How Vulnerabilities Became Commodities. The Political Economy of Ethical Hacking (1990-2020).

David Bozzini

How Vulnerabilities Became Commodities

The Political Economy of Ethical Hacking (1990–2020).

Prof. David Bozzini
Anthropology Unit, Department of Social Sciences
University of Fribourg, Fribourg, Switzerland

david.bozzini@unifr.ch

Vulnerabilities are forever!

Cybersecurity has come to constitute a major concern in recent years. Viruses and secret backdoors have been politicized and weaponized, but they have also been marketized—sold in closed and hidden markets for underground operations or leveraged to extort money.[1] At the core of these operations, be they involved with military, law enforcement, or criminal activities, lie digital vulnerabilities that had been kept secret. These vulnerabilities represent cracks in digital systems that can be exploited to introduce malware to networks or serve as hidden backdoors, which enable malicious actors to monitor activity and exfiltrate or modify data. In this way, they can disrupt the operations of critical infrastructures, hospitals, schools, government administrations, voting machines, manufacturers, financial institutions—and essentially anything else connected to the Internet, likely including the cell phone in your pocket and that new car you've been thinking of buying.

Considering the near-universal digitalization and datafication of all goods and services, this frightening potential has become a prominent concern. The more code there is, the more vulnerabilities there are to exploit.[2] With industries increasingly embracing the digital turn (e.g., transportation, healthcare, retail), new code will certainly be vulnerable, and processes to improve the digital security of products will take time to be properly

1 Common extortion schemes include ransomware encrypting systems. Ransomware generates hundreds of millions of USD per year for successful groups, such as Conti, which is individually believed to have extorted at least $180 million from victims in 2021. Total ransoms paid that same year are estimated to be more than $600 million according a recent report from Chainanalysis (https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/). As the attacks on Colonial Pipeline, MS Exchange, Kaseya, and Solarwind show, data leaks and disruption have massively increased in scale in recent years. See the following articles for more information on this topic: https://krebsonsecurity.com/2020/12/solarwinds-hack-could-affect-18k-customers; https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software.

2 Of course, this depends on the quality of the code. In general, however, cybersecurity experts argue that code will be vulnerable for at least the foreseeable future despite the steady increase in testing and hardening among software companies and open-source initiatives over the last two decades.

implemented. This complex situation has led to the emergence of a market for vulnerability information. Hackers[3] who uncover vulnerabilities can sell information on them through a hidden market[4] to criminal organizations or vulnerability brokers,[5] who then relay that information to intelligence, military, and law enforcement agencies. This shady and relatively unknown offensive market emerged in and has been developing since the 1990s.

However, cyber-defense capabilities and mechanisms have developed alongside this offensive market. Companies have invested in security and testing teams, digital security audits are now required by law in many polities around the world and the cybersecurity industry has grown considerably since the earliest anti-virus and firewall companies. In fact, processes, mechanisms, and institutions aimed at securing digital systems have all developed considerably since the mid-1980s. One such mechanism is vulnerability disclosure, which entails reporting a vulnerability to a company or organization in order to improve the security of its infrastructure, products, or services. This is often called "ethical hacking."[6] Notably, however, vulnerability disclosure existed well before computers; in fact, it was already a known practice in cryptography (Kerckhoffs 1883) and locksmithing (Hobbs 1853) back in the 19th century.

My research focuses on the defense mechanism of vulnerability disclosure, which has become immensely valuable to the digital tech industry and beyond.[7] This paper addresses the history of vulnerability disclosure and the emergence of the defensive market that has developed alongside the offensive one discussed earlier. In fact, the defensive market for vulnerability information is a recent model of vulnerability disclosure organized in the form of bug bounties programs. Bug bounties are initiatives managed by companies or organizations looking for information on their own vulnerabilities through which they pay individuals—ethical hackers—to uncover bugs in their systems

3 The hackers to which I am referring in this piece are individuals who are particularly interested in exploring, testing, breaking, and improving the security of technology. Thus, what characterizes hackers is an attitude toward technology rather than belonging to any specific group or culture.

4 Notorious markets included the Cyber Arms Bazaar, Dark0de, and TheRealDeal.

5 e.g., Zerodium, Endgame

6 The term "ethical hacker" is said to have been coined by John Patrick at IBM in 1995 amid the founding of the Global Security Analysis Laboratory, a service aimed at reporting vulnerabilities in customers' networks by hacking into them (Anthes 1995 and Palmer 2001, cited in Goertzen and Coleman 2022). Palmer (2001) notes that this practice was not new at that point, as it had been used by the US Army since the 1970s and publicized in 1993 by Farmer and Venema (discussed further in a later section). Ethical hacking is intimately related to the idea of simulating real attacks or providing the necessary environment to conduct real attacks in order to secure systems. In this sense, ethical hacking is part of a myriad of governing techniques developed since the mid-20th century with a focus on preparedness or, as described by Lakoff (2008), "techniques of imaginative enactment to generate knowledge about internal system vulnerabilities" (403). He opposes this rationality to the ones that manufacture security by prevention or interdiction (ibid.). As Goertzen and Coleman (2022) note, "ethical hacker" was not necessarily a label used by hackers who reported vulnerabilities in the 1990s. The term gained a renewed glow when bug bounties were put in place in the 2010s. However, for the sake of clarity, I use "ethical hackers" to refer to those who reported vulnerabilities they uncovered with the aim to secure systems.

7 Today, ethical hackers not only find vulnerabilities in computers but also help to secure other pieces of hardware that entail embedded code, such as cars, medical devices, home appliances, public facilities (e.g., airports, seaports, warehouses), and infrastructure systems (e.g., the electrical grid).

and, in turn, improve the security of their products and services. Oftentimes, these initiatives are managed by platforms that work to connect companies with ethical hackers. These companies, organizations, or platforms define and place a value on the types of bugs that they want to be identified. In this paper, I analyze the historical processes that have transformed models of vulnerability disclosure over the years and have given rise to a defensive market that has monetized disclosure, turned ethical hacking into labor, and made information on vulnerabilities a commodity.

To explore the history of vulnerability disclosure and the emergence of a defensive market, I conducted online archival research. This paper represents the first step of a larger research project that features multiple sources and methodologies, including interviews with key participants. The reasons behind this research agenda and the methods guiding the study are outlined toward the end of the paper. However, it is important to note that the story I am recounting is strongly biased; the material collected from the web was essentially all produced by U.S.-based actors, be they hackers, institutions, or companies. To answer an important call made by Janet Abbate (2017) about the need for research on the history of digital technologies (especially the Internet), additional research is necessary to understand how models of vulnerability disclosure were emerging elsewhere, such as Europe and Asia.

Introduction

My exploration of the history of vulnerability disclosure focuses on how the many models of disclosure emerged and evolved over time. The so-called full disclosure model rose in the 1990s in response to rising tensions between hackers and digital tech companies. This model was staunchly contested, and a crisis ultimately unfolded around 2000 led to a critical shift in the relationship between hackers and digital tech companies. This shift gave rise to multiple new models of disclosure, paving the way to the market model of vulnerability disclosure—bug bounties.

One of the most intriguing questions that arose from this exploration was how a defensive market for vulnerability information[8] emerged and how this development impacted the ways in which digital security is devised and performed by ethical hackers. This question is intriguing because ethical hackers had previously willingly reported vulnerabilities free of charge. For decades, it was inconceivable for ethical hackers to search for vulnerabilities with the intent to sell their findings, and companies were reluctant to compensate hackers in exchange for their information until quite recently. The emergence of a defensive market is, thus, far from being trivial, which leads me to investigate how both parties reconsidered the use of monetary reward as a potential dimension of their interactions and collaborations.

It is far from certain that this was inevitable. Despite markets being powerful institutions that are useful for structuring exchanges, they are not a natural or necessary outcome of human activities.[9] Markets are inherently social constructs and, therefore, can take different shapes and characteristics. In addition, vulnerability information markets, both offensive and defensive, do not structure all vulnerability exchanges; they co-exist with non-market forms of exchange that follow various models of disclosure. In fact, many vulnerabilities are still disclosed without being traded for monetary compensation. This clearly indicates that markets are not the only possible outcome of—or, necessarily, the best solution for—vulnerability information exchanges.

Economic rationales emerged around 2000, when the full-disclosure model began to be contested. Of course, it is important to go beyond discourse and opinions and identify the dynamics and institutions that supported the emergence of the market-led model of disclosure as well as the factors that hindered the emergence of this kind of model. The

8 For the sake of being concise, I use the simple terms “offensive markets” and “defensive markets” to refer to markets for vulnerability information.

9 This is a fairly well-founded assumption in anthropology and sociology at least. However, beyond these disciplines and outside academic circles (including in hacker groups and cybersecurity circles), markets are often viewed as a logical consequence of (or even a precondition of) complex human organizations.

history of vulnerability disclosure is a history of the integration of ethical hacking into the digital tech industry through which both hackers and companies have changed to accommodate each other. Comparing modern bug hunting—a way to report vulnerabilities in exchange for monetary compensation—with the practice of full disclosure in the 1990s shows how much ethical hacking has changed in recent decades.

However, this comparison could mislead us to an interpretation of hacking as having been swallowed and subsumed by the industry and its market rationality. Recent critical accounts have largely adopted this miserabilist perspective[10] on hackers active in bug bounties (i.e., bug hunters). For instance, Elis and Stevens (2022) present a compelling picture of bug hunters as "vulnerable workers […] enrolled to fix our vulnerable software and systems" (79); "an army of low-cost workers" (79) whose strategies are nothing more than individualistic opportunities to secure a better treatment (62) from platforms that "buy silence, causing hackers to lose the power to define aspects of their hacking and working lives" (46). Others view hackers as naive actors misled by platforms about the supposedly strong potential to make a living off of high bounties[11] and argue that a straightforward pest-control job is generally more lucrative than hunting bugs on digital systems.[12]

There is no doubt that disclosing vulnerabilities through a bug bounty program leaves little to no decision-making power to bug hunters. However, despite the existence of many severe issues crippling the bug-hunting business, I do not consider ethical hackers and hunters as helpless victims of market integration. Hacking has certainly changed throughout the years: it has been disciplined and governmentalized through the historical transformation of vulnerability disclosure models, but this does not necessarily mean that hackers have become a docile workforce coerced and exploited by powerful companies. This miserabilist perspective seems to have emerged from the pairing of two observations: 1) the severe imbalance of power in modern market-led disclosures and 2) the hacker ethos and bravado of full disclosure promoted in the media in the 1990s.[13] What is certain is that hackers' norms, institutions, and power were impacted and redefined by the marketization of vulnerabilities and the transformation of vulnerability research into labor. This paper examines these changes throughout the history of vulnerability disclosure but leaves further considerations about bug hunting to a future paper.

Significant ethical and institutional changes occurred in hackerdom and the larger arena of cybersecurity in the late 1990s. Were these changes only caused by the market

10 By this, I mean a perspective that frames social actors as helpless victims (see Olivier de Sardan 2008).

11 https://duo.com/decipher/taking-hype-out-of-bug-bounty-programs

12 https://www.infosecurity-magazine.com/opinions/life-crowdsourced-hacker/ and https://www.infosecurity-magazine.com/opinions/crowdsourced-gig-economy/

13 For information on the strategic use of bravado in the media by hackers, see Goertzen and Coleman (2022). I argue that the miserabilist perspective wrongly presupposes the existence of an authentic hacker culture in the practice of full disclosure during the 1990s.

integration of ethical hacking? To what extent did ethical and institutional changes pave the way to the emergence of a new market? Empirical evidence from the archive shows that important changes in disclosure practice occurred prior to the inception of a defensive market.[14] However, these changes were not deliberate steps to build up a market. Considering they were intentionally aiming at the inception of a market is not only an abusive interpretation (and a teleological perspective) but it would also assume that market-led disclosure was inevitable.

One of these important pre-market changes was initiated by the crisis of full disclosure mentioned earlier. Notably, the way in which this crisis was understood is key. Carefully assessing the debates allows us to understand the reasoning behind model transformations—as well as points of resistance against them—but it also reveals the strength of a new perspective on security. The problem at the core of the crisis was considered "social"; therefore, the problem couldn't be fixed through technical means. In other words, the process of defining the threats and the technical measures to address them (i.e., securitization) were viewed as irrelevant and led some actors to consider that the problem at stake—now framed as a socio-technical problem—needed to be addressed by economics instead. This process of framing security issues as problems that must be addressed using economic means (i.e., economization) is a key step in the development of a market model of vulnerability disclosure and represents a more general shift in cybersecurity at that time.

My approach to the digital history of vulnerability disclosure is inspired by Roseberry's (2008) anthropological political economy approach, which aids me in detailing both the historical development of the emergence of a defensive market and the current dynamics of ethical hacking. My approach frames the emergence of ethical hackers as intimately linked to the development of the digital tech industry, accounting for the history of both ethical hackers' interactions regarding vulnerability disclosure and their relationships with the digital tech industry.

To account for the transformation of vulnerability disclosure models and the emergence of a defensive market in a way that considers both interactions between ethical hackers and companies and the larger development of the digital tech industry, we must understand how vulnerabilities became commodities and, in turn, how hacking to identify vulnerabilities came to be viewed as labor. Dan Geer, an active participant of this historical phenomenon and a renowned hacker, tells us that this shift occurred around 2006 for a very simple reason: vulnerabilities became harder to find due to security improvements in the digital tech industry, resulting in a need for people to be dedicated and incentivized to find them.[15] However, this explanation oversimplifies a historical process, reducing it to a mere technical improvement. Michel Callon, in contrast, offers

14 Of course, other institutional and ethical changes have occurred since the market integration.

15 http://geer.tinho.net/geer.blackhat.6viii14.txt

some theoretical arguments that markets—and, in turn, wage-labor relationships—do not come into existence overnight. He provides a general explanation of what makes a market (2017), including the goods exchanged, which must be formatted as commodities in some manner; to be transferable, they must go through processes of detachment and re-attachment (2017: 66; see also Appadurai 1988). These processes have costs; and sometimes, these costs are too substantial to transform a good into a commodity (Callon 2017: 74).

Articulating the insights of Geer and Callon, we can hypothesize that, until 2006, vulnerabilities were circulating from hackers to companies, but they were not yet commodities traded in a market with an economic value attached to them, as the costs to set up such a market were still prohibitive. To better understand the weight of these costs and how they were reduced, we must consider what the new institutional economists are saying about "transaction costs." Additionally, Callon urges us to delve into the new institutionalist political economy for another reason: a market requires the clear definition and operation of a set of rules, conventions, inclinations, routines, and cultural norms to achieve functional stability and to ensure the security (42) and enforcement (32) of transactions. Once the effort is made to facilitate trade, other costs are incurred by the processes of value measurement, information gathering, and decision-making.

Anthropologist Jean Ensminger clarifies the concept of a transaction cost: "it takes resources to gather information, negotiate, monitor, and enforce property rights and contracts. Transaction costs are incurred whenever people try to measure the quality of the goods and services they want […] Societies may *not* benefit from trade or specialization if the 'transaction costs' incurred in the process of exchange outweigh the benefits of that exchange. It is exactly these costs that governments reduce by clearly specifying property rights, by regulating weights and measures, and by providing third-party enforcement of property rights and contracts" (1996: 18).

Institutional change may facilitate the reduction of these costs and, in turn, market development. For institutional economists like Jean Ensminger and Douglass North, an institution is understood as "[…] a combination of formal rules (such as those regulating the structure of the polity, property rights, and contracting), *informal constraints* (by which North means norms of behavior or the customary rules of the game), and *enforcement* (including self-imposed standards of behavior)." (Ensminger 1996: 5–6). With these definitions in mind, we are ready to approach the enigma of the emergence of a defensive market and a couple of recent publications will contribute to help us in providing a provisional answer to this enigma.[16]

16 The publication of these two reports in early 2022 overlapped with my own research on the same topics, which I presented in a preliminary form in a workshop entitled "The Promise of the Fix" at the University of Warwick's Centre for Interdisciplinary Methodologies on December 14–15, 2021 organized by Professor Matt Spencer. These reports helped me to refine my own perspective on the history of vulnerability disclosure and complemented some of my analyses by contributing a few important sources

Elis and Stevens (2022) offer two important explanations regarding motivations that drove companies to embrace bug bounties by the 2010s. First, they argue that the existence of an offensive market pushed companies to introduce countermeasures to limit the risk of attacks (40) and that some hackers played a key role in pushing companies to commodify vulnerabilities and, in turn, normalize their activities (41). Second, they identify a pattern with regard to outsourced testing. Testing is a costly element of the development of code: "By 2002, estimates suggested that debugging, testing, and program verification accounted for between 50% to 75% of total development costs. A substantial market for security testing services, pen test companies, in particular, grew to complement and support in-house testing" (45). In this way, bug bounties may well have become a new outsourced testing service that allows companies to reduce their costs (42).

The economic perspective of Elis and Stevens is contrasted by another important report that focuses more on the social and cultural aspects of hackers in the 1990s. Coleman and Goerzen (2022) explore the history of hacking in the 1990s with the aim of explaining how hackers involved in vulnerability disclosure gained a voice and a reputation that encouraged companies to employ them in the early 2000s. They provide insightful remarks about the early involvement of hackers in vulnerability disclosure and their strategies to be taken seriously in the fast-growing digital tech industry. They argue that hackers succeeded in shifting their image in the media from "agent of insecurity" (64) to independent security experts raising concern about the weak security implemented by tech companies in their devices and services. In this way, hacking operated as a "bottom-up securitization" (64) involving many diverse individuals regrouping into a community of concern around mailing lists where information on vulnerability was disclosed. The process through which hackers became a respectable voice in the nascent cybersecurity industry and the role played by mailing lists are key to understanding how, in the early 2000s, dialogue between hackers and companies emerged. These observations are important to consider in the history I am recounting. However, before presenting additional elements to explain the emergence of a defensive market, it would be helpful to outline the history of vulnerability disclosure models.

to my archive.

The periodization and definition of vulnerability disclosure models

Four models of vulnerability disclosure devised and implemented between the 1990s and the early 2020s can be identified: full disclosure, responsible disclosure, coordinated disclosure, and bug bounties. All of these models' names are routinely used in cybersecurity and the sources I collected. Full disclosure began being practiced in the 1980s, reaching its peak in the 1990s. In the early 2000s, important issues with full disclosure prompted some hackers to devise a new model, responsible disclosure, which redefined their collaboration with the digital tech industry. Coordinated disclosure was introduced by Microsoft in 2010 to highlight a few changes to their disclosure policy and demonstrate that digital tech companies were now in charge of redesigning the standards of disclosure. This model of disclosure reinforced companies' power to decide when hackers could go public with their findings. Interestingly, bug bounties (i.e., the market-led disclosure model) gained considerable traction at the same time, around 2010, when some big tech companies began to adopt this model.

While certain models may gain more traction than others, it is important to note that these models are not mutually exclusive—they can and do co-exist. Therefore, we cannot consider each model to represent a different hacking era (e.g., the 1990s as the full disclosure era) or anything along those lines. These models simply do not correspond to epochal shifts in ethical hacking history in any way. In fact, full and responsible disclosure both still play important roles in the early 2020s despite bug bounties having been prominent for over a decade.[17]

The history of vulnerability disclosure models is one of the governmentalization[18] of ethical hacking. This paper focuses on changes in the nature of exchanges between hackers and companies and what these changes tell us about the governmentalization of ethical hacking. The full disclosure model emerged out of a bitter relationship between hackers and the nascent digital tech industry. Unable to get the attention of companies, hackers publicly disclosed vulnerabilities they found to force them to act to prevent potential security breaches. Collaboration between the two was almost non-existent, and defiance amplified their antagonism over the years. Responsible disclosure was developed with another logic in mind. At one point, which I analyze later in greater detail, collaboration between companies and hackers was considered imperative, and both hackers and companies set some basic rules. Eventually, companies engaged in consistent and active dialogue with hackers. The terms regulating this dialogue were refined into established standards, expectations, and mutual commitments, heightening

17 The two obvious reasons for this are that not all vulnerabilities can be reported through a bug bounty program and that not all organizations have such a program.

18 It is important to mention here that vulnerability disclosure models were not controlled by state governments. Simply put, governmentalization is a process that shapes people's conduct—here, the conduct of ethical hackers. It implies the emergence of institutions, procedures, assessments, and tactics aimed at governing and regulating a population (Foucault [1978] 2009).

predictability for both parties. However, friction and conflict did not disappear completely. The model of full disclosure persisted, but it was no longer dominant. In fact, fully disclosing a vulnerability came to be seen as an irresponsible act.

As companies increasingly took on the role of governing disclosure, initiatives incentivizing responsible and coordinated disclosure were put in place, giving rise to a model of vulnerability transactions in which ethical hackers who reported vulnerabilities to companies would receive monetary compensation for their findings. Therefore, some non-market forms of exchanges evolved into a defensive market comprising reward programs at first and bug bounties shortly after, providing a new model of collaboration between hackers and the digital tech industry. Nowadays, as presented by Elis and Stevens (2022), several issues are crippling the model and its implementations. Labor conditions are certainly the most important of these issues, but bug bounties have also reshaped ethical hacking and hackers, creating new communities of hunters and new forms of collaboration. They have also promoted hacking to a larger audience and lowering the barriers to entry in offering hacking tutorials and trainings.

Full disclosure: When companies did not care, hackers did!

Let's go back in time to when hacking for the common good was in its so-called "golden age"—the era of full disclosure that shaped the image of hackers as young rebels ridiculing digital behemoths, such as IBM, Microsoft, and Sun Microsystems. While full disclosure is widely seen today as a problem rather than a solution, it was the dominant model in the 1980s and 1990s—a way to fix common issues that hackers faced when reporting bugs to companies. At that time, companies were, at best, ignoring vulnerability notifications by hackers but would often threaten them with legal action.[19] Unresponsiveness—and, from hackers' perspectives, arrogance, and irresponsibility—were the issues that full disclosure sought to fix. For many hackers, this situation was unacceptable. Thus, going public with a vulnerability became the strategy to rectify companies' behavior.

The BTX hack is an exemplary case in this regard as well as one of the first of its kind.[20] In 1986,[21] the German Chaos Computer Club (CCC)—one of the oldest hacker collectives—found a vulnerability in BTX, a pre-Internet system similar to the Minitel in France. They reported it to the manufacturer and never heard back from them, but the flaw they identified was corrected shortly thereafter. Perturbed by the impolite silence of the company, they looked for and found another vulnerability, this time deciding to go public: they prompted journalists to observe them restituting the money that they had transferred to their account the night before. This disclosure was effectively a poignant prank done to get back at the company for not engaging in dialogue with the hackers. In revealing that BTX was insufficiently secure to handle money transfers, the CCC publicly contradicted information that the manufacturer had advertised to their customers.

In addition to forcing companies to fix security issues with their products and infrastructure, hackers were framing full disclosure as a way to warn and protect customers. In 1997, Mudge, an American hacker member of the famous hacking group "The L0pht," declared that "I wanted the L0pht to be *Consumer Reports* and Rachel Carson and Ralph Nader" (Menn 2019: 71). In this way, ethical hackers considered themselves to be valiant watchdogs dedicated to revealing hidden defects in digital products to otherwise defenseless users who were unable to assess the marketing claims of booming digital tech companies. "We're doing this because Microsoft is shoving stuff down people's throats, and you don't have the ability to look and see how good it is" (Mudge quoted by Lange in 1997).[22] This care for users and consumers appears to have been a core ethical value held by the hackers. An ethos of chivalry radiated from their

19 Elis and Stevens (2022) aptly explain, "Paying hackers for bugs was once a radical idea. Up through the early 2010s, most companies and government agencies were far more likely to threaten hackers rather than to offer them a reward" (5).

20 I do not claim to know for certain the first full disclosure in the history of computing. The BTX hack is simply the oldest full disclosure that I uncovered online during my data-collection process.

21 https://monoskop.org/images/2/2f/Die_Hackerbibel_1_(German).pdf

22 https://g.foolcdn.com/EETimes/1997/EETimes970418.htm

explanations of their deeds: they spent a lot of time and mustered a significant amount of courage in the face of prosecution to speak truth to power and provide valuable information to vulnerable consumers. Instead of attributing this ethos to a pre-existing hacker culture,[23] I would argue that it emerged from the very frictions caused by the corporate silence faced by hackers during this period. From this perspective, a series of missed encounters—rather than a pre-existing ethos—modeled what is known as the full disclosure model.

The BTX story tells us that the users were not the primary interlocutors targeted by the CCC full disclosure hackers. They first contacted the company, only turning to another audience (the consumers) once the company ignored them. What they cared about was primarily the security of the technology. Notably, however, hackers' concerns over security were not universal. In fact, many companies disregarded them entirely. In 1994, the renowned computer scientist Eugene Spafford wrote: "I approached one major vendor about some support for the next version of Tripwire and some work on an intrusion detection system. The response: 'We are not concerned about the security of our systems.'"[24] During this period, receiving no response from companies was considered standard. At best, companies were slow to fix identified vulnerabilities, leaving their products open to attack.

Hackers and system administrators were concerned over the unresponsiveness of companies, so they took action as Mike Parker, a UNIX expert, wrote: "Also, history indicates that fixes won't become available from vendors, regardless of the seriousness of the problem, until enough white hats [i.e. ethical hackers] find out to start kicking up a fuss. But if full details are released, fixes start appearing magically from all over the place, as different people independently secure their systems. The quickest way for me to get a fix for my system is, experience teaches, full disclosure."[25] Free access to information is a key principle here, as it allows hackers and system administrators to test their systems and maintain their capacity to independently secure them. In addition, it puts "[…] pressure on the vendors by making these things public sooner [and may] help to light a fire under them to get their code cleaned up, which would be a big plus for all of us." according to a Dell UNIX developer.[26] Therefore, care for users is only part of the story and potentially a residual one. Instead, two important principles lay at the heart of full disclosure and warrant further exploration: antagonism and transparency.

Full disclosure is adversarial in at least two different ways: it is adversarial toward companies but, more fundamentally, vulnerability research itself is shaped by an adversarial logic. Hackers publicly disclosed vulnerabilities to force companies to act and

23 As a social anthropologist, I must dismiss the former option for its culturalist stance that tends to attach discrete traits to a specific group or culture.

24 https://seclists.org/bugtraq/1994/Apr/65

25 https://seclists.org/bugtraq/1994/May/3

26 https://seclists.org/bugtraq/1994/Apr/71

fix the security breaches they discovered, and this arguably built up antagonism between the two parties during the 1990s. However, we must bear in mind that collaboration between the two was not off the hacking table. The Internet archive shows that hackers often contacted companies before going public.[27] Therefore, full disclosure does not represent a complete lack of communication between hackers and companies. However, vulnerability research is more fundamentally adversarial at its very logical core: it entails attacking a system to better defend it. This idea stems from an influential paper published in 1993 by Farmer and Venema[28], "Improving the Security of Your Site by Breaking Into it". In this paper, the authors explain that SATAN[29], a free vulnerability auditing software of their own, allows the administrator system to test their infrastructure with known vulnerabilities and, therefore, "to look at her or his system in a new way."[30] SATAN was educational, as it was meant to make system administrators aware of some hacks known in secretive "underworld[s]".

Farmer and Venema sought to freely spread arcane information and techniques circulating among black-hat hackers.[31] Their approach to information was justified by rationales about transparency: the free flow of information could lower the risk of system misuse or misconfiguration and limit illegal or criminal activities. The transparency principle here applied to security finds its root in what Levy called the "Hacker ethics" (1984), which applies to a larger set of hacking practices and open-source software development: "All information should be free" to prevent "the dreaded, time-wasting ritual of reinventing the wheel: instead of everybody writing his own version of the same program, the best version would be available to everyone, and everyone would be free to delve into the code and improve on that" (Levy 1984: 28). Autonomy and self-governance (or self-help) are what motivates transparency at the heart of these movements (Hellegren 2017): "Full disclosure is in many ways akin to the open-source movement that's taking the computer world by storm. Open source allows for peer review, learning, and collaboration that leads to making better software. Full disclosure has similar goals. By making the details of vulnerability public, it seeks to educate and inform, and at the same time to provide a basis upon which to take further action".[32]

This model of security by transparency was not new. It was devised more than a century prior against the common model known as security by secrecy, first by the locksmiths Hobbs (1853) and later by Kerckhoffs for military-grade cryptography (1883). For them, secrecy limits the ability to discover vulnerabilities in order to fix them but doesn't prevent malicious actors from discovering those flaws. Instead, by publishing the

27 For instance, see https://seclists.org/bugtraq/1994/Sep/7 ,https://seclists.org/bugtraq/1994/Nov/143, and https://seclists.org/bugtraq/1995/Jun/8.

28 http://fish2.com/security/admin-guide-to-cracking.html

29 Security Administrator Tool for Analyzing Networks

30 http://www.porcupine.org/satan/admin-guide-to-cracking.html

31 This term refers to individuals hacking for their own interest or amusement (i.e., unwilling to disclose vulnerabilities to secure a system).

32 https://www.usenix.org/publications/login/november-1999-special-issue

blueprint of a lock, locksmiths can evaluate its security themselves and report their skepticism if necessary. It promotes curiosity and innovation that, in turn, serves the public interest (Hobbs 1853: 3–4). In other words, transparency works with the attack-defense logic. Of course, the principle works also for known vulnerabilities: publishing them limits their reproduction in newer products, at least in theory.

In concrete terms, full disclosure took place online. The details of vulnerabilities were posted on public mailing lists, such as Bugtraq[33] and the Cypherpunks mailing list,[34] to both share knowledge and techniques with peers and to raise system administrators' awareness and educate developers. Therefore, admins and security-savvy users could take appropriate measures themselves without remaining dependent on reluctant companies, at least until the companies were able to make their patches available to everyone. The mailing-list Bugtraq was founded in 1993 by Scott Chasin and was active until recently. It was a pragmatic answer to a situation that became unsustainable at the time: for some hackers and system administrators information about known vulnerabilities was not circulating well enough.

Before Bugtraq opened a public forum through which to disclose and discuss vulnerabilities, flaws discovered in the US could be reported to CERT-CC,[35] an institution founded in 1988 at Carnegie Mellon University in Pittsburg with federal funding to coordinate an emergency response in the wake of major cyber-incidents.[36] Rapidly, CERT-CC took up the role of informing companies about vulnerabilities found in their products. However, CERT-CC appeared to not sufficiently push the companies to fix their flaws and was reluctant to disclose enough information about an unpatched vulnerability in their advisories:[37]

"Scott [Chasin] started the list as a reaction to a lack of useful information about security vulnerabilities. At the time CERT was almost useless […] and vendors did little to help. Systems were ridiculously easy to break into. System administrator [sic] started to depend on each other to stay informed. The firewall mailing list was used sometimes to discuss vulnerabilities but it was outside it[sic] charter and the list owned[sic] did not want exploits or detailed information on his list. This environment prompted Scott to start BUGTRAQ in 1993." (Elias Levy quoted by Seifried).[38]

---

33 https://seclists.org/bugtraq/

34 A partial archive is available at the following link: https://cryptoanarchy.wiki/getting-started/what-is-the-cypherpunks-mailing-list.

35 Computer Emergency Response Team Coordination Center

36 The CERT-CC was founded in the aftermath of the first massive incident on a remote network, which was caused by the infamous Morris worm in 1988. Similar institutions were founded in other countries. Today, national CERTs and computer security incident response teams (CSIRTs) are present in many countries, though some are notably dedicated to a specific sector (e.g., finance, military, universities) or large company (e.g., Airbus, Deloitte, Morgan Stanley).

37 See Shepherd (2003), https://www.schneier.com/crypto-gram/archives/2001/1115.html, and the excellent description of hackers' resentment toward CERT-CC from Goerzen and Coleman (2022).

38 https://seifried.org/security/articles/20011015-elias-levy-interview.html

In 2001, the list had 40,000 subscribers,[39] and hundreds of messages were being posted every month. For Chasin, the list created a community that pushed the companies to react.[40] However, the list was also the location where many debates on full disclosure took place. Very well presented by Goerzen and Coleman, Bugtraq could indeed be considered a "trading zone" (2022: 63) in which the full disclosure model was discussed, contested and developed in addition to being, like other lists, a place to share information and remediation about new vulnerabilities.[41] Overall, there is no doubt that mailing-lists like Bugtraq induced rising antagonism between hackers and companies.

One of the main reasons behind this antagonism is the publication of exploit code on mailing-lists. In addition to vulnerability information, the exploit code allows the sysadmin to rapidly test their systems and was sometimes necessary to convince companies that the identified vulnerabilities had a substantive impact.[42] This emphasizes an important trade-off of the full disclosure model that we must not minimize: if the publication of vulnerability information could improve security in both the short and long terms, this information (and, even more so, the publication of an exploit code) could also be misused, encouraging ill-intentioned hackers to attack vulnerable systems. This critique of full disclosure has existed at least since the publication of SATAN in 1995.

Often, the use of vulnerability information and exploit code was intentionally disregarded as an ethical issue by the full disclosure hackers, for whom transparency prevailed. Tweetyfish, a cDc[43] member involved in the development of a hacking tool named Back Orifice 2000, declared to CNN: "Users might include the National Security Agency, the FBI or their foreign counterparts, which all conduct network surveillance. I don't care […] It's for everyone."[44] Moreover, vulnerability information and exploit code were not only published on Bugtraq or other public lists; they were sometimes (and still are) packaged in various free and ready-to-use hacking tools.[45]

The publication of clever hacks, nasty exploits, and powerful hacking tools became the values by which to gauge hackers' reputations. Considering the adversarial nature of full

39 Ibid.

40 https://www.slonepartnerscybersecurity.com/newsletters/slone-partners-cybersecurity-exclusive-interview-with-scott-chasin-information-security-pioneer-and-serial-entrepreneur

41 It is important to note here that the concept of a trading zone does not imply that vulnerability information was traded. What was exchanged were different views and opinions about the disclosure of vulnerability information and companies' behavior.

42 "If a researcher just publishes vague statements about the vulnerability, then the vendor can claim that it's not real. If the researcher publishes scientific details without example code, then the vendor can claim that it's just theoretical. The only way to make vendors sit up and take notice is to publish details: both in human- and computer-readable form. (Microsoft is guilty of both of these practices, using their PR machine to deny and belittle vulnerabilities until they are demonstrated with actual code)" (https://www.schneier.com/crypto-gram/archives/2001/1115.html)

43 Cult of the Dead Cow is a hacker group closely associated with the L0pht.

44 http://edition.cnn.com/TECH/computing/9907/21/badrap.idg/

45 Today, many hacking tools are suites (e.g., Mimikatz) integrated into frameworks (e.g., Metasploit), and they are sometimes included by default in operating systems (e.g., Kali Linux).

disclosure, bravado and mockery against companies quickly became hackers' or hacker collectives' means of achieving glory.[46] The public shaming of companies at hacking conferences was common in the second half of the 1990s. On several occasions, media outlets reported on such events, bringing digital security issues to a wider audience. Full disclosure was sometimes made into a media event for which journalists were courted, as was the case with the BTX hack a decade earlier.

For Goerzen and Coleman (2022), who offer a more detailed account of 1990s hacking practices, full disclosure was a way for hackers to reform their public image and, ultimately, to become employable. In this sense, media-covered vulnerability disclosure enabled hackers to present themselves as the "good guys" who were committed to improving the digital security of companies, or the "dunces" on this matter. Full disclosure was a way for them to showcase their skills and, soon enough, some of them attracted the interest of companies and governments. The most prominent example of this dynamic was the invitation of members of The L0pht to provide testimony on the state of digital security to the U.S. Senate in 1998.[47]

Hackers fully disclosing their results and exploits definitely succeeded in raising awareness about the concerning security situation in the fast-growing digital tech industry. Thus, I concur with Goetzen and Coleman (2022) that full disclosure entailed "bottom-up securitization" (64) in which hackers were able to outline and publicize a new type of threat to the emerging digital society. While full disclosure was certainly more than the sum of the vulnerabilities revealed by it, the impact of the securitization process remained limited compared to other issues, such as terrorism and immigration, which became far more successful in terms of securitization over the last two decades.

Companies were reluctant to accept the information provided by hackers. Additionally, if full disclosures forced them to react, securitization did not yet prompt them to significantly change their software-development process or to invest massively in security testing at the turn of the century. Several factors contributed to this situation and explain companies' unresponsiveness. The first set of reasons has to do with the economic context in which digital tech companies were operating during the 1990s, namely the widespread adoption of digital technology and the democratization of the Internet. The booming digital tech industry offered companies the opportunity to yield enormous profit. However, they were caught by a competitive economic race and extensive financial speculation, ultimately triggering the burst of the so-called dot-com bubble in 2000. Notably, the fierce competition for innovation and market share resulted in security issues constituting a secondary concern. Security did not directly produce value. Indeed, it produced only costs and testing requirements, making up a significant part of the cost

46 One good example of this glorification is the presentation of the Back Orifice 2000 hacking tool in 1999 at DEFCON: https://www.youtube.com/watch?v=oHxNEvkIKqE.

47 A video of the hearing is available at the following link: https://www.youtube.com/watch?v=VVJldn_MmMY.

of software development. Moreover, due to recent developments in digital innovation, many companies were benefitting from a quasi-monopolistic situation. Whatever bad security their products exhibited, customers had few alternatives. A rare *mea culpa* comment on Bugtraq from a security engineer working for a company facing a recent vulnerability disclosure revealed some important tensions from within a company:

"We were slacking; we'd had more than enough time to produce fixes. We didn't really start working on it until they said they were going to post the advisories. […] We started working in earnest on a set of fixes when they told us they were going to post the advisories. My complaint is that after we told them this, they refused to delay the advisories long enough for us to deliver those fixes. (They have now been delivered, in haste and poorly packaged.) […] I'm a strong advocate of security and have been asking the company to produce security fixes for a while now. What 8LGM [the hacker group that notified the vulnerability to the company] is doing helps me a lot: makes it impossible for management to ignore the problem. But they also cause a lot of trouble and grief by being too inflexible."[48]

The second set of reasons is related to non-economic factors. First, ordinary customers, ignorant of the computing technology, were completely oblivious to the risks posed by the software they were purchasing (which is still the case today). They had no ability to verify the claims of the producers or evaluate the security and reliability of their purchases. In addition, digital tech companies were not liable for insecure code (which, again, is still the case). In other words, they would not be considered legally responsible for a security breach or harm suffered by their consumers due to their own security flaws. This stands in stark contrast to other industries (e.g., the automotive industry), which are liable for defective components in, or safety issues with, their products. Moreover, the enactment of anti-hacking bills in the late 1980s and 1990s (e.g., the CFAA and the DMCA in the US, the CMA in the UK) protected companies and prevented them from collaborating with hackers. Finally, as shown, CERT-CC was not in a position to exert pressure on companies to fix their identified vulnerabilities. In short, despite the fact that companies were incrementally forced to deal with security issues due to their public disclosure, they were largely uninterested in working harder to ensure the security of their products and services. In summary, companies had no financial, marketing, or legal incentives to engage with hackers. On the contrary, ignoring hackers was far more cost-effective for companies than prosecuting them or allocating resources to receive and process vulnerability information. In other words, the costs involved with vulnerability transactions were too high, and the incentives were too low.

Surprisingly, hackers who stood to gain from vulnerability exchange were not calling for remuneration to pay them back for the many hours that they spent finding security bugs. There are at least three reasons for this absence of pretense. First, the ethical hacker's

48 https://seclists.org/bugtraq/1994/Nov/143

model of security was fundamentally based on transparency. For ethical hackers, better security can be achieved through free access to vulnerability information, and full disclosure was certainly aimed at boosting transparency. This principle in the model limited the claims to payment. Second, hacking was not yet considered a profession. Instead, hacking and disclosing vulnerability on a public mailing list was viewed as a service offered to an imagined community. Third, in both a moral and legal sense, requesting a sum of money to disclose information on vulnerabilities could be considered extortion. Ethical hackers not only refrained from engaging in criminal activities, but they were also actively contending against the common view that hacking is an inherently criminal activity. According to Goerzen and Coleman (2022), they were campaigning to be publicly viewed as the skilled good guys. This refusal to hack for money also reflects a value underlying Levy's Hacker's ethics: "You could call anywhere, try anything, experiment endlessly, but you should not do it for financial gain." (1984: 86). From this perspective, hacking phone or computer networks was a non-profit activity solely driven by curiosity and exploration. We can consider all three of these reasons as hindrances to the emergence of a defensive market. Therefore, we should seek out explanations for the decline of these reasons in the 2000s following the crisis of the full disclosure model.

Of course, this does not mean that vulnerabilities and full disclosure lacked value entirely. On the contrary, both were entangled in a dense net of technological, educational and moral values aimed at advancing digital security.[49] However, the antagonism created by full disclosure between hackers and companies as well as the dynamics of glory and reputation worked against the emergence of a conducive environment in which to lay down basic rules of conduct necessary for the development of a market. This time for the hackers, transaction costs were too high for them to engage in corporate affairs. Full disclosure was simply easier and faster, as there were no other mechanisms yet in place to reduce transaction costs and alter the incentive structure. Tracking these changes is the objective of the next sections. However, before we do that, we must consider two important pre-2000 developments related to the practice of full disclosure.

As already stated, the full disclosure model led ethical hackers to compete for fame and reputation. Hackers were taking credit for publicly shaming companies without receiving any compensation. Hacking was viewed as rebellious and contentious, with hackers publicly insulting companies like Microsoft in the media, showcasing hacking tools like Back Orifice at conferences, and pointing out exploitable vulnerabilities on Bugtraq. Media agencies were, of course, eager to cover these hacks and pranks, and hackers were able to leverage these public demonstrations of digital virtuosity. Beyond building up their reputation in hacking circles gravitating around full disclosure mailing lists, ethical hackers were gaining interest among other actors. In a sense, Bugtraq was used to build up an attractive resume.

49 While this may initially seem counterintuitive, forms of collaboration are inherent in full disclosure. Hackers disclosing their findings have not only tried to collaborate with companies, but have also promoted collaboration in the form of sharing knowledge, educating the public, and raising awareness.

What Goerzen and Coleman called “security by spectacle” helped hackers to professionalize their ability to identify vulnerabilities (2022). However, as Auray and Kaminsky (2007) have shown, the process of professionalization is diverse; they could choose to be employed, to become independent consultants, to lean toward fraud, or to seek remuneration on hidden markets. According to Zufferey (2018), this career choice was likely determined by sociological factors. Most often, hackers were employed as security engineers or members of development teams at auditing companies to run intrusion tests (Auray and Kaminsky 2007). Another career path hackers sometimes followed was the development of their own company that provides security tools and services (ibid.). Others uncovered ways to sell information on vulnerabilities (ibid.): during the second half of the 1990s, hackers were increasingly hired by vulnerability brokers and exploit boutiques or invited to set up similar businesses. These vulnerability brokers and boutiques, as Perlroth (2021) recounts, all provided information and services to the intelligence community, including the NSA in the case of the US. Again, full disclosure certainly aided hackers in being identified as worthwhile freelancers to be hired by companies and organizations active in the offensive market.

The first strategies to monetize vulnerabilities for defense emerged at the tail end of the 1990s, when some ethical hackers began founding security start-ups. Interestingly, vulnerabilities were not directly monetized, but full disclosures of vulnerabilities served to promote products that would mitigate or neutralize their impact. Notably, such initiatives were strongly criticized in the ethical hacking circle, indicating that the idea of generating profit from hacking was largely anathema. Schneier offers a short description of both this strategy and its unambiguous critique:

“I call this kind of thing a publicity attack. It's a blatant attempt by nCipher to get some free publicity for the hardware encryption accelerators, and to scare e-commerce vendors into purchasing them. And people fall for this, again and again. This kind of thing is happening more and more, and I'm getting tired of it. […] I’m a fan of full disclosure—and definitely not a fan of Microsoft's security—and believe that security vulnerabilities need to be publicized before they're fixed. (If you don't publicize, the vendors often don't bother fixing them.) But this practice of announcing "vulnerabilities" for the sole purpose of hyping your own solutions has got to stop.”.[50]

The reality of ethical hacking was already slowly shifting toward a new paradigm in which full disclosure hackers were being hired or becoming entrepreneurs.[51] A new cohort of companies emerging from the practice of ethical hacking and full disclosure was joining the growing cybersecurity industry. This dynamic greatly impacted the way in which ethical hacking was handled, especially as problems identified via full disclosure became

50 https://www.schneier.com/crypto-gram/archives/2000/0115.html

51 For instance, nCipher was founded in 1996, and the L0pht was incorporated into the company @Stake in 2000.

too serious to continue avoiding them. Economic rationality became increasingly prominent in the very act of redefining hacking at the turn of the century. In the next section, I discuss the crisis of the full disclosure model, the ways in which problems were identified and handled among ethical hackers, and how they shaped a new disclosure model.

Full disclosure in crisis

Debates over the full disclosure of vulnerabilities can be found in the earliest conversations on Bugtraq back in 1994. By the end of the decade, however, concerns grew bigger and louder. The crisis of full disclosure at the end of the 1990s is key to understanding the transformation of ethical hacking in the early 2000s and the inception of a new disclosure model. Cracks in the full disclosure model appeared to be related to hackers' reputation, which rapidly inflated and thrived toward the end of the decade. Alongside favorable publicity, marketing strategies, and public displays of bravado or mockery, some voices rose to propose another means of disclosure that insisted on giving prior notice to companies before publicly disclosing a vulnerability. In fact, Bugtraq's own FAQ page advised hackers to take this approach.[52]

However, the main problem with full disclosure came from the already contested practice of publishing exploit codes alongside vulnerability information or releasing hacking tools capable to launch several attacks on a target. Ethical hackers did this to provide quick help to those looking to test the vulnerability of their system. In this way, they also increased pressure on companies to act. Ultimately, however, these exploit codes were accessible to anyone, including an increasing number of careless individuals willing to experiment with these attacks made available by ethical hackers. Attacks using published hacking tools or exploit codes were routinely identified, with some causing tremendous impact. In other words, full disclosure spun out of control, with some using identified vulnerability information to launch real attacks. Many web defacements and viruses (mostly worms) are said to have been engineered using full disclosure information between 1999 and 2001.[53]

Interestingly, all these attacks were thought to have been launched by "script kiddies," a vague category of actors defined by hackers as lacking "technical skills to understand an exploit or to create an attack tool [and who] download attack tools and launch them blindly against the public Internet" (Shepherd 2003). In other words, "script kiddies" roamed full disclosure lists to collect vulnerability information and exploit codes to mess around with. This derogatory category of actors emerged to differentiate ethical hackers from those who were "playing" with the explosive power of full disclosure information. Most importantly, however, this new class of actors served as a way to identify an unavoidable problem related to the practice of full disclosure.

52 Bugtraq's FAQ is accessible online, but I was unable to determine the year in which Bugtraq issued its advice to notify the companies: https://web.archive.org/web/20020602204128/http://www.securityfocus.com/popups/forums/bugtraq/faq.shtml. Cencini et al. (2005) mention the existence of an NTBugtraq disclosure policy from 1999 written by Russ Cooper, but I was unable to access it.

53 This includes the Melissa virus (1999), the I LOVE YOU worm (2000) and the Anna Kournikova virus and the Ramen, Lion, Sadmind, Code Red, and Nimda worms (2001).

Marcus Ranum, a hacker famous for developing cybersecurity defenses (including early firewalls and intrusion-detection systems) in the 1990s, played a crucial role in delineating the full disclosure crisis stemming from script kiddies. Ranum presented his critique of full disclosure in a keynote speech at the Las Vegas Black Hat conference in July 2000:[54]

"In fact, what we are doing today by releasing tools through the full disclosure mechanism, releasing tools and exploit information, is […] creating hordes and hordes of script kiddies, right—these guys are like cockroaches. On one hand, we are complaining about the fact that our dorms are infested with cockroaches yet, on the other hand, we have diligent security analysts who are putting roach food down the hall, all the time. For some reason, these two don't add up."

Following this statement, Ranum enumerated a long list of claims often made by proponents of full disclosure that he considered dubious or blatantly false. He argued that disclosing vulnerability information for educational purposes was failing and highlighted that users were more vulnerable because they were late in implementing patches prepared by companies in the wake of full disclosure vulnerability information. However, this issue of delayed patch adoption was dropped from the disclosure debate because it was understandably considered to be an issue that companies alone should deal with. For Ranum and several others, it was clear that problems were of a social nature and that determining what needed to be addressed required the determination of what information could be disclosed to re-establish productive collaboration between hackers and companies. Thus, those who agreed with Ranum considered the disclosure of vulnerability information to be due for a change.[55]

The problems of security caused by full disclosure were understood in behavioral terms. On the one hand, the disclosure of some vulnerabilities served to advertise for technical solutions to be purchased. On the other hand, the disclosure of information and exploit code triggered irresponsible actions from the so-called script kiddies. The first one entailed tweaking disclosure to a situation in which only purchasers would be secure, while the second was the result of exploit code actionable by a rising number of irresponsible actors. Beyond agreeing to continue prosecuting the script kiddies, the debate turned to the root cause of the attacks: Was it necessary to publish exploits, including ready-made exploit suites packaged in user-friendly interfaces, with the clear intent to boost one's own reputation in hackerdom?[56] This debate was immense, with

54 Ranum's keynote is available at the following link: https://www.youtube.com/watch?v=g93ofG4OYJU.

55 Interestingly, hackers in defense of non-disclosure surfaced shortly after Ranum's speech, collectively presenting themselves as the "anti-sec" movement. They argued against full disclosure, highlighting the marketization of hacking and advocating for a focus on the underground hacking scene: http://web.archive.org/web/20010402024501/http://anti.security.is/.

56 Ranum's talk clearly used several strategies to ridicule full disclosure hackers, the most profound one being a critique of the logic assuming that attacking a system is necessary to improve defense. As a defensive hacker, so to speak (or, at least, the owner of a firewall company), Ranum called his attacker peers to rally with him on behalf of the "bright side of the force": defending systems instead of just ransacking them (https://www.youtube.com/watch?v=g93ofG4OYJU).

countless arguments in favor and against that could not possibly be adequately covered within the scope of this paper.[57] However, the publication of exploits became questionable and, in 2000, CERT-CC declared in its policy that "the number of people who can benefit from the availability of exploits is small compared to the number of people who get harmed by people who use exploits maliciously."[58]

More generally, debates over full disclosure revolved around the timing of disclosure (e.g., how long before releasing the information), information to disclose (e.g., about vulnerability only or also exploit code), and the definition of "the public" for vulnerability information (i.e., who gets what information and when) (Granick 2005). In addition, it seems that ethical hackers generally sought a solution to the "social" problems surfacing at that time (i.e., the script kiddies but also, more fundamentally, the balance of interests related to the dimensions highlighted by Granick: time, information, and public) by relying on economics and economic rationality. In other words, hackers' securitization processes were economized, understood, and framed not only in technical terms but also in economic terms.

The script kiddies-oriented critique of full disclosure was not only based on the alleged cause of an increased number of attacks in the late 1990s. The question of releasing exploit code and hacking tools was already a debate among ethical hackers;[59] the concerns were merely reframed and scaled up with the emergence of the script kiddies trope. For many, it was no longer possible to dismiss or ignore this outcome of full disclosure. It simply became too risky and, potentially, too costly for both hackers and companies to maintain their attitudes toward each other. As a result, the root cause of these attacks was re-evaluated. In other words, script kiddies attacks inverted the balance of transaction costs: it became too costly for companies and many hackers to maintain the status quo. On the one hand, companies could no longer ignore the diligent hackers providing them with vulnerability information free of charge. On the other hand, it became more morally complicated for hackers to publicly drop an exploit code or hacking tool after the repeated script kiddies attacks. While the recruitment of hackers by some companies at the turn of the century may indicate that both parties were reassessing their antagonism toward each other, it is important to note that both the economization of the full disclosure debate and the change in transaction cost did not

57 In the debates that followed Ranum's speech, defenders of full disclosure argued that it remained the only possible way to pressure companies to improve the security of their products. They also warned that, if full disclosure were to be banned, ethical hackers would stop disclosing their findings, ultimately favoring malicious attackers who would eventually find vulnerabilities that would have otherwise been detected by ethical hackers. This interesting perspective considered the ban on full disclosure to be a threat to security itself. See for instance: https://web.archive.org/web/20041122124010/https://www.infoworld.com/articles/op/xml/00/08/14/000814opswatch.html

58 However, despite these arguments (see http://www.kb.cert.org/vuls/html/disclosure), attempts to control the release of exploit code were largely unsuccessful when considering the development of auditing tools like Nmap and Metasploit in the 2000s.

59 https://www.schneier.com/crypto-gram/archives/1999/0815.html#BackOrifice2000 and before that, in 1994: https://seclists.org/bugtraq/1994/Nov/113

immediately result in the establishment of a market. Contact and collaboration needed to occur first.

To fully understand the coming together of companies and hackers, we must return to Ranum inviting his peers to think in terms of cost-benefit analysis regarding the threats that hackers could face if they continued to engage in full disclosure. These threats were conceived with the state and national security in mind. Indeed, in his talk, Ranum warned his peers about the rising risk of legal prosecutions, which could be viewed as a rising cost of practicing full disclosure. He conveyed the idea that, under counter-terrorism measures, the publication of exploit code could soon be considered by authorities as supplying weapons to terrorist groups.[60] The idea of a cyber version of Pearl Harbor was looming large in political circles, and this concern only grew more prominent following the September 11th attacks the following year, impacting hackers' assessment of risks and costs. Notably, Ranum also eagerly conveyed a more mundane threat: the potential that federal administration lawyers could seize control over the situation at any time and impose new regulations on both hackers and companies that would curtail the autonomy and freedom that tech libertarians from both camps hold so dear. An alignment of interest was devised: to keep the state at bay in order to retain the freedom to self-regulate both camps had to come together and find themselves the solutions to their problems. This perspective may have been one driver of the development of collaborations that ultimately led to the model of responsible disclosure. Before discussing the emergence of this new model, however, I want to discuss one more factor that may have influenced the re-evaluation of transaction costs between hackers and companies.

The full disclosure model suffered from another notable problem: the scale of digital development changed dramatically during the 1990s with the emergence of the commercial use of the Internet; consequently, attacks could target more users and services than ever before. The increasing number of users also complicated the implementation of patches, making well-known vulnerabilities even more widespread. The management of digital infrastructure changed too. System administrators had to manage more complex and diverse machines than ever before. Full disclosure relied on

60 "Over the next few years, society's tolerance of hackers will lessen once hacking is regarded as "non-ideological terrorism". […] As home users increasingly find themselves the target of hackers, there will be less and less patience with break-ins. […] In the next five years, we are going to move to a counterterrorism model. It will turn into a witch hunt unless we stop the script kiddies today" (http://web.archive.org/web/20010805221436/http://www.zdnet.com/zdnn/stories/news/0,4586,2608077,00.html).

the idea that system administrators were able to carefully follow full disclosure fora, run frequent tests, and implement their own circumvention strategies before digital companies would release their patches. However, the extent and complexity of these systems as well as the increased reliance of standard business functions on digital operations limited the capacity of system administrators to tinker with and patch their systems at their own discretion. As a result, the timely advantage provided by full disclosure vanished. In other words, the full disclosure mindset was no longer aligned with the management and maintenance of regular business-level digital infrastructure at the turn of the century.

Responsible disclosure

A new model of interaction between ethical hackers and companies emerged from the crisis of full disclosure in the early 2000s. This new model was coined "responsible disclosure", the name itself offering a glimpse of how people involved in solving disclosure issues sought to reform the procedure. The new model was an attempt to develop solid collaboration between ethical hackers and companies. Within about three years, ethical hacking was radically redesigned by a handful of hackers and a risky (but smart) move by Microsoft. This chapter discusses the inception of this new model of disclosure, which represented the first attempt to mitigate antagonism prior to the creation of a market environment for the exchange of vulnerability information. Interestingly, the new model promoted transactions without facilitating monetary rewards, meaning that responsible disclosure promoted collaboration and exchange between two parties in a non-market fashion. This arrangement indicates that vulnerabilities were not yet conceived as commodities to be purchased.[61]
The first encounters between ethical hackers and companies aiming to find a solution to the perceived problems caused by full disclosure took place prior to Ranum's keynote speech. The first such encounter took place in 1997 after The L0pht released an upgraded version of its L0phtcrack tool.[62] Microsoft invited the hacker group to dinner, though the company representatives' intentions remained unclear to the hackers,[63] meaning that this first encounter did not ease their relationships (Goerzen and Coleman 2022). However, directors and senior managers from important companies (e.g., Microsoft, Novell, Sun) expressed a willingness to collaborate with hackers.[64]

The debates over full disclosure on Bugtraq and those provoked by Ranum's keynote speech regarding the crisis caused by the so-called script kiddies clearly indicate that ethical hackers were far from a homogeneous group. The concept of full disclosure was understood by ethical hackers in countless different ways.[65] As a result, they did not start conversing with companies as a coherent community. Instead, only a few companies and some ethical hackers acknowledged their common interests to define the conditions in which transactions could occur between them shortly after Ranum's keynote speech in 2000. Despite being some of the most antagonizing hackers, members of The L0pht and the CdC were key participants in discussions with companies, CERT-CC, and other institutions.

---

61 Appadurai (1988) and Callon (2017) drew our attention to the non-trivial social process involved in the transformation of an artifact into a (legitimate) commodity. In some cases, a strong moral basis prevents goods from being traded in daylight (Zelizer 1979, Steiner and Trespeuch 2015). It seems that a few more developments were necessary to commodify digital vulnerability information.

62 L0phtcrack allowed its users to gain access and brute-force encrypted passwords on Windows NT systems.

63 https://www.washingtonpost.com/archive/politics/1998/04/04/into-the-breach/8ae3cf86-fbd7-4037-a1b6-842df39d9db7/

64 https://www.blackhat.com/media/bh-usa-97/blackhat-eetimes.html

65 This difference of opinion and practice can be easily identified among the subset of ethical hackers contributing to Bugtraq.

One remarkably rapid shift that responsible disclosure brought about was the erosion of a major principle of the hackers' ethics at the heart of full disclosure: the free flow of information. The initial responsible behavior devised to limit the impact of full disclosure was to delay the publication of vulnerability information, providing companies with time to remediate the issue first prior to publication. Of course, this was necessary to establish the relationship between companies and hackers. To encourage hackers to postpone disclosure, companies had to prove their commitment to appropriately addressing their vulnerabilities in a timely manner. The principle of the free flow of information was tweaked in the interest of facilitating collaboration but remained influential in the debate over exploits.

From this perspective, we can understand the inception of responsible disclosure as a means of integrating ethical hackers into the digital tech industry. This is supported by the fact that, at the same time, ethical hackers were routinely getting hired or founding their own companies, expanding the growing cybersecurity business. The idea of this integration is supported by several authors, including Delfanti and Söderberg (2018) and Elis and Stevens (2022). However, perspectives on this integration vary quite a bit. While the latter view this integration as a capture of hackers, the former interpret it as a recuperation of hacker practices and innovations by corporate and political actors through a "coevolving relation between them [the hackers] and institutional and industrial actors" (2018: 9). The former's perspective seems to more accurately depict what was happening at the inception of the responsible disclosure model:

"On the one side, an industry or a branch of a state puts in place methods and routines to render systematic its interactions with hackers, aiming to increase benefits and reduce uncertainties. On the other side, anxiety over incorporation feeds into the self-representations, community norms, and practices of hackers, accommodating or resisting to various extents incorporation processes." (ibid.:12)

Such a perspective accommodates the diversity of ethical hackers' positions amid the simultaneous operation of multiple models of disclosure and bypasses the predicament of assuming "a pristine hacker subculture that at one moment was corrupted by industry" (ibid.:12). This, in turn, reverberates Mintz and Wolf's anthropological political economy theory, in which the formation of subjects (here, ethical hackers) lies at the intersection of the local history of interactions and larger political and economic processes (Roseberry 1998). The practice of full disclosure and the subsequent development of hacker identities and communities centered on full disclosure was the product of hackers' interactions and experiences with companies in the nascent digital tech industry competing for market share in the 1990s.[66] Of course, what took place at

66 I cannot help but agree with Söderberg and Maxigas (2022) when they understand hacking from within capitalist relations but never outside: "The notion of a free-floating subject position located 'outside' the social totality of capital is illusory" (27); "Something else that is ruled out by our historical approach is the

the inception of the responsible disclosure model is even more of a product of interactions between these two parties.

The idea of fixing the relationship between hackers and companies did not appear out of thin air in 2000. Attempts to correct problems inherent to the practice of full disclosure emerged in the late 1990s when a few hackers composed a set of disclosure policies to indicate to companies what was expected from them. The earliest policy that I found in the Internet Archive is the NMRC policy published online in September 1999,[67] though the RFP policy[68] published in June 2000 is better known and more detailed. These policies stated that the hackers would refrain from publishing vulnerability information if companies would agree to acknowledge their notification within a few days, develop a realistic plan to address the vulnerability, and negotiate their plan with the hackers who identified the vulnerability. These policies were the forerunners of the standards of the disclosure process—a crucial pre-market institution that established and spread many rules that are now widely accepted. I discuss this standardization of disclosure procedure further in another section, but it must be noted here that these hackers already reconsidered the transparency principle that was central to the model of full disclosure. Accepting a delay of information represented a major shift that contradicted the ethical, practical, and ideological concerns of the ethical hackers used to publishing vulnerability information via mailing lists, such as Bugtraq. In this sense, these policies resulted in a degree of value alignment between the two parties and, therefore, the introduction of a new disclosure model based on collaboration. In limiting behavioral unpredictability by setting the expectations of both parties, these policies constituted the first attempt to find common ground on disclosure, something that political economists would describe as lowering the transaction cost between hackers and companies.

The responsible disclosure model was inspired by but went further than these initiatives. The term "responsible disclosure" was introduced by CERT-CC when it defined its vulnerability policy in October 2000, two months after Ranum's keynote speech.[69] However, discussions about responsible behaviors (of both hackers and companies) were already circulating in the aftermath of Ranum's speech. The search for an agreeable basis on which to disclose vulnerabilities to companies revolved around the timing of disclosure (e.g., how long before going public, how long before a patch), the information to disclose (e.g., what to disclose, what form), and the definition of "the public" for vulnerability information (i.e., who gets what information, when do they receive the information). For some ethical hackers who were strong advocates of full disclosure, such as Weld Pond from the L0pht, it made sense to delay the publication of vulnerability

notion of a pristine, golden age of hacking that at some point was forsaken" (28).

67 https://www.nmrc.org/pub/advise/policy.txt

68 https://dl.packetstormsecurity.net/papers/general/rfpolicy-2.0.txt

69 http://www.kb.cert.org/vuls/html/disclosure

information so long as companies were committed to addressing the vulnerabilities identified by hackers in a timely manner.[70]

Parallel to these regulatory developments was the inception of other important institutions that formed the building blocks of vulnerability management. CVE[71] was established in 1999 to create a comprehensive database of known vulnerabilities. This database was a key element of the collaboration and communication between the two parties.[72] It provided an ID number and general description to each reported vulnerability, avoiding the confusion that previously came with using multiple names for a single vulnerability. OWASP[73] was founded in 2001 to bridge security knowledge with online application development. CERTs began to spring up in various countries, and CVSS, a standard with which to determine the severity of vulnerabilities, was developed by NIAC in 2004.[74] All of these initiatives contributed to various standardization processes and measurements necessary to facilitate a common language, common coordination tools, and common means of vulnerability analysis. Developing such interoperability through the establishment of institutions like CVE and CVSS—thus easing communication and understanding between the two parties—reduced the cost incurred during transactions, namely the cost of gathering relevant information to assess the usefulness of a potential transaction.

In 2001, Microsoft finally publicly entered the debate over full disclosure through a brilliant and provocative article[75] penned by Scott Culp, the founder of MSRC.[76] This influential article reignited the debate that Ranum started a year earlier. Following a series of unprecedented attacks by script kiddies between February and September 2001, Culp struck while the iron (prepared by Ranum) was hot. Although the article never explicitly mentioned Ranum, Culp was obviously restating Ranum's points about threats to full disclosure hackers, calling on ethical hackers to stop building and distributing "weapons" to be used against innocent and vulnerable users who do not patch their systems quickly enough—but he went further. He argued that the actions of full disclosure hackers constituted "information anarchy" and needed to be eradicated. In the context of post-9/11 America, such threats were taken very seriously.

In other words, Microsoft exploited the winds of change that were blowing in the hacking scene. Culp invited hackers to cooperate with Microsoft to disclose vulnerabilities to the

70 https://defcon.org/html/links/dc_press/archives/8/zdnet_weldpond.htm

71 Common Vulnerabilities and Exposures is a directory of security bugs that are known and traceable with a unique identifier.

72 https://www.cve.org/Resources/General/Towards-a-Common-Enumeration-of-Vulnerabilities.pdf

73 Open Web Application Security Project

74 National Infrastructure Advisory Council (https://www.cisa.gov/sites/default/files/publications/niac-common-vulnerability-scoring-transmittal-letter-11-22-04-508.pdf)

75 https://web.archive.org/web/20011109045330if_/http://www.microsoft.com:80/technet/treeview/default.asp?url=/technet/columns/security/noarch.asp

76 Microsoft Security Response Center

company in a responsible and polite manner without putting users at risk through the distribution of exploit code. Culp's idea for vulnerability disclosure was to wait for a patch release to publicize the vulnerability information in order to improve the rate of patch adoption. Thus, his strategy was twofold: limit the information available to script kiddies and promote update adoption among users, mitigating another important issue indirectly connected to the practice of full disclosure. Finally, Culp called hackers to join a new coalition, the OIS (Organization for Internet Safety), which would work to formulate an industry-wide standard for vulnerability disclosure policy.

Culp advocated for rules that were already at least partially mentioned in hacker groups' policies. The core elements of responsible disclosure were defined in five points. First, companies should be informed prior to public disclosure. Second, companies should acknowledge hackers' notifications and negotiate a reasonable work schedule with them to provide a patch. Third, companies should acknowledge hackers' contributions in the security advisory notice published alongside each patch. Fourth, the publication of vulnerability information should occur around the time of the relevant patch's release to boost patch adoption. Fifth, the publication of exploit code should be dismissed by default or at least limited to the smallest group of relevant people. This fifth point was certainly the most controversial, as it curbed what hackers saw as their freedom of speech. In other words, while most ethical hackers could agree to delay information and potentially create temporary guilds[77] or privileged enclaves of knowledge, many resisted the pressure to refrain from publishing exploit code, especially when a vulnerability was actively exploited at the time of disclosure to the company.[78] In such cases, many ethical hackers were in favor of expeditious full disclosure—including exploit code—to let as many people as possible devise quick fixes to block potential attacks.

Despite the disagreements and indignation following Culp's article, a new collaborative framework was clearly emerging and spreading. With it came new ideas about the logic and ethics governing vulnerability disclosure. The new model was nothing more than a collaboration perceived in economic terms to efficiently regulate the transaction of information on vulnerabilities. It is not a coincidence that security economics sprang up at the same time responsible disclosure surfaced. The first Workshop on Economics and Information Security (WEIS) took place in 2002, and Ross Anderson, one of the workshop's organizers, recently recalled the importance of debates on disclosure models:

"When we started doing work on the economics of information security, 20 years ago, one of the first big problems that came up was responsible disclosure. Back in those days, people were split between the Bugtraq guys who wanted to disclose everything at

77 https://web.archive.org/web/20210216174403/https://www.securityfocus.com/news/270

78 Sometimes, ethical hackers discover vulnerabilities that had already been discovered and used in cyberattacks or underground operations but never disclosed.

once, and the company lawyers who want to keep everything quiet forever. And the current responsible disclosure regime has come out from that."[79]

Notably, the collaboration induced by the responsible disclosure model emerged in a context in which some ethical hackers were being directly hired or contracted by companies (Goerzen and Coleman 2022: 39). Shifting their skills in vulnerability research into paid opportunities implied the establishment of guiding principles, and this had a significant impact on the definition of the responsible disclosure model. Therefore, we can assert that the antagonism "regulating" the relationship between ethical hacking and the digital tech industry was weakening at this point. However, frictions never completely faded despite the existence of agreed-upon guidelines. In fact, full disclosure continues to be practiced today, driving strong resentment between the two parties.[80] This is also the case in the more recent vulnerability transactions taking place in bug bounties.

The term "responsible" has a clear moral connotation, and it is important to fully understand how the new model introduced an ethical shift in disclosure and in the practice of ethical hacking. Responsible disclosure partially shifted ethical hackers' target. While full disclosure emphasized care for security technicalities (even if user awareness and sysadmin education were also included), the main concern of responsible disclosure was human and social. The emphasis was on care for collaboration between hackers and companies with the objective to improve digital security (i.e., limit attacks and online disruption), which would ultimately benefit users. As vulnerability disclosure practices became increasingly dependent on collaboration, the cost of opting for full disclosure increased.[81] However, this collaboration did not constitute an inevitable moral obligation. Full disclosure was still taking place, and ethical hackers could still resort to the public disclosure of vulnerability information if companies responded in an unsatisfactory manner.

This shift in hackers' primary ethical concern also revised the value attached to the free circulation of information, which was paramount in full disclosure, often considered to be one of hackers' most fundamental ethical tenets (Levy 1984). Indeed, responsible disclosure demanded important sacrifices: disclosure to the public needed to be delayed as vulnerability information needed to be first shared only with a small group of individuals. In addition, more control was exerted over the publication of exploit code. In

79 https://www.youtube.com/watch v=EtZxpoxXr7I&list=PLeUGLKUYzh_gEM00XPd6fZZNkHrkLtr_5&index=20

80 Scandals over full disclosure are not rare nowadays. See, for instance, the 2021 disclosure pertaining to Apple's iOS (https://web.archive.org/web/20210216174403/https://www.securityfocus.com/news/270), the unintentional release of information on printer drivers (https://www.bleepingcomputer.com/news/microsoft/remote-print-server-gives-anyone-windows-admin-privileges-on-a-pc/), and Fortinet's accusation of Rapid7 releasing vulnerability information before the agreed-upon timeframe (https://www.zdnet.com/article/fortinet-slams-rapid7-for-disclosing-vulnerability-before-end-of-90-day-window/).

81 This can be compared to what political anthropologist Laura Nader has referred to as the harmony ideology (1990), which was particularly influential in the US around the same time.

a way, increased secrecy was the price to pay to get companies to engage with ethical hackers and limit "avoidable" attacks.

This is a clear indication that ethical shifts in disclosure, including the shift in control over vulnerability information that made vulnerability disclosure more predictable for digital tech companies, were devised by models preceding the inception of a defensive market. Indeed, the history of vulnerability disclosure models shows that predictability and stability were not the consequence of bug bounty programs, as argued by Elis and Stevens (2022: 78); rather, the predictability of disclosure and the stability of the relationship between hackers and companies were already at the core of the responsible disclosure model by the early 2000s. Therefore, instead of asserting that the market is the cause of a new moral order (Elis and Stevens 2022: 25), we can acknowledge that the ethical changes that took place around the inception of responsible disclosure may have paved the way for the emergence of a market several years later. What the defensive market introduced later on was more complete control and ownership of vulnerability information by purchasing them and enforcing non-disclosure agreements—but hackers' freedom to do what they want with their findings was already curtailed by the shift in vulnerability transaction practices at the turn of the century.

Soon after the primary principle of the free circulation of information faded away, another crucial principle began to crumble. Financial gain from vulnerability disclosure became desirable, and bug bounties institutionalized the provision of monetary rewards in exchange for vulnerability information. However, before presenting this shift, we must take a deeper look at the development of standards and other institutions that emerged prior to the making of a defensive market.

Fleshing out responsibilities and the shift to coordination

The idea of devising a new "responsible" model opened the floodgates to defining norms in vulnerability disclosure and working on standardized procedures guiding the discloser and the maintainer (i.e., the hacker and the companies), fostering their collaboration, and framing their expectations. Norms and ideas considered to be standards did not come out of thin air: in a way, they were already floating around people involved in disclosure practice. Developing standards also involved the reformulation of pre-existing written norms from early policies, such as the RFP policy.

Such standards tend to formalize the minutia of collaboration from the perspective of responsible disclosure. In addition to simply formalizing the various terms of conduct (i.e., casting the customs into written form), the formalization process can help to refine or tweak former norms, be they written or unwritten. Legal anthropologists interested in the codification of customary law during the colonial period referred to this phenomenon as "double institutionalization" (Bohannan 1965, see also Channock 1985 and Ranger 2006). Of course, this phenomenon is not limited to colonial settings, as it also applies to contemporary legal processes (Latour 2002). Once norms are translated into a formal document, attitudes and behaviors toward the new regulation can change the way in which the norms are interpreted and mobilized. In other words, the responsible disclosure model promoted the demise of unwritten customary rules in the practice of vulnerability disclosure.

Below is an example of standardization and double institutionalization. As mentioned in the previous chapter, attempts to solve the problems of full disclosure fostered a degree of moral care for collaboration between ethical hackers and companies. Thus, this norm was floating around for a while.[82] Normative behaviors aimed at preserving collaboration (e.g., promoting mutual understanding) were codified into policies and standards in many different ways. One standard published around 2002[83] stipulated that, in the event of a dispute, parties should search for common ground to mediate their disagreements using alternative dispute resolution (ADR[84]) procedures. Here, seeking consensus through arbitration or mediation was devised to mitigate the risk of full disclosure in the event of friction. Many contentious events have occurred since the introduction of formal clauses aimed at regulating conflicts between parties, but hackers' decision to litigate and put an end to collaboration with a company may have become more difficult once the moral value of protecting collaboration and communication began to be actively promoted in standards and policies.

---

82 Collaboration was, of course, mentioned by Marcus Ranum in his keynote address (see previous section). The call to "get together" was echoed by Scott Culp and CERT-CC in their 2000 policy.

83 https://datatracker.ietf.org/doc/draft-christey-wysopal-vuln-disclosure/

84 ADR was a recent legal hack used to avoid long and costly court litigations in the US. In this sense, ADR served to reduce antagonism and address the refusal to compromise. For a perspective on ADR from an anthropological perspective, see Nader (1995).

This process of codification emerged at least, if not before, 1999 with the NMRC and RFP policies. Shortly thereafter, in October 2000, CERT-CC revised its own policy to include a vulnerability information embargo period of 45 days, during which the company can develop an appropriate patch. The intention of the policy was "to balance the need of the public to be informed of security vulnerabilities with the vendors' need for time to respond effectively".[85] "We are trying to help build an ethos of how to release vulnerability information," said Shawn Hernan, CERT-CC's team leader for handling vulnerability (ibid). Then came initiatives to set up industry range standards to avoid the proliferation of various competing norms. Around 2001, Microsoft, through its newly founded OIS (Organization for Internet Safety) pursued the following ambition: bring various actors together, including ethical hackers, to devise an industry-level standard for responsible disclosure. Among OIS members, two people were pivotal in the first attempt to write a standard: Steve Christey from the MITRE Corporation (the co-founder of CVE) and, surprisingly, Chris Wysopal (also known as Weld Pond) from The L0pht, a former full disclosure aficionado who had been involved in the release of famous Microsoft hacking tools in the 1990s. The standard proposal was submitted to the IETF in 2002;[86] it begins with the following declaration:

"During the process of disclosure, many vendors, security researchers, and other parties follow a variety of unwritten or informal guidelines for how they interact and share information. Some parties may be unaware of these guidelines, or they may intentionally ignore them. This state of affairs can make it difficult to achieve a satisfactory outcome for everyone who uses or is affected by vulnerability information. The purpose of this document is to describe best practices for a responsible disclosure process that involves vulnerability reporters, product vendors or maintainers, third parties, the security community, and ultimately customers and users."

This draft sought to increase effectiveness in disclosure, minimize the risks of and time required for vulnerability management, and mitigate antagonism between parties stemming from a lack of consistent and explicit disclosure practices. It also provided guidelines for providing information to customers and the security community. Overall, the document provided a framework of incentives and controlling processes in line with the economic rationality underlying responsible disclosure. However, while it specifies, that transactions should take place, it does not mention monetary rewards.[87] Despite this first attempt, standards were still being discussed at a conference organized by Jennifer Granick at Stanford in late 2003 (Goerzen and Coleman 2022: 58).

85 https://web.archive.org/web/20080725172731/http://news.zdnet.co.uk/security/0,1000000189,2081837,00.htm

86 The IETF (Internet Engineering Task Force) is an organization that defines and publishes technical standards for the Internet. (https://datatracker.ietf.org/doc/draft-christey-wysopal-vuln-disclosure/).

87 However, two years later, in 2004, two companies initiated an open vulnerability market by paying hackers in exchange for vulnerability information. This is discussed further in the next section.

Other standards were drafted in the years that followed, including some by state lawyers and regulators[88]. In other words, many standardization initiatives in vulnerability disclosure were competing for influence. Notably, controlling the norms of disclosure and the narratives surrounding vulnerability disclosure through codification became an important goal for Microsoft around this time. A few years later, the company promoted the creation of an ISO standard by assigning one of its employees, Katie Moussouris, a former hacker from @Stake and a close friend of Weld Pond and the cDc hacker group, to author and follow up on the long ISO procedure. The proposal was submitted in 2008, and the finalized standard was published in 2014 (ISO/IEC 27147:2014). Microsoft's concern was shared by other big tech companies at the time, including Google, indicating that managing the norms of disclosure had become a more important issue for big digital tech companies. These initiatives also point to the increasing professionalization, internationalization, and governmentalization of vulnerability disclosure. As a result, the norms dictating the practice of vulnerability disclosure slipped from hackers' grasp and became a concern of corporate and state institutions. In 2010, Microsoft renamed its standard "coordinated vulnerability disclosure" (CVD), and, just two days before Microsoft's announcement of the name change, Google published a blog post[89] raising several criticisms of responsible disclosure and adjusting the embargo period to 60 days.[90] From there, just to name a few, ENISA went public with a document in 2015,[91] FIRST did so in 2017,[92] and CERTCC refined its framework in 2019.[93]

The term "responsible disclosure" as a descriptor of new disclosure standards largely faded, replaced by the more neutral term: coordinated vulnerability disclosure (CVD). At first, it seemed that CVD largely represented a Microsoft PR operation rather than a radical shift in ethics or practice. The company merely sought to rebrand responsible disclosure in 2010, announcing CVD with the following statement:

"CVD does not represent a huge departure from the current definition of 'responsible disclosure,' and we would still view vulnerability details being released broadly outside these guidelines as putting customers at unnecessary levels of risk".[94]

That same blog post argues that "responsible" was too loaded of a word, asserting that "coordinated" was more neutral. The significant change that Microsoft wanted to

88 For instance the DHS: https://www.dhs.gov/xlibrary/assets/vdwgreport.pdf

89 https://security.googleblog.com/2010/07/rebooting-responsible-disclosure-focus.html

90 Previously, the CERT-CC had fixed the embargo time to 45 days and the IETF standard to 30 days with the possibility of an extension upon agreement.

91 ENISA is the European Union agency for cybersecurity (https://www.enisa.europa.eu/publications/vulnerability-disclosure)

92 Forum of Incident Response and Security Teams (https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.0)

93 https://vuls.cert.org/confluence/display/CVD

94 https://msrc-blog.microsoft.com/2010/07/22/announcing-coordinated-vulnerability-disclosure/

publicize was about the control over "how issues are addressed publicly."[95] Compared to the search for a consensus previously instituted by the responsible disclosure model, CVD constituted a move to extend the patch-development period and, in turn, postpone public disclosure. The stated reason for this was testing: "For Microsoft, even a 1% test failure rate could affect millions of our customers, so we take testing for functionality impact as seriously as we do the testing to make sure the update comprehensively addresses the vulnerability."[96] The matter of what constitutes sufficient time to produce quality patches was not new; in fact, it had been discussed back in the 1990s.[97] What was new is that both Microsoft and Google effectively unilaterally redefined the central issue of embargo time in disclosure through their policies.

Along these lines, the trend over the last decade has been to extend the pre-disclosure period for big companies like Microsoft and Google. Handling complexity has always been the main reason for these adjustments. In 2020, Google extended the embargo period to 90 days to ensure the thoroughness of patch development[98] and boost patch-adoption rates.[99] This change demonstrated that reassessments of vulnerability disclosure norms no longer required a consensus. Big tech companies, which had long rejected the very practice of disclosure, now had control over the process.

Two years before Microsoft's announcement of CVD, the company founded the Microsoft Vulnerability Research Program (MSVR) to "improve the security [not only] of Windows, but of the entire Windows ecosystem, responsibly researching vulnerabilities in third-party software most commonly used by Windows customers."[100] Google did something similar in founding its Project Zero in 2014. In doing so, the two giants positioned themselves as the new champions of vulnerability research by dedicating teams to searching for bugs in both their own products and those of other companies, enabling them to act as *de facto* coordinating parties in cases of multi-party vulnerabilities,[101] regulating not only the process of vulnerability disclosure but also the way in which

95 Ibid.

96 Ibid.

97 e.g. https://seclists.org/bugtraq/1994/Nov/143

98 "Too many times, we've seen vendors patch reported vulnerabilities by 'papering over the cracks' and not considering variants or addressing the root cause of a vulnerability. One concern here is that our policy goal of 'faster patch development' may exacerbate this problem, making it far too easy for attackers to revive their exploits and carry on attacking users with little fuss" (https://googleprojectzero.blogspot.com/2020/01/policy-and-disclosure-2020-edition.html).

99 "End user security doesn't improve when a bug is found, and it doesn't improve when a bug is fixed. It improves once the end user is aware of the bug and typically patches their device. To this end, improving timely patch adoption is important for ensuring that users are actually benefiting from the bug being fixed" (https://googleprojectzero.blogspot.com/2020/01/policy-and-disclosure-2020-edition.html).

100 https://msrc-blog.microsoft.com/2008/08/07/threats-in-a-blender-and-other-raisons-dtre/

101 In some cases, a vulnerability can affect multiple companies and organizations, each of which must develop a patch. This was the case with the Heartbleed vulnerability uncovered in 2014 (https://web.archive.org/web/20140407202308/http://heartbleed.com/). CVD provides guidelines to establish a coordinating party in such cases. More recently, supply-chain attacks and attacks involving multiple vulnerabilities have reinforced the need for coordinating parties. This was the case in attacks on Solarwind in 2022 and Kaseya in 2021, for which coordination was necessary to address vulnerabilities (https://www.trojansource.codes/trojan-source.pdf).

vulnerabilities are handled to other companies. Thus, their control over vulnerability disclosure no longer applied only to norm standardization. Their power now extended across the entire process, from research to disclosure. In other words, the shift from "responsible" disclosure to "coordinated" disclosure represented a gain in power and capacities by companies like Microsoft and Google. These developments can largely be attributed to the complexity and embeddedness of organizations and code into a dense digital ecosystem. Considering them in the context of the security ecosystem reveals that these two companies opted to position themselves in the zone already occupied by CERTs and CISRTs, which were set up to coordinate complex vulnerabilities that affect multiple companies and organizations. Alongside these developments, market-led initiatives have flourished since 2002, developing into the bug bounty model and, in turn, having a significant impact on the practice of vulnerability disclosure.

The development of a defensive vulnerability market

The defensive market did not suddenly emerge at an easily identifiable point in time. Rather, we can point to different moments in the history of disclosure in which information on vulnerabilities was exchanged for monetary compensation. The first public initiative was devised by Netscape in 1995. For several months, the company advertised a "bug bounty".[102] Anyone who could find a vulnerability in its browser (the defunct Netscape navigator) was eligible for a bounty.[103] As Elis and Stevens (2022) aptly recount, the Netscape bug bounty was the company's answer to three public disclosures that had compromised the reputation of the company only a few weeks after it had become a publicly listed company on the NASDAQ. The initiative was immediately criticized by hackers on the Cypherpunks mailing list.[104] For Elis and Stevens, this first initiative largely constituted a public relations stunt (ibid.: 38) that disappeared in 1997 shortly before the collapse of the company. The Netscape bug bounty was revived in 2004 when Mozilla funded a bug bounty for its Firefox browser, offering $500 for a critical vulnerability.[105] These initiatives constitute the precursors to the bug bounties that began to develop significantly around 2010.

However, another type of marketplace for vulnerability information was created in 2002 by iDefense, a company founded in 1998 to provide "comprehensive and actionable security intelligence" to its customers.[106] Through its Vulnerability Contributor Program, iDefense paid hackers for undisclosed vulnerability information so long as they agreed to postpone public disclosure for at least one week;[107] in this way, the company could secure some exclusive information to sell to its customers. According to Sunil James, the manager of the program in 2003, the "VCP, which began in August 2002, was established to respond to the needs of government agencies, financial institutions, and private organizations to protect their critical information infrastructures against an unprecedented incidence of cyber attacks."[108] As with responsible disclosure, which was gaining prominence around the same time, iDefense's VCP was curbing the free flow of

---

102 The idea of offering a reward to anyone identifying a flaw or error has an old and famous origin in computer science: the Knuth reward checks. Donald Knuth is the author of *The Art of Computer Programing*, a highly revered five-volume book series that he started writing in 1962. Knuth offered a check for $2.56 to anyone who could find an error in his publications. Only a few of these checks were ever cashed, as owning one is widely considered to be a prestigious trophy in "computerdom" (https://web.archive.org/web/20181109034030/https://www.technologyreview.com/s/400456/rewriting-the-bible-in-0s-and-1s/).

103 https://web.archive.org/web/19970501041756/ and http://www.netscape.com/newsref/pr/newsrelease48.html

104 See the following thread, "Netscape rewards are an insult": https://mailing-list-archive.cryptoanarchy.wiki/archive/1995/10/c6e4c6d1d79368e681d83309783ae690bb612e456433dc0e79a231a0b3fdde83/.

105 https://blog.mozilla.org/press/2004/08/mozilla-foundation-announces-security-bug-bounty-program/

106 https://www.helpnetsecurity.com/2003/04/01/interview-with-sunil-james-manager-of-idefenses-vulnerability-contributor-program/

107 https://web.archive.org/web/20020812035333/ and http://www.idefense.com/contributor.html

108 https://www.helpnetsecurity.com/2003/04/01/interview-with-sunil-james-manager-of-idefenses-vulnerability-contributor-program/

information to limit the exploitation of vulnerabilities with the intent to generate value from its intermediary role between the company and its customers. In 2005, TippingPoint, a company founded in 1999 that was part of 3Com at the time, launched a similar program—the Zero Day Initiative (ZDI[109])—which aimed to match monetary compensation for vulnerability information with hackers' expectations, which had increased since the introduction of iDefense's VCP.[110] At that time, both programs were competing with brokers active in the offensive market.

A few other initiatives were already creating a marketplace for vulnerability information. The first ones were brokers selling vulnerabilities to state intelligence agencies and driving up the prices for hackers' services in the early 2000s. In her book, Perlroth recounts three hacking boutiques in the late 1990s recruiting hackers and buying vulnerability information on behalf of US intelligence agencies (2021: 84). However, the intelligence agencies of many other states, including France, had been recruiting hackers since at least the 1980s (Coleman 2021). Thus, hackers were first recruited directly by state agencies before intelligence agencies began to promote the establishment of private brokers to reach more hackers and acquire more information on vulnerabilities. Since then, Vupen, Zerodium, NSO, HackingTeam, and many other companies have bought vulnerability information to provide information, exploits, and hacking suites to state agencies all over the world. Back in the early 2000s, rates offered by brokers to hackers for vulnerabilities were already far higher than those offered by iDefense and ZDI (Perlroth 2021: 81), but the offensive market suffered from key shortcomings, according to one hacker with first-hand experience selling information on vulnerabilities to US intelligence agencies.[111] To attract more hackers frustrated by the offensive market's shortcomings, iDefense and ZDI began to organize contests with special rewards as early as 2006.[112] A year later, Dragos Ruiu, the founder of the CanSecWest conference, initiated the Pwn2Own contest, which offered an Apple laptop to the hacker who submitted the best Apple vulnerability[113]. ZDI partnered with the conference and offered a cash prize to the winner on top of the laptop (ibid), attracting even more hackers, including some active in the offensive market.

What is particularly interesting to note about these initiatives is that their initiators and earliest contributors constituted a relatively small clique. Brokers, ZDI and iDefense staff, and hackers involved in Pwn2Own were contributing to the other initiatives as well (some of them worked also for US intelligence agencies) and, thus, constituted a dense network

109 David Endler worked at iDefense before joining TippingPoint in 2004 to found ZDI (Perlroth 2021: 583).

110 https://www.cnet.com/tech/mobile/verizon-wireless-consumers-leave-despite-dangling-cheaper-unlimited-plan/

111 https://econinfosec.org/archive/weis2007/papers/29.pdf

112 Similar hacking challenges offering rewards were already available: iDefense inaugurated its quarterly challenges in early 2006: https://web.archive.org/web/20061018113231/http://labs.idefense.com/vcpchallenge.php#more_q1+2006%3A+%2410%2C000+vulnerability+challenge.

113 https://duo.com/decipher/lawyers-bugs-and-money-when-bug-bounties-went-boom

of actors interacting with one another.[114] The idea for Pwn2Own was sparked in 2007 out of frustration with the way that Apple was treating hackers revealing vulnerabilities in their products.[115] Two years later, after several vulnerabilities in Apple products had been revealed at Pwn2Own contests, a handful of hackers started to call for a change in vulnerability disclosure. Frustrated by the shortcomings of the offensive market, the limited rewards available from reporting a vulnerability to iDefense and ZDI, the reluctance of companies to pay for the vulnerabilities found in their products, and the threats that some companies levied against hackers—despite the well-established existence of responsible disclosure guidelines—Dai Zovi, Sotirov, and Miller, three successful hackers at the Pwn2own contests, went onstage at the CanSecWest Conference in 2009 with a placard reading "No more free bugs".

"There [are] people who work for the companies that are doing the exact same thing as we do and they get a paycheck. So, then, we just had the idea that we were going to do this 'no more free bugs' thing. […] We found a marker somewhere and we made the sign. So, Dino and Alex held the sign while I proselytized about it, at the mic." (Miller interviewed by Fisher).[116]

By the late 2000s, Pwn2own, ZDI, iDefense, the existing offensive market, and a growing number of hackers accustomed to receiving money for vulnerability information were collectively pressuring companies to acknowledge that monetary compensation for the hard work of uncovering vulnerabilities was reasonable. The taboo of claiming monetary rewards for vulnerability information was fading. What was once considered a fundamental ethical principle of hackers was eroding, eventually allowing for a surge of bug bounty programs.

These early market-led initiatives and the offensive market began to significantly impact vulnerability disclosure practices in 2010. As mentioned earlier, Google instituted its Vulnerability Reward Program in 2010, and Facebook developed its bug bounty program the following year. Bugcrowd became the first operational bounty platform in 2011, and HackerOne followed suit in 2012. Microsoft followed the trend in 2013, and Apple embraced the idea of vulnerability disclosure later on, starting to offer monetary rewards in 2016. Of course, these are just a few of the companies that began to include monetary rewards in their vulnerability disclosure programs or started a bug bounty program.

To better understand the confluence of the history of vulnerability disclosure with the influence of the offensive market through defensive market initiatives in the form of a widespread bug bounty model, it may be necessary to reassess the essential points made so far in this paper. In the 1990s, companies had no interest in interacting with hackers

114 Ibid.

115 http://web.archive.org/web/20070324154342/, http://blogs.techrepublic.com.com/Ou/?p=451, and https://seclists.org/dailydave/2007/q1/289

116 https://duo.com/decipher/lawyers-bugs-and-money-when-bug-bounties-went-boom

trying to provide them with vulnerability information for both economic and non-economic reasons. From a purely economic perspective, the incentives to make more secure products were simply insufficient and companies were already pouring a significant amount of money into testing. This was a major source of frustration[117] among a generation of ethical hackers who cared for technology and consequently resorted to the practice of public disclosure (the full disclosure model).

Alongside the development of a corresponding ethos of chivalry (though generally not one that entailed ideological motivation to act against companies), the principle of free access to information was dear to full disclosure hackers who embraced the transparency model of security, an adversarial model that had been devised by cryptographers and locksmiths. Autonomy and self-governance were also key principles of this model of security. In addition, vulnerability information could not be conceived as a legitimate commodity in disclosure processes for legal and ethical considerations. At the same time, an offensive market began to thrive. In other words, as a defense mechanism, disclosure was developing as a practice opposed to the shadowy realm of black hats selling vulnerability information and exploits to intelligence agencies and criminal organizations. All these reasons hindered the development of a defensive market.

Full disclosure developed significantly through mailing lists. Among them, Bugtraq was prominent in the development of a forum to share and discuss vulnerability information.[118] These forums were sites where hackers could learn, develop their reputations and have fun shaming companies. Bugtraq played a role in building up antagonism between hackers and the digital tech companies that they were hacking. Despite—or perhaps on account of—full disclosure not developing a conducive environment between hackers and companies, the former were able to publicize their capabilities and gradually professionalize. Once taken seriously, they were able to be heard on crucial security issues with the potential to cripple digital infrastructure. The recruitment of full disclosure hackers indicated that antagonism could also be reevaluated by both parties at the end of the 1990s. Concomitantly, full disclosure served to promote hackers' start-ups, which were taking off rapidly in the fast-growing cybersecurity industry. However, transaction costs remained too high for both hackers and companies to engage in sustained collaboration on vulnerability disclosure.

This situation gradually changed due to rising concerns over the practice of full disclosure. Around 2000, these concerns were heightened by an increase in cyberattacks caused by the so-called "script kiddies" using vulnerability information and exploit codes made public by full disclosure hackers to launch widespread attacks over the Internet. Internal debates among full disclosure hackers at this time indicate that there was

117 Another frustration was related to the perceived inability of the CERT-CC to serve as a facilitator institution in vulnerability transactions between hackers and companies.

118 Hacking conferences and BBS (Bulletin Board System) were crucial for hackers to connect with their peers (Coleman 2010).

nothing even approaching a consensus among them regarding their disclosure practices, including the time of release and the information provided.[119] This diversity in the practice of full disclosure demonstrates the heterogeneity[120] of this community and its fragmentation in the wake of corporate demands. This crisis of full disclosure made antagonistic attitudes among hackers and companies toward each other too risky and, potentially, too costly. At the same time, however, the crisis aligned the interests of both hackers and companies to solve their disagreements and find common ground in order to avoid interference from state regulators.

The many dimensions of the full disclosure crisis prompted a redefinition of the antagonistic relationship between hackers and companies. The development of a functional collaborative relationship was motivated by multiple converging interests, resulting sometimes in hackers being hired or contracted by companies. In addition to their care for security, the preservation of the relationship between hackers and companies was sustained the rising costs of engaging in full disclosure. It became necessary to define the conditions in which vulnerability transactions could occur between the two parties and limit unpredictable behaviors. The diminution in transaction costs was caused by ethical, relational, practical, and institutional changes in disclosure practice. Agreements to regulate the dissemination of information eroded the principles of transparency and autonomy that hackers held dear. Institutions like disclosure policies, CVE, CVSS, OWASP, CERTs, OIS, WEIS, and many others contributed to the development and dissemination of vulnerability disclosure standards. Standardization and the phenomenon of "double institutionalization" marked the progressive demise of unwritten customary rules causing unexpected behaviors and, in turn, friction between parties. Standards were designed along a framework of incentives and processes backed by economic rationale, gaining significant traction among hackers as well as companies. In other words, hacking was disciplined and governmentalized. Companies developed a stronger interest in controlling the norms of disclosure. Consequently, the development and deployment of vulnerability disclosure models became more professionalized, internationalized, and governmentalized. At the same time, companies acquired the capacity to unilaterally dictate disclosure norms—gradually positioning themselves on the terrain occupied by CERTs and CISRTs—and developed capabilities to champion vulnerability research and the management of disclosure processes.

During the same period (2000–2010), a few initiatives led to the development of a defensive marketplace for information on vulnerabilities for financial and state institutions and attracting (frustrated) hackers active in the offensive market that emerged during the previous decade. Hackers active in these markets publicly promoted and legitimized the

119 In addition, the adequate attitude of system administrators implied by the full disclosure model did not match the changes in the field driven by the tremendous developments in the business environment's digital infrastructure.

120 This heterogeneity is reflected by the diversity of political sensibilities already identified in hacker circles by Coleman and Golub (2008).

idea of monetary compensation for the identification of vulnerabilities. I argue that all of the historical transformations outlined above made both the commodification of vulnerability information and the emergence of an extensive defensive market possible around 2010. In other words, the emergence of bug bounties as a model of disclosure in which vulnerability information is traded is the result of a complex and diverse historical process during which control over vulnerability information and vulnerability processes shifted incrementally.

But what kind of markets are the markets for vulnerability information? First, they differ significantly from typical commodity markets, which tend (at least in theory) to have a perfectly competitive structure. Vulnerability markets are inherently imperfect: sellers and buyers are limited in numbers, and the latter doesn't have a wide choice of equivalent vulnerabilities to purchase. In addition, the power to set the price of a vulnerability often resides with a single actor. Second, the structures of the two vulnerability markets—the offensive vulnerability market and the defensive vulnerability market—are distinct. While the offensive market is characterized by the presence of several buyers and few sellers, the defensive market features numerous sellers and few buyers. In addition, the early defensive markets established by iDefense and TippingPoint accommodate more buyers than in bug bounty programs, which generally feature just one buyer for any given vulnerability. That said, in the case of a multi-party vulnerability, buyers offering bounties can be scarce in the defensive market. Therefore, the general form of a defense market is an oligopsony while that of bug bounties is a monopsony.

Through the transformation of vulnerability disclosure models, some hackers were progressively channeled, disciplined, and regimented in bug bounty programs as freelance service providers for digital tech companies at first and increasingly across multiple sectors, including transportation, finance, and retail. Notably, however, the process of disciplinarization does not mean that the changes occurring in the practice of hacking stemmed from an overarching intentional "ploy" or a single type of actor involved in the business of vulnerability disclosure. Rather, they were the result of interactions, tweaks, and fixes in countless vulnerability disclosure processes over several decades. The emergence of bug bounties in 2010 marks a novel step in the integration of ethical hackers in the digital tech industry, but hackers had long been prominent and successful actors in the historical trajectory of vulnerability disclosure, especially in "stitching" ethical hacking to business operations.[121]

121 For example, a recent Twitter thread discusses how hackers hired by Microsoft instigated themselves into new technology projects, including the Microsoft bug bounty program: https://twitter.com/mattt_cyber/status/1526729401068445696?s=21.

The bug bounty model: Hacking as a service

A bug bounty is a program that incentives vulnerability research and disclosure of information by offering a reward to hackers who identify valid vulnerabilities on a specific target. Programs can be set up by companies or hosted by third-party platforms.[122] Either way, these programs allow companies to buy vulnerability information about their products from hackers (or, as they often refer to themselves, bug hunters).[123] For the companies, these programs promote ethical hacking as a form of active security testing for their products, services, and infrastructure. For the hackers, they serve as invitations to hack (sometimes more safely) and be rewarded for doing so.

Each program establishes a "scope" that defines the range of valid vulnerabilities to qualify for compensation. A scope is defined in term of asset (subdomain, application, product) and the types of vulnerability the company is interested about (Li 2021). Thus, hackers must follow specific guidelines and demonstrate the impact of their identified vulnerability in a written report. Submitted reports are typically evaluated by a team of company employees. This process is referred to as triage, and it involves multiple distinct tasks, including sometimes dialogue between the triager and the bug hunter. If the reported vulnerability is valid (i.e., within the scope of the program and not previously reported) and has security implications for the product, service, or infrastructure, this team determines the reward for the provided information. The reward is based on the type and significance of the vulnerability. Hunters are paid a lump sum for a valid report —not a wage based on the time they put into the report. In the event that a valid vulnerability is reported more than once, only the hunter who submitted their report first is compensated.

Today, bug bounties are universally recognized as an important instrument for improving an organization's technological security alongside (though sometimes instead of) a vulnerability disclosure policy. According to Elis and Stevens, "Finding, disclosing, and fixing bugs is important infrastructure work. […] Bug bounty programs now structure and govern much of this work" (2022: 77). Even national governments have implemented bug bounties. In both the US and France, the military was the first state institution to do so. This section focuses only on the changes in vulnerability disclosure brought about by the bug bounty model. It also specifies a few consequences that bug bounties have for the definition of ethical hackers in the role of bug hunters.

---

122 These platforms (e.g., HackerOne, Bugcrowd, Intigriti, Yeswehack) have been key to the adoption of the bug bounty model of disclosure in non-digital-tech industries while also publicizing the benefits of hacking to the general public through the mainstream media.

123 Bug hunters are ethical hackers operating in the context of a program. They can also serve as pen testers and disclose vulnerabilities without seeking monetary rewards. There are no clear-cut lines that differentiate a bug hunter from a hacker aside from the fact that, in certain situations, hackers and hunters demarcate themselves (sometimes in a derogatory manner) from each other. Notably, the term "bug hunter" was already in use before bug bounties—since at least 2005 (https://web.archive.org/web/20070111151903/, http://news.com.com/Bug+hunters%2C+software+firms+in+uneasy+alliance/2100-1002_3-5846019.html).

Bug bounties are much more than just incentive mechanisms. They are complex governing instruments through which companies can manage the flow of vulnerability information instead of just publicizing a vetted hackable perimeter (or scope) and gathering a crowd of hackers around it. As a matter of fact, disclosure policies had already defined a scope within which hackers were permitted to hack. However, policy-defined scopes are typically more durable than those defined in bug bounty programs. The ability to modify a bug bounty program's scope is commonly emphasized by platforms: a company can modify its program's scope at any point.[124] Of course, this has a significant impact on the hunter's ability to secure compensation for the time and effort that they invest in identifying vulnerabilities. For companies, this flexibility enables them to maintain a successful program. Companies are advised to start small in terms of scope in order to avoid an avalanche of reports to evaluate up front that could drain their budget.[125] For this purpose, platforms and companies have devised "private programs" that feature a small scope and availability only to a small group of hunters before they are opened up to everyone. Thus, the ability to control these programs' rewards and scopes allows companies to regulate the flow of vulnerability information and maintain a manageable active crowd of hunters to secure the success of the program in the long run. An overly restrictive program could inhibit the maintenance of a sufficient number of active hunters. This is important because, as programs began to compete against one another, retaining the best hunters became a pressing issue, prompting companies to modify their policies, scopes, and rewards to remain attractive. Hacking events, special programs, invitations to social gatherings, and presentations on new programs at hacking conferences are regularly organized by large tech companies to promote their bug bounty programs. Of course, platforms also offer to help their customer companies in this regard in order to secure their customers' program visibility as well as boost the reputation of some hunters in the hacking community.

Bug bounty managers often use hacking conferences as opportunities to present their programs and outline the types of vulnerabilities they are looking for.[126] Additionally, they discuss strategies that hunters can use to improve the quality of their reports, often emphasizing that a high-quality report could result in a higher reward.[127] Effectively, bug bounties are instances of the fine-grained disciplinarization of hacking and disclosure, and this goes well beyond the mandatory NDAs that hunters need to sign to participate. This disciplinarization doesn't limit itself to technical guidelines; it also applies to social

124 Bugcrowd n.d.; https://blog.yeswehack.com/best-practices/cybersecurity-bug-bounty-attack-is-the-best-form-of-defence/

125 This is a common situation faced by many companies in the first few months of their bug bounty program. See, for example: https://www.yeswehack.com/companies/launch-a-program/.

126 Apple presented its bug bounty in 2016 at the Blackhat USA conference (https://www.youtube.com/watch?v=BLGFriOKz6U), while Microsoft launches its Azure bug bounty at the same conference in 2019 (https://www.zdnet.com/article/microsoft-announces-azure-security-lab-azure-bug-bounty-expansion/).

127 For instance, Jarek Stanley, manager of the bug bounty program at Microsoft, gave a talk in this vein at Nullcon in Goa in 2019: https://www.youtube.com/watch?v=F9tbzgpe270.

interactions. Harmonious relationships are widely promoted through guidelines, presentations, online tutorials, and tweets. Aside from compliance, kindness, patience, and diligence are the most common values promoted in such discourse,[128] often with a focus on points of contact: interactions between the hackers and the triagers. Many disagreements and misunderstandings can arise in bug bounty programs, and triagers are usually the program workers who are in direct contact with those reporting vulnerabilities. Program managers and platforms have sought to explain the difficulty of triage work and companies' organizational reality in order to make hunters more patient and persuade them of the importance of establishing a friendly, productive working relationship with triagers. According to one triager, a good personal contact could even be a way to get tips about the program and its scope.[129] More generally, the idea to take time to delve into a program and "stick around", to know the program, its scope, and its triagers, and to develop an understanding of the companies' operational processes and structures is commonly presented as a must in tutorials and presentations on bug hunting.[130]

This value of bonding, despite the anonymity of online messaging characterizing vulnerability disclosure, emphasizes the importance for companies operating a bug bounty program to facilitate sustained relationships with certain hunters; the lack of a well-trained workforce amid fierce program competition compels them to use various strategies to attract and retain promising and talented hunters. Published statistics (Elis, Huang et al. 2017), accessible program databases, and interviews with several program managers indicate that the concept of "crowdsourced security" does not effectively describe the practical substance of bug bounties. If hundreds of hunters are registered in a program, only a small fraction are sending reports, and, among them, only a few are submitting valid vulnerabilities. Therefore, only a relatively small number of hunters actually report previously undetected critical vulnerabilities to legitimize, maintain, and develop a program year after year.[131] Managers have various metrics with which to monitor program performance and, in turn, the performance of participants (hunters) and employees (triagers). Platforms rank hunters according to their ability to identify vulnerabilities. Some of the diverse metrics with which they rank hunters are quite complex, covering multiple aspects of hunting. For example, the HackerOne platform ranks hunters by "reputation," "signal," and "impact." Reputation points indicate "report validity," signal points indicate the consistency of a hunter in submitting valid reports,

128 This is the case in this video, "How to get started in bug bounty," from Stök, a bug hunter who provides tutorials on his YouTube channel: https://www.youtube.com/watch?v=CU9Iafc-I. See another example from a panel hosted by HackerOne at the following link: https://www.youtube.com/watch?v=gul-DFzibaE&list=PLxhvVyxYRviYrJ7S2WhJB6P5cwSIjbL4w&index=6.

129 https://www.youtube.com/watch?v=P6USwfEENuk

130 https://www.youtube.com/watch?v=CU9Iafc-Igs

131 This number varies by company size and program size, though it rarely exceeds 50—even for big tech, including GAFAM. For national IT companies, the number of hunters keeping the bug bounty program afloat year after year rarely exceeds 20 (personal discussions with bug bounty program managers)

and impact points indicate the severity of the reported vulnerabilities.[132] Platforms often offer "badges" and other collectibles symbolizing milestones, such as a certain number of resolved reports, and situations, such as patiently waiting six months for a report to be closed. These rankings and badges serve as incentives to foster a competitive environment among the hunters. Gamification has become a centerpiece of bug bounty management. In addition to boosting competitiveness among bug hunters, it also aids in visualizing hunter skills and strengths in an accessible but still adequately complex way. The indicators enable managers to pool a small but well-suited group for a special hacking event or closed-door program and to advertise the skills of their hunters to prospective client companies. More importantly, however, indicators help managers to identify and retain promising and talented hunters. In the context of a significant shortage of digital security experts, bug bounty programs are highly useful for identifying talented hackers.

Over the years, bug bounty platforms have developed their own training capabilities by sponsoring hunters' YouTube and Twitch channels, organizing CTFs and mentoring programs, and putting together online tutorials on hacking tools, techniques and research approaches. Additional materials have been produced to guide hunters in effectively communicating vulnerabilities and their impacts. Katie Moussouris, a key actor in the development of the bug bounty model, highlighted education as a crucial dimension of bug bounty operations: "So, is it money? Is that it? We just need to pour more money into it? The answer's no. When we modeled the system, we basically were like, 'Look, people come in, they aren't born with this skillset, they have to grow it somehow, and both the offense side of the market, and the defense side of the market need to grow people with these skill sets'" (Katie Moussouris interviewed by Fisher)[133]. Comparing these bug bounty educational initiatives with the information-sharing practice among full disclosure hackers reveals a significant contrast: learning from specific vulnerability details and exploit code published on mailing lists has been replaced by learning from tutorials and commentaries. While most vulnerabilities remain walled off behind NDAs, new models for learning to hack through bug bounties have emerged and are often considered to be complementary to professional certification training. Tutorials and other educational contents also indicate how hacking-as-labor has been increasingly standardized beyond the definitions of a scope, policy or vulnerability disclosure standard. It also indicate that security hacking is no longer an elitist and confidential niche, at least in the context of bug bounty programs.

Based on what has been established, bug bounty programs may be considered an entry point into hacking or, more generally, a career in cybersecurity.[134] This could partially

132 https://docs.hackerone.com/hackers/reputation.html and https://docs.hackerone.com/hackers/signal-and-impact.html

133 https://duo.com/decipher/uprising-in-the-valley-when-bug-bounties-went-boom-part-two

134 See, for instance, Vicky Li's 2021 keynote address at Hactivitycon: https://www.youtube.com/watch?v=Rwkx8yzY6IU.

explain the statistics mentioned earlier indicating that only a few hunters submit valid reports relative to the overall number of hunters active in any given program. Many hunters use the platforms to test their skills without necessarily competing for rewards, while project managers view bug bounty programs as a means to facilitate the identification and training of hunters who may be valuable in the future as potential contractors or employees. From this perspective, we can understand bug bounties as contributing to the training of a workforce that is, and will continue to be, highly demanded in the digital tech industry. Accordingly, setting up bug bounties is a sound strategy for a company looking to establish itself in the hacker community in pursuit of cheap security labor in the short term or reliable employees in the long term. Some even assert that companies may set up bug bounty programs with the intent to outsource most of the security labor necessary in their product development.[135] In other words, bug bounties provide companies with a degree of flexibility that hiring does not. These programs can be adjusted or canceled at any point and, more importantly, the people working on these programs are (generally) more numerous and more diverse than a hired security team.[136] Beyond these arguments that could lead companies to reduce their security teams in favor of setting up bug bounty programs, there is another important reason: "By 2002, estimates suggested that debugging, testing, and program verification accounted for between 50% [and] 75% of total development costs. A substantial market for security testing services, pen test companies, in particular, grew to complement and support in-house testing" (Elis and Stevens 2022: 45). The difficult yet interesting relationship between penetration testing and bug bounty programs is beyond the scope of this article. However, it is important to note that outsourcing security is not something new that was initiated by the bug bounty model of vulnerability disclosure. Bug bounties have certainly altered the pattern and magnitude of security outsourcing, but fully understanding the differences between penetration testing and bug bounty and their impacts on companies would first require a historical account of penetration testing and its transformations over several decades.

Bug bounties (and the few initiatives in the emerging defensive market before them) have incorporated a gig economy into the practice of hacking. However, not all hackers have become gig workers reporting vulnerabilities for monetary compensation. The complex transformation of vulnerability disclosure models and practices that I recounted in this paper exists within the larger international context of the flexibilization of work (Boltanski and Chiapello 1999), the externalization of company costs onto workers (Neff 2012), and the increasing magnitude of free labor in the digital economy (Terranova 2000). There is no doubt that, amid capitalist dynamics and powerful corporate actors, bug hunters have begun to suffer, at least to a degree, from exploitation. However, to

135 Katie Moussouris is someone with this belief, as shown here: https://duo.com/decipher/taking-hype-out-of-bug-bounty-programs.

136 The idea that diversity in technical skills as well as diversity in gender and sociocultural background increases a group's chance to detect security issues is considered to be an unshakeable truth in cybersecurity. This idea can be traced back to the famous Linus's law formulated by Eric Raymond: "Given enough eyeballs, all bugs are shallow" (1999).

argue that hackers have simply been progressively channeled, disciplined, and regimented in bug bounty programs as gig workers misrepresents the story of ethical hackers, their aspirations, and their desire to contribute (even without compensation) to the development of the digital industry. This assessment aligns with Terranova's understanding of incorporation being "not about capital descending on authentic culture but a more immanent process of channeling collective labor (even as cultural labor) into monetary flows and its structuration within capitalist business practices" (2000: 39). Therefore, we must make an effort to understand why bug bounties are attractive to young hackers and seasoned hackers alike beyond the basic financial incentives and marketing campaigns and despite the many tensions constantly unfolding in bug bounty programs.

Conclusion

In this paper, I sought to understand the emergence of new disclosure models and, ultimately, the defensive market. Of course, several elements and processes must be addressed further through the use of other methodologies, such as interviewing key actors. Among others, two important avenues for future research are: understanding the role that venture capitalism has played and still plays in the emergence of bug bounty platforms and understanding the socio-technical dimension of the emergence of big tech's in-house bug bounties around 2010.

After comprehensively reviewing the collected material, my perspective has been shaped by one simple idea: from the earliest case of disclosure considered in this article, ethical hackers have sought a way to collaborate with the digital tech industry, sometimes unsuccessfully and sometimes somewhat successfully. However, from this perspective, it is clear that full disclosure is not the traditional *modus operandi*[137] for hackers. Rather, it is the result of failed attempts to collaborate, though these attempts have been largely productive for the hackers,[138] who, through these missed opportunities, elaborated a powerful answer that ultimately enabled them to be more visible in and relevant to digital security. More generally, we can postulate that ethical hacking—in terms of its principles and practices—is the result of a series of encounters between hackers and companies throughout the history of vulnerability disclosure. In addition, the political economy approach that I adopted in this paper has shed light on the transformative changes in disclosure models, the emergence of a market, the partial reorganization of hacking into a flexible and legitimate professional option, and the production of a more widespread and accessible form of hacking training and education for bug hunters and hackers.

These changes have taken place through various processes that I have tried to account for with the material available to me. Interests, incentives, and relative transaction costs are critical to a proper understanding of these changes. However, beyond these, we can also identify the roles of crises, rhetoric, and narratives that have securitized and economized situations, dynamics, and events. We can clearly see the repetitive interplay of small groups of key actors pushing together in certain directions and challenging dominant positions and ideologies. Ethical principles have been quite adjustable to accommodate or make room for new models and institutions. Here, a lot must still be done to continue exploring these transformations in greater detail with key informants who have played an active role in this fascinating history.

137 The circulation and exploitation of vulnerability information was indeed a crucial dimension shaping ethical hacking. However, in contrast to what Elis and Stevens (2022) declare, we cannot argue that companies, in enforcing the enclosure of vulnerability information, are "threatening one of the traditional ways in which hacker communities were built and sustained" (34). The educational dimension at the core of vulnerability disclosure has been reconfigured in the context of bug hunting.

138 In another context related to cultural encounters, anthropologist Marshall Sahlins has used the concept of "working misunderstanding" (1983) to highlight the emergence of a significant collective practice created by misunderstanding during cultural encounters.

In this history, markets did not emerge to provide a solution to a problem but were rather a potential outcome of certain complex and unsteady dynamics. However, we don't need to consider them as the logical outcome of increasing complexity and scale. After all, vulnerability transactions take place within *and* beyond markets. Some are traded while others are simply reported. In other words, different models of disclosure and hacking co-exist today as they did in the past. Bug bounty is a relatively new model that can take several different shapes. The most obvious distinction is that between in-house programs and platforms, though there are many less obvious distinctions that can be identified by practitioners, researchers, and ethnographers. CVD is another recent and fast-developing model that is adapting to new complexities and, in particular, to the so-called "supply-chain attacks" comprising bugs in essential pieces of software that spread across innumerable codebases, processes, and systems. However, this article does not argue that any particular model is dominant today.

Instead, this paper shows a relatively long process of the standardization, disciplinarization, and govermentalization of hacking. Of course, this does not mean that hackers have simply become a docile workforce subsumed by the powerful companies of the digital tech industry. The perspective provided by the relative transaction costs aided in identifying several processes that governed the transformation of disclosure models and the introduction of governing principles into hacking and vulnerability reporting: the formalization and codification of the minutia of collaboration, standardized expectations, institutions, databases, frameworks, and common definitions, among others. These processes facilitated the emergence of a defensive market despite the ethical resistance to make vulnerability information a commodity in a defensive market. The first defensive market initiatives produced a sort of middle ground between an existing offensive market and the practice of disclosure without retribution, introducing a business model in which hackers are paid to identify vulnerability information and keep it secret while a patch is developed. This economic, ideological, ethical, and social intermediation between offensive (secret and paid) initiatives and free ethical disclosures paved the way for another defensive market-led model in the form of bug bounty programs. However, these defensive market initiatives became possible only when the hacker principle of free access to information had been partially lifted by the acknowledgment of the necessity of certain responsible disclosure standards.

With the inception of the bug bounty model, guidelines and, in turn, diciplinarization became even more precise than in vulnerability disclosure policies. The model also allows for rapid changes to the scope of the program, making disclosure subject to minute regulations. Bug bounty managers can fine-tune the flow of vulnerability information that they receive. They can also select a pool of hunters to work within a specific scope. The hunters' selection for an event or a specific task is eased by the metrics gathered by the platforms through reputation scores. In this way, bug bounty programs are much more

than just incentive mechanisms to gather a crowd of flexible workers. They constitute a complex governing apparatus that enables companies to manage workflows and crowds and managers to take closer, more personal care to facilitate the work of bug hunters viewed as particularly valuable. Thus, the model also works through investment in activities and strategies aimed at fostering personal relationships, bonding mechanisms, loyalty, and reciprocal systems of exchange between valuable hunters and managers. Therefore, the disciplinarization of bug hunters goes far beyond technical guidelines and the classical disciplinary model devised by Foucault; it is more akin to that which constitutes the core apparatus of Foucault's biopolitical model—an apparatus of surveillance that oversees flows and crowds (Foucault 2009). Although, the modularity in bug bounty programs also points to Deleuze's understanding of control in Postscript on the Societies of Control (1990). In one way or another, bug bounty programs constitute a complex technology of security governance. However, it would be wrong to assume that bug bounty programs have disciplinarized hacking, as the disciplinarization and governmentalization of hacking had already been at play for several years prior to the development of the bug bounty model.

One last issue should be addressed through the following questions: Is bug hunting the same as hacking? Are bug hunters hackers, or at least a type of hacker? These questions emerge from the historical trajectory of hacking and the many transformations of vulnerability disclosure models that have been analyzed in this paper. It is clear that bug hunting in the context of bug bounty programs is quite different than what hacking was in the 1990s, when hackers would disclose vulnerability information and exploits on Bugtraq. I highlighted several changes in terms of norms, principles, practices, institutions, and power over the years but collective boundaries are always ambiguous, performed and negotiated in a specific situation or context. Therefore, it is not only difficult to define two clearly separate categories—hacking and hunting—but doing so may also unnecessarily essentialize the two into discrete communities. Bug hunting is a form of hacking, and they share a common historical trajectory. Today, they co-exist, meaning that hunting has not replacing hacking. We can also note some obvious similarities between full disclosure in the 1990s and bug hunting in the 2020s: regardless of means, both processes helped hackers/hunters develop their street credentials. Both venues have been effective in identifying promising talent, and both models have been influential in publicizing and normalizing hacking as a legitimate educational and professional option.

My references to "bug hunting" instead of just "hacking" are justified only by the context of bug bounty programs in which the hacking occurs. In other words, bug hunting in this article refers to certain hacking practices framed by a specific model of disclosure. There is nothing else within the scope of this article that prompts me to argue that bug hunting and bug hunters must be clearly defined separately from hacking and hackers despite the fact that research participants active in ethical hacking were sometimes keen to draw a

clear boundary between the two. This is not to say that the practices are the same. Ethical hacking have changed over time taking on new shapes and contours depending on the specific context and the chosen model of disclosure. What remains to be explored is the ethics, practice, and motivations of bug hunters to hack in the context of bug bounty programs through a long-term ethnographic approach.

A few thoughts on the research process and the open data archive of collected materials

To explore the historical economic and technological processes behind ethical hacking, I embarked on a wild ride that entailed collecting the remaining digital traces of its historical trajectory instead of immediately jumping from one hacker conference to another to interview the key actors in this history. The rationale for this choice was simple and based on the principle of conducting due diligence prior to fieldwork or interviews. It considered the fact that key actors who have been engaged in disclosure debates for many years have already expressed their opinions online and would likely be inclined to repeat what they have already written about. Conducting interviews like this would have run the risk of providing little to no additional relevant data. It would also limit the range of rationales and opinions that actors could express during an interview, especially given that the research topic is focused on the past. In this situation, nuances and processual dimensions of a debate, including changes in the interviewee's opinions or argumentations, can be easily truncated by a *post hoc* personal understanding of the interviewee using traditional social science interview techniques.

Considering the large number of texts on vulnerability disclosure since the 1990s and the fact that many of them have been published and archived online, it appears to be possible to adequately reconstruct the debates surrounding disclosure models using online sources. Of course, such an endeavor could not account for that which has not been archived, for works that were never published texts, or for discussions or presentations that were never transcribed. Additionally, it could not account very well for the context in which the texts were written. However, reading and listening to the collected materials and placing them on a timeline did offer a relatively dense intertextuality. Even when a piece did not explicitly refer to another, it was often possible to assume which published papers authors had in mind in their arguments.

My search for archived material online followed a few guidelines. I searched for existing histories and timelines of vulnerability disclosure. I searched for dozens of keyword combinations on Google search engine and the Wayback Machine. Finally, I gathered documents written by relevant experts and organizations with which I was already familiar. However, I mainly relied on references within examined documents to explore the debates on vulnerability disclosure, following relevant hyperlinks and searching for talks, articles, events, and opinions mentioned in every document until I reached the point of saturation. The main data-collection period ran from June to November 2021, and the data was gradually analyzed throughout the following year.

The data-collection process aimed to capture the history of vulnerability disclosure models and the moments, debates, and rationales behind them. The intent was to

construct a preliminary digital history of vulnerability disclosure models and debates to retrace the history of vulnerability disclosure from the early 1990s to the early 2020s. This project aligns with the definition that Rogers gave to this particular digital research orientation: "telling the history of an idea, individual, organization, institution or other entity to which a website has been dedicated" (Rogers 2019: 95). Notably, however, I did not only focus on a particular website in this case. The websites on which vulnerability disclosure models and practices are debated are numerous; exploring such a history on the web means researching the remaining traces of "transnational events on the web" (Brügger et al. 2020: 4). However, it's important to note that most of the collected materials were produced by US-based actors.

Some of the collected materials were still online, though many necessitated the use of the Wayback Machine[139] (https://web.archive.org), which allows us to access websites at different time through snapshots. I always selected the oldest available snapshot when accessing archived webpages to see them as they were originally published. While I often checked later snapshots to see whether the pages were significantly edited or commented on, I never identified any worthwhile or relevant changes. Material still online on their original location was simply collected from company websites (e.g., Microsoft, SecurityFocus.com), newspapers (e.g., NYTimes, CNN), personal websites (e.g., Schneier.com, porcupine.org), magazines (e.g., ZDNET News, Cnet.doc, PCworld.com, TheRegister.com), distribution lists archived on Seclists.org, and YouTube channels (e.g., Blackhat, DEFCON). I copied every source as text, PDF, or audio/video files to build my own archive and secure continued access to these documents.

At the time of this article's publication, my archive comprises 179 documents, of which 129 are available online at cva.unifr.ch (using the PECE framework)[140] and displayed on a timeline thanks to Elise Vuitton, a student assistant. In line with the open-data standard, this archive is fully accessible to any interested individuals, be it to further their own research or to contribute to the archive's development. In addition to securing easy online access to the documents, this archive serves the methodological purpose of enhancing my interviews with key actors. Accordingly, some of these interviews will use the timeline as a methodological artifact to focus the discussion on precise moments in the past. The second part of this research project will undoubtedly open up new avenues for research on the past and present of vulnerability disclosure models.

139 For a discussion of the value and limitations of the Wayback Machine, see Rogers (2019).

140 The PECE (Platform for Experimental, Collaborative Ethnography) was developed by a group of anthropologists led by Kim Fortun and Mike Fortun at RPI and at UC Irvine.

References List

Abbate, Janet. 2017. "What and where is the Internet? (Re)defining Internet histories." Internet Histories 1 (1-2):8-14.

Appadurai, Arjun, ed. 1988. The social life of things: commodities in cultural perspective. Cambridge: Cambridge University Press.

Auray, Nicolas, and Danielle Kaminsky. 2007. "The professionalisation paths of hackers in IT security: The sociology of a divided identity." Annales Des Télécommunications 62 (11):1312-1326.

Bohannan, Paul. 1965. "The differing realms of the law. The ethnography of law." American Anthropologist 67:33-42.

Boltanski, Luc, and Ève Chiapello. 1999. Le nouvel esprit du capitalisme. Paris: Gallimard.

Brügger, Niels, Valérie Schafer, and Jane Winters, eds. 2020. Perspectives on web archive studies: Taking stock, new ideas, next steps. Aarhus: research network WARCnet.

Callon, Michel. 2017. L'emprise du marché. Paris: La Découverte.

Cencini, Andrew, Kevin Yu, and Tony Chan. 2005. Software Vulnerabilities: Full-, Responsible-, and Non-Disclosure. Seattle: University of Washington.

Chanock, Martin. 1985. Law, custom and social order: the colonial experience in Malawi and Zambia, Cambridge: Cambridge University Press.

Coleman, Gabriella, and Alex Golub. 2008. "Hacker practice: Moral genres and the cultural articulation of liberalism." Anthropological Theory 8 (3):255–277.

Coleman, Gabriella. 2010. "The Hacker Conference: A Ritual Condensation and Celebration of a Lifeworld." Anthropological Quarterly 83 (1):47-72.

Coleman, Gabriella. 2021. The Hackers. BBC Radio 4. https://www.bbc.co.uk/programmes/m0012fjk

Deleuze, Gilles. 1990. "Post-scriptum sur les sociétés de contrôle." In Pourparlers (1972-1990), edited by Gilles Deleuze, 240-247. Paris: Editions de Minuit.

Delfanti, Alessandro, and Johan Söderberg. 2018. Repurposing the hacker. Three cycles of recuperation in the evolution of hacking and capitalism. Davis, CA: UC Davis.

Ellis, Ryan, Keman Huang, Michael Siegel, Katie Moussouris, and James Houghton. 2017. "Fixing a Hole: the Labor Market for Bugs." In *New Solutions for Cybersecurity*, edited by Howard Shrobe, David L. Shrier and Alex Pentland, 129-159. Cambridge, MA: MIT Press.

Ellis, Ryan, and Yuan Stevens. 2022. Bounty Everything: Hackers and the Making of the Global Bug Marketplace. New York: Data and Society.

Ensminger, Jean. 1992. Making a market: the institutional transformation of an African society, The Political economy of institutions and decisions. Cambridge England; New York: Cambridge University Press.

Foucault, Michel. 2009. Sécurité, territoire, population. Cours au Collège de France (1977-1978). Paris: Editions EHESS, Gallimard, Le Seuil.

Goerzen, Matt, and Gabriella Coleman. 2022. Wearing Many Hats. The Rise of the Professional Security Hacker. Data & Society.

Granick, Jennifer Stisa. "The Price of Restricting Vulnerability Publications." International Journal of Communications Law & Policy Vol. 9 (Spring 2005).

Hellegren, Z. Isadora. 2017. "A history of crypto-discourse: encryption as a site of struggles to define internet freedom." Internet Histories 1 (4):285-311.

Hobbs, Alfred Charles. 1853. Locks and Safes. The construction of locks. London: Virtue and Co.

Kerckhoffs, Auguste. 1883. "La cryptographie militaire." Journal des sciences militaires IX (Janvier):5–38.

Lakoff, Andrew. 2008. “The generic Biothreat, or, how we became unprepared” Cultural Anthropology 23 (3):399-428

Latour, Bruno. 2002. La fabrique du droit : une ethnographie du Conseil d'Etat. Paris: Ed. La Découverte.

Levy, Steven. 1984. Hackers: Heroes of the Computer Revolution. New York: Anchor Press/Doubleday.

Li, Vickie. 2021. Bug Bounty Bootcamp. San Francisco: No Starch Press.

Menn, Joseph. 2019. Cult of the Dead Cow. How the Original Hacking Supergroup Might Just Save the World. New York: PublicAffairs.

Nader, Laura. 1990. Harmony Ideology: Justice and control in a Zapotec mountain village. Stanford, CA: Stanford University Press.

Nader, Laura. 1997. "Controlling Processes: Tracing the Dynamic Components of Power." Current Anthropology 38 (5):711-737.

Neff, Gina. 2012. Venture Labor. Work and the Burden of Risk in Innovative Industries. Cambridge, MA MIT Press.

Olivier de Sardan, Jean-Pierre. 2008. La rigueur du qualitatif. Les contraintes empiriques de l'interprétation socio-anthropologique. Louvain: Academia Bruylant.

Perlroth, Nicole. 2021. This Is How They Tell Me the World Ends. London: Bloomsbury.

Raymond, Eric.1999. The cathedral & the bazaar : musings on Linux and open source by an accidental revolutionary. Beijing: O'Reilly.

Ranger, Terence. 2006 [1983]. "L'invention de la tradition en Afrique à l'époque coloniale." In L'invention de la tradition, edited by Eric J. Hobsbawm and Terence Ranger, 225-278. Paris: Editions Amsterdam.

Rogers, Richard. 2019. Doing Digital Methods. London: Sage.

Roseberry, William. 1988. "Political Economy." Annual Anthropological Reviews 17:161-185.

Sahlins, Marshall. 1983. "Other Times, Other Customs: The Anthropology of History." American Anthropologist 85:517-544.

Shepherd, Stephen A. 2003. How do we define Responsible Disclosure? North Bethesda, MD: SANS Institute.

Söderberg, Johan, and Maxigas. 2022. Resistance to the Current. The Dialectics of Hacking. Cambridge, MA: MIT Press.

Steiner, Philippe, and Marie Trespeuch, eds. 2015. Marchés contestés. Quand le marché rencontre la morale. Toulouse: Presses universitaires du Midi.

Terranova, Tiziana. 2000. "Free Labor: Producing Culture for the Digital Economy." Social Text 18 (2):35-58.

Zelizer, Viviana. 1979. Morals and Markets: The Development of Life Insurance in the United States. New York: Columbia University Press.

Zufferey, Eric. 2018. Changer le travail ou changer la société ? Les hackers entre conformation à l'ordre social et volonté d'innover. Fribourg: Thèse de doctorat: Université de Fribourg.