Cyberproofing Corporate Governance

A SEMINAR PAPER PRESENTED
BY
ERAN SHMUELI
I.D 206574337
TO
THE FACULTY OF LAW
FOR
THE SEMINAR ON CORPORATE GOVERNANCE
AND CAPITAL MARKET REGULATION
DIRECTED BY
PROF. KOBI KASTIEL

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
BACHELOR OF LAW
WORD COUNT: 7,228

TEL AVIV UNIVERSITY
TEL AVIV, ISRAEL

JANUARY 31, 2024

Principal advisor: Professor Kobi Kastiel Eran Shmueli

Cyberproofing Corporate Governance

Abstract

In today's digital age, cybersecurity is an increasingly significant concern for corporations of all sizes. As technology advances, so do the risks of cyberattacks and data breaches, which can cause serious adverse effects on corporations. To address these risks, it is essential for corporations to implement strong cybersecurity measures.

This paper identifies two important and interconnected cybersecurity corporate governance policies that are often undeservedly overlooked by most corporations, except for the most technologically prominent ones.

One key aspect is a Vulnerability Disclosure Policy (VDP), which allows third-party reporting of vulnerabilities in a responsible and ethical manner. This allows corporations to fix cyber vulnerabilities before they can be exploited by malicious hackers.

In addition to a VDP, corporations may also implement a safe harbor policy. This policy provides legal protection for individuals who report vulnerabilities to corporations, allowing them to do so without fear of legal repercussions.

Often bundled together, these policies offer individuals a way to securely and ethically point out cybersecurity vulnerabilities to corporations without the fear of being legally implicated themselves.

However, a staggering number of the corporations that would allegedly benefit from these policies are either unaware or unconvinced of their importance. Therefore, these corporations *de facto* choose not to provide third parities with a secure option to disclose vulnerabilities.

This paper will make the claim that these two policies are so crucial for corporate cybersecurity, that corporate law ought to compel all corporations to *consider* their implementation. It will start by laying down the terminological framework necessary to discuss the cybersecurity issue at hand, and examine the role of cybersecurity VDPs in the field of cybersecurity and corporate law. After that, it will explore the corporate law considerations surrounding these policies, as well as best solutions for implementing and following them.

I hope this paper will provide a comprehensive understanding of the importance of cybersecurity VDPs in corporate law and corporate governance.

Contents

Listing of figures

1

Introduction

John Deere is the brand name of Deere & Company, a Fortune 500 American corporation listed on the New York Stock Exchange (NYSE) that mainly manufactures agricultural machinery, and is most recognized for its iconic green and yellow tractors. In particular, John Deere is also the biggest player in the high-tech farming market. Many of its products are Wi-Fi-enabled, app-controlled, and autonomously piloted machines, doing most of the agricultural work by themselves, instead of their owners.

But according to a bomb-shell presentaion by a hacker known as Sick Codes at the Def Con 29 hacking conference, a group of researchers conducted a "good faith" audit of John Deere and found a "tractor load of vulnerabilities".

These researchers, also known as "white-hat" hackers, discovered a way to jailbreak John Deere tractors, allowing all sorts of non-company sanctioned access to the devices. The researchers warned that a cyber attack on the customers of agricultural companies, spear-headed by John Deere, could severely compromise crop yield and trade secrets.

During the presentation, Sick Codes went through a series of vulnerabilities his group of researchers found, culminating in vulnerabilities allowing them to upload files to any user, log in as any user, destroy any farm, run any farm off the road, upload whatever they want, download whatever they want, destroy any data, log in to any third party accounts, and more. Basically, gaining access that enables them to do whatever they

wanted with anything they wanted on the John Deere Operation Center and have a rope on the whole organization.

But the implications of the findings are even more severe. Not only would such an attack could be devastating for the business of John Deere itself, but it could also pose an overwhelming national security risk on an unimaginable scale. Like the researchers, an attacker would be able to access farms across entire nations, and do things like overspray chemicals (such as insecticides) onto fields in such a way that could permanently damage the soil, rendering it unsuitable for crop growing many years and decades into the future, and potentially starve nations in the process.

With these jaw-dropping findings, the researchers raced to give all the information directly to John Deere in record time. Initially they were granted a Safe Harbour by John Deere, which allowed them to submit a form that got them into John Deere's "hacker one" program. Surprisingly to them, they were the first ones in the program. After looking more closely, they found out that the program was created that very same day and that it does not allow public disclosure. Furthermore, it was an NDA program (meaning John Deere could bury their findings while also preventing the researchers from sharing them with others). Subsequently, they left the program.

They promptly tried to contact the relevant employees of John Deere, in order to share the findings with the authorized individuals, capable of understanding the professional technical details and their implications – hopefully giving the company a chance to close any leaks in their cyber security before an ill-intentioned attacker would exploit them.

But the researchers had a hard time getting into contact with John Deere, Succeeding only weeks after. In April 2021, they resorted to printing out all of their findings and binding them into a book, hand-delivering it to the security office at the John Deere headquarters because they wouldn't reply to them in any way, shape, or form, just

reminding them that they have identified a large amount of devestating risks, namley, that they can log in as anyone in John Deere's platform, and that it should probably get looked into.

So it was pretty hard to get in touch with someone at John Deere, but eventually they handed it off to someone who probably had no idea what they were doing with it, and they didn't actually hear back from them about this.

Because John Deere still were not responsive, the researchers eventually had to get CISA involved, And CISA actually took over for a bit and helped John Deere remediate the vulnerabilities.

Because John Deere still were not responsive, the researchers eventually had to get CISA involved, And CISA actually took over for a bit and helped John Deere remediate the vulnerabilities.

Cybersecurity

Cybersecurity is the practice of protecting computer systems, networks, and data from cyber threats, such as unauthorized access, use, disclosure, disruption, modification, or destruction. Cyber threats can come from a variety of sources, including malware, ransomware, and other forms of cyberattack. The perpetrators of these are commonly known as hackers.

The field of cybersecurity encompasses a wide range of technologies, practices, and policies that are designed to protect against these threats. This includes measures such as firewalls, antivirus software, intrusion detection and prevention systems, and encryption. It also includes best practices to recognize and avoid potential cyber threats.

Cybersecurity is an increasingly significant field, as the use of computer systems and networks has become widespread in both personal and commercial contexts. The

increasing reliance on technology has also led to an increase in the number and sophistication of cyber threats. This makes it more pertinent than ever for corporations to have effective cybersecurity measures in place.

Regulation

Often, when cybersecurity issues arise in the field of corporate law, the conversation is about the relation ship between corporations and the state, whether by form of statues or the regulator-corporation relation ships. for example, in recent years the SEC introduced unbinding guidelines for publicly traded corporations on cybersecurity.

This paper claims that instead of a bilateral relationship, there is actually a Trilateral relationship between the regulator, the corporations, and third parties - which in the context of this paper are independent researchers who want to disclose vulnerabilities altruistically.

2

Cybersecurity Actors: the Good the Bad & the Ugly

2.1 Background

In order to understand where we are, we first need to understand the lay of the land. Before any changes could be recommended, we must first know with whom and with what we are dealing here. But in order to do that, we must take a look at the different actors playing in the theater of cybersecurity.

Throughout the paper I would be using the terms "hackers" and "researchers" interchangeably, which can inadvertently carry a euphemistic undertone in certain contexts. By using either term, I do not mean to confer moral gravitas on one while denying it to the other. In a sense, a criminal hacker also operates as a researcher, and what are traditionally called researchers could be engaging in borderline behaviors that would usually be associated with 'hackers'.

2.2 Main Actors

There are many types of cybersecurity actors known in the literature, mainly differentiated by their organizational affiliation (i.e state-sponsored, insiders,

hacktivists) and motivation (i.e for profit, for sport, for reputation, and altruism). However, for the purposes of this paper, there is no need to delve into all of them, and it will suffice to mention only the three well-known categories of independent researchers: white-hat, black-hat, and grey-hat hackers.[1]

When using the term "Independent Researchers" in this paper, my intention is to exclude all those individuals who practice cybersecurity research or hacking, whether legal or not, with any affiliation to an organization in the broad sense of the word. Meaning, I want to exclude state-sponsored individuals, and researchers who work for corporations. Basically, I want to this category to include all those who are not a part of or affiliated with any legally recognized organization. After that, we are left with individuals, who act independently, based on different types of motivations.

2.2.1 Black Hat Hackers

As their name might suggest, black hat hackers are the stereotypical bad-guy hackers everyone knows about from action movies and TV shows. Their objectives are criminal in nature, meaning they set out to find cybersecurity vulnerabilities of corporations and attempt to exploite them, or sell the information to others who might do that themselves. exploiting the vulnerability could mean different things depending on the circumstances. it could mean stealing information from a corporation, shutting down its operation electronically, or critically hurting it in exchange for ransom, and so forth.

---

[1] Chris Hoffman, *Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats*, How-To Geek (Apr. 20, 2014), http://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/.

2.2.2 White Hat Hackers

In stark contrast to their black hat counterparts, white hat hackers use their skills for constructive purposes. These ethical hackers are crucial in identifying and addressing security weaknesses. They conduct penetration tests - a simulated cyber attack - to assess the security of a system. Unlike black hats, white hats report vulnerabilities to improve the system's defenses, aligning their work with legal and ethical standards. They can (and often do) participate in bounty programs, where they are rewarded for disclosing security flaws, thereby contributing positively to the digital security ecosystem. However, the pursuit of bounties is not an integral part of their classification as white hats. Rather, bounties are a trending phenomenon by corporation to remedy the sub-optimal incentives white hats face in order to further incentivize them to find and disclose vulnerabilities

2.2.3 Gray Hat Hackers

Gray hat hackers occupy the ambiguous middle ground between black and white hats. Their actions, while not driven by malicious intent or personal gain, often skirt the edges of legality and ethical standards. For instance, a gray hat might penetrate a system without permission for sport—instead of exploiting or damaging it—but without reporting the vulnerability to the respective organization. This unauthorized access still constitutes a legal breach. Gray hats might also publicly disclose a security flaw, a move that, while not profit-driven, can lead to unintended harmful consequences as it opens a window for black hats to exploit the vulnerability before it is rectified.

2.3 Incentive Analysis

At this point, the astute readers are probably asking themselves why would anyone want to disclose vulnerabilities to corporations? In some cases the incentives are obvious. Hired researchers are payed exactly for that. In other cases, such as in the case of independent hackers things are a little bit more tricky. Black hat hackers stand the most to gain by finding cybersecurity vulnerabilities and either exploiting them personally, or selling the information to others who might exploite them, and in the process make a profit. Gray hat hackers, as mentioned before, exploite vulnerabilities for sport. they are not incentivised by personal financial gain. Rather, they pursue the intrinsic incentive of successfully exploiting a cybersecurity vulnerability in the technical sense, the accomplishment of overcoming the cybersecurity defenses of a corporation, and not by harming the target itself.

However, white hat hackers are the most interesting among them all. It is hard to explain their incentives. One explanation could be that it is a matter of reputation. By finding and disclosing cybersecurity vulnerabilities to corporations, one can gain experience and establish a track record over time of a talented and sophisticated cybersecurity researcher that is able to identify paralyzing cybersecurity vulnerabilities. Although white hat hackers do not gain directly from the disclosure itself, after building this sort of track record one can position itself among prominent leaders in the industry. Another non-utilitarian explanation, could be that white hat hackers just want to disclose vulnerabilities for altruistic reasons. After all, when it comes to cybersecurity, the question is just who gets to the vulnerabilities first. the cybersecurity vulnerabilities are already out there. If either corporations or white hat hackers who might come across vulnerabilities are not the first to identify and fix

vulnerabilities, it just means that the next person could be a black hat hacker. Since white hat hackers are familiar with that, they could just simply be acting out of a sort of 'good citizenship' incentive—meaning since I came across this vulnerability, if I will not disclose this, the next person will exploite this.

2.4 Conclusions

The definitions and distinctions made in this chapter offer a framework to discuss the main actors in the field of cybersecurity. However, it is important to point out that they are still not a set in stone, and others might use different terms for the same things, or base them on somewhat different distinctions.

The reason I am making the first distinction, between hired and independent researchers, is due to the fact that responsible disclosure and safe harbor policies *by themselves* offer no financial gain to the disclosing party. It means that in order to separate the contribution of these policies to a corporation's cybersecurity, one needs to isolate the disclosures that were made due to a financial incentive, such as a salary or a bounty reward, from those that were not. the secondary intent-based distinction, is made in order to identify even more precisely which hackers are the ones to whom these policies are addressed.

3

Vulnerability Disclosure Policies & Safe Harbor Policies

Vulnerability Disclosure Policies (VDPs) are formalized frameworks within which an organization outlines its processes and procedures for reporting, handling, and disclosing security vulnerabilities. These policies provide a defined channel for security researchers, customers, or employees to responsibly report potential security flaws to capable individuals within the organization who can take appropriate action. Safe Harbor provisions are often included in VDPs to protect well intentioned security researchers from legal consequences when disclosing vulnerabilities responsibly.

The first question at the center of this paper is whether VDPs significantly improve an organization's cybersecurity posture by enhancing transparency and enabling early detection of vulnerabilities, and should therefore be mandatory. Although implementing these policies does entail some administrative effort, this burden is generally minimal compared to the catastrophic consequences that could arise from the absence of such policies to individuals, businesses and countries. I will aim to empirically demonstrate that the adoption of these policies leads to an overall increase in an organization's cybersecurity resilience.

It is possible for even the most closely monitored corporations to benefit from having

more eyes examine their products' cybersecurity. The implementation of VDPs and safe harbor policies eliminates the legal chilling effect on researchers caused by fear of retribution or legal liability, prevents accidental leaks or unwise dismissals due to the information not reaching qualified employees, streamlines the disclosure process and allows corporations to respond promptly to threats. At the same time, they cost practically nothing to implement.

Therefore, it can be said that cybersecurity responsible disclosure and safe harbor policies are must haves in today's corporate arsenal against cyber threats, and corporations who's commercial operations entail a cyber dimension should have pretty good reasons not to use them.

4

A Troubled Relationship: Corporations & Researchers

4.1 History

The relationship between corporations and white hat hackers has often been a troubled one.

4.2 Why

It is hard to pin point exactly why there is often bad blood between corporations and cybersecurity researchers. however, it seems like it is rooted in the misguided thinking that by discouraging independent researchers and making them disappear, the problem would go away.

This is likely the result of a couple of issues corporations have trouble with in the cyber space.

4.2.1 Lack of knowledge

of cybersecurity cost, risk, and so forth

4.2.2 Counterintuitive

corporations think that burglers go after easier targets, it is good enough to be better than your neighbour. but in reality cyber hacking could be tacking place at multuple places at the same time, and there are no costs for taking what you want. So you actually need to be better than most hackers and not just better than your neigbour. They don't estemate the costs of a hack, the easiness of taking something, and the number of hackers that can target you. It's as if yout bicycle are accessable to all burglers in the world. There is an erronus natural estamate of all the elemnts regarding the risk. Our natural intuition is incorrect regarding all risk elements

4.3 How

Corporations that seek out to discourage white hat hacker from disclosing vulnerabilities can either try to deter them, or full-out initiate law suits against them.

4.3.1 Deter Researchers

Past legal proceedings of going after researchers serve as a very strong chilling effect that impedes them from reporting *ex ante*, unless they are explicitly authorized to report vulnerabilities to the corporations under responsible disclosure and safe harbour policies

4.3.2 Go After Researchers

Launching Legal Procedings against researchers.

4.3.2.1 Criminal Prosecution

Some what alleviated by the new DOJ guidelines that shift the burden of proof to corporations to show bad faith on the side of the white hat hacker.

There have been several instances where corporations have attempted to start criminal prosecutions against cybersecurity researchers for reporting cybersecurity vulnerabilities.

4.3.2.2 Civil Suits

4.3.3 Avoidance

4.4 Conclusions

Not only researchers do not disclose the vulnerabilities they uncover because of a lack of positive *ex ante* incentives, but also because of negative *ex ante* incentives. Some Technicality savvy corporations go further to address this issue than setting Disclosure and Safe Harbour Policies, and also introduce a positive *ex ante* incentive by setting Bug Bounties that offer disclosing parties a cash reward

4.4.1 Bugcrowd

4.4.2 Hacker 1

5

A Fringe Corporate Issue?

5.1 Background

As Christopher Mims titled his Wall Street Journal's article, every company is now a tech company.[2] When talking about cybersecurity in the corporate context, there is a real problem to demonstrate through data the scale and severity of the problem. That is due to the great significance of *ex ante* incentives and the lack of transparency of corporations when it comes to sharing statistics about the number of vulnerabilities that were exploited or disclosed to them.

Ideally, the best way to show the importance of VDPs would be to look at all cybersecurity breaches in all of history, and figure out how many of the targeted companies without these policies. The issue is that this data is not available publicly. Therefore one needs to look elsewhere.

Another option is picking a few example of companies that experienced major cybersecurity breaches, and see if they had these policies in place or not. However, the problem is that this reasoning could be countered by the (often correct) argument of cherry picking.

[2] *Every Company Is Now a Tech Company*, The Wall Street Journal, https://www.wsj.com/articles/every-company-is-now-a-tech-company-1543901207.

So the question is what sort of objective data can demonstrate both the existence of the problem, meaning it is not just a fringe issue but really a problem that plagues corporations, and also how severe the problem is, meaning exposing corporations to existential risks.

The first indication, is that it is a general rule of thumb—a common practice among white hat hackers *themselves*—not to bother with corporations who do not have VDPs because it is much riskier for them personally. That is not to say they would never take that risk, such as in the example of John Deere, but it makes it much less likely from the practice standards of white hat hackers. However, by itself, this is not enough of an evidence to really give any sense of scale and severity.

Another thing that one could do is looking at all the fortune 500 companies, lets say, and dividing them into a group with VDPs (the treatment group) and a group without them (control group). After that, one would look at all the significant cybersecurity hacks that happened, and see if there is a correlation between the number of them and the existence of a VDP.

A third option is a bit more difficult, but seems to me like the best way to demonstrate the claims of this paper. The Common Vulnerabilities and Exposures (CVE) system is a method for cataloging publicly known information-security vulnerabilities and exposures. It is maintained by The MITRE Corporation, under the United States' National Cybersecurity FFRDC, with support from the US National Cyber Security Division of the Department of Homeland Security. Launched in September 1999, this system assigns CVE IDs to each vulnerability. These IDs are utilized in the Security Content Automation Protocol and are recorded in both MITRE's system and the US National Vulnerability Database. CVEs are unique identifiers that are given to specific vulnerabilities that are disclosed to corporations.

However, these corporations do not necessarily have VDPs policies. a CVE identifier is not given to every vulnerability that is uncovered. If for example a hired researcher of a corporation finds a vulnerability, it is usually not publicly reported to the public and therefore will not be assigned with a CVE, since corporations usually would rather not sharing such information.

Although ideally it would be best to look at all vulnerabilities and not just the publicly reported ones, this systems allows us to look at a very large portion of all vulnerabilities—even though we could never know the true scale of vulnerability prevalence. By looking at the CVEs of corporation over time, one could look for a change of trend in the number of CVEs after the introduction of VDP to a certain set of corporations (e.g Fortune 500, S&P 500). After that, one would need to rule out those companies that have bug-bounty programs. That is because bug-bounties introduce an additional financial incentives to disclose. If we trim the data set to include only companies without bug-bounties, we would be left only with the independent researchers disclosures that are not financially motivated. Also, vulnerabilities reported by hired researchers are carved out from the VDP because they are protected by contracts, and therefore do not need to go through a public procedure of disclosure. In a large enough of a group, a correlation is likely not accidental.

Again, given the lack of transparency it is really hard to claim the evidence is conclusive. Nonetheless, I think this way of a approximation is a very good way to give *an idea* of how problematic things really are.

5.2 Methodology

This data was hand coded by first compiling a list of all S&P 500 companies listed on the iShares Core S&P 500 ETF index fund, as of the end of 2022.[3] Then I went through the list, and removed any overlaps caused by having more than one class of shares of the same corporation on the list. After that, I removed any component of the list that is not a share of a corporation, such as derivatives and currencies- Being left with a list of the 500 biggest corporations. I then attempted to look specifically at the flagship brands of those corporations, much in the same way one would do if they were about to disclose a vulnerability, since vulnerabilities are found in specific products or services. Therefore, I amended the list to reflect the flagship brands of those corporations when ever I identify they had any prominent one (e.g, Google instead of Alphabet, and Facebook instead of Meta).

Because the scale of 500 companies was too big, I decided not to continue the research with this set of companies. Instead, I decided to look at the top 50 companies with the highest number of public disclosures.[4] This is a much more manageable number of companies, and the relatively high number of data points would allow to more easily see if a particular date when a policy was enacted also correlates to an increase in the number of disclosures afterwards.

After the list was complete, I began to collect information about the corporations' cybersecurity policies, namely, if they have a VDP, a safe harbor policy, and if they offer any bug-bounties. To accomplish this, I used well-known methods among the white hat

[3] *iShares Core S&P 500 ETF*, iShares, https://www.ishares.com/us/products/239726/ishares-core-sp-500-etf.

[4] *Top 50 Vendors by Total Number of Distinct Vulnerabilities*, CVE Details, https://www.cvedetails.com/top-50-vendors.php?year=0.

community itself. For example, leading websites such as Bugcrowd, hackerOne, and Disclose.io offer up-to-date information regarding many companies' status of VDP and safe harbor policies and bug bounties. The data with regard to corporations' policies was gathered in the following way. I first looked for the existence of a `security.txt` file in a company's `/.well-known/` website directory.[5] Second, I went through all three of Bugcrowd, hackerOne, and Disclose.io, to see what information existed over there. Third, I Googled the terms "vulnerability," "disclosure," and "security" along with the company name and flagship brand.

After I had this information, I then tried to look into the companies that had a VDP, and try to asses what was the exact date it went into effect. I first started by looking at the usual trio of suspects—Bugcrowd, hackerOne, and Disclose.io—since they sometimes provide that information. Second where that information wasn't available, I tried to look for an alternative solution. what I came up with was using the Internet Archive's Way Back Machine[6] —that stores copies of various web pages from snapshots at specific points of time. This tool allowed me to look at a web page and see how it evolved and changed over time. this method was applied to all three ways of finding if a company had a VDP as described above. The earliest date where a VDP was found was registered by me as the date the VDP went into effect.

Based on the date when a VDP went into effect (if there was one), I then set that year as year "0", and gathered the data on the number of CVEs that were filed to that company in the five years before and four years after the fact. By synchronizing this information to all companies as to make year "0" the same for all of them, I could now

[5] E.g *Tesla Security Policy*, Tesla, https://www.tesla.com/.well-known/security.txt.
[6] *Wayback Machine*, Internet Archive, http://wayback.archive.org/.

look at how the introduction of a VDP had influenced the number of CVE reports. I then measured the percentage point increase or decrease in the number of CVE reports from year to year, and averaged the results of each yearly change in all companies.[7]

It is important to state that some companies that seem not to offer these policies or bug bounties, do in fact offer them. I conducted my survey independently, within the confines of my scarce resources, and it is important to note that depending on when this is being read - companies can also change their policies over time - especially in the ever changing world of cybersecurity. However, despite those limitations, it is also important to mention that finding those policies should not be hard. If companies "hide" their VDPs - white hat hackers will not be able to find them too. By design they should not be hard to find, and if they are, they are as good as not having them at all.

It is also important to note that this survey didn't intend to asses the effectiveness of the companies' policies, and it is beyond the scope of this paper. I neither have the technical skills nor is it important for the topic of this paper.

5.3 Results

According to the survey, among the S&P 500 companies only 163 companies had some sort of a vulnerability policy.[8] Rapid7's 2021 Industry Cyber-Exposure Report (ICER) found that out of the corporations listed on the Fortune 500, only around 20% have a Vulnerability Disclosure Policy.[9]

The results of the survey about the prevalence of VDPs among S&P 500 companies

---

[7] Figure 5.3

[8] Figure 5.1

[9] *2021 Industry Cyber Exposure Report*, Rapid7, https://www.rapid7.com/research/report/2021-industry-cyber-exposure-report/.

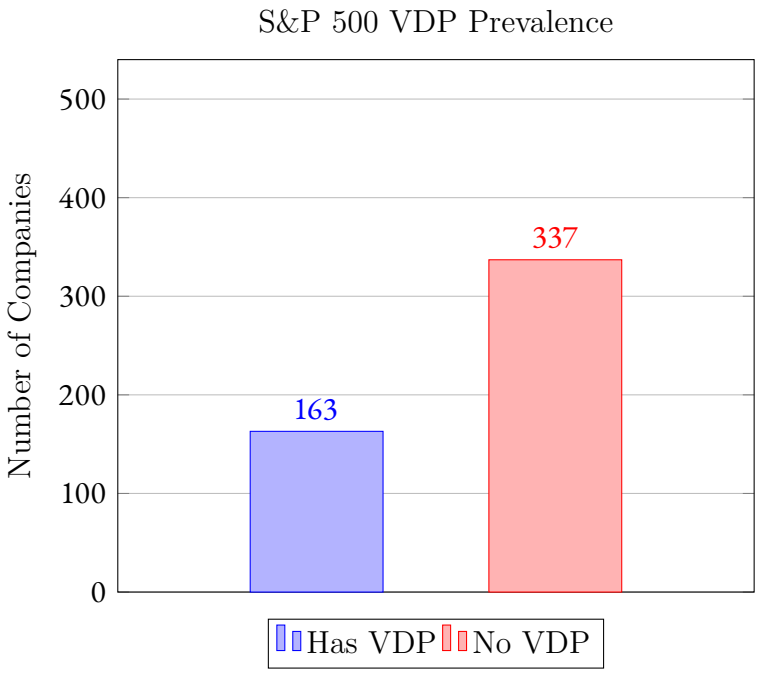

Figure 5.1: S&P 500 VDP Prevalence

reveals that 163 of them have such a policy. Meaning 1 in 3 companies. Although Rapid7's report (which was the only one I could find trying to measure the same thing) surveyed the Fortune 500 companies, and I did the S&P 500, as far as they overlap enough—it seems like there has been a positive trend in this short amount of time of companies adopting VDPs.

when you break down the information to quintiles, more details are revealed. In the first quintile, the proportions are exactly opposite—only 1 in 3 companies doesn't have a VDP, and the other 2 companies do have one. In the following 4 quintiles the numbers vary, with the portion of companies that have a VDP in each ranging from 20 percent to 35 percent. So this give the impression that even amongst the largest and most profitable companies in the world, there is a fundamentally different approach on how to address these issues depending on where on the ranks you are.

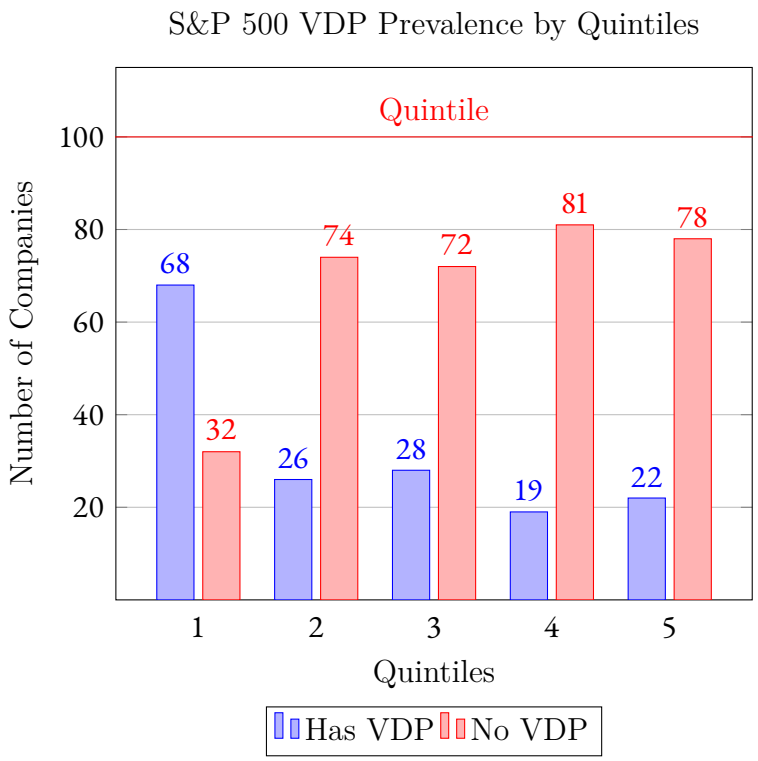

Figure 5.2: S&P 500 VDP Prevalence by Quintiles

With regard to the survey of the 50 companies on the correlation between a VDP and the number of CVE-vulnerabilities that were reported, the information suggests a very strong correlation on its face (Figure 4.3). There are a few things worth mentioning here. the data shows that the average increase in reporting from year to year in the years before a VDP was introduced was big (30 percent to 110 percent a year). However, the increase on the second year*after* a VDP was introduced suddenly sky rocketed by a staggering to 294 percent. This is quite an abrupt change. Not less interestingly, it seems like in the year after a VDP was introduced it had no effect on the number of CVE reportings—falling in the same range it used to be in the years before (30 percent to 110 percent). On the third year after a VDP was introduced, the number of CVE

reportings is almost exactly the same as the year before—only a 2 percent increase. And finally, on the forth year after a VDP was introduced, the number of reportings compared to the previous one was again large (130 percent) but not by an overwhelming amount compared to the years before the VDP was introduced.

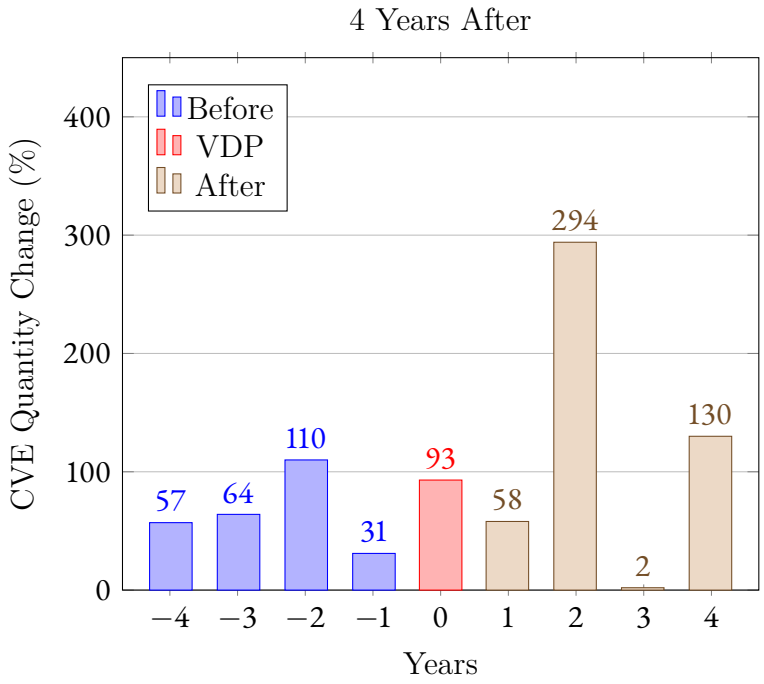

Figure 5.3: Average Change of CVE Quantities Per Year (Percent): 4 Years

5.4 Discussion

I suspect the big difference in the S&P 500 survey between the first quintile and the other four was not caused by the balance in their bank accounts. Due to the constraints on what I was able to achieve within the relatively short time frame in which I wrote the paper, I couldn't verify this suspicion, but in a more extended version of this paper I am hoping to be able to show that this chasm could be caused due to a much more

significant prevalence of "tech" companies in the first quintile compared to the the other four. This in turn, forces these companies to take a much more pro-active approach—at least because they understand the playing field better if for no other reason.

Concerning the results of the survey on the correlation between the CVE vulnerability reportings and the introduction of a VDP, it defiantly seems like the introduction of a VDP had a disruptive effect on the number of reports of vulnerabilities, and that they are correlated. I'm not sure how to account for the fact that the sudden increase only occurs (or only manifests itself) on the second year after the introduction and not the first. However I think I do have an explanation for the almost zero increase on the third year could be explained. If for some reason white hat hackers were unaware of the fact that a given company introduced a VDP a year after it did, they definitely paid attention by the second year. And once they knew of it, the sharp and significant increase in reporting suggests that potentially a lot of people were suddenly looking for the vulnerabilities to report them. But not all vulnerabilities are equal, and one can easily imagine that some 'fruits' may be hanging lower than the others. Not all hackers have the same skills and experience too. If that is the case, an extreme increase in the number of 'more obvious vulnerabilities can result with stagnation on the next year—sort of like a crowed of people clearing out all the low hanging fruits on a given tree. The forth year seems to suggest some return to pre-VDP normalcy, although still somewhat effect by the disruption resulted by the introduction.

A very important thing which I was not able to do within this course's time frame was to contrast this information with the data I had on the prevalence of bug bounty programs. Since I am planning to continue this research, I will take this on in a newer version of this paper. But essentially, I want to make sure that a correlation is independent of any influence an existing bug bounty program has on the number of

reporting. In order to do that I would probably also also need to increase the sample size.

6

Possible Solutions

The increasing push in recent years to address corporate cybersecurity risks by using corporate law can be especially felt, As Gail Weinstein, Philip Richter, and Steven Epstein noted, by the sudden increase in the number of *Caremark* cases brought to the Delaware Court of Chancery on cyber related grounds. The increase began following the Delaware Supreme Court's 2019 *Marchard v. Barnhill* decision, in which the Supreme Court, overturning the Court of Chancery, found that the defendant directors were potentially liable under Caremark.[10]

However, a *Caremark* claim is only one tool, one solution, through which corporate law can address cybersecurity risks. The most important question of this paper, is what would br the best solution to implement responsible disclosure and safe harbor policies. this chapter will examine whether it is a change in positive law or expansion of the *Caremark* standard to encompass the lack of responsible disclosure and safe harbor.

---

[10] *See* Gail Weinstein, Philip Richter, and Steven Epstein, *Chancery Court Addresses Board Responsibility Under Caremark for Cybersecurity Risk*, Harv. L. Sch. F. on Corp. Governance & Fin. Reg. (Nov. 17, 2022), https://corpgov.law.harvard.edu/2022/11/17/chancery-court-addresses-board-responsibility-under-caremark-for-cybersecurity-risk/.

6.1 The Caremark Standard

The famous *Caremark*[11] case established the key precedent surrounding corporate director responsibilities and liability when it comes to the exercise of risk oversight.[12] Ever since, its omnipresence in the back of directors' heads fundamentally shaped the ways in which they operate *ex ante*.

A successful *Caremark* claim requires that the plaintiff shows: (i) the directors "utterly failed" to put into place a board-level system to obtain information about and monitor the critical risks facing the company, or (ii) if such a system is in place, they "consciously failed" to monitor or oversee its operation.[13]

The application of the *Caremark* standard on cyber related claims was most recently examined by the Delaware Court of Chancery when it dismissed a derivative suit asserting Caremark claims against the directors of SolarWinds Corporation for their alleged failure to oversee the company's cybersecurity risk.[14]

The court emphasized in SolarWinds that no Delaware decision yet has found

---

[11] In re Caremark Int'l, 698 A.2d 959 (1996) (Directors are potentially liable for a breach of duty to exercise appropriate attention if they knew or should have known that employees were violating the law, declined to make a good faith effort to prevent the violation, and the lack of action was the proximate cause of damages.)

[12] Paul Ferrillo and Christophe Veltsos, *Boards Should Care More About Recent "Caremark" Claims and Cybersecurity*, Harv. L. Sch. F. on Corp. Governance & Fin. Reg. (Sep. 15, 2020), https://corpgov.law.harvard.edu/2020/09/15/boards-should-care-more-about-recent-caremark-claims-and-cybersecurity/ (criticizing the . . .).

[13] For example by deliberately disregarding "red flags" that put them on notice of the likelihood of potential corporate trauma relating to such risks (thus disabling themselves from being informed of risks or problems requiring their attention). *See* Gail Weinstein, Philip Richter, and Steven Epstein, *Chancery Court Addresses Board Responsibility Under Caremark for Cybersecurity Risk*, Harv. L. Sch. F. on Corp. Governance & Fin. Reg. (Nov. 17, 2022), https://corpgov.law.harvard.edu/2022/11/17/chancery-court-addresses-board-responsibility-under-caremark-for-cybersecurity-risk/.

[14] Id Gail Weinstein

directors potentially liable under *Caremark* based on a "failure to monitor business risk" outside the context of "noncompliance with positive law."[15]

1. The directors did not act in violation of "positive law."
2. The directors did not ignore "red flags."
3. The directors did not "utterly fail" to establish an oversight mechanism for cybersecurity risk.

6.2 Statute

6.3 Regulation

6.4 Discussion

6.5 Conclusions

[15] Id Gail Weinstein.

7

Conclusion

This research was not perfect. Academically speaking, this was my first real attempt at trying to do an empirical research of any kind and scale. In this exploration I have delved into the intricate and often challenging world of white hats and VDPs and their role in the aggregate cybersecurity of corporations. My findings point to a landscape marked by significant variation in the adoption and effective implementation of these policies, highlighting a fragmented approach in the industry's response to cybersecurity threats. A key insight from my research is the vital yet under-recognized role played by white hat hackers. Their efforts in identifying system vulnerabilities are crucial, yet they face an array of obstacles, such as the absence of standardized processes (VDPs). This situation not only hampers the effectiveness of individual corporations' cybersecurity measures but also impacts the broader digital security infrastructure.

My attempt to empirically establish a correlation between the presence of VDPs and the frequency of vulnerability reporting encountered certain limitations, particularly in terms of data accessibility and transparency. This issue reflects wider challenges faced in cybersecurity research. Though this paper represents only a preliminary attempt to uncover the relationship between the introduction of VDPs and the incidence of vulnerability reports, it seems to me that the findings are promising. They suggest a potential correlation, even if not to the extent indicated by the initial data. This

discrepancy is partly due to not yet accounting for the influence of bug bounty programs in the analysis. Reflecting on these findings, it's evident that enhancing corporate cybersecurity is a multifaceted and ongoing challenge. The research underscores the need for more uniform adoption of VDPs and greater collaboration among cybersecurity stakeholders.

while this study has started to piece together a complex puzzle, it also opens the door to further research and dialogue. It calls for a continued, collaborative effort to adapt and refine strategies against evolving digital threats, paving the way for a more secure and resilient digital corporate landscape.

A

S&P 100 Companies

The S&P 100, a sub-set of the S&P 500®, is designed to measure the performance of large-cap companies in the United States and comprises 100 major blue chip companies across multiple industry groups. Individual stock options are listed for each index constituent.[16]

[16]https://www.spglobal.com/spdji/en/indices/equity/sp-100/#overview

S&P 100 Companies Table

No.	Corporation	Weight (%)	Sector
1.	APPLE INC	9.22	Information Technology
2.	MICROSOFT CORP	8.05	Information Technology
3.	ALPHABET	4.72	Communication
4.	AMAZON COM INC	3.76	Consumer Discretionary
5.	BERKSHIRE HATHAWAY INC CLASS B	2.69	Financials
6.	**********	2.23	Communication
7.	JOHNSON & JOHNSON	2.16	Health Care
8.	UNITEDHEALTH GROUP INC	2.14	Health Care
9.	EXXON MOBIL CORP	2.14	Energy
10.	JPMORGAN CHASE & CO	1.92	Financials
11.	NVIDIA CORP	1.87	Information Technology
12.	VISA INC CLASS A	1.71	Information Technology
13.	PROCTER & GAMBLE	1.7	Consumer Staples
14.	HOME DEPOT INC	1.55	Consumer Discretionary
15.	TESLA INC	1.5	Consumer Discretionary
16.	MASTERCARD INC CLASS A	1.49	Information Technology
17.	CHEVRON CORP	1.48	Energy
18.	META PLATFORMS INC CLASS A	1.41	Communication
19.	ABBVIE INC	1.33	Health Care
20.	MERCK & CO INC	1.33	Health Care
21.	ELI LILLY	1.31	Health Care
22.	PFIZER INC	1.26	Health Care
23.	PEPSICO INC	1.16	Consumer Staples
24.	COCA-COLA	1.14	Consumer Staples
25.	BANK OF AMERICA CORP	1.12	Financials

TABLE CONTINUED FROM PREVIOUS PAGE

No.	Corporation	Weight (%)	Sector
26.	BROADCOM INC	1.1	Information Technology
27.	THERMO FISHER SCIENTIFIC INC	1.05	Health Care
28.	COSTCO WHOLESALE CORP	1.01	Consumer Staples
29.	WALMART INC	0.96	Consumer Staples
30.	CISCO SYSTEMS INC	0.95	Information Technology
31.	ABBOTT LABORATORIES	0.94	Health Care
32.	MCDONALDS CORP	0.93	Consumer Discretionary
33.	VERIZON COMMUNICATIONS INC	0.83	Communication
34.	DANAHER CORP	0.82	Health Care
35.	WALT DISNEY	0.82	Communication
36.	ACCENTURE PLC CLASS A	0.82	Information Technology
37.	NEXTERA ENERGY INC	0.79	Utilities
38.	COMCAST CORP CLASS A	0.77	Communication
39.	TEXAS INSTRUMENT INC	0.76	Information Technology
40.	WELLS FARGO	0.76	Financials
41.	LINDE PLC	0.75	Materials
42.	NIKE INC CLASS B	0.75	Consumer Discretionary
43.	PHILIP MORRIS INTERNATIONAL INC	0.75	Consumer Staples
44.	ADOBE INC	0.74	Information Technology
45.	BRISTOL MYERS SQUIBB	0.72	Health Care
46.	SALESFORCE INC	0.7	Information Technology
47.	CONOCOPHILLIPS	0.69	Energy
48.	RAYTHEON TECHNOLOGIES CORP	0.69	Industrials
49.	AMGEN INC	0.69	Health Care
50.	NETFLIX INC	0.69	Communication

TABLE CONTINUED FROM PREVIOUS PAGE

No.	Corporation	Weight (%)	Sector
51.	HONEYWELL INTERNATIONAL INC	0.67	Industrials
52.	AT&T INC	0.65	Communication
53.	ORACLE CORP	0.63	Information Technology
54.	QUALCOMM INC	0.62	Information Technology
55.	INTERNATIONAL BUSINESS MACHINES CO	0.62	Information Technology
56.	CHARLES SCHWAB CORP	0.62	Financials
57.	UNION PACIFIC CORP	0.62	Industrials
58.	UNITED PARCEL SERVICE INC CLASS B	0.62	Industrials
59.	CATERPILLAR INC	0.61	Industrials
60.	LOWES COMPANIES INC	0.59	Consumer Discretionary
61.	STARBUCKS CORP	0.57	Consumer Discretionary
62.	INTEL CORPORATION CORP	0.57	Information Technology
63.	GOLDMAN SACHS GROUP INC	0.57	Financials
64.	CVS HEALTH CORP	0.56	Health Care
65.	MORGAN STANLEY	0.55	Financials
66.	BOEING	0.55	Industrials
67.	BLACKROCK INC	0.54	Financials
68.	ADVANCED MICRO DEVICES INC	0.52	Information Technology
69.	GILEAD SCIENCES INC	0.52	Health Care
70.	LOCKHEED MARTIN CORP	0.51	Industrials
71.	MEDTRONIC PLC	0.49	Health Care
72.	AMERICAN TOWER REIT CORP	0.49	Real Estate
73.	CITIGROUP INC	0.44	Financials
74.	MONDELEZ INTERNATIONAL INC CLASS A	0.43	Consumer Staples
75.	AMERICAN EXPRESS	0.43	Financials

TABLE CONTINUED FROM PREVIOUS PAGE

No.	Corporation	Weight (%)	Sector
76.	T MOBILE US INC	0.42	Communication
77.	PAYPAL HOLDINGS INC	0.42	Information Technology
78.	BOOKING HOLDINGS INC	0.41	Consumer Discretionary
79.	ALTRIA GROUP INC	0.39	Consumer Staples
80.	GENERAL ELECTRIC	0.39	Industrials
81.	DUKE ENERGY CORP	0.38	Utilities
82.	SOUTHERN	0.37	Utilities
83.	TARGET CORP	0.34	Consumer Discretionary
84.	3M	0.33	Industrials
85.	COLGATE-PALMOLIVE	0.31	Consumer Staples
86.	US BANCORP	0.3	Financials
87.	EMERSON ELECTRIC	0.27	Industrials
88.	GENERAL DYNAMICS CORP	0.26	Industrials
89.	GENERAL MOTORS	0.25	Consumer Discretionary
90.	FORD MOTOR CO	0.24	Consumer Discretionary
91.	METLIFE INC	0.22	Financials
92.	AMERICAN INTERNATIONAL GROUP INC	0.22	Financials
93.	FEDEX CORP	0.21	Industrials
94.	EXELON CORP	0.2	Utilities
95.	CHARTER COMMUNICATIONS INC CLASS A	0.19	Communication
96.	DOW INC	0.19	Materials
97.	SIMON PROPERTY GROUP REIT INC	0.18	Real Estate
98.	CAPITAL ONE FINANCIAL CORP	0.18	Financials
99.	BANK OF NEW YORK MELLON CORP	0.17	Financials
100.	BLK CSH FND TREASURY SL AGENCY	0.16	Cash and/or Derivatives