STI Policy Note

www.oecd.org/sti

Encouraging vulnerability treatment

How policy makers can help address digital security vulnerabilities

Digital security risk undermines trust in digital transformation and generates significant economic and social costs. Estimates suggest that the cost of digital security incidents ranges between USD 100 billion and USD 6 trillion per year. Digital security risk also poses an increasingly serious threat to individuals' safety, as more consumers and businesses adopt vulnerable Internet of Things (IoT) devices.

Most digital security incidents are caused by malicious actors (e.g. cybercriminals and state-sponsored groups) exploiting vulnerabilities in organisations' digital ecosystems. Addressing these vulnerabilities before attackers take advantage of them is an effective means to reduce the probability of incidents.

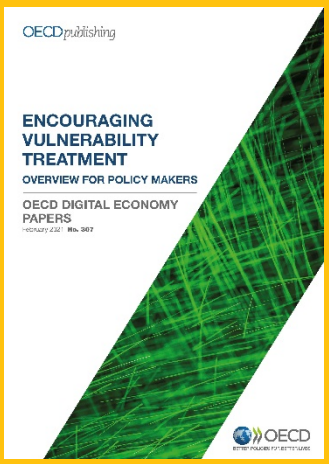
Vulnerabilities are weaknesses that can be exploited to damage economic and social activities, and are a major source of digital security risk. Code, the engine of digital transformation, is never perfect, and almost always has vulnerabilities; and information systems have vulnerabilities related to how software is implemented, configured and updated. Criminals and other ill-intentioned actors actively seek to discover such vulnerabilities, and develop or use tools such as "malware" to exploit them through incidents that harm businesses, governments and individuals, threaten critical activities and undermine trust in digital transformation.

The quick read

Addressing vulnerabilities in products' code and in the way products are implemented in information systems is key to a successful digital transformation. Over the last few years, the technical community has progressed in developing good practice for treating vulnerabilities, including through co-ordinated vulnerability disclosure (CVD). However, significant economic and social challenges prevent stakeholders from adopting good practice, including a lack of awareness and co-operation, limited or opposite market incentives, legal barriers, and a lack of resources and skills.

Governments need to take action to change the culture related to vulnerabilities, encourage the adoption of good practice and remove obstacles such as imperfect legal frameworks that create risk for security researchers.

This policy note summarises the main findings of OECD work in this area, available in OECD (2021a; 2021b).



To reduce security risk, developers should therefore look and test for vulnerabilities in their code, develop patches that fix them, and distribute these patches to other actors across the value chain towards end-users. Organisations should also monitor their information systems to ensure that patches are appropriately applied and to avoid product misconfigurations. These are complex, burdensome and expensive endeavours. They are also never-ending tasks because malicious actors continuously discover and exploit new vulnerabilities. Fortunately, security researchers can discover vulnerabilities and report them to organisations. Also known as "ethical hackers", these researchers are willing to

help reduce risk and facilitate the adoption of good practice, though there are many obstacles to leveraging their expertise. As recent OECD analysis has shown, public policies aimed at removing existing obstacles and encouraging vulnerability treatment have the potential to significantly reduce digital security risk for all (OECD, 2021a; 2021b).

Effectively addressing vulnerabilities is key to a successful digital transformation

Not all vulnerabilities are equal

Malicious actors exploit digital security vulnerabilities for a variety of reasons: to steal money, personal data, or trade and State secrets; to disrupt business operations; and/or to hold stakeholders such as firms, cities, and hospitals for ransom. OECD work has focused on how public policies can help address challenges raised by vulnerabilities in products' code (*code vulnerabilities*) and in how products are implemented in organisations' information systems (*system vulnerabilities*), leaving aside other types of vulnerabilities such as human weaknesses.

Code in software and in hardware (i.e. firmware) almost always contains vulnerabilities, which vary in severity and risk. *Code vulnerabilities* can be mitigated if producers develop patches and distribute them through security updates. *Zero-days* are code vulnerabilities for which no patch has yet been released. They attract a lot of media attention because it is very difficult for product users to detect and mitigate them. Incidents based on a zero-day are often high-profile, with examples including the 2010 Stuxnet attack that partially destroyed an Iranian nuclear enrichment facility and the 2016 attack against the United States Democratic National Committee.

Attackers do not often use zero-days, however, because they are difficult to discover, expensive to buy on black and grey markets (see below), and lose value after detection by defenders. Most attacks instead leverage *system vulnerabilities*, which include weaknesses in the ways system owners implement or configure products in information systems. Failure to implement the latest security updates is a major source of system vulnerabilities, together with misconfigurations. Successful attacks such as WannaCry and NotPetya, which caused multi-billion dollars damages globally, as well as incidents that affected Equifax (USD 1.4 billion in damages) or generated a blackout in Ukraine in 2016, were all based on system vulnerabilities. In a 2019 survey of information technology professionals, 60% of respondents said one or more breaches they faced occurred because a patch that was available for a known vulnerability was not applied.[1]

Treating code and system vulnerabilities is a key opportunity to reduce risk and increase trust

Vulnerabilities are a fact of digital life. They are a by-product of the increasing complexity of code and systems, combined with weak digital security practices among producers and users. It is not possible to completely eradicate vulnerabilities from all code and systems; but improving their treatment is a major opportunity to reduce digital security risk and increase trust in the digital transformation era.

Vulnerability treatment includes discovery, handling, management and public disclosure. Once vulnerabilities are identified (discovery), code owners need to fix them by developing and distributing patches or other mitigations (handling). It is then incumbent upon system owners to apply these patches (management). Lastly, vulnerabilities usually need to be disclosed publicly to enhance security knowledge and facilitate protection.

Treating vulnerabilities is therefore a shared responsibility amongst all vulnerability owners. These include:

- *Code owners*, i.e. developers of products that include code (goods, services, or hybrid products, commercialised or available for free, proprietary or open). In addition to making their code as robust as possible, they should ensure duty of care by discovering and handling vulnerabilities in their products after they are available to users.
- *System owners*, i.e. organisations that use products in information systems supporting their economic and social activities. They should manage vulnerabilities to protect their activities as well as any third parties that incidents could harm.

In the era of digital transformation, it is grossly irresponsible to develop code and maintain systems while ignoring the consequences of vulnerabilities that may emerge over time. Producers and system owners need to establish vulnerability handling and management processes to treat vulnerabilities systematically and proactively in order to decrease risk for themselves and others, as well as for society as a whole.

Significant economic and social challenges prevent stakeholders from treating vulnerabilities effectively

Treating vulnerabilities is as much an economic and social issue as it is a technical one

Challenges to treating vulnerabilities include a lack of awareness and co-operation amongst stakeholders, limited or opposite market incentives, legal barriers, and a lack of resources and skills. Treating vulnerabilities can be complex, especially when they are located in code developed by third parties or affect numerous products. This combination of cost, time and complexity can be overwhelming for small- and medium-sized enterprises, public sector bodies, and organisations with low digital maturity, such as traditional manufacturers entering consumer or industrial IoT markets. Furthermore, treating vulnerabilities is a race against the clock, as malicious actors are constantly striving to find and exploit existing and new vulnerabilities.

Vulnerability treatment is a sensitive risk-based process

To treat vulnerabilities responsibly, vulnerability owners have to assess the risk associated with each vulnerability they have knowledge of, in order to prioritise those on which to spend their efforts and resources.

Code owners have to decide which patch to develop in priority. This is difficult in part because the risk associated with a code vulnerability depends on the product's use context, which varies considerably across users and is unknown to the code owner.

Prioritising which patches to implement is also difficult for system owners because they have to understand the risk of applying each patch to their system. This risk can be significant. While silent and automatic patching is a reasonable objective for consumer products, it is less so for more complex information systems in organisations. Many organisations often need to test security updates prior to applying them, in order to assess whether the patch itself is going to disrupt business operations or introduce compatibility, performance or instability issues through domino effects. The 2020 SolarWinds supply chain attack, which affected United States government departments and private firms, showed that malicious actors can also distribute security threats through compromised security update mechanisms. According to surveys, it takes organisations an average of 102 days to test and fully deploy patches, ranging from 16 days to patch a critical vulnerability, to 151 days to patch a medium- or low-priority vulnerability.[2]

Security researchers are a significant but underappreciated resource

Security researchers are individuals or organisations who identify a potential code or system vulnerability with the intention to reduce security risk. The media often calls them "white hats" or "ethical hackers", though "hacker" is an ambiguous term with negative connotations. Researchers are driven by different goals and operate under different constraints. Many hunt for vulnerabilities as part of their professional activities in academia, digital security companies, product security teams, government agencies or civil society. Others search for vulnerabilities as a personal hobby in their spare time.

In practice, security researchers help vulnerability owners find and disclose vulnerabilities before malicious actors exploit them, yet many vulnerability owners do not welcome their vulnerability reports. In many cases, vulnerability owners do not feel responsible, can feel threatened by researchers' reports and/or are not sufficiently aware of good practice.

Security researchers can face significant legal threats as they attempt to help reduce security risk

Furthermore, in many countries, vulnerability owners can threaten researchers with legal proceedings instead of welcoming their vulnerability reports. Areas of legal risk for researchers include criminal law, intellectual property law, data protection law and contract law. This legal risk is aggravated when stakeholders are located across borders, and creates powerful disincentives and a chilling effect in the security community. Its significance depends on whether the legal framework in the vulnerability owner's jurisdiction has been designed to protect security researchers. The vulnerability owner's culture and level of awareness of good vulnerability treatment practice, as well as the researcher's behaviour when reporting a vulnerability, are also important factors.

Examples of researchers threatened of legal proceedings

In 2011, the Finnish online game platform Habbo (273 million users in 150 countries) brought criminal charges against a teenager who reported how he could log into the site's helpdesk system. Two years later, the courts ruled that there was no case to answer.

In 2013, academic researchers at Radboud University (Netherlands) informed a chip manufacturer about weaknesses in a chip widely used in immobilisers for various brands of cars. The same year, a British court, acting at the request of Volkswagen, ruled that the scientific article detailing the vulnerability had to be withdrawn. Two years later, Volkswagen ultimately agreed to the release of the publication.

In 2015, a security researcher reported a vulnerability to the producer of an e-voting application in Argentina that was going to be used for elections the following week. Three days before the elections, the police raided his apartment and seized his electronic equipment based on criminal charges presented by the company. The case was dismissed one year later on the grounds that he had not accessed the company's systems unlawfully or caused any harm.

In 2016, researchers received a cease-and-desist letter three days after reporting a serious vulnerability to the global consulting and auditing company PwC. Another researcher had his home raided and was arrested by the FBI after he reported that a dental software company left unencrypted sensitive health information of 22 000 patients at risk of access by others.

In 2017, a Danish citizen discovered a vulnerability in a municipality web site that enabled the harvesting of personal information of any citizen by entering their birth date in a form. He reported the vulnerability to the municipality. The service provider discreetly fixed the vulnerability and reported the researcher to the police.

In 2018, the FBI investigated a university student who had been reported by the mobile voting company Voatz for illegally attempting to hack its application. In 2020, Massachusetts Institute of Technology (MIT) researchers uncovered vulnerabilities in Voatz's e-voting system that could allow hackers to alter, stop, or expose how an individual user voted. The application had already been used in several local and state elections in the United States. The researchers reported their findings to the Cybersecurity and Infrastructure Security Agency (CISA). The company disputed the severity of the vulnerabilities, making aggressive public statements against the researchers. Ultimately, an independent audit requested by Voatz confirmed MIT's findings.

Sources: OECD (2021a), "Encouraging vulnerability treatment: Overview for policy makers", https://doi.org/10.1787/0e2615ba-en; OECD (2021b), "Encouraging vulnerability treatment: Background report – Responsible management, handling and disclosure of vulnerabilities".

Co-ordinated vulnerability disclosure is a key best practice that is insufficiently adopted

In a CVD process, vulnerability owners and researchers work co-operatively to discover vulnerabilities, develop, disseminate and apply patches that fix them, and disclose vulnerability information broadly without giving attackers a chronological advantage. However, CVD may be complex, particularly when co-ordination involves numerous stakeholders, such as cases where the vulnerability is located in a component disseminated across many products. Furthermore, each discovery of a vulnerability is unique, and CVD may be neither appropriate nor possible in some cases.

Stakeholders can use several tools to facilitate CVD and vulnerability treatment more generally:

- A **vulnerability disclosure policy** is a public statement whereby a vulnerability owner invites researchers to send vulnerability reports, giving them assurance that reports will be handled seriously, and reducing the risk of legal action if it is well designed by the vulnerability owner and complied with by the researcher.
- A **co-ordinator** can assist as a trusted third party in a variety of cases, from easing stakeholders' relationships to orchestrating complex multi-party co-ordination, or facilitating stakeholders' relationships across borders. For example, some computer emergency response teams (CERTs) and computer security incident response teams are also vulnerability co-ordinators. These include CERT/CC at Carnegie Mellon University, the Dutch National Cyber Security Centre (NCSC-NL), CISA at the United States Department of Homeland Security and the French National Agency for the Security of Information Systems.
- **Standards and best practice** provide parties with a shared understanding of processes and procedures for vulnerability management, handling and disclosure co-ordination.

- Under **bug bounty programmes**, vulnerability owners reward researchers for reporting vulnerabilities under certain predefined conditions. Several online platforms facilitate the organisation of such programmes by offering a marketplace for vulnerability owners and researchers.

Stakeholders often do not trust governments

In some cases, law enforcement, intelligence and national security agencies look for vulnerabilities to exploit for their own purposes. Policies often allow these agencies to discover vulnerabilities without reporting them to vulnerability owners, and to stockpile, weaponise and exploit them against public or private targets. These agencies can also buy vulnerabilities to carry out "offensive operations". In some cases, government may require developers to insert "backdoors" in their products, which are equivalent to intentional vulnerabilities. This practice is condemned by other stakeholders and some governments. A government's ambiguity with respect to vulnerability exploitation can diminish the effectiveness of policies to promote vulnerability treatment by undermining other stakeholders' trust in government efforts to reduce risk.

The grey market for code vulnerabilities can make offence more attractive than defence

Ideally, all code vulnerabilities discovered by non-legitimate actors would be reported to vulnerability owners, who would then develop a patch for all products' users to implement, thereby reducing risk. However, other actors are willing to buy critical code vulnerabilities at high prices, and with no intention of fixing them. These actors include criminals who buy vulnerabilities on the black market, but they also include government intelligence and defence agencies, as well as companies developing and selling tools based on the exploitation of vulnerabilities, such as tools purchased by police forces or intelligence agencies to access the content of mobile phones. Many experts agree that this grey market can distort prices, divert researchers from reporting to vulnerability owners, and make offence more financially rewarding than defence.

Policy makers can play a decisive role

Vulnerability treatment deserves more policy attention

So far, vulnerability treatment has not received enough policy attention. Although the acceleration of digital transformation brings tremendous benefits, it also relies dangerously on billions of potentially vulnerable IoT devices, and complex information systems cumulatively running hundreds of billions of lines of code. Even as criminals and other attackers seize every opportunity to cause harm, as seen during the COVID-19 pandemic, there have been limited policy efforts to encourage stakeholders to treat vulnerabilities more effectively.

Governments can take action in many areas

To encourage vulnerability treatment and reduce digital security risk, public policies can:

- **Change cultures and mind-sets** by breaking the "vulnerability taboo", and recognising that vulnerabilities are a "fact of digital life" that can be mitigated through the adoption of best practices. In many cases, organisations' business leaderships assume that their products and/or systems are "safe and secure", and they view vulnerabilities as a failure that will undermine their reputation and partners' trust. They need to understand that all products that contain code also contain vulnerabilities, and all information systems have a high likelihood of containing vulnerabilities related to misconfiguration or unpatched software, including firmware. In the digital era, leaders and decision makers need to:
  - abandon the idea of a perfectly secure digital environment
  - recognise that their products and information systems can be vulnerable
  - establish trust by demonstrating that they are responsible for monitoring vulnerabilities and swiftly addressing them through a continuous effort to treat vulnerabilities, i.e. discover, manage, handle and disclose them.
- **Mainstream good practice**. They can do so by:
  - *Leading by example*. Governments can adopt CVD as well as vulnerability handling and management within the government. For example, CISA in the United States issued a binding operational directive (BOD 20-01) requiring each federal agency to publish a vulnerability disclosure policy, and several governments have launched bug bounties (see Box below). They can also leverage public procurement to promote a cultural shift with respect to vulnerability treatment.

- *Including vulnerability treatment in regulation, standards and guidance*, or using it as indicators of compliance. This may include, for example, product regulation; regulation related to critical activities, such as the EU NIS Directive (currently being reviewed); certification schemes, such as those established by the EU Cybersecurity Act; government-supported standards (e.g. NIST Cybersecurity Framework 1.1, ETSI Technical Specification "Cyber Security for Consumer Internet of Things"); IoT regulation (e.g. draft UK regulation); and privacy regulation (e.g. EU General Data Protection Regulation and the US Health Insurance Portability and Accountability Act).
- *Providing tools and encouraging standards development and adoption*. All stakeholder groups can facilitate CVD adoption with template Vulnerability Disclosure Policies, quick start guides, and other best practice documents. The "early stage" US NTIA CVD template aimed at safety-critical industries and the NCSC-NL Guidelines on CVD provide examples of such initiatives. Recent OECD work provides a high-level overview of good practice for CVD based on current guidance (OECD, 2021a; 2021b).

- **Foster trust and remove obstacles**. They can do so by:
  - *Ensuring access to a trusted co-ordinator*, who can help connect stakeholders when needed and provide additional technical analysis and support. Co-ordinators need to have enough resources to accomplish their task, which may be demanding. It is not necessary for every country to have at least one domestic co-ordinator. For example, stakeholders can turn to a foreign, regional, international or industry-led trusted co-ordinator.
  - *Updating imperfect cybercrime and intellectual property frameworks to enable "safe harbours" protecting researchers*. Policy makers need to change the legal environment to better protect responsible security researchers and reduce the risk of lawsuits and criminal prosecution wherever it is an obstacle to CVD. Governments can take stock of legal risk for researchers in their jurisdiction, develop a plan to reduce it, and ensure that any new legislative or regulatory frameworks do not create new obstacles.
  - *Increasing stakeholders' trust in the government*, for example by separating offensive functions from digital security agencies and CERTs, and establishing transparent processes regarding how the government processes vulnerability information.
  - *Addressing the grey market for code vulnerabilities*. If legitimate actors need to buy vulnerabilities for lawful purposes, governments need to take action to ensure that such transactions do not distort prices, disincentivise researchers from reporting vulnerabilities, and prevent vulnerability owners from developing mitigations and protecting users. More research is needed to better understand the size and pricing mechanisms of the grey market and ways to reduce its negative impact on vulnerability disclosure, as well as the incentives and disincentives that could be leveraged to change actors' behaviours.
- **Encourage international co-operation**, such as the establishment of a non-governmental international co-ordinator, the internationalisation of vulnerability databases, the development of common principles to establish safe harbours for researchers, and the development of international standards and best practices.

In taking action, policy makers need to keep in mind that:

- **There is no one-size-fits-all solution to vulnerability disclosure**. It is a "wicked problem" without a panacea. It requires an open mind, flexible solutions and case-by-case consideration, often on the basis of international standards and guidelines;
- **Governments should use mandatory regulation with caution**. For example, mandatory reporting of vulnerabilities to the government is particularly challenging, and many experts suggest adopting a voluntary approach based on mutual trust.

What is a bug bounty?

Bug bounties or bug bounty programmes (BBPs) are crowdsourcing initiatives undertaken by vulnerability owners to reward individuals for discovering and reporting vulnerabilities as part of a CVD process. In addition to helping find vulnerabilities, BBPs can motivate internal staff to consider security, and help maintain a high level of security awareness. They can also act as a recruitment tool, facilitating the identification of talent and helping researchers select companies in line with their expectations for a job. From a public policy perspective, they can contribute to draining the black market by providing an alternative option to researchers motivated by monetary gains, provided that they are established only under the authority of vulnerability owners, as opposed to grey market brokers.

Bug bounties are increasingly popular among many well-known firms, including large information and communications technology (ICT) industry players (e.g. Apple, Google, Microsoft), other digital and communications companies (e.g. Airbnb, Alibaba, AT&T, Deezer, Deutsche Telekom, Facebook, Nintendo, OVH, Samsung, Uber, Twitter) and traditional businesses (e.g. Audi, Fiat Chrysler, Ford, Goldman Sachs, Mastercard, Starbucks). Bug bounty platforms, meanwhile, have facilitated the organisation of BBPs.

Governments are launching BBPs, as well. For example, the United States Department of Defense invested USD 34 million in BBPs in 2018, following the success of its earlier "Hack the Pentagon" and "Hack the Army" initiatives. In Singapore, two agencies (GovTech and CSA) distributed a total of USD 26 000 rewards to 290 researchers in 3 BBPs targeting government systems in 2018-19. The Swiss government offered USD 150 000 for vulnerability reports in its Internet-based e-voting system in 2019, with rewards between USD 100 to 50 000. It also launched a bug bounty programme for its "SwissCovid Proximity Tracing System" in 2020. The French government launched a BBP focusing on its Tchap instant messaging application for civil servants, with bounties from EUR 50 to EUR 1 500. The Korean Ministry of Science and ICT and the Korean Information Security Agency (KISA) have established a BBP focusing on the web sites of volunteer private companies as well as KISA.

However, bug bounties are neither a panacea nor a turnkey security solution. They are suited for sufficiently resourced and mature organisations that already have a well-organised vulnerability management or handling process in place. Furthermore, a BBP is a reactive measure that, alone, is unlikely to improve the underlying design security limitations in a product or product line. BBPs should be used as one tool among many others to reduce risk, such as software code reviews, audits and network penetration tests.

Sources: OECD (2021a), "Encouraging vulnerability treatment: Overview for policy makers", https://doi.org/10.1787/0e2615ba-en; OECD (2021b), "Encouraging vulnerability treatment: Background report – Responsible management, handling and disclosure of vulnerabilities", https://one.oecd.org/document/DSTI/CDEP/SDE(2020)3/FINAL/en/pdf; www.bugcrowd.com/bug-bounty-list/.

Notes

1 Ponemon Institute (2019), *Costs and consequences of gaps in vulnerability response*, https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf.

2 Ponemon Institute, 2019, and Ponemon Institute (2018), *The 2018 State of Endpoint Security Risk*, https://cdn2.hubspot.net/hubfs/468115/whitepapers/state-of-endpoint-security-2018.pdf.

Further reading

OECD (2021a), "Encouraging vulnerability treatment: Overview for policy makers", *OECD Digital Economy Papers* No. 307, OECD Publishing, Paris, https://doi.org/10.1787/0e2615ba-en.

OECD (2021b), "Encouraging vulnerability treatment: Background report – Responsible management, handling and disclosure of vulnerabilities", OECD, Paris, https://one.oecd.org/document/DSTI/CDEP/SDE(2020)3/FINAL/en/pdf.

Website

https://oe.cd/security

Directorate for Science, Technology and Innovation Policy Note

This series of Policy Notes is designed to make available, to a wider readership, selected studies that have been prepared for use within the OECD.

Comment on this Policy Note is invited, and may be sent to OECD, 2 rue André Pascal, 75775 Paris Cedex 16, France, or by e-mail to digitalsecurity@oecd.org.

Please cite this note as:

OECD (2021), "Encouraging vulnerability treatment: How policy makers can help address digital security vulnerabilities", *Directorate for Science, Technology and Innovation Policy Note*, OECD, Paris, www.oecd.org/digital/encouraging-vulnerability-treatment.pdf.