both Identity and Access Management and Risk Management, I would hypothesize

3www.infosecurity-magazine.com/news/cloud-security-spending-set-to-top/
that these areas are ripe for additional entrants into the market. Finally, Consumer Security Software has not received much private equity investment in the 16-year period but may be ripe for disruption as the market size is nine times the amount of investment, the largest ratio of market size to total invested of any of the categories previously discussed.

**Overinvested Areas**

Two areas that seem overinvested include blockchain ($6.1B) and cryptocurrency ($5.9B), as per Table 14-5. In particular, I would make an educated guess that more money has been invested in these areas than seems necessary to date, and I will discuss why shortly. I would guess that we should generally keep an eye out for further returns from the investments made thus far in these areas before investing more. At the same time, if some truly revolutionary startup comes together in one of these areas that is so above the bar with regard to its potential to make impact, it may deserve further investment, but one would have to be quite convinced against a backdrop of so much already invested.

**Table 14-5. Possible Overinvested Categories**

| Category         | Approx $ Invested | Comments                                                                 |
|------------------|-------------------|--------------------------------------------------------------------------|
| Blockchain       | $6.1B             | No one “killer app” apparent, aside from Bitcoin to date. By comparison, within just a few years after the birth of TCP/IP, email arose as a killer app. At the same time, the Web took two decades, so we should monitor over the coming decades to determine what additional investments are warranted. |
| Cryptocurrencies | $5.9B             | Even 10 years after the birth of Bitcoin, no other virtual currency has achieved similar dominance. |
Blockchain and Cryptocurrency

Note that blockchain and cryptocurrencies have been split out separately in our tables. Many cryptocurrencies are built on blockchains. Blockchain is a technology that allows one to securely maintain a distributed ledger of transactions, and blockchains can be used for many different types of transactions. Cryptocurrencies use blockchains to track transfers of digital currency, but blockchains can more generally be used to track contracts of all sorts.

Blockchains may indeed have many applications beyond cryptocurrencies, but it is unclear as to why most systems might require the level of decentralization that blockchains have to offer. I would argue that many such applications can be possible with a more centralized architecture in which at least some small number of parties trust each other. Certainly, Bitcoin has also evolved over time to a state in which there are a relatively small number of parties that can control the currency should they decide to collude.

That said, the reason for my “overinvested” hypothesis for blockchain and cryptocurrency is that there does not seem to be many “killer apps” that have achieved mainstream usage, either in consumer or business settings. Although the Bitcoin currency has been quite successful and is deeply technically interesting, mainstream consumers and businesses do not transact in Bitcoin, as of the writing of this book. Bitcoin has been successful in representing a relatively small, single-digit percentage of the value of the world’s gold and an even smaller percentage of the world’s currency. As of the writing of this book, there does not seem to be any other blockchain initiative that has achieved a significant fraction of what Bitcoin has achieved. (Some cryptocurrencies are catching up to Bitcoin, but I am not aware of any non-cryptocurrency blockchain applications that have enjoyed a similar level of success.)

While there is an overlap of more than $2 billion invested in companies that have been attributed both Blockchain and Cryptocurrency
categorizations, I list both categories separately as there is an important distinction between the underlying technology (blockchain) and an application of it (cryptocurrency). Both blockchain and cryptocurrency are likely overinvested, though, at least for the moment until more killer apps arise and we see further impact from investments to date.

By comparison, almost immediately after the formalization of TCP/IP (the protocol suite upon which the entire Internet is based), email arose in the form of the Simple Mail Transfer Protocol as a killer app, and advancements that enabled the Web as we know it today (including the Domain Name System) emerged relatively quickly thereafter. At the same time, the Web as we know it took another decade to mature and start commercialization, so we should monitor over the coming decades to determine what additional investments are warranted in the blockchain and cryptocurrency space.

Underfunded Areas

Most other areas in security that I now discuss seem underfunded based on the amount of investment that has been made to date and based on what the market will most likely need in the next several years. We discuss a few of these areas and why they are likely underfunded to date.

Artificial Intelligence

Approximately $7.7 billion of investment has been made to date in applications of artificial intelligence (AI), machine learning (ML), and natural language processing (NLP) to security. As there are not enough security analysts to manually look at alerts generated by defensive systems, there is a deep need to automate the processing of such alerts, and technologies such as AI and ML can help eliminate the need for as many security analysts.
Back in the early 1900s, many companies used to hire electrical engineers and keep them on staff in order to keep the electricity coming in. Today, electricity is a utility in which power companies keep electrical engineers on staff, and most companies can rely on the power companies to keep the electricity coming in. Such may occur with security analysts and engineers as well. Managed Security Service Providers (MSSPs) may be contracted by most companies, and they may use a combination of both automating many of the entry-level security analyst positions away and keeping more talented “second-level” security analysts and engineers on their staff to provide managed security services as a utility to other organizations. The bulk of the security market ($64 billion out of $124 billion) in 2019 as per Gartner is in fact made up of MSSPs and security consulting services, potentially exhibiting a trend toward outsourced security and a utility-like model. Although spending on MSSPs has varied over time, it is possible that over the long term only the largest of companies will hire information security teams that number in the hundreds of employees and manage the bulk of their security operations in-house, and the bulk of companies will rely more on MSSPs.

As there is a short supply of security analysts and professionals, there has been significant investment in applications of AI/ML to security to automate detection, attack containment, incident response, and recovery. As we had seen in the Target breach in 2013, Target was a FireEye customer and was seeing malware detections from their FireEye devices. Although those detections were being forwarded from their India-based team to their US-based team, there were too many such alerts that were mistaken for noise and could not be processed by the US-based team fast enough to stop the attack. Further investment in applications of AI can help in both eliminating the noise and detecting actual attacks with higher fidelity, also while using much less staff. Such automation through AI/ML will be employed both by the largest of companies and the MSSPs that supply security services for the majority of the rest of the world.
In addition to leveraging AI/ML to automate security systems, investment will also be required to ensure that AI/ML systems cannot be abused or taken advantage of by attackers. In one example, machine learning systems can be used to recognize particular human faces based on input from a camera, but an attacker can wear a set of special sunglasses such that when the attacker looks at the camera, the ML system misclassifies the attacker as another person. In the field of computer science, such attacks are called “adversarial machine learning” attacks, and as AI/ML systems will be used in applications ranging from automated driving to surveillance, further investment will be required to defend AI/ML systems from such attacks. AI/ML systems were typically developed with the assumptions that algorithm training and classification tasks are done based on “good” input, and not input that may be bad or adversarial, as will inevitably occur when such algorithms are used for security applications.

Adversarial machine learning focuses on the security of machine learning (security of ML) instead of using machine learning for security (ML for security). Most of the $7.7 billion of investment has been made to date in applications of artificial intelligence (AI) to security (such as ML for security), as opposed to security of AI/ML. Given that many consumer and enterprise systems ranging from autonomous driving to cyber defense are leveraging more and more artificial intelligence techniques, it is important to defend such techniques from adversarial input that could pierce AI-based defenses. Key threats to AI-based defenses include input manipulation, training data manipulation, model manipulation, input extraction, training data extraction, and model extraction. The interested reader is referred to “The Top 10 Risks of Machine Learning Security” by Gary McGraw, Richie Bonett, Harold Figueroa, and Victor Shepardson of the Berryville Institute of Machine Learning.4

---

4 Security Engineering for Machine Learning. McGraw, Bonett, Figueroa, Shepardson, Computer Volume 52 No. 8, IEEE Computer Society.

5 The Top 10 Risks of Machine Learning Security. McGraw, Bonett, Figueroa, Shepardson, Computer, vol. 53, no. 6, pp. 57-61, June 2020.
### Table 14-6. Artificial Intelligence Security Investment

| Category           | Approx $ Invested | Recommendation/Comments                                                                 |
|--------------------|-------------------|----------------------------------------------------------------------------------------|
| Artificial Intelligence | $7.7B             | **Ripe for further investment.** AI helps automate and leverage understaffed cybersecurity workforce (in the United States, hundreds of thousands of open positions, approximately 1M in workforce). Adversarial machine learning R&D also required for use of AI for security applications. |

### Table 14-7. Possible Underinvested Cybersecurity Categories

| Category       | Approx $ Invested | Recommendation/Comments                                                                 |
|----------------|-------------------|----------------------------------------------------------------------------------------|
| Analytics      | $4.0B             | **Ripe for further investment.** More needed as analytics and automation are required to compensate for cybersecurity staffing and skills gap. |
| Privacy        | $1.6B             | **May warrant further investment.** May not reflect private investment by Google, Facebook, etc., but private equity and public IPO investment is less than $5B fine FTC imposed on Facebook in 2019. Not sure if GDPR mandated DPOs thus far have budget or are just influencers. |
| Fraud Detection| $1.6B             | **May warrant further investment.** As of 2018 alone, FBI reports $2.7B in fraud annually. Exit multiples may be a concern for this category. |

---

*CyberSeek, [https://www.cyberseek.org/heatmap.html](https://www.cyberseek.org/heatmap.html).*
Cybersecurity companies that are attributed the Analytics category generally have some focus on using data analytics to help drive better security decisions and outcomes. As a former CISO, such analytics are critical in helping direct where future investments in a security program should go. For instance, if security analytics from a SIEM (security incident and event management) platform identify that particular adversaries are targeting an organization using a particular set of methodologies and techniques, one can use that information to beef up specific defenses that thwart such adversaries, as a complement to general defenses and countermeasures.

However, of the $45 billion that has been invested in cybersecurity, only $4.0 billion has been invested in Analytics. Given the thousands of breaches that have been taking place, including many dozens of mega-breaches, one might argue that as an industry we are still searching in the dark. Although we have outlined six key technical root causes in this book, every organization is different and may have different levels of susceptibility to the root causes. As such, security analytics tools have the potential to provide CISOs and other security leaders hard data and business intelligence types of analytics to help direct their spending decisions. CEOs typically have business intelligence teams that help aggregate and present analytical data about a business such that the CEO can make data-driven decisions about how to increase revenue and grow a company. Shouldn’t CISOs have similar tools and analytics at their disposal to help mitigate risk?

As a CISO, when I had to prepare a budget for the following year, I would sometimes employ consultants to interview more staff than I could on my own to gather input on where future spending should go and why. I was surprised with the relative lack of data that would come from our security tools and the reliance that we had on the expertise in the heads of our most senior staff. That is not to say that we should not leverage such human expertise, but the balance definitely seemed off—I feel that such
expert analysis should be based on both a combination of senior staff expertise and data from the security tools that are monitoring, detecting, and blocking attacks. Senior staff may be the best bet for helping fill in where we think we might be missing potential attacks (false negatives), but certainly analytics and hard data around what attacks are being attempted (true positives) should also be part of the equation.

As such, I believe that more can be fruitfully invested in security analytics to help make better decisions around where security program budget should be spent going forward.

Big Data and Database Security

Big Data and Database Security is an area for future investment with $2.9 billion attributed to it thus far. Through the 1980s and 1990s, most data that was stored in databases was of the form that can neatly be organized into tables and relations in which one or more table columns were functionally dependent on special columns called keys. Such databases were called relational databases as the columns of the tables that stored data were relationally structured in nature, and Structured Query Language (SQL) was the language of choice used to query or interact with such databases. Database security implementation typically involved specifying authorization, access controls, and confidentiality requirements in the form of SQL statements, in addition to the operating system and network layer security controls around the databases themselves.

Starting in the early 2000s, with more and more of the world’s data being semi-structured (as opposed to fully structured neatly in tables), in the form of web pages, XML (Extensible Markup Language) documents, JSON (JavaScript Object Notation), audio, and videos, semi-structured databases quickly grew in popularity. Most of the world’s data (simply in terms of the amount of petabytes stored) may eventually be stored in semi-structured databases (if that is not already the case), and as such implementation of security for such data is of growing importance.
Systems such as Hadoop, an open source implementation of MapReduce, a programming paradigm used for processing semi-structured data, were originally not built with security designed in. Much work to support basic authentication as well as access controls for data stored on Hadoop systems had to be done in the late 2000s. Hadoop is also just one of many such types of systems that support computation on Big Data. Cassandra, MongoDB, CouchDB, and Redis are other such systems.

Although attackers have been able to steal billions of records from relational databases, there is no reason to believe they are going to stop there. In 2017, for instance, tens of thousands of MongoDB databases holding as much as 93 terabytes of data\(^7\) were compromised and encrypted by ransomware, simply because the default communication channels that MongoDB used to talk to its administrators were left open and unauthenticated. Most of these MongoDB servers were hosted on the Amazon Web Services platform (making them easy for attackers to search for) and also had a default insecure configuration. As such, I believe that it is unlikely that all holes in these fairly new (e.g., less than a couple decades old) databases have been found, fixed, and forward-guarded against. Further investment in Big Data and Database Security will be worthwhile.

**Social Media and Online Advertising Security**

Social Media and Online Advertising Security has a special place in my (Neil’s) heart as I have worked both at Google and at Twitter in the past. After my time at Google, I co-founded a company by the name of Dasient that was focused on helping protect the largest ad networks from malicious advertising, or malvertising. Ads that conduct malvertising simply infect desktops and mobile devices via malware drive-by-downloads when they

\(^7\)www.bankinfosecurity.com/mongodb-ransomware-compromises-double-in-day-a-9625
are simply loaded and viewed—no user interaction or social engineering required.

Dasient was acquired by Twitter, and I spent my first year at Twitter focused on helping defend its advertising systems from click fraud. I then spent two years after that building an internal threat intelligence platform that would identify malicious links (drive-by-downloads, phishing, “regular” malware, etc.) that might appear in any of the 500 million tweets that would be posted per day. (Approximately one out of five tweets had a link of some sort, and the systems that we built would determine whether or not those links might pose phishing, malware, or other threats to the user.)

In my work at Twitter, I would also collaborate with security engineers, product managers, and CISOs at other social media companies including Facebook, Google, and Yahoo as we worked to protect the entire ecosystem from a whole variety of security threats. Alas, the job was bigger than I think any of us could have predicted. I left Twitter in early 2015 to take on the CISO role at LifeLock.

Although the online advertising ecosystem has made progress in fighting threats such as malvertising and click fraud, I am not quite sure that anyone predicted that ads used for political purposes (including disinformation and misinformation campaigns) could have had as much impact as they did. And it is not just about government and politics. There is no reason that corporations do not target each other in such campaigns. In addition, video content can be relatively easily created or manipulated these days. “Deep fake” videos, in which videos are created, altered, and/or heavily edited, can be made to seem authentic and used to achieve propaganda goals.

Some might argue (and I would agree) that the trustworthiness of information needs to become a security goal, just like confidentiality and basic message and data integrity have been. Trustworthiness is, of course, a much thornier topic from a technical perspective. As such, further investment is probably required in Social Media and Online Advertising Security. My expectedly biased view on this topic is that the $1.8 billion
that has been invested in companies that touch the topic of social media and online advertising security is probably just the tip of the iceberg in terms of what will be needed going forward.

**Privacy**

Privacy is another category for future, more aggressive investment given the mere $1.6 billion invested in the 17-year period. Facebook’s fine of $5 billion alone (imposed by the Federal Trade Commission in 2019) is more than three times the amount that has been invested in startups that have a Privacy categorization attributed to them. While some of the largest high-tech players such as Facebook and Google are making significant internal investments in privacy, the GDPR (General Data Protection Regulation) that they are working to satisfy applies to all businesses that have data about EU citizens. California has passed similar such privacy regulation in the form of the CCPA (California Consumer Privacy Act), and other states may follow suit. Even with huge security and privacy teams, some of the largest social media sites have found it challenging to comply, based on the magnitude and number of fines that have been imposed to date. The average organization will need tools and help if they hope to comply as well. As such, I believe that further funding (or at the absolute least, further focus) on Privacy from startups that are already in the cybersecurity space will be required.

**Fraud Detection**

Fraud Detection is another area for further investment, with $1.6 billion currently invested thus far. The FBI reported in 2019 that there was $2.7 billion in fraud in that year alone, and the number rose to that from previous years. There is therefore more fraud generally taking place every year than dollars invested to solve the problem over the 17-year period from 2003 to 2020. Note that the $1.6 billion figure does not include private investments that banks and other financial institutions make in internal
fraud management departments and technologies. Also, given the amount of existing fraud, credit card companies make the assumption that there will be billions of dollars of fraud per year as part of their business model. Although they have been accounting for fraud taking place as part of their business model, there is much room for improvement. If every dollar that is invested in reducing fraud can eliminate $10 of fraud every year ongoing, those dollars are likely very worthwhile investments. As such, I believe that fraud detection is another area ripe for future investment.

IoT Security

I mentioned IoT security in the introduction of this chapter as an underinvested category. Devices connected to the Internet first included minicomputers, then servers, then desktops, then mobile devices. The next wave of devices to be connected to the Internet will be the billions of web cameras, Alexas (voice command), Nest thermostats, Ring doorbells, home security systems, fitness devices, and wearable computers, among many others. These devices often have CPU power and other resources, but are not always being designed with security in mind. Such devices historically have not always had the ability to be patched should security vulnerabilities be found at some point and as a result significantly change the security landscape on the Internet.

The Mirai botnet of 2016 took some of the largest sites on the Internet offline with a distributed denial-of-service attack conducted by hundreds of thousands of compromised IoT devices and was one of the first big examples of how important it is to secure IoT devices. Since the Mirai botnet attack, many variants of it have continued to appear, even if their impact has not been as significant. It is possible that the Mirai botnet attack could be as significant for the Internet of Things as the Morris Worm, one of the first network worms to ever propagate on the Internet, was in 1988.
One of the main challenges in securing IoT devices is that they are often produced by manufacturers who are working to absolutely minimize the cost of the devices and at this early stage determine the potential market viability of their relatively new IoT device. Achieving security while also keeping costs low, maintaining convenience, and allowing for fast innovation has always been a challenge. Such challenges are worthwhile technical and business problems for new cybersecurity startups to focus on.

Internet of Things security has received $1.3 billion of investment. Given the overall growth in IoT devices expected in the coming years, one might expect that a level of investment commensurate with network security may be eventually required.

**Additional Underfunded Areas**

Finally, some areas to note into which less than $100 million of investment has gone thus far include drone security, virtual reality security, and quantum computing security. Those seem like exciting areas in which further investment will most likely be necessary, but the market need is far off enough that most startups would be concerned about the immediate market size and revenue opportunity. As has happened in many other areas (web security, IoT security, etc.), security investment may ramp up only once significant hacks or breaches occur with drones, virtual reality systems, and quantum computing! Unfortunately, history tells us that the world generally tends to be reactive when it comes to security, with significant amounts of investments being made only after breaches and hacks occur.
Root Causes

When I started doing research on cybersecurity investments, I was hoping to determine how much investment to date had been made into addressing the top six technical root causes of data breaches outlined in Chapter 1. The categories used on Crunchbase were significantly broader than most of the technical root causes: unencrypted data, phishing, malware, third-party risks, software vulnerabilities, and inadvertent employee mistakes. Some categories seem to be a superset of some of the technical root causes. For instance, Email Security is a superset that can help address phishing. That said, the Email Security categorization was not attributed to enough cybersecurity companies to account for even $500 million in investments, which suggests the categorization was not being used effectively in the data set.

In an attempt to identify the sets of cybersecurity startups that help address the root causes of breaches, I then turned to the descriptions of the companies in the Crunchbase data set. An example of such a description from the data set was “Agari provides email threat prevention and protection service leverages AI cybersecurity to protect organization.” Interestingly enough, while Agari is a well-known email security startup that helps organizations leverage the DKIM and DMARC security standards to prevent their domain names from being used by phishers, the Email Security category was not attributed to the company. In addition, it was a little disappointing that the description was not grammatically correct. Although the Crunchbase data are definitely not perfect by any means, there is much that we have been able to learn from them thus far.

Looking at the most frequently used words in cybersecurity company descriptions (eliminating “stop words”), the results were as shown in Table 14-8.
It seems that most cybersecurity companies therefore seek to be “platforms” and “solutions” as do many other enterprise software companies. Some types of cybersecurity companies do seem to focus on domain-specific areas, such as blockchain, mobile, or network security.

Instead of just looking for companies that may address root causes based on the most frequently used words in descriptions, I ran searches for specific terms that may be indicative of a company that focuses on root causes, and Table 14-9 shows the results.
Out of all the companies, less than a total of 5% of them typically describe themselves in a way that is focused on what they do to address the root causes of breaches. As companies may want to attempt to be as broad as possible, they can be fairly generic in terms of their descriptions.

### Summary

My advice to CISOs as well as VCs is to focus on the root causes of breaches. CISOs can get inundated with security vendor marketing or can sometimes get overly focused on checking the many, many boxes required to achieve a compliance bar. Compliance, however, is not synonymous with secure. In fact, most companies that get breached can usually produce their annual certificates of compliance. Sometimes compliance standards committees may then retroactively work to show that the breached organization actually was not compliant, in an attempt to show that their compliance certificate is actually meaningful. In addition, most of the items on compliance checklists could potentially be baggage from standards that are designed by committee.
Venture capitalists should invest in areas that are underinvested and address root causes as well as avoid areas in which there has already been much market hype. Focusing on root causes can help avoid the overwhelming majority of breaches, and compliance can mostly be achieved as a side effect of good IT, product, and information security hygiene.