Crime Science

THEORETICAL ARTICLE

Open Access

Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure

Marleen Weulen Kranenbarg[1*], Thomas J. Holt[2] and Jeroen van der Ham[3]

Abstract

In the computer science field coordinated vulnerability disclosure is a well-known practice for finding flaws in IT-systems and patching them. In this practice, a white-hat hacker who finds a vulnerability in an IT-system reports that vulnerability to the system's owner. The owner will then resolve the problem, after which the vulnerability will be disclosed publicly. This practice generally does not focus on potential offenders or black-hat hackers who would likely exploit the vulnerability instead of reporting it. In this paper, we take an interdisciplinary approach and review the current coordinated vulnerability disclosure practice from both a computer science and criminological perspective. We discuss current issues in this practice that could influence the decision to use coordinated vulnerability disclosure versus exploiting a vulnerability. Based on different motives, a rational choice or cost–benefit analyses of the possible reactions after finding a vulnerability will be discussed. Subsequently, implications for practice and future research suggestions are included.

Keywords: Coordinated vulnerability disclosure, Responsible disclosure, Interdisciplinary, Bug bounty, Rational choice theory, Criminal motives, Hacking, Cybercrime

Introduction

Computer hardware and software products are designed to be as user-friendly as is possible, trading security for usability in some cases (Newman and Clarke 2003; Van Schaik et al. 2017). Consequently, enterprising security researchers and criminal hackers may identify flaws within computer devices in order to make them operate in unintended ways (Jordan and Taylor 1998; Taylor 1999). These flaws are commonly referred to as vulnerabilities, as they enable an attacker to gain access to computer systems and data for malicious use. When an individual identifies a vulnerability, they basically have four options: (1) do nothing about it, (2) report the flaw to the vendor or a related security organization for mediation, (3) report the flaw publicly, (4) keep this information private so that it can be used for attack, either by the person who identified the vulnerability, or by selling the vulnerability to someone else at an underground market.

Public reporting on vulnerabilities has evolved over the last 30 years, reflecting shifts in the dynamics between security organizations and the hacker community. Initially many security researchers tried to shame vendors by disclosing all details as soon as the vulnerability is discovered. Such a move would enable attackers to use the vulnerability to compromise systems before they can be corrected. In the last few years, reporting has tended more towards coordinated disclosure, where a researcher privately contacts a vendor to resolve the vulnerability before going public with his findings. Additionally, there has been an increase in "bug bounties" where a person is paid for vulnerability disclosures by security vendors (NTIA 2016).

*Correspondence: M.WeulenKranenbarg@vu.nl
[1] Department of Criminology, Faculty of Law, Vrije Universiteit (VU) Amsterdam, De Boelelaan 1105, 1081 HV Amsterdam, The Netherlands
Full list of author information is available at the end of the article

The general term that will be used in this article to refer to vulnerability disclosures is coordinated vulnerability disclosure (CVD). In general, CVD is a practice in which a hacker who finds a vulnerability in an IT-system reports that vulnerability to the system's owner. The owner will then resolve the problem, after which the vulnerability can be disclosed publicly. In order to prevent criminal use of the vulnerability, it is key that the hacker does not share or publicly disclose the vulnerability before the problem has been fixed. The details and different CVD-forms will be discussed later in this paper. The overarching goal of having a CVD policy is to make IT-systems more secure and prevent the criminal use of vulnerabilities in IT-systems (ISO/IEC 2014; NCSC 2013; NTIA 2016).

The Netherlands is one of the few countries in the world with official guidelines for vulnerability disclosure. In 2013, the Dutch National Cyber Security Centre (NCSC) introduced a guideline for Responsible Disclosure (NCSC 2013). This document provided guidelines for the vulnerability disclosure process both from the researchers as well as organizational point of view. The Dutch Public Prosecutor has officially endorsed this guideline and has taken elements of it as a decision framework for when to prosecute (Public Prosecution Service 2013). Since 2013, there have been many successful CVD-cases, ranging from large disclosures by academic researchers to small disclosures that lead to configurational changes (NCSC 2017). There have been several cases where a discloser even ended up with a job at the vulnerable organization, but also cases with successful prosecution when the discloser went too far (Van't Hof 2016). Last year the US guidelines have been published (Department of Justice 2017), but for the sake of clarity the focus of this paper will be on the Dutch guidelines.

The overarching goal of CVD shows a focus on the victim side and data-breach prevention and other victimization types. This makes sense as the CVD policy originates from the computer science field, which generally focuses on making IT-systems more secure. CVD policies also seem to target so-called white-hat or ethical hackers. Criminological inquiries, however, focus on the offenders engaged in criminal hacks and misuse of vulnerabilities (for a review see Holt and Bossler 2016).

So, what can we learn from a combined computer science and criminological perspective on CVD? What are the key requirements for a successful CVD policy and how do these relate to criminological explanations for criminal hacking? What are the main problems with current CVD policies and how do these relate to ethical and criminal use of vulnerabilities? Will a CVD policy mainly work for white-hat or ethical hackers or can we expect it to help potential offenders to choose the ethical instead of the criminal path? And lastly, which empirical research questions should be addressed to further inform us about these questions? In this paper, we will shed light on these questions from both a computer science and criminological perspective.

Coordinated vulnerability disclosure

The Netherlands was one of the first countries to legally recognize the practice of CVD policies. At the time it was called responsible disclosure. The need for a formal policy on vulnerability disclosure arose as a result of some cases that were reported in Dutch media, in which it was unclear if a hacker acted responsibly or if the hacker crossed a line and acted criminal (Van't Hof 2016). Therefore, in 2013 the NCSC of The Netherlands published guidelines for responsible disclosure policies. Later the term "responsible" has been deemed too loaded; the new term "coordinated" conveys that CVD is a process between two equal participants. Coordinated vulnerability disclosure is now used nationally and internationally. The vulnerability disclosure process is described in the guidelines for disclosure of potential vulnerabilities in products and online services (the ISO/IEC 29147:2014) of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), see ISO/IEC (2014).

In order to look at CVD from a criminological perspective, it is first necessary to discuss all aspects of CVD as it arose from computer science. The main goal of an established CVD policy is to invite white-hat hackers to report any vulnerabilities they find in an IT-system to its owner. They should also not discuss the vulnerability with anyone else or disclose it publicly somewhere. In this way, the vulnerability is likely only known to the owner and the discloser, which means that the exploitation risk of that vulnerability is minimized. The owner will then try to mitigate the vulnerability as soon as possible, ideally in consultation with the discloser. After the vulnerability has been fixed, the discloser and owner will decide if and how it should be disclosed to the public (ISO/IEC 2014; NCSC 2013; NTIA 2016).

This policy is beneficial for the IT-systems' owners, as they will learn about their vulnerabilities and potentially improve their security posture. This policy provides some certainty for both parties, especially the disclosers who may have committed a crime by finding the vulnerability. As long as the discloser abides by the policy's terms, the IT-system's owner should generally not report their actions to the police. In this way both parties collaborate in their common goal to improve cybersecurity (NCSC 2013). It should be noted, that currently there is no guarantee that the public prosecutor will not prosecute a discloser for any crimes that have been committed.

Representative information about the type and amount of vulnerabilities that are disclosed by using CVD is not available. Nevertheless, some descriptive information based on recent reports is helpful in understanding the nature of CVD. The NCSC of The Netherlands generally only handles CVD reports about their own infrastructure, central governmental organizations, and private organizations who handle critical infrastructure. Their latest annual report (NCSC 2017) indicates that the large majority of CVDs are about vulnerabilities in websites (78%), like cross-site scripting (32%). Other reports included software vulnerabilities (9%) and configuration errors in hardware and software (3%).

While the NCSC sees a rise in CVDs in comparison to previous years, they see a decline in false positives, i.e. reports that eventually did not include a real vulnerability. The NCSC (2017) argues this reflects a maturation process on the disclosers' side. A survey from the National Telecommunications and Information Administration (NTIA 2016) among security researchers showed that 92% of their respondents disclose vulnerabilities by using CVD.

Bug bounties

Initially CVD programs gave out small rewards for successful disclosures, such as t-shirts, small gadgets or listing the researcher in a hall of fame. Many researchers accept this and use it to boost their reputation. Recent years has seen some professionalization of CVD by offering monetary awards, so called bug bounties (Finifter et al. 2013). Microsoft (Microsoft Bounty Programs https://technet.microsoft.com/enus/library/dn425036.aspx, 2018) and Google (Android Security Rewards Program Rules, https://www.google.com/about/appsecurity/android-rewards/, 2018) have programs where researchers may be eligible for up to $250,000 for specific disclosures. At the same time several companies have started that help other companies in setting up CVD and bug bounty programs. HackerOne, a third-party platform for hosting vulnerability disclosure and bug bounty programs, claims to have over 800 active disclosure programs (Hackerone 2017). It should be noted, however, that bug bounties are only a small part of CVD. Most organizations with a CVD policy do not offer monetary rewards. Bug bounty programs seem to assume a financial motive for finding and exploiting vulnerabilities, something that criminological research discussed later in this paper has shown to be only partially true.

Problems with current CVD practices

Although the goal of CVD policies is clear and statistics indicate a positive development of these policies and their users, current policies have some problems that should be discussed in order to understand the possible problems of these policies in preventing crime on both the victim and the offender side. Taking a traditional deterrence approach, problems with the reporting process may influence a person's decision to following CVD guidelines.

The organization's response

Organizations should adopt a CVD policy because they want to increase their security, though this also means that the organization should be able to respond to a reported vulnerability. In addition, organizations without a CVD policy may also receive a vulnerability report. When there is no CVD policy, it is not clear to disclosers how the organization will respond. The expected reaction of such an organization may influence the behavior of a possible discloser: these organizations could (1) respond gratefully and patch the vulnerability as soon as possible, (2) ignore it, (3) deny it, or (4) report to the police. An organization that does not have a CVD policy may, for example, not know how to respond or not understand the vulnerability and could therefore decide to ignore it or deny the vulnerability's existence. They may even misinterpret the intentions of the reporter and report it to the police as a crime.

Even organizations that do have a CVD policy might not have the capacity to handle big vulnerabilities, which may delay the patching process. The longer a vulnerability has not been patched, the higher the risk of rediscovery or that the discloser decides to make it public anyway (Herr et al. 2017). Most CVD policies state how much time they would take before fixing a vulnerability, but that could easily be 6 months. In a response to that, new companies now arise who handle coordinated vulnerability disclosure for small companies (Huang et al. 2016).

Moreover, the goal of having a CVD policy is to keep vulnerabilities private until they are patched. This means, however, that the outside world including the discloser cannot see that an organization is working on a patch. Therefore, it is key that an organization keeps communicating with the discloser about the patching process, which is also what the majority of the researchers in the NTIA (2016) report expect. Nevertheless only 58% received a notification when the vulnerability had been patched. Depending on a person's motive, this could influence the discloser's behavior.

Unclear or unjust rules

In order for a CVD policy to work, both the company and the discloser need to stick to the rules in the policy. An absence of clearly identified rules may lead to a lack of disclosures, as would guidelines that are too strict. For

example, deadlines in the policy could force a company to publicly disclose a vulnerability that has not yet been patched, as they do not know how the discloser would respond if they would not.

For the discloser, there is no guarantee that he or she will not be prosecuted under current CVD guidelines (NTIA 2016). An organization without a policy may report it to the police immediately, as could organizations with clear policies if they believe the discloser did not abide by their rules. In The Netherlands, the public prosecutor could also decide to prosecute if they believe a crime has been committed. For most disclosures some form of system-trespassing is necessary, as it is not possible to ask for permission from the system owner. For example, in the survey from the NTIA (2016), researchers indicated that they generally find vulnerabilities in their daily activities, without actively looking for them. In that sense, requiring asking for permission partly defeats the purpose of having a CVD policy.

For some organizations, it is publicly known how they generally handle vulnerability disclosures. First, bug bounty programs are publicly known and some organizations are very open about their CVD policies and they actively encourage the hacker community to test their systems. However, there is a big difference between open and closed communities, even in the same sector. For example, while the Linux community actively encourages people to find vulnerabilities, Microsoft historically tended to prosecute people who disclose vulnerabilities (e.g., Steinmetz 2016; Taylor 1999). Similarly, when looking at the hacker subculture, there is a general tendency to share vulnerabilities within the subculture, but not with others like law enforcement or large commercial companies that are not open source (Taylor 1999). These unclear and sometimes unwritten rules result in a situation in which one person will be prosecuted for the same behavior for which someone else would get an acknowledgement or even a bounty. This could result in the opinion that the rules are not fair or even unjust, which may influence if and how someone discloses a vulnerability.

Public disclosure

When the vulnerability has been patched, or when the deadline as described in the CVD policy has expired, the discloser and the IT-system's owner can decide together to disclose the vulnerability to the public. There are several reasons to do so. First, it could be a way to provide the discloser with some acknowledgement for his or her work and abilities to find this vulnerability. 53% of the researchers in the NTIA (2016) report stated that they expect to get some form of acknowledgement, although it should be said that a minority (14%) prefers to remain anonymous.

Another reason to disclose these vulnerabilities is to inform the public about the vulnerability and what should be done to prevent exploitation of the vulnerability. It could be the case that other IT-systems have similar vulnerabilities or patching the vulnerability in software requires an update from users (Department of Justice 2017). The amount of information that a company is willing to share about the vulnerability may, however, be limited. The discovery of the vulnerability may be embarrassing for the company, affect their finances, or reveal too much of the underlying operation. This limits the usability of the disclosed information and may influence a person's decision to report a vulnerability to a party that has not shown openness about vulnerabilities.

In a similar fashion, some recent incidents have shown that governments are sitting on vulnerabilities in order to engage in offensive attacks (Ablon and Bogart 2017). They may have found these vulnerabilities themselves, but it is also very likely that they have bought these vulnerabilities at underground markets for exploits (Fung 2013; Healey 2016). They do not disclose these vulnerabilities, not even to the system owners, which has caused some major damages when these vulnerabilities ended up in the wrong hands. For example, the Wannacry ransomware used the EternalBlue vulnerability, which is said to be discovered by the National Security Agency (NSA) several years ago (Nakashima and Timberg 2017; Titcomb 2017), and was not disclosed until the ShadowBrokers published it. Microsoft patched the vulnerability, but 3 months later many systems were still vulnerable which enabled the large and worldwide damage of the Wannacry ransomware (Newman 2017). This is likely one of the reasons that some parts of the hacker culture have a tendency to share vulnerabilities within the community, but not with others and especially not with governments (Taylor 1999). Additionally, by buying these vulnerabilities at underground markets, governments may send the message that they are not supporting CVD, as they are rewarding criminals who sell their exploits.

Knowledge about CVD among possible offenders

Several of the problems discussed above may influence a person's decision about how to handle a vulnerability. To be able to make a decision a person first needs to know about the possibility to report a vulnerability through CVD, and then must know the policy's rules. From the NTIA (2016) report, it is clear that most people who could be regarded as security researchers know about these policies. As also acknowledged by the NTIA it may very well be the case that their respondents have an interest in CVD or at least already know about it. It is unknown to what extent this can be said for the general

population. For the purposes of this work, we will assume that a person with the skills necessary to identify vulnerabilities in the wild knows about the possibility to use CVD.

Motives for CVD reporting

A first step in understanding the criminological side of CVD is to understand the motives for both criminal use of vulnerabilities and using CVD instead. Based on the general idea behind CVD, one could say the main reason to report a vulnerability is to increase cybersecurity. For example, Van't Hof (2016) describes a hacker who has made thousands of CVD reports and who sees it as his *"personal mission"* (p. 226). Even though this particular hacker does not go public after a successful disclosure, in general CVD may also be a way to gain status in the hacker community as most researchers who responded to the NTIA (2016) indicated that they expect some form of acknowledgement for their actions. Experiences from some organizations that have CVD policies and experiences at the National Cyber Security Centre also show that some security researchers specifically ask for recognition so that they can use that to build their CV by showing their skills.

Additionally, vulnerabilities may result from fairly easy-to-fix and well-known problems. Reporting that kind of vulnerability may even result from some form of frustration about the system's owner's inability to prevent these well-known vulnerabilities. Lastly, bug bounty programs added an important reason to report a vulnerability: money. Bounties may not be a pivotal drive, as only 15% of the researchers in the NTIA (2016) report indicated they expected a payment. A description of a young hacker by Van't Hof (2016) can be seen as a reflection of the motives above:

> *"I ask whether the cash bounties are important to him. Not really, he tells me. He hacks for the recognition in whatever form that comes. He wants to solve the puzzle and he wants to show other people that he has done so" (p. 215).*

The motives to report may not be substantial enough to warrant reporting for some individuals due to the inherent risks involved. The NTIA (2016) shows that the unclear rules and risk of prosecution could be enough to keep individuals from reporting a vulnerability. Additionally, the previously discussed frustration around the communication about a vulnerability is a reason to consider disclosing it publicly for 50% of all researchers in the NTIA (2016) report, and 32% actually disclosed publicly because of unmet timelines. Even though these researchers may not exploit the vulnerability they identify, their public disclosure may help others to do so instead. Nevertheless, their public disclosure may be the only way to force a company to fix the problem, inform other system administrators who have the same vulnerability, or to warn the users of the affected systems. In short, even with good intentions the decision between keeping a vulnerability private and public disclosure may not always be clear.

Motives for criminal hacking

It is important to note that not reporting a vulnerability, if identified, is not currently criminal. Using that vulnerability to engage in criminal hacks is, however, illegal and viewed as part of the hacking-process. An individual may use a vulnerability to gain access to a system, and then access the data on that system or use its functionality for other criminal purposes (Holt and Bossler 2016; Taylor 1999). Criminological research has indicated some motives for hacking and related behaviors. These motives could shed some light on the reasons why a person would decide to exploit a vulnerability or sell it at an underground market, instead of disclosing it or doing nothing with it (Holt and Bossler 2016).

Three different categories of motives for hacking and related offenses can be informative in understanding offending versus CVD. First, some criminal hacking occurs due to the challenge of breaking into a system, curiosity, a need to learn or understand a system, feelings of addiction, feelings of power, etcetera (e.g., Holt 2007; Voiskounsky and Smyslova 2003; Weulen Kranenbarg 2018; Woo 2003). These intrinsic motives could also account for the desire to identify vulnerabilities without exploiting them. However, after breaking in a person may be curious about the data that is stored on a system and may download that data. This is against the rules of most CVD policies. An example of this is a well-known case described in Van't Hof (2016), where a person hacked into the computer systems of a hospital. While the defendant said he had ethical motives, he also states that his "*curiosity drove him to access the server on more than one occasion*" (p. 183) and he also accessed patient records of specific celebrities. In this case, the court ruled that the defendant had gone too far and his behavior was no longer proportional.

A second motive is related to peer associations and personal ego development. In the criminal hacking community, showing that you broke into a system will give you more social status (e.g., Holt 2007; Nycyk 2010). By extension, identifying an unknown vulnerability and selling that or utilizing it in personal hacks would be a demonstration of serious skill. In the more white-hat community, however, showing that you reported a vulnerability through CVD or legitimate reporting channels may increase an individual's social status (Van't Hof 2016). In fact, there is anecdotal evidence that some

hackers have begun to donate bug bounty payments to charities, which helps to elevate an individual's reputation and status (Hackerone 2017). The community that a person is part of could therefore strongly influence a person's actions after finding a vulnerability.

Third, many modern criminal hacks are driven by the desire for monetary gain (e.g., Chan and Wang 2015; Grabosky 2017; Holt and Kilger 2012; Kshetri 2009; Provos et al. 2009; Smith 2015; White 2013). This could have two effects on vulnerability reporting. First, a person could decide to sell a vulnerability in the underground community or, second report vulnerabilities to bug bounty programs to turn a profit. We will now further discuss how these motives may influence the rational choice decision to exploit or disclose a vulnerability and we will discuss some things that may influence this decision in favor of using CVD.

Rational choice theory

One of the oldest criminological frameworks applies the rational choice perspective, where an individual considers the costs and benefits of offending when presented with opportunities to engage in crime. Should the benefits outweigh the costs that person may be more likely to offend (e.g., for a review on cybercrime see Holt and Bossler 2016). Regarding vulnerability disclosure, most researchers just find vulnerabilities during their daily online activities (NTIA 2016). They do not specifically look for them in specific IT-systems. Similarly, both traditional criminal opportunities as well as cybercriminal opportunities generally arise during normal daily activities (Weulen Kranenbarg et al. 2017, 2018).

One of the main costs associated with offending is the negative social consequences stemming from detection, such as arrest, prosecution and any resulting punishments (e.g., Pratt et al. 2006). The decision to offend is based on the perceived detection risk and costs relative to the benefits the individual receives. For most cybercrimes, apprehension rates are still very low (e.g., Holt and Bossler 2016; Wall 2007) which may make some individuals more likely to offend in cyberspace. Under current CVD practices, the risk of legal action after disclosing a vulnerability may be an important cost in the cost–benefit analyses for CVD. Additionally, if there are too many rules or if the disclosure process is too time consuming, this may also have a negative effect on this cost–benefit analyses for CVD.

Since the costs may be somewhat high for following CVD processes, individual motives may be an equally important factor in the outcome of vulnerability reporting. Individuals motivated by curiosity and social rewards may be more willing to report a vulnerability if they can receive some sort of additional social rewards for their actions. For example, if a company invites a discloser to help testing a patch for the vulnerability, it may make them feel more integrated into the process and see enough benefit to use CVD. Similarly, a person seeking peer recognition may be more affected by leveraging well-known role models such as regarded white-hat hackers who actively argue for the importance of using CVD instead of exploiting vulnerabilities.

Lastly, with respect to financial motives, some researchers have tried to make a costs-benefit analysis between bug bounty programs and the underground market. Allodi (2017) analyzed a Russian cybercrime forum. The results showed that the prices in the underground forum are the same or higher than in bug bounties or other legitimate markets. Also, a vulnerability could be sold more than once in the underground market, while it generally can only be sold once in the legitimate market. Additionally, in most criminal hacking cultures, working together with governments or large companies is not accepted (Holt 2007; Taylor 1999). Therefore, even if bounty payments are very high, reporting vulnerabilities may be offset by social costs to an individual's reputation. However, in general the costs of possible negative social consequences in combination with some payment seems to make bug bounty programs at least somewhat effective (Ransbotham et al. 2012; Zhao et al. 2015). Additionally, as some governments also buy exploits through underground markets, selling an exploit at those markets may also have a negative impact on a person's reputation.

Conclusions and discussion

The rise of coordinated vulnerability disclosure policies presents a unique challenge for criminological and computer science research as it is not entirely clear what factors affect the decision to handle a vulnerability. A person could decide to do nothing, exploit the vulnerability or sell it at an underground market, disclose the vulnerability publicly, or disclose the vulnerability privately by using CVD. The motives of the individual actor will directly shape their cost–benefit analyses regarding the organizational and criminal justice system responses to such a disclosure.

In light of the issues identified in this analysis, it is clear that there are ways to improve the current CVD policies' structure to increase the likelihood that actors report when they identify a vulnerability. From a situational crime prevention perspective (e.g., Newman and Clarke 2003), there are ways to affect the attackers' decision-making calculus in ways that could increase reporting or minimize criminal use. One potential avenue would be to increase awareness of CVD, which would remove excuses for not reporting vulnerabilities through CVD. Without this information, a hacker's knowledge base is limited,

thereby rendering their decision-making process substantially bounded. Creating programs that try to teach young hackers about the rules and possibilities around CVD, may increase awareness of the mechanisms and potentially improve the likelihood of reporting.

Additionally, providing a positive form of peer recognition through overt positive acknowledgements from the legal hacking community about successful CVD strategies, a potential offender may see the benefits of using CVD. This could be achieved through actively pushing information about successful CVDs to the general media, so that they can also show the positive and constructive side of hacking instead of only the negative criminal side. Such a strategy could not only increase compliance but also further eliminate hackers' excuses to not report (e.g., Holt and Bossler 2016; Newman and Clarke 2003). Additionally, this may stimulate the debate about the rules of CVD policies and when a discloser has crossed the line. More positive public information about CVD among large companies or governments may also demonstrate the value of reporting vulnerabilities to these organizations, despite the negative image this may have in some parts of hacking culture.

Another option based on situational crime prevention models would be to provide easy access to positive alternatives in the event of identifying a vulnerability to remove offender excuses for not reporting. For example, just as studies that use banners to inform potential system trespassers about the negative consequences of system trespassing (Maimon et al. 2014; Testa et al. 2017; Wilson et al. 2015), clear and eye-catching information about a website's CVD policy could help a person understand there are rules and guidelines to report a vulnerability. Additionally, it would be advisable to keep the threshold for reporting low, to make sure that the potential costs of CVD are as low as possible. This would also call on organizations to respond seriously, act quickly and set a date for making it public, keep the discloser updated, and make sure that their rules are clear and easy to find. Taking such steps would reduce the provocations and excuses of hackers that they have no clue what occurs when a vulnerability is reported. If an organization struggles with the fact that a discloser may have committed a crime in finding a vulnerability, organizing hackathons or other ways of actively inviting hackers to test systems, may partly reduce the chance that a person does something that is against the rules.

With respect to the organization's response, it may be valuable to keep an open communication line with the discloser. During the disclosure process, the discloser can be invited to test possible patching, or perform additional (paid) research for the organization for new products or services. As mentioned before, some organizations even use the disclosure process as a recruitment tool. These follow-ups after the disclosure process may provide disclosers with an interesting challenge or lead to legitimate profession.

It should be noted that these concepts have yet to be empirically tested, as with most situational crime prevention research related to cybercrime (e.g., Holt and Bossler 2016). In order to understand the potential of CVD in preventing cyber-offending some empirical research implications should be discussed. The current empirical work from, for example, the NTIA (2016) cannot tell us to what extent CVD is also being used by people who would otherwise exploit a vulnerability, or how much people actually know about CVD. Examining these issues with both general population samples and groups of IT-professionals would improve our understanding of the awareness of CVD. Additionally, there is no empirical research that directly asked disclosers why they used CVD. This may inform our knowledge of the relationship between individual motives and CVD reporting. Additionally, it would be very informative to see if individual reporting decisions vary based on situational factors specific to an individual, such as the type of vulnerability, organization impacted, motives, potential bounty or acknowledgement, and other related factors.

By addressing these research questions in interdisciplinary research, in the future CVD may be even more effective in achieving its main goal: preventing the exploitation of vulnerabilities in IT-systems. In the future it may not only achieve that goal by making IT-systems more secure in patching vulnerabilities, but also by steering potential offenders in the direction of CVD instead of exploitation.

Abbreviations

CVD: coordinated vulnerability disclosure; IEC: International Electrotechnical Commission; ISO: International Organization for Standardization; NCSC: National Cyber Security Centre; NSA: National Security Agency; NTIA: National Telecommunications and Information Administration.

Authors' contributions

MWK wrote the majority of the introduction and main text. TH provided context, additions and edits. JvdH provided context, additions and edits. All authors read and approved the final manuscript.

Author details

[1] Department of Criminology, Faculty of Law, Vrije Universiteit (VU) Amsterdam, De Boelelaan 1105, 1081 HV Amsterdam, The Netherlands. [2] School of Criminal Justice, Michigan State University, 434 Baker Hall, 655 Auditorium Road, East Lansing, MI 48824, USA. [3] National Cyber Security Centre-NL & University of Twente, PO Box 20301, 2500 EH The Hague, The Netherlands.

Acknowledgements

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Availability of data and materials
Not applicable.

Funding
Not applicable.

Publisher's Note

Received: 5 June 2018 Accepted: 8 November 2018
Published online: 19 November 2018

References

Ablon, L., & Bogart, A. (2017). *Zero days, thousands of nights: The life and times of zero-day vulnerabilities and their exploits*. Santa Monica, California: Rand Corporation.

Allodi, L. (2017). *Economic factors of vulnerability trade and exploitation*. Paper presented at the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, Texas, USA.

Android Security Rewards Program Rules. Retrieved May 30, 2018, from https://www.google.com/about/appsecurity/android-rewards/.

Chan, D., & Wang, D. (2015). Profiling cybercrime perpetrators in China and its policy countermeasures. In R. G. Smith, R. C.-C. Cheung, & L. Y.-C. Lau (Eds.), *Cybercrime risks and responses: Eastern and western perspectives* (pp. 206–221). London: Palgrave Macmillan UK.

Department of Justice (2017). *A framework for a vulnerability disclosure program for online systems*. US Department of Justice. CCIPS Division. Retrieved from https://www.justice.gov/criminal-ccips/page/file/983996/download.

Finifter, M., Akhawe, D., & Wagner, D. (2013). *An empirical study of vulnerability rewards programs*. Paper presented at the 22nd USENIX Security Symposium, Washington, D.C., USA.

Fung, B. (2013). The NSA hacks other countries by buying millions of dollars' worth of computer vulnerabilities. *The Washington Post*. Retrieved Aug 31, 2013, from https://www.washingtonpost.com/news/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/?utm_term=.2fe86803e816.

Grabosky, P. N. (2017). The evolution of cybercrime, 2006–2016. In T. J. Holt (Ed.), *Cybercrime through an interdisciplinary lens* (pp. 15–36). New York: Routledge.

Hackerone (2017). *The hacker-powered security report 2017. HackerOne's benchmark study on the hacker-powered security ecosystem.* Retrieved from https://www.hackerone.com/sites/default/files/2017-06/The%20Hacker-Powered%20Security%20Report.pdf.

Healey, J. (2016). The U.S. government and zero-day vulnerabilities; from pre-heartbleed to shadow brokers. *Journal of International Affairs*, 1–22. Retrieved from https://jia.sipa.columbia.edu/sites/default/files/attachments/Healey%20VEP.pdf.

Herr, T., Schneier, B., & Morris, C. (2017). *Taking stock: Estimating vulnerability rediscovery*. Belfer Cyber Security Project White Paper Series. Retrieved from https://ssrn.com/abstract=2928758.

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior, 28*(2), 171–198.

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. London: Routledge.

Holt, T.J., & Kilger, M. (2012). Know your enemy: The social dynamics of hacking. *The Honeynet Project*. Retrieved from https://honeynet.org/papers/socialdynamics.

Huang, C., Liu, J., Fang, Y., & Zuo, Z. (2016). A study on web security incidents in China by analyzing vulnerability disclosure platforms. *Computers & Security, 58*(2016), 47–62.

ISO/IEC (2014). International Standard: Information technology—Security techniques—Vulnerability disclosure (29147:2014(E)). International Organization for Standardization & International Electrotechnical Commission. Retrieved from https://www.iso.org/standard/45170.html.

Jordan, T., & Taylor, P. A. (1998). A sociology of hackers. *The Sociological Review, 46*(4), 757–780.

Kshetri, N. (2009). Positive externality, increasing returns, and the rise in cybercrimes. *Communications of the ACM, 52*(12), 141–144.

Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology, 52*(1), 33–59.

Microsoft Bounty Programs. Retrieved May 30, 2018, from https://technet.microsoft.com/en-us/library/dn425036.aspx.

Nakashima, E., & Timberg, C. (2017). NSA officials worried about the day its potent hacking tool would get loose. Then it did. *The Washington Post*. Retrieved May 16, 2017, from https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html?noredirect=on&utm_term=.f652694f1b42.

National Cyber Security Centre (NCSC). (2013). *Policy for arriving at a practice for responsible disclosure*. Retrieved from https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/news/responsible-disclosure-guideline/1/Responsible%2BDisclosure%2BENG.pdf.

National Cyber Security Centre (NCSC). (2017). *Cyber security assessment Netherlands 2017*. Retrieved from https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/cyber-security-assessment-netherlands/cyber-security-assessment-netherlands-2017/1/CSAN2017.pdf.

National Telecommunications and Information Administration (NTIA). (2016). *Vulnerability disclosure attitudes and actions: A research report*. Retrieved from https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf.

Newman L.H. (2017). The ransomware meltdown experts warned about is here. *Wired*. Retrieved May 12, 2017, from https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/.

Newman, G. R., & Clarke, R. V. (2003). *Superhighway robbery*. London: Routledge.

Nycyk, M. (2010). *Computer hackers in virtual community forums: Identity shaping and dominating other hackers.* Paper presented at the Online Conference on Networks and Communities: Debating Communities and Networks.

Pratt, T. C., Cullen, F. T., Blevins, K. R., Daigle, L. E., & Madensen, T. D. (2006). The empirical status of deterrence theory: A meta-analysis. In F. T. Cullen, J. P. Wright, & K. R. Blevins (Eds.), *Taking stock: The status of criminological theory* (pp. 367–396). New Brunswick/London: Transaction Publishers.

Provos, N., Rajab, M. A., & Mavrommatis, P. (2009). Cybercrime 2.0: When the cloud turns dark. *Communications of the ACM, 52*(4), 42–47.

Public Prosecution Service (2013). *Policy letter: Responsible disclosure (how to act in cases of 'ethical' hackers?* Retrieved from https://www.om.nl/publish/pages/22742/policy_letter_responsible_disclosure.pdf.

Ransbotham, S., Mitra, S., & Ramsey, J. (2012). Are markets for vulnerabilities effective? *Mis Quarterly, 36*(1), 43–64.

Smith, R. G. (2015). Trajectories of cybercrime. In R. G. Smith, R. C.-C. Cheung, & L. Y.-C. Lau (Eds.), *Cybercrime risks and responses: Eastern and western perspectives* (pp. 13–34). London: Palgrave Macmillan UK.

Steinmetz, K. F. (2016). *Hacked: A Radical Approach to Hacker Culture and Crime*. New York: NYU Press.

Taylor, P. A. (1999). *Hackers: Crime in the digital sublime*. London: Routledge.

Testa, A., Maimon, D., Sobesto, B., & Cukier, M. (2017). Illegal roaming and file manipulation on target computers. *Criminology & Public Policy, 16*(3), 689–726.

Titcomb, J. (2017). Microsoft slams US government over global cyber attack. *The Telegraph*. Retrieved May 15, 2017, from https://www.telegraph.co.uk/technology/2017/05/15/microsoft-slams-us-government-global-cyber-attack/.

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior, 75*(2017), 547–559.

Van't Hof, C. (2016). *Helpful hackers: How the Dutch do responsible disclosure*. Rotterdam: Tek Tok Uitgeverij.

Voiskounsky, A. E., & Smyslova, O. V. (2003). Flow-based model of computer hackers' motivation. *CyberPsychology & Behavior, 6*(2), 171–180.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. New York: Polity.

Weulen Kranenbarg, M. (2018). *Cyber-offenders versus traditional offenders: An empirical comparison* (Unpublished doctoral dissertation). Vrije

Universiteit Amsterdam, The Netherlands. Retrieved from http://dare.ubvu.vu.nl/handle/1871/55530.

Weulen Kranenbarg, M., Holt, T. J., & Van Gelder, J.-L. (2017). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior*. https://doi.org/10.1080/01639625.2017.1411030.

Weulen Kranenbarg, M., Ruiter, S., Van Gelder, J.-L., & Bernasco, W. (2018). Cyber-offending and traditional offending over the life-course: An empirical comparison. *Journal of Developmental and Life-Course Criminology, 4*(3), 343–364.

White, K. (2013). The rise of cybercrime 1970 through 2010. A tour of the conditions that gave rise to cybercrime and the crimes themselves. Retrieved from https://www.slideshare.net/bluesme/the-rise-of-cybercrime-1970s-2010-29879338.

Wilson, T., Maimon, D., Sobesto, B., & Cukier, M. (2015). The effect of a surveillance banner in an attacked computer system. *Journal of Research in Crime and Delinquency, 52*(6), 829–855.

Woo, H.-J. (2003). *The hacker mentality: Exploring the relationship between psychological variables and hacking activities*. The University of Georgia, Athens, Georgia. Retrieved from https://getd.libs.uga.edu/pdfs/woo_hyung-jin_200305_phd.pdf.

Zhao, M., Grossklags, J., & Liu, P. (2015). *An empirical study of web vulnerability discovery ecosystems*. Paper presented at the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, Colorado, USA.