GFCE Global Good Practices

Coordinated Vulnerability Disclosure (CVD)

GFCE
Global Forum on Cyber Expertise

Preface

The unprecedented uptake of information and operational/industrial control system technologies (IT and OT/ICS) worldwide leads to a growing dependency of economic sectors, public institutions and societies. Vulnerabilities in software and hardware are abundant. When vulnerabilities are found by a third party, the challenge arises on how to report the vulnerability in a prudent way to those actors who can remove the vulnerability. Time is needed to fix the vulnerability before a wider audience gets informed.

Coordinated Vulnerability Disclosure (CVD) pertains to the mechanisms by which vulnerabilities are shared and disclosed in a controlled way. This Global Good Practice document helps to shape a concerted international approach and support establishment of national CVD policies. The emphasis of these good practices is on software manufacturers, vendors, and user organisations as they are key to a successful CVD policy. The government usually plays a facilitating role, for instance in diminishing legal challenges and promoting CVD. This document provides the necessary insight to political leadership, government policy-makers and other stakeholders to implement the most important elements of a CVD policy.

This Global Good Practice document is based on international expert meetings dedicated to CVD which were held in March and November 2016. The expert meetings were attended by representatives of governments, international organisations, businesses, legal sector, academia and technical communities. Earlier reports and literature related to this topic are also incorporated. To keep this document brief, the content of these meetings and documents is summarised. A full list of sources can be found in the annex.

1. Introduction

What is vulnerability disclosure?

Cyber security has become a priority for many organisations and governments the last few years. The ever-increasing use of and dependency on information technology (IT) and interconnectivity brings many advantages, but also introduces increasing risk for individuals, organisations, and the society as a whole. Cyberattacks and unintentional incidents can cause damage in both the digital and physical world.

Reducing software vulnerabilities is a key concept in strengthening cyber security. Vulnerabilities are flaws in software code of information systems that may be exploited to compromise the confidentiality, availability or integrity of the affected systems, with possible effects further in the IT network as well as in the monitoring and control of cyber-physical processes (through so-called Operational Technology). Vulnerabilities provide a point-of-entry for malicious activities and as such pose several, potentially severe security and safety risk. Remedying vulnerabilities is therefore crucial and a vulnerability disclosure process is a significant element in reducing the risk for system owners, third parties, and the society.

The vulnerability disclosure process is seemingly straightforward, but the landscape is complex. Several stakeholders are involved, such as technology user organisations and their stakeholders (clients, personnel, investors etc.), independent researchers and other reporters, software manufacturers and vendors, IT security providers, malicious users and, ultimately, the media and the general public. These stakeholders may have conflicting interests, leading to challenges and pressing questions concerning dealing with discovered vulnerabilities. Challenges include legal constraints, lack of trust between key actors, awards and different appreciation of timelines.

However, as software-dependent technologies are becoming increasingly embedded in everyday life, it is vital for the economy and society at large to face these challenges and to have appropriate procedures in place for disclosing vulnerabilities.

Cooperation between organisations and the cyber security community can be helpful in finding and fixing vulnerabilities. Proven mechanism of cooperation in that regard is *coordinated vulnerability disclosure (CVD)/responsible disclosure*. Essentially, this is a form of cooperation in which a reporter informs a manufacturer or owner of the information system of a vulnerability, allowing the organisation the opportunity to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties and/or the general public. CVD and responsible disclosure are terms often used interchangeable. The concept behind both terms is to have both the organisation and the reporter work together to disclose information about the vulnerability at a time after a resolution is reached. Strictly defined, however, the distinction between the terms is that CVD

refrains from defining any specific time frames and only permits public disclosure after a resolution or evidence of exploitation is identified. Objectives of a CVD policy include:

- ensuring that identified vulnerabilities are addressed in a risk-based way (some vulnerabilities may be more critical to address, especially in a timely way, than others);
- reducing the security risk from identified vulnerabilities;
- providing users with sufficient information to evaluate the risk from vulnerabilities to their systems;
- setting expectations to promote positive communication and coordination among involved parties;
- responding to and communicating with reporters (confirmation of receipt and an opportunity to engage when there are investigative, remediation, etc.).

Why should one adopt a CVD policy?

Organisations that develop, manage and use software carry most of the work involved with implementing CVD. They will need to overcome some key challenges outlined in the section below, including with resourcing and in terms of culture and expectations, attached to adopting a CVD policy for themselves. To stimulate the adoption of CVD by organisations, a national Computer Security Incident Response Team (CSIRT) or other relevant governmental agencies should actively promote its benefits:

- An effective CVD policy can lower the threshold for the reporting of vulnerabilities, thus increasing the chance that the organisation can fix a vulnerability before malicious actors take advantage of it against the organisation. Voluntary reporters, such as ethical hackers and security researchers, help strengthen the organisation's cyber security.
- It builds customers' trust by a public and increased interest of the organisation in security of their (personal) data.
- Sharing vulnerability information also brings external information about new relevant vulnerabilities to the organisation.
- It is a socially responsible and effective way of handling software vulnerabilities, thus contributing to cyber security for all.
- Finally, a CVD program complements an organisation's individual capacity and efforts to test its own products and/or services (i.e., there's value in doing both, not just one or the other).

Therefore, CVD benefits both society and the interests of individual organisations.

Basic steps of vulnerability disclosure

Though implementation may differ per organisation (or nation state), the vulnerability disclosure process usually involves the following steps:[1]

1. discovery of a vulnerability (by the reporter, for instance a security researcher or employee);
2. notification to the owner, manufacturer or vendor of the affected system or software;
3. investigation of the potential vulnerability and its impact by the owner, manufacturer or vendor;
4. confirmation (or not) of the vulnerability;
5. resolution by patching or otherwise reducing or eliminating the vulnerability;
6. public disclosure of information about the vulnerability (and the patch).

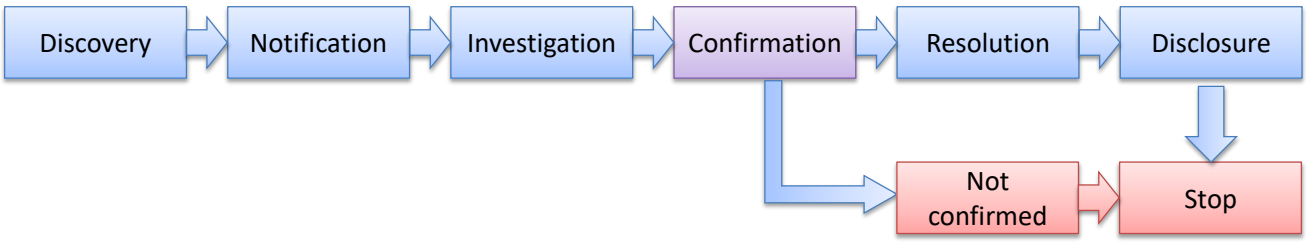

Figure 1: key steps of vulnerability disclosure

In practice, many varieties of the disclosure process can exist. A discovery may not lead to disclosure at all, but to secrecy and possible sale of the vulnerability to a third party. On the opposite, a reporter can also choose immediate full public disclosure, offering owners, manufacturers and vendors little or no time to resolve the vulnerability. In the case of many users of the vulnerable technology, such users will be put at significant risk without a patch or other remediation. In between those two opposites is *coordinated vulnerability disclosure*, in which the reporter and the owner (and/or manufacturer or vendor) coordinate actions and timelines before disclosure. A variant is *limited disclosure* in which only specific parties are informed about a discovered vulnerability. Such parties could be trusted third parties like a national CSIRT.

[1] Based on (ENISA, 2015).

2. Good practices

Good practices for political leadership and policymakers

Governments and the political leadership have a facilitating role in introducing and implementing a CVD policy. This paragraph highlights some good practices for this role.

Good Practice 1: Introduce or enhance a third party 'good office' (e.g. CSIRT)

Conflicting interests such as lack of trust, uncertainty, and resourcing issues of a software manufacturer/vendor or user organisation on the one hand, and vulnerability reporters on the other hand may hamper direct communications. A trusted third party acting as coordination centre could be established. In many countries, the national CSIRT takes on the role of a coordinator. Increasingly, bug bounty platforms (e.g., HackerOne, Bugcrowd) also act as coordinators. For reporters of vulnerabilities, benefits include limiting the legal exposure of the reporter and allowing the reporter to (potentially) remain anonymous. However, anonymity may limit reporters', manufacturers' and vendors' abilities to work together to build trust and communicate seamlessly to clarify issues.

In addition, for manufacturers and vendors that are new to CVD, the involvement of coordination centres may also help them manage scale that is difficult to predict and increase trust in reporters that are helping them improve the security of their products and services.

Good Practice 2: Implement a mechanism for international harmonisation of coordinated vulnerability disclosure and relevant legislations

Reporters, manufacturers, vendors, and user organisations are more often than not located in different countries. Differences between national CVD approaches and corresponding legislations can lead to misunderstandings between key players in CVD, hence complicating the process. This requires an international approach to the topic of CVD. The ISO/IEC 29147:2014 standard may be of help to this process. Stakeholder gatherings at the international level can be used to discuss successful cases in certain countries or regions for the development of good practices. Simultaneously, national prosecution guidelines can be collected and disseminated to foster a harmonised legal framework.

Good Practice 3: Stimulate a more open culture in which vulnerabilities are accepted and acknowledged

Because of the potential risk of reputational damage, organisations could be reluctant to acknowledge the existence of vulnerabilities. Awareness-raising is important in moving society in a direction where the existence of vulnerabilities is accepted. Building trust by sharing CVD successes and promote the value of disclosure for the society as a whole are good practices.

Good Practice 4: Stimulate Information sharing platforms, such as ISACs, to facilitate openness and transparency about vulnerability information

Because of the confidential nature of vulnerabilities and fear of digital, physical or reputational damage, there might be a lack of openness and transparency. Platforms could be established for sharing information on vulnerabilities in a trusted setting. As a good practice, the Information Sharing and Analysis Centres (ISACs), which are established in multiple countries, should be mentioned. ISACs are usually dedicated to specific critical infrastructure sectors. In these public-private partnerships, amongst others, technical information about threats and vulnerabilities is exchanged.

Good Practice 5: Engage with the security researcher community and build trust by example

Security research projects without malicious intent can lead to discovery of vulnerabilities and not seldom it is the objective of security research projects to do just that. Reaching out to this group to discuss the terms of an acceptable and responsible form of vulnerability disclosure helps building trust. Equally important is living up to those terms and prove to the community that this approach to disclosure works for all parties. Security researchers – for instance from universities and academia - can also help to develop further norms on what is an acceptable CVD practice.

Good Practice 6: Support the legal sector in identifying possibilities and mitigate risk with regards to coordinated responsible disclosure

Legal challenges are a primary issue of concern, especially for reporters (e.g. prosecution, liability) and for user organisations, software manufacturers and vendors (e.g. civil liability). The technical nature of cyber security and vulnerabilities makes assessing vulnerability disclosure matters a challenging matter for legal professionals. Providing the legal sector with more insight in the background and workings of vulnerability disclosures improves their ability to make proper assessments for policy or case issues.

Good Practice 7: Ensure that the primary responsibility rests with the organisation and reporters involved

In the end, every stakeholder is responsible for its own actions (or lack thereof) in vulnerability disclosure. Governments can provide conditions, like policies, prosecution guidelines, promotion and if need be a trusted third party, but should refrain from regulation. It is the individual manufacturer, vendor, the user organisation responsible for IT systems with vulnerabilities, and the reporter finding and reporting vulnerabilities that has to take guidelines and the interests of the stakeholders into account. This clear message is part of CVD policy discussions and implementation.

Good practice 8: Include CVD in procurement requirements

The buying power of government can be used as an extra impulse for implementation, also for CVD. Procurement requirements could include an implemented CVD-procedure for potential suppliers, for instance based on open standards such as (ISO/IEC 29147:2014).

Good practice 9: Be an example

The governmental sector (ministries and agencies) can take the lead in adopting and publishing a CVD policy regarding its own information systems and services.

Good practices for manufacturers, vendors and user organisations

In this document organisations appear in two roles: as a manufacturer or vendor of software that is used for information systems or as a user organisation, applying that software in its information systems. Both are critical parties in solving software vulnerabilities. Please note that especially for organisations more elaborate good practices can be found in standards and community-based documents (good practice 1 below).

Good practice 1: Use existing documents and apply them in a flexible manner when implementing a CVD policy and corresponding procedures

Good practice documents have already been developed. Although still lacking in certain stakeholder communities, they reduce the required efforts to implement CVD and prevent carrying out activities which are already done. Since every organisation is unique, the guidelines in these documents should be adapted to the organisation's characteristics. Amongst others, the following documents referenced in the Annex can be used as a guide or background reading:

- ISO/IEC standards 29147 and 30111;
- The framework of the Organization for Internet Safety (OIS);
- The Internet Engineering Task Force (IETF) Responsible Vulnerability Disclosure Process;
- FIRST's Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure;
- Coordinated Vulnerability Disclosure Implementation Guide / Model Policy and Procedure by the CIO Platform Nederland;
- Good Practice Guide on Vulnerability Disclosure by ENISA;
- The "Early Stage" Coordinated Vulnerability Disclosure Template and the Vulnerability Disclosure Attitudes and Actions report by NTIA.

Good practice 2: Organisations should implement the necessary processes, develop a policy and publish the policy on the website

Organisations should implement the required processes to deal with incoming reports, to investigate the reported vulnerabilities, and to communicate with reporters, being as transparent as practicable about risk-based remediation timelines. To inform users on how the organisation processes vulnerability reports, an explicit CVD policy should be published on the website. An example procedure and policy can be found in each of the publications listed in the good practice 1 above.[2] For a successful implementation of CVD, multiple activities need to be performed, as described in the implementation guide by CIO Platform Nederland:

[2] For example, see CIO Platform Nederland, 2016b, available in English and Dutch.

1. The organisation's readiness for CVD must be determined. If the organisation cannot properly respond to an incoming report, a reporter may disclose the vulnerability to the media. For example, when there is no IT incident procedure, and no clear process to receive a vulnerability report and confirm receipt, the organisation may not be ready.
2. Determine the important decisions which need to be made, such as the responsibilities between the various layers within the organisation, the products and services covered by the policy and limitations imposed on the reporter activities.
3. Reach agreements and determine an effective structure for consultation. External and internal stakeholders should be consulted. In case of multi-party disclosure, the implementation of CVD is not limited to the organisation itself. For instance, third parties such as cloud providers might play a key role (see NTIA (2016)). Internal stakeholders include the legal department and IT-support.
4. The procedure and the policy must be developed. An important aspect is the embedding and alignment of the procedure and policy with existing processes policies and agreements, such as incident and supplier management. Decisions need to be made for the identified decision points in step 2.
5. Implement the procedure and policy. Senior management needs be involved, as CVD may influence the organisation as a whole. Hereafter, the CVD policy and procedure should be practiced, evaluated and eventually be made operational. This includes publishing the CVD policy on the website.[3]

Good practice 3: Reserve adequate resources for the implementation of CVD

The implementation of CVD requires resources, time and attention. Processes need to be implemented and new organisational roles must be established, which require certain (technical) expertise. Some key challenges need to be overcome (chapter 3). A good practice is to start small: run a pilot and start with a narrow set of in-scope products/services, use a third-party bug bounty platform, and/or consult with similarly situated organisations that have CVD policies and processes in place to get a sense of the amount of resources that will be required.
Tools may have to be acquired for the management of the incoming reports.

Organisations should therefore reserve adequate resources for the necessary people, processes and technology. Reusing good practices helps decrease required efforts, so can participation in trusted platforms for information sharing.

Good practice 4: Ensure continuous communication with different stakeholders

Communication with the different stakeholders one of the most important aspects of a successful CVD. Manufacturers, vendors, and user organisations need to explicitly state their expectations

[3] (CIO Platform Nederland, 2016a) guide available in English and Dutch.

towards reporters, ideally through a published policy on the website. The organisation should respond as soon as possible to a report and then, if the vulnerability is confirmed, keep the reporter informed on the developments. The ISO/IEC standard state that within a maximum of seven calendar days an initial response should be provided. Another key aspect is the continuous communication with third party organisations, such as the supplier of the software or system and other organisations who are affected (for multi-party disclosure, see (FIRST)).

Good practice 5: Agree on timelines on a case-by-case basis

Timelines for an individual CVD case should consider risk-based assessments and the differences between various vulnerability discovery cases as well as the products or systems affected. There is not one size that fits all, but timelines must involve regular communication with the reporter to ensure reporter confidence that efforts are ongoing, ideally facilitating coordination and a degree of flexibility should unexpected complications arise. Publishing CVD steps and timeline considerations upfront also helps with managing expectations.

Good practice 6: Provide a clear explanation of pros and cons to the legal council

Legal councils of organisations may be inclined to point out the risk of a CVD, for instance reputational damage, litigation by clients (or third parties) or public prosecution. Their advice is crucial for the overall decision of an organisation to implement a CVD policy. This advice should ideally also be based on a good understanding of the importance and advantages of CVD for an organisation (see the high-level benefits in the introduction as a starting point), as well as the national legal framework on CVD (including public prosecution CVD guidelines). Providing a clear overview of all this information is a worthwhile investment for the discussions with 'legal' experts.

Good practices for reporters

There is no CVD without reporters of vulnerabilities. They trigger the process and enable security improvements. The success of a CVD case largely depends on reporters agreeing to act accordingly. Please note that also for reporters more elaborate good practices can be found in the documents listed in the Annex.

Good practice 1: The reporter is responsible for his own actions and should act proportionally

Reporting a discovered vulnerability immediately to the general public can hurt the interests of other stakeholders. Even though sharing vulnerabilities helps to improve security in the long run, user organisations (owner of systems involved), manufacturers and vendors should have the opportunity to respond to discoveries and take the appropriate actions. It is the reporter that is leading in the first stages of a CVD process (when to disclose what to whom) and as such he/she is responsible for all of his/her own actions. Following CVD guidelines (if available) in all stages is advised. Depending

on the exact legal framework it can protect the reporter and/or organisation against legal claims to some extent and is therefore in his or her own interest.

Responsibility also implies acting proportionally, like abstaining from installing any new software (such as backdoors), copying, deleting or editing data, or sharing access with others. In short, the reporter should try to do the minimum possible intrusion into the system to confirm that there is a vulnerability.

Good practice 2: The reporter shall report the vulnerability as soon as possible to the owner of compromised system or the manufacturer/vendor

It is easily conceivable that a vulnerability discovered, is also found by another actor, with more malicious intentions. Reporting the vulnerability directly to the owner of the compromised system or the manufacturer or vendor of the product used for the system in the shortest possible time is important to minimise the chances of abuse.

Direct communication between reporter and owner through a secure and trusted channel is good practice to minimise the number of steps in communication between reporter and organisation (for reasons of speed, correctness of information, etc.). However, the reporter and organisation can decide to include an independent, coordinating third party in the conversation.

Good practice 3: The reporter will not publish the vulnerability prematurely

Ideally reporter and owner (and possibly the manufacturer or vendor) of a compromised system come to an agreement on informing each other on the vulnerability found, informing whether it is patched or otherwise solved in the system and if or when (and how) the vulnerability can be disclosed publicly. The manufacturer, vendor, or user organisation should be allowed reasonably sufficient time to fix the software.

Good practices for the legal sector

In this document, legal sector refers to organisations tasked with public prosecution, administration of justice and other legal professions like lawyers.

Good Practice 1: Publish prosecution guidelines, including some level of protection for reporters

Reporters of vulnerabilities might be inclined to think better of reporting when there is a possibility of prosecution under criminal law. A set of guidelines by the public prosecutor's office can provide clarity on key legal concepts with regards to vulnerability disclosure and diminishes uncertainty for reporters.

Such key legal concepts could include the notion of ethical hacking (usually not included as such in law), the relationship between CVD guidelines and criminal law, and conditions under which discovering and reporting vulnerabilities could or should be considered a criminal offence (e.g.

necessity and proportionality of actions). The main purpose of these prosecution guidelines is identifying grey areas of law and assisting public prosecutors in deciding on prosecution of specific cases. These guidelines also identify the role of public prosecution in relation to other stakeholders. Even though it does not provide a carte blanche to reporters, it does demonstrate that the public prosecution office takes this matter seriously.

In the Netherlands, public prosecutors are instructed[4] to take the following aspects into consideration for deciding whether to proceed with criminal investigation:

- Did the discovery concern the general interest (acting in good faith)?
- Were the actions proportional (no actions beyond what is necessary to confirm the vulnerability)?
- Was the vulnerability immediately reported to the manufacturer or vendor, or were other actions performed, such as deletion of traces?

Good Practice 2: Use case law to make vulnerability disclosure cases more predictable for reporters and other stakeholders involved

Like public prosecution guidelines, jurisprudence / case law provides more clarification for all parties on how courts of criminal law interpret vulnerability disclosure practices. This is especially true in legal environments where there are no public prosecution guidelines, and/or civil law suits are the primary course of action. Bundling and publishing relevant case decisions or verdicts on a CVD-related website increases the chance that the target audience will read it.

Good Practice 3: Explain legal framework to a non-legal audience

The legal framework is usually not the first thing in mind for reporters, manufacturers, vendors, and user organisations. A clear and concise explanation of the most important elements of civil and penal law can be part of national CVD guidelines and their promotion.

4 Openbaar Ministerie (Public Prosecutor NL), 2013

Good practices for national CSIRTs

In some cases, a national Computer Security Incident Response Team (CSIRT a.k.a. CERT) can fulfil a role in promotion and/or coordination of CVD, due to their independence (to some extent), cyber security knowledge and national and international network.

Good Practice 1: Raise awareness & promote good practices

To stimulate the adoption of CVD by organisations, CSIRT or other relevant governmental agencies should actively promote its benefits. The CISRTs should provide organisations with good practices on the implementation of CVD. For example, in the Netherlands the National Cyber Security Centre (NCSC-NL) launched a guiding example policy[5] in 2013, which has been adopted by many Dutch government institutions and companies. This has increased the overall maturity of CVD in the Netherlands.

Good Practice 2: When a vulnerability is reported, try to connect the reporter and the organisation whose product/service is affected the vulnerability

CSIRTs may take on the role of a trusted third party within the CVD-process. As a 'coordinator' they can connect the reporter and the organisation. However, the CSIRTs should encourage reporters to first contact the organisation itself. When they cannot come to an agreement with the organisation or when their report is not taken into consideration, they should approach the CSIRT. Reporters could also approach the CSIRT directly when they prefer to stay anonymous, are unable to contact the organisation or if multiple organisations are involved in the vulnerability.

Good Practice 3: Share the vulnerability-information, in correspondence with the organisation and reporter, to relevant stakeholders within the IT-community

Because of their coordinating role and their participation in multiple networks, CSIRTs are in a position to be able to disclose the vulnerability to a selected group of key stakeholders or members. For example, critical infrastructure operators can be made aware of a vulnerability to take the appropriate actions before malicious actors obtain the information.

5 (NCSC-NL, 2013a)

3. Key challenges

Given the complex nature of the CVD landscape and the conflicting interests of the stakeholders involved, multiple challenges are associated with the disclosure of vulnerabilities. In this paragraph, key challenges are highlighted.

Key challenge 1: Reporters can face legal threats when discovering a vulnerability (civil liability, criminal liability, liability under patent and other laws)

The methods used and actions taken by reporters to find and disclose a vulnerability are illegal in some countries. Moreover, the laws and regulations with regards to vulnerability disclosure (if there are any) are often ambiguous. Reporters may therefore find themselves in a grey legal area and might face legal threats when they decide to report vulnerabilities. These threats can derive from not only criminal law but also contract law, licensing, patent law and other types of legislation. A lack of clarity on key legal concepts may discourage the disclosure of vulnerabilities by reporters.

Key challenge 2: There can be conflicts between the involved stakeholders. This may very well lead to lack of trust between stakeholders, public disclosure, and increased risk to technology users.

Manufacturers, vendors, and user organisations may not act upon vulnerability reports despite of the damage the vulnerabilities might induce. There are all sorts of reasons for organisations to disregard the incoming reports, including uncertainty about reporters' motives, uncertainty about legal/ reputational risk, other near-term priorities that shift attention, and lack of a policy and process, which may result in the vulnerability landing in the inbox of someone who doesn't know how to address it. Reporters may therefore choose to make the vulnerability public prematurely, hence providing malicious actors the opportunity to abuse the vulnerability and increasing risk to technology users. Moreover, reports may be inadvertently published or leaked before an agreed publication date.

Key challenge 3: manufacturers, vendors, and user organisations may have no vulnerability reporting processes and may therefore be ill-prepared to act timely on vulnerability reports

Implementing a CVD requires commitment of time and (scarce) resources. Especially small companies and companies with limited resources or knowledge, may lack the appropriate processes for handling and reporting vulnerabilities. They are therefore less prepared to accept vulnerability reports and act upon them. If this is the case, it is not always clear from the outside for reporters, leading to a mismatch of expectations. Complications may also arise in the case of outsourcing of information (and communication) technology services, cloud computing, and when working with multiple (cross-border) legal entities within one organisation.

Key challenge 4: Going public about discovered vulnerabilities may introduce new risk for organisations, such as reputational damage or litigation

Acknowledging that one of its products (for a manufacturer or vendor) or information systems (for a user organisation) contains a vulnerability may lead to reputational damage or litigation. Organisations could therefore be unwilling to publicly recognise the existence of vulnerabilities. The existence of a (working) CVD process based on international good practices should build trust with 'customers' and /citizens, and partially mitigate such risk. Moreover, because every organisation is vulnerable, so having a method in place to discover vulnerabilities as early as possible seems a prudent thing to do.

Key challenge 5: Because of the growing zero-day market, reporters may sell vulnerabilities

The motivation of the reporter can influence the decision he/she makes regarding what to do with the vulnerability. The growing zero-day market may tempt some researchers to sell vulnerabilities (or exploits, which often contain multiple vulnerabilities). However, there has also been recent growth in bug bounty programs. While some are concerned that this may lead to over-incentivising the search for vulnerabilities, those that have implemented such programs find that they are successful in focusing researcher attention on newer and more critical products and services. Moreover, they do not necessarily lead reporters to expect that they will always receive a monetary reward for their discovery; rather, other forms of rewards, such as public credit, have widely been adopted and remain meaningful.

Key challenge 6: Reporter may lack the experience to report vulnerabilities properly and may be unwilling to comply

Just like organisations may lack experience in accepting vulnerability reports, also researchers and other types of reporters might lack sufficient experience in reporting vulnerabilities. In that case, reporters may approach manufacturers or vendors in a way that prevents fruitful cooperation (threatening, non-conducive, unclear etc.). Inexperienced reporters may also be unwilling to compromise on, for example, timelines identified by the manufacturer or vendor. A specific issue for reporters is sufficient knowledge about legal issues.

Key challenge 7: User organisations are often reluctant to apply the provided patches for the reported vulnerabilities directly, thus leaving software insecure

Once a vulnerability and patch or other remediation are made public by the manufacturer or vendor, organisations (and or individuals) must install the proposed patch to resolve the vulnerability. Because the information about the vulnerability is now public, organisations and individuals are more vulnerable for a cyberattack which may compromise their system. But for several reasons, organisations may choose to postpone patching or dismiss the patch. This leaves their systems vulnerable.

Key challenge 8: Resourcing at especially newer technology manufacturers and vendors

Newer technology manufacturers and vendors (e.g., in the automotive industry, internet-of-things, robotics) face specific start-up phase challenges regarding vulnerabilities within their products or services:

1. knowing how many vulnerability reports are about to come their way, what and how many resources will be needed to deal with them appropriately;
2. understanding why reporters are reporting such vulnerabilities to them, i.e. the need to build trust with security researchers, and getting to a place and culture in which the organisation values the reports/exchange.

Annex: sources on Coordinated Vulnerability Disclosure

Besides the two expert meetings mentioned in the introduction, the following sources were used to draft this Global Good Practice document. These sources can also be used for local implementation by individual governments and/or organisations.

CIO Platform Nederland. (2016a). Coordinated Vulnerability Disclosure Implementation guide. Retrieved from: https://www.cio-platform.nl/nl/publicaties/publicaties

CIO Platform Nederland. (2016b). Coordinated Vulnerability Disclosure Model policy and procedure. Retrieved from: https://www.cio-platform.nl/nl/publicaties/publicaties

CIO Platform Nederland. (2016c). Coordinated Vulnerability Disclosure Q and A. Retrieved from: https://www.cio-platform.nl/nl/publicaties/publicaties

CIO Platform Nederland. (2016d). Coordinated Vulnerability Disclosure Manifesto. Retrieved from: https://www.cio-platform.nl/nl/publicaties/publicaties

ENISA (European Union Agency for Network and Information Security). (2015). Good Practice Guide on Vulnerability Disclosure. Retrieved from: https://www.enisa.europa.eu/publications/vulnerability-disclosure/at_download/fullReport

FIRST (2017). Guidelines and Practices forMulti-Party Vulnerability Coordination and Disclosure. Retrieved from: https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRST-Multiparty-Vulnerability-Coordination-v1.0.pdf

Global Conference on Cyberspace (GCCS). (2016). Introducing Responsible Disclosure. Retrieved from: https://www.gccs2015.com/sites/default/files/documents/BestPracticeRD-20150409_0.pdf

International Organization for Standardization (ISO). (2013). ISO/IEC 30111:2013 (Information technology -- Security techniques -- Vulnerability disclosure). Retrieved from: https://www.iso.org/standard/53231.html (to be replaced by ISO/IEC NP 30111).

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

Internet Engineering Task Force (IETF). Responsible Vulnerability Disclosure Process (work-in-progress; expired draft 2002).

NCSC-NL (Nationaal Cyber Security Centrum). (2013a). Leidraad om te komen tot een praktijk van Responsible Disclosure. Retrieved from: https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html

NCSC-NL (Nationaal Cyber Security Centrum). (2013b). Kamerbrief responsible disclosure. Retrieved from: https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/nieuwsberichten/leidraad-responsible-disclosure/1/Kamerbrief%2BResponsible%2BDisclosure.pdf

New Zealand Internet Task Force (NZITF). (2014). Coordinated Disclosure Guidelines. Retrieved from: http://www.nzitf.net.nz/pdf/NZITF_Disclosure_Guidelines_2014.pdf

NTIA (2016). "Early Stage" Coordinated Vulnerability Disclosure Template, Version 1.1, US National Telecommunications and Information Administration. Retrieved from: https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf

NTIA (2016). Vulnerability Disclosure Attitudes and Actions, US National Telecommunications and Information Administration. Retrieved from: https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf

Openbaar Ministerie (OM, Dutch Public Prosecutor). (2013, March 18). Letter to: Aan alle parkethoofden. Retrieved from: www.om.nl/publish/pages/22742/03_18_13_beleidsbrief_college_responsible_disclosure.pdf

Organization for Internet Safety (OIS). (2014). Guidelines for Security Vulnerability Reporting and Response. Retrieved from: http://www.symantec.com/security/OIS_Guidelines%20for%20responsible%20disclosure.pdf

Romanian National Computer Security Incident Response Team CVD. Online: https://cert.ro/pagini/CVD

This document was drafted and developed in cooperation with TNO for the Global Conference on Cyberspace GCCS in India (2017). Many thanks to all others who participated in the realisation of this document.


GFCE
Global Forum on Cyber Expertise