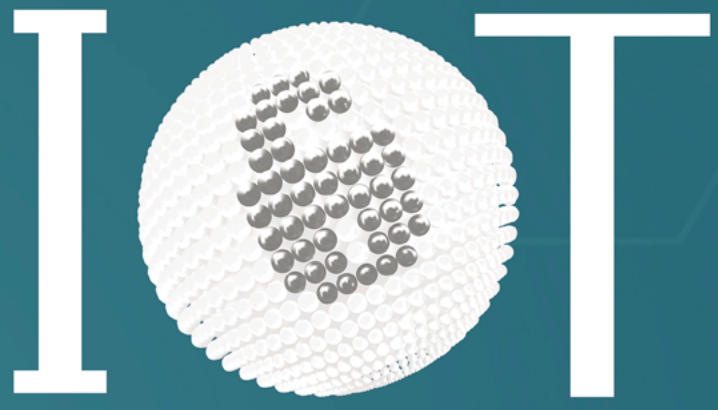
The Contemporary Use of Vulnerability Disclosure in IoT

Report 4: November 2021



IoT Security Foundation

TO PRINT CLICK HERE

next page

About the IoT Security Foundation

The IoT Security Foundation was established to respond to the myriad of challenges and concerns over security:

- It is a non-profit organisation dedicated to driving security excellence.
- It is a collaborative, vendor-neutral, international initiative aspiring to be the expert resource for sharing knowledge, best practice and advice.
- It is a member-driven, interactive resource led by an executive steering board.
- It has an on-going programme designed to propagate good security practice, increase adopter knowledge and raise user confidence.

Background

IoT's great potential: As technology costs have fallen, the benefits of the Internet of Things across sectors such as consumer, domestic, retail, manufacturing, energy, transport, health and public infrastructure have become increasingly attractive and realisable. The economic opportunity for those diverse connected systems is often estimated in trillions of dollars and employing billions of devices. With the advent of IPv6, the number of available individual addresses is a staggering 340 trillion, trillion, trillion. The trend is clear; systems are increasingly embedded, connected, scalable and growing in complexity.

Along with the opportunity comes the security challenge: with more and more devices becoming connected, the attack surface for adversaries is target-rich. What is considered secure today may not be tomorrow. A typical IoT system will rely on data and networks of variable provenance, devices may be expected to run on batteries for many years and new vulnerabilities are likely to be required to be patched in the field and at scale. Whilst we can learn lessons from the pc and mobile era's, IoT systems are breaking new ground and so are the security challenges.

IoT security is top concern for executives. Along with the technical challenges, IoT security is on the board room agenda. With more than just reputations at stake, it is imperative that technology providers, system adopters and users work together to ensure security is fit-for-purpose. It is fundamental to the adoption of systems and reaping the social and business benefits.

About this Report

This is the fourth research report in a series which began in 2018 to examine the adoption of vulnerability disclosure in Consumer IoT.

The report is commissioned by the IoT Security Foundation (IoTSF) and prepared by Copper Horse[1] - a UK based specialist in cyber security across several sectors including automotive, IoT and mobile.

The research was carried out in August 2021 and IoTSF is grateful to the research team – Rohan Panesar, James Tyrrell and David Rogers and the continued support of Copper Horse in helping raise awareness of this essential cyber security practice.

Our mission is to help secure the Internet of Things and make it safe to connect.

In doing so we aim to:

- Aid confident adoption of secure IoT solutions, enabling their technology benefits.
- Influence the direction and scope of any future necessary regulation.
- Influence IoT procurement requirements including by Governments.
- Increase capacity and the levels of security expertise throughout the IoT sector.
- Deliver business value to our members by building an eminent, diverse and international IoT security network.

1 https://www.copperhorse.co.uk/

Table of Contents

What is a Vulnerability Disclosure Policy and why Should you be Interested?

A Vulnerability Disclosure Policy (Policy) is a publicly available document, typically accessed via the Vendor's reporting web page. It is the Vendor's statement as to how they will handle any vulnerability report passed to them.[2]

Reporting a product security issue should be made simple so that a vendor can get to work on applying a fix as soon as possible. Coordinated vulnerability disclosure policies cover all stages of the process from advertising the correct point of contact, through to the timescale for fixing any issues and recognition for any bugs discovered.

To further assist organisations in navigating the requirements, the IoT Security Foundation (IoTSF) published a five-page Quick Guide[3] in 2020, which includes a list of dos and don'ts and highlights the roles and responsibilities of anyone who needs to be aware of coordinated vulnerability disclosure standards and regulation. More recently, the IoTSF updated its popular Vulnerability Disclosure Best Practice guide[4] to release 2.0. Due to advances in practice since it was first published, providing 21 pages of information written in simple language helping guide vendors to implementation.

Vulnerability disclosure, backed by a Vulnerability Disclosure Programme (VDP), benefits multiple parties - governments, businesses, security researchers and customers – so much so, that the process is well on its way to becoming a mandatory requirement at an international level.

Governments

For governments, Internet-connected (IoT) products deployed on commercial and domestic networks represent an attack point for bad actors to exploit. The need to secure and maintain security hygiene has therefore been of increasing concern as more connected products become available on the market and used in new contexts. For example, consider the rise in demand for home working, remote schooling and tele-medicine observed during the coronavirus pandemic. Under this scenario, domestic internet traffic carries much higher levels of sensitive data – while the trend for greater numbers of smart devices in our homes continues[5]. With ever-more human interaction, these IoT solutions can also create safety concerns if compromised.

Promoting the adoption of vulnerability disclosure practices by IoT vendors significantly helps to remove gaps in security that could otherwise be targeted by attackers.

Businesses

IoT product developers with a policy in place, gain an advantage and benefit from security vulnerabilities reported by customers or security researchers around the globe. Implementing a policy is straightforward thanks to standardisation[6], free-to-download best practice guidelines[7] and, more recently, tools and third-party service providers who can manage the administration, including the distribution of bug bounties (all elements described below).

Security Researchers

For security researchers, coordinated vulnerability disclosure provides a reliable point of contact and reassures the hacking community that the issues they discover will be taken seriously, as well as setting expectations on the timescales involved.

Customers and Users

Customers expect that the IoT devices they buy will be safe and remain so in use. Yet, due to the complexity of modern supply chains and systems, security flaws are likely to emerge for even the most reputable firms. The reassuring news for customers is that these issues are much more likely to be identified and fixed, if those firms have embraced vulnerability disclosure as part of their business operations and act on any issues reported to them.

2 https://www.iotsecurityfoundation.org/wp-content/uploads/2021/09/IoTSF-Vulnerability-Disclosure-Best-Practice-Guidelines-Release-2.0.pdf
3 https://www.iotsecurityfoundation.org/wp-content/uploads/2020/08/IoTSF-Vulnerability-QG_FINAL.pdf
4 https://www.iotsecurityfoundation.org/major-update-released-for-iotsfs-vulnerability-disclosure-best-practice-guide/
5 https://www.aviva.co.uk/aviva-edit/in-the-news-articles/families-more-connected-than-ever/
6 https://www.iso.org/standard/72311.html
7 https://www.iotsecurityfoundation.org/consumer-iot/

Methodology

This research report updates our analysis published in November 2020[8], which has evolved during the series as follows:

- **2018:** Makers of 330 popular consumer IoT products across a range of categories, all readily available in retail channels, were surveyed via the web to determine the current state of vulnerability disclosure in the sector. The data set included companies of different sizes and maturity – from start-ups to global brands, located all around the world.

- **2019:** Covers the same data set as 2018. The original websites surveyed in 2018 were revisited to determine how the reporting landscape had developed one year on. New features of the analysis included the usage by companies of certain elements of disclosure, such as a /security page or a redirect to their actual security page, and companies with a security.txt file located at <domain>/.well-known/security.txt.

- **2020:** 50 new products were added to the data set. These were chosen to i) reflect developments in the market and ii) build out a harmonised set of categories such as health fitness and wellbeing, laptop PCs, tablets, wearables, Wi-Fi and networking. 38 companies first surveyed in 2018 are either no longer operating or no longer provide the product via the link (or as a redirect) listed in the study.

- **2021:** A new category has been added to gauge the state of vulnerability disclosure across providers of business-to business (B2B) IoT products in addition to consumer (B2C) categories. We are interested to get an indication of comparative differences between enterprise and consumer offerings and this supplementary list features an additional 49 companies. A further 21 companies in the main data set have become inactive or no longer supply the IoT product listed in the previous study.

8 https://www.iotsecurityfoundation.org/wp-content/uploads/2020/11/Vulnerability-Disclosure-2021.pdf

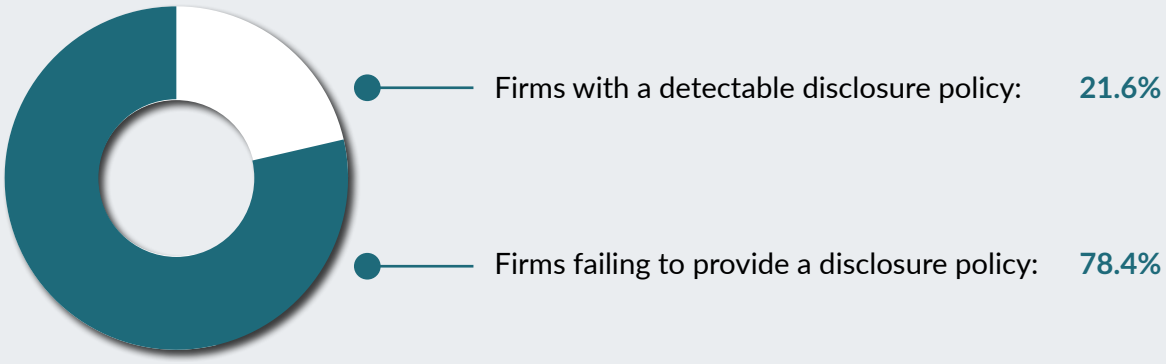
Key Findings

Our research shows that the uptake of the vulnerability disclosure amongst our study cohort remains low and should be of significant concern for regulators, consumers, and business users alike.

Unacceptably Low

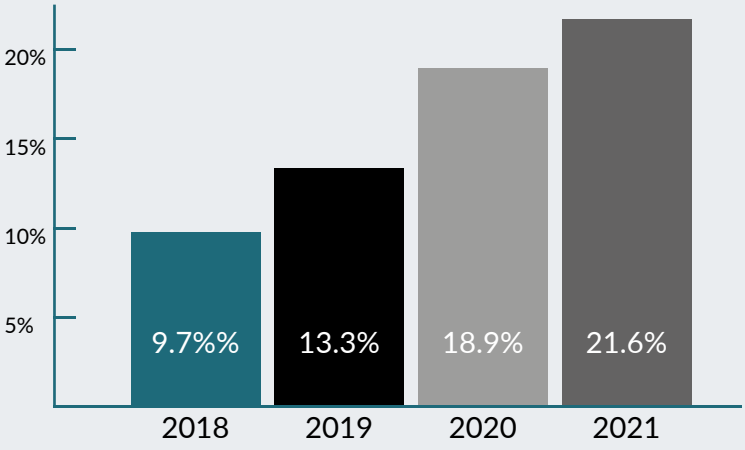
The results reveal that only 21.6% (68 of 315) firms surveyed have a readily detectable policy in place. This means that almost 4 out of 5 companies are still failing to provide the very basic security hygiene mechanism to allow security vulnerabilities to be reported to vendors so they can be fixed. This is unacceptably low.

Majority of firms are failing simple vulnerability reporting



This figure compares with 9.7% in 2018, 13.3% in 2019 and 18.9%[9] in 2020 - which was artificially boosted by the addition of laptop, PC and tablet categories that had relatively high levels of vulnerability disclosure policy adoption.

Vulnerability Disclosure in Practice Trend



The trend, whilst progressive, is glacial. Our common goal is to have 100% of connected-product (IoT) vendors practicing good security hygiene – achieving a mere 21.6% in the age of digital transformation simply supports the call for market regulation. Especially when the figure may flatter to deceive.

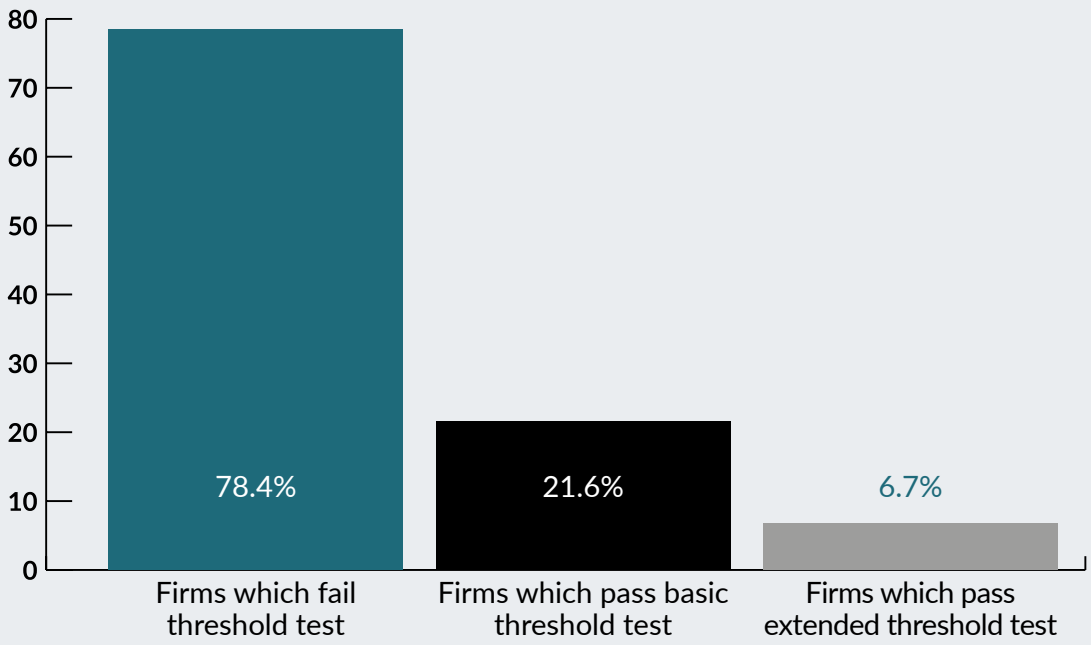
9 Note that figures included new product types from the original data set. This figure was 16.3% based on prior years product categories.

Yet Artificially High?

In our last report we noted that only 4 of firms we surveyed would likely meet regulatory requirements – we applaud those few companies of course – they are demonstrating trustworthy market behaviours.

This survey found that this number has improved as we identified 21 companies that now meet our simple, extended threshold test (see below). This equates to a meagre 6.7% that would likely meet expected regulatory requirements.

Few firms will meet anticipated regulatory requirements



What Else?

In the 2021 survey, there was a modest increase - a net gain of 3 - in the number of IoT providers surveyed with vulnerability disclosure information, yet also noting that some providers with policies dropped off the list as their products were no longer available.

In some cases, matters appear to have gone into reverse with companies who had previously implemented some form of vulnerability disclosure, either no longer advertising those details on their websites or having failed to renew their proxy service. Examples of this include Tile, whose HackerOne page appeared to no longer be active, and Dyson, which was counted as having a policy in our 2020 analysis.

Research Analysis and Developments

Regulating IoT Security

More and more countries are emphasizing the importance of vulnerability disclosure, with the US, France[10], Singapore[11], India[12] Australia[13] and the UK all reaffirming guidance for IoT providers. The EU Council Conclusions on the cybersecurity of connected devices in December 2020 specifically noted the IoT security standard ETSI EN 303 645 which contains requirements for vulnerability disclosure, as an important step in developing standards to support the EU Cybersecurity Act.

The passing of the USA Internet of Things Cybersecurity Improvement Act of 2020[14] is also a notable development since the publication of our previous report. Significantly, the act prohibits US federal agencies '*from procuring, obtaining, renewing a contract to procure or obtain, or using an IoT device*' that prevents compliance with NIST recommendations. Currently in draft, these recommendations[15] include the following -

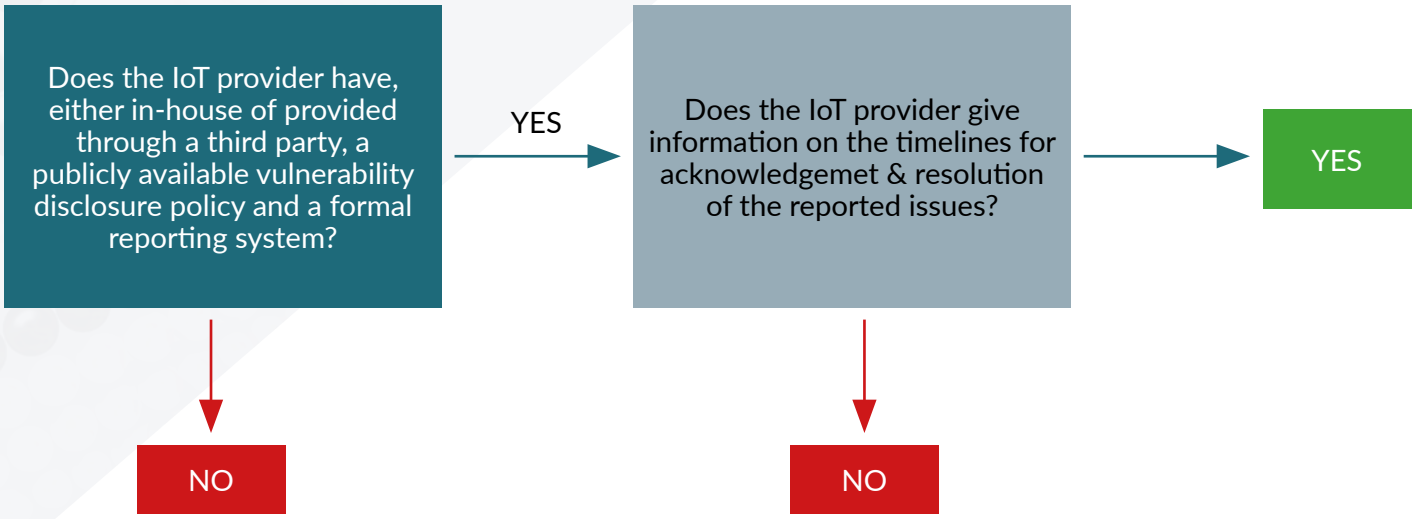
'The ability for the manufacturer and/or supporting entity to receive maintenance and vulnerability information (e.g., bug reporting capabilities, bug bounty programs) from their customers and other types of entities'.

This effectively compels IoT providers to have a vulnerability disclosure policy in place if they choose to work with US federal agencies. Given that companies will be keen to win contracts, it's anticipated that the Act could have a wide-reaching impact[16].

Legislation, drawn from the UK Government's Code of Practice for consumer IoT security[17] and key provisions from ETSI European Standard (EN) 303 645[18], mandating that IoT providers selling into the UK market must have a vulnerable disclosure policy in place is imminent. What's more, compliance will (in line with ETSI and ISO/IEC 29147:2018 vulnerability disclosure[19]) entail providing -

1. Contact information for the reporting of issues.
2. A timeline for acknowledging receipt of the information provided by the security researcher together with status updates until the reported issue has been resolved.

In our 2020 report, we introduced this concept as a threshold test explained in the following diagram.



Of the 338 entries in the 2020 data, a staggering 274 would fail at the first hurdle. And of the 64 that meet basic threshold criteria, just 4 pass the second test.

10 https://www.ssi.gouv.fr/uploads/2021/09/anssi-guide-securite_des_systemes_objets_connectes_iot-v1.0.pdf
11 https://www.csa.gov.sg/Programmes/cybersecurity-labelling/about-cls
12 https://tec.gov.in/pdf/M2M/Securing%20Consumer%20IoT%20_Code%20of%20pratice.pdf
13 https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf
14 https://www.congress.gov/bill/116th-congress/house-bill/1668/text
15 https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8259B.pdf
16 https://www.gibsondunn.com/new-federal-law-for-iot-cybersecurity-requires-the-development-of-standards-and-guidelines-throughout-2021/
17 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf
18 https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
19 https://www.iso.org/standard/72311.html

Applying the threshold test to our data set in 2021, we found that 78.4% (247/315) of companies fall at the first hurdle (the basic threshold) simply because they have no advertised vulnerability disclosure policy.

Yet, while 21.6% (68/315) satisfy the basic threshold, only a mere 6.7% (21/315) go further by providing timeline information (extended threshold). This figure is up from 1.2% (4/338) on last year's analysis, however concern remains as the current situation is no cause for celebration – especially as it is worth remembering that the extended threshold is highly likely to be a requirement for many regulations in development.

The 21 companies meeting the extended threshold test are:

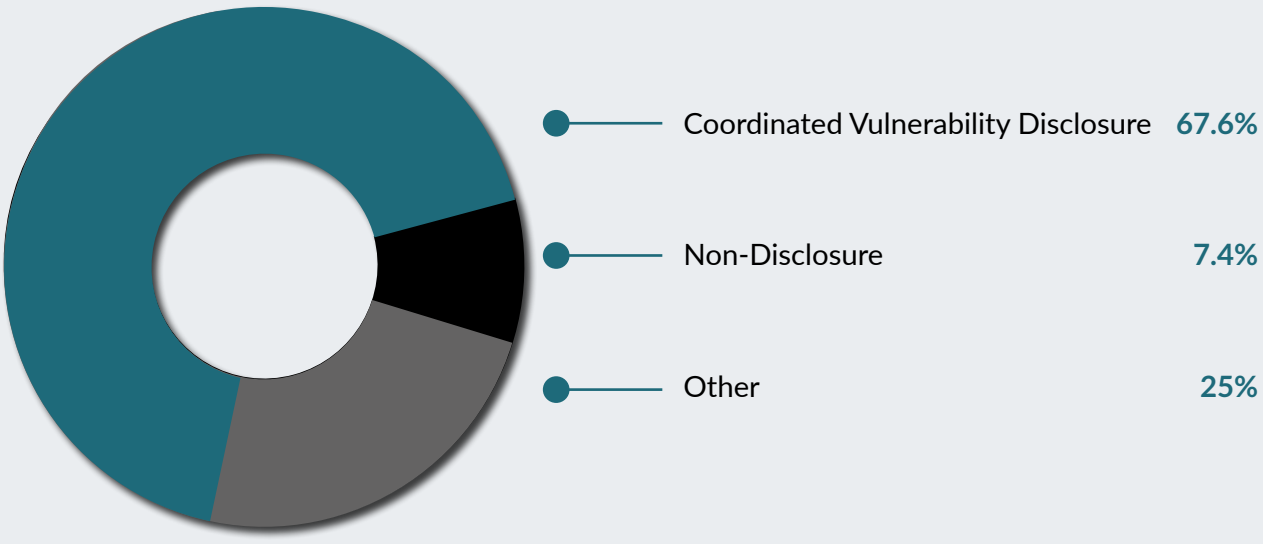
1. Bosch
2. BT
3. Canon
4. Ecobee
5. Google
6. LG
7. Microsoft
8. Motorola Mobility
9. Oculus
10. Panasonic
11. Philips
12. Siemens
13. Signify – Philips Lighting
14. SimpliSafe
15. SonicWall
16. Sonoff
17. Tom Tom
18. TP-Link
19. Western Digital
20. Wink
21. Xiaomi

Where companies have employed proxy disclosure (results provided later in the report) these services often show statistics based on the reports received that will help researchers to determine how responsive an IoT provider is likely to be. However, this is no substitute for a formal timeline commitment included as part of a vulnerability disclosure policy.

Types of Vulnerability Disclosure Policy

Many firms in the survey with a vulnerability disclosure policy appear to follow Coordinated Vulnerability Disclosure (CVD) – communicating with, and keeping the security researchers in the loop, and allowing the findings to be made public (for example, at a conference) once a fix has been applied. This last step – disclosing the vulnerability - is considered important as it allows security researchers to receive recognition for their efforts and can play an important role in furthering their careers, whilst protecting the public from malicious exploitation of the vulnerability.

Disclosure Type Usage

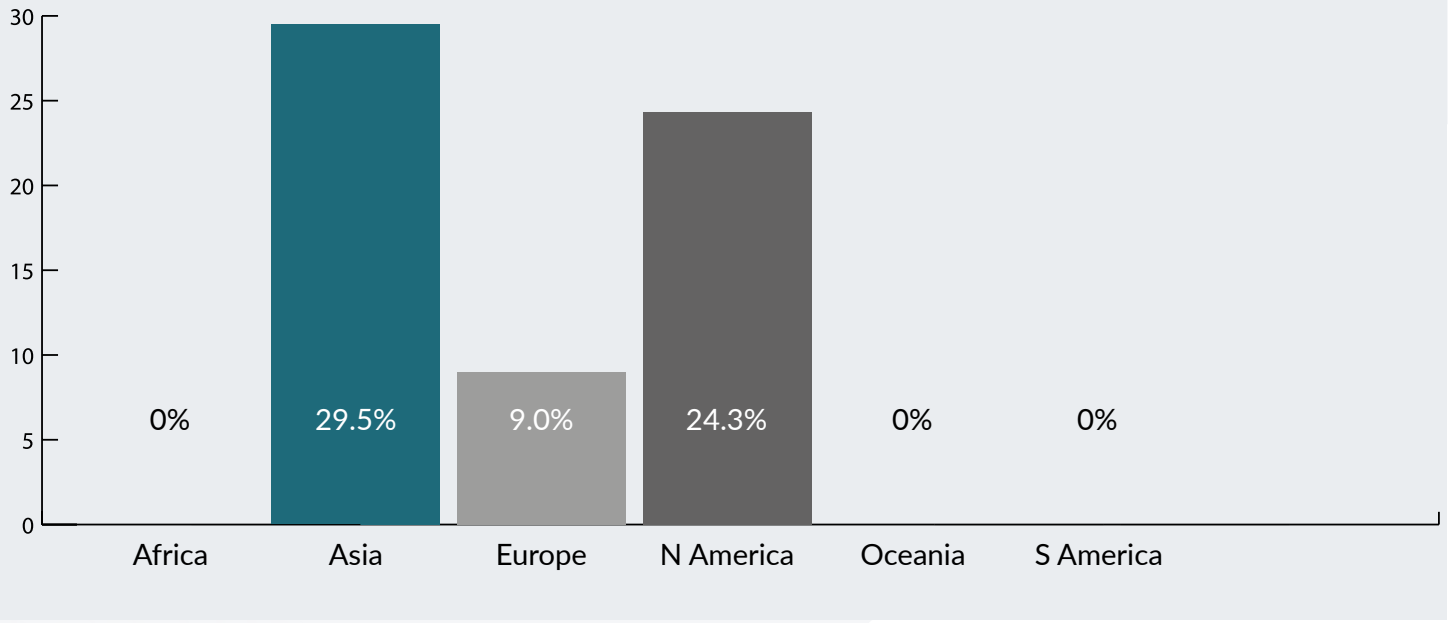


However, despite the benefits and positive publicity, some 7.4% of the companies with a public policy (5/68) elect to keep their own security efforts and those of the security researcher reporting the vulnerability, out of the public eye by insisting on 'non-disclosure'. When managed correctly, public disclosure is generally seen as good practice and private handling – whilst acceptable – misses the opportunity to build market awareness and trust.

Regional Differences

Based on a firm's headquarters location, 24.3% (35/144) of North American firms in this year's survey offered a vulnerability disclosure policy. This compares with 29.5% (26/88) of Asian companies and 9.0% (7/78) of European IoT providers.

Disclosure Practice by Region



Overall, the result is broadly similar to the 2020 findings with Asia out in front and Europe lagging – although, it will be interesting to see whether the imminent introduction of legislation will change this picture in 2022.

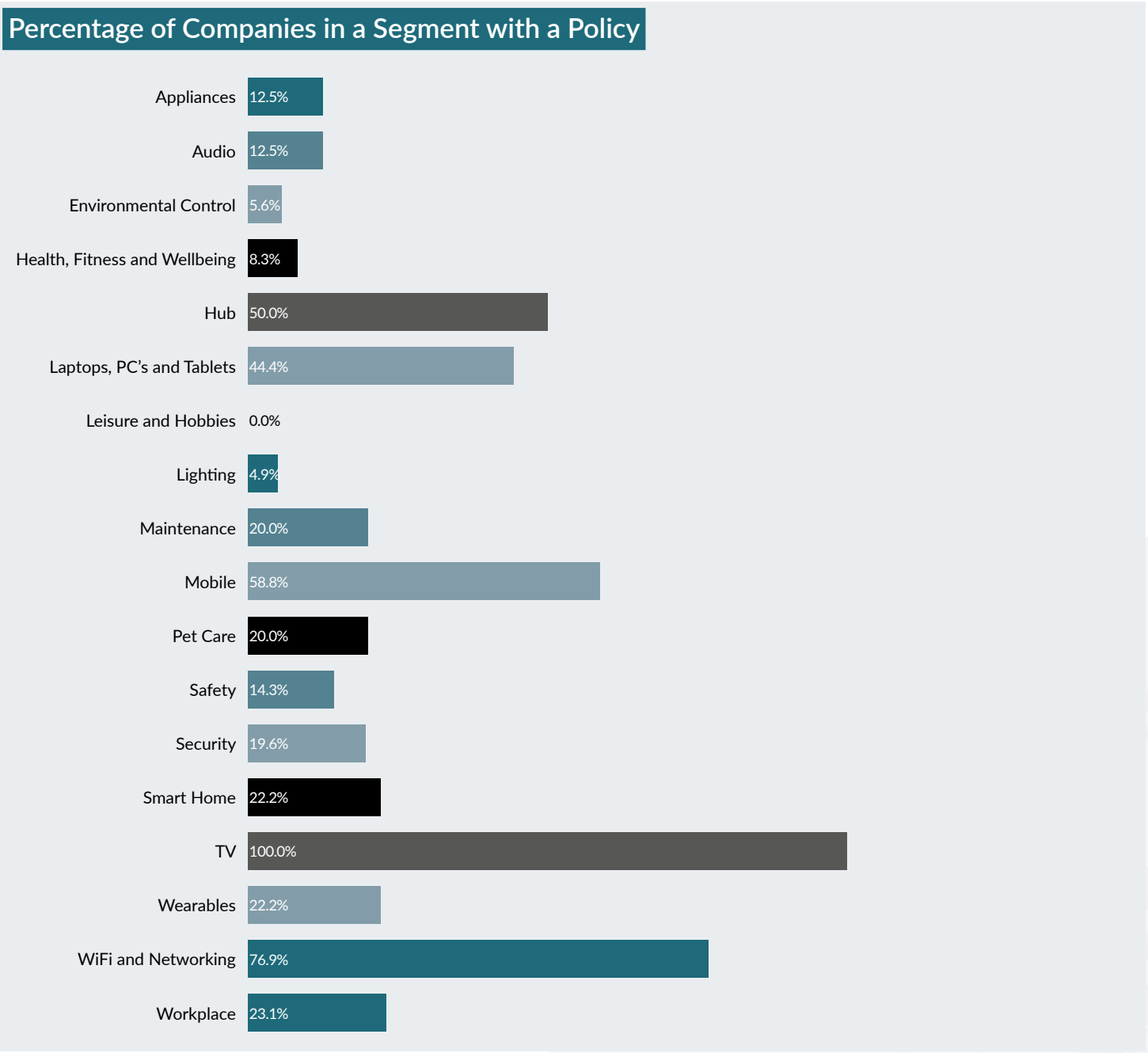
Performance Across Product Categories

Throughout the lifespan of this report, we have observed that companies which tend to have effective CVD programmes are often large, well established tech companies. Outside of this group, however, the policy coverage is much less extensive. The number of connected devices is exploding, and they are prevalent in almost every sector. When adding categories such as wearables, we saw companies that traditionally are not tech-focused, like fashion companies producing smart watches (e.g., Fossil and Armani), are suddenly confronted with all the security expectations and challenges of releasing an IoT product.

Much like in 2020, the sectors that fare better in terms of vulnerability disclosure are TV, Wi-Fi and Networking, Mobile, Hub and Laptops, PCs and Tablets. These are all categories that feature large, well known tech firms such as Sony, Panasonic, Samsung, LG, Google, Microsoft, Dell, Lenovo, Amazon, Logitech, Apple and other global brands.

Categories such as Lighting, Security, Smart Home and Wearables – which include a much more diverse range of companies – continue to perform poorly in providing policy details. Similarly, we also find low levels of adoption in sectors such as Pet Care, Maintenance, Safety, Leisure and Hobbies - which, in these cases, could suggest that the message is not reaching firms on the fringes of IT.

Interestingly, the Workplace category also shows low levels of accessible vulnerability disclosure policy information. Products here included printers and relatively new devices to the market such as smart pens. And while some security details were available, they often described how the IoT provider would notify the customer of any issues rather than addressing communication in the other direction.



Proxy Disclosure and Bug Bounties

This year, 5.1% (16/315) of companies surveyed (or 23.5% of the firms with a policy) formally employed the services of a third party to manage a vulnerability disclosure program on their behalf.

And while this proportion is down on 2020 (5.9%, 20/338), the concept remains an area to watch. Once regulations bite, the number of IoT clients of these companies could rise. Over the past 12 months, proxy services have been active in highlighting that the legislative wheels are turning[20] and positioning themselves as an aid to compliance.

Of the firms using proxy disclosure, the majority opted for either HackerOne or Bugcrowd, with one instance of ZeroCopter. There are other providers too, beyond those encountered in our data set, such as Intigriti. Typically, these firms provide their clients with a dedicated platform for vulnerability disclosure including triage capabilities for assessing and prioritising reports to simplify the administration handling.

While this report focuses on consumer IoT, it's worth adding that a wide range of sectors are engaging with proxy disclosure providers. Categories mentioned in HackerOne's annual security report[21] include travel & hospitality, healthcare, media & entertainment, and government in addition to the more traditional computer software and hardware.

30.9% (21/68) of IoT providers surveyed who had a vulnerability disclosure policy offered a bug bounty, either directly or via a third party, as part of their proxy disclosure agreement.

20 https://www.hackerone.com/vulnerability-management/us-government-mandates-vulnerability-disclosure-iot
21 https://www.hackerone.com/resources/reporting/the-4th-hacker-powered-security-report

The proportion is consistent with last year's figures and reflects that companies incentivise the work of security researchers in different ways – for example, through 'hall of fame' lists or acknowledgement pages and other written statements of thanks.

Financial rewards may not be universal, but there are signs that bug bounties are working for some firms – with some entries in our data set choosing to expand and upgrade their programs in 2021 (see Talking Points section).

Lists of top bug bounty programs can be found online, but sometimes these external pages can complicate the reporting of vulnerabilities where links are out of date or program details have changed. On the positive side, such hurdles emphasise the need for standard locations for discovering policy details.

Use of /security

Providing a standard location on a company website for publishing vulnerability disclosure policy information sounds like a straightforward and useful feature that all firms should be able to apply. In the research, we looked at each product website to see if the domain had an easy to access security page, under */security*. We found that use of the */security* convention continues to remain low with just 5.4% (17/315) companies choosing to adopt it – a similar number compared with 2020.

Use of Security.txt

Security.txt[22] – a text file placed under the */.well-known/* path on a company's web-server – is an efficient mechanism for directing security researchers to policy details so that they can disclose security vulnerabilities swiftly and securely.

An example from https://www.bosch.com/.well-known/security.txt is shown below.

```
Contact: https://psirt.bosch.com/report-a-vulnerability/

Encryption: https://psirt.bosch.com/media/pgp/psirt-at-bosch-dot-com.asc

Encryption: https://certsrv.bosch.com/

Acknowledgments: https://psirt.bosch.com/hall-of-fame/

Preferred-Languages: en, de

Policy: https://psirt.bosch.com/bosch-responsible-disclosure-policy/
```

Despite guidance[23] from the UK's National Cyber Security Centre describing a security.txt[24] file as '*one of the most important elements of vulnerability disclosure*', only 2.9% (9/315) of firms in this survey provided such details. Last year, the number was 7.

22 https://securitytxt.org/
23 https://www.ncsc.gov.uk/files/NCSC_Vulnerability_Toolkit.pdf
24 https://datatracker.ietf.org/doc/html/draft-foudil-securitytxt-12

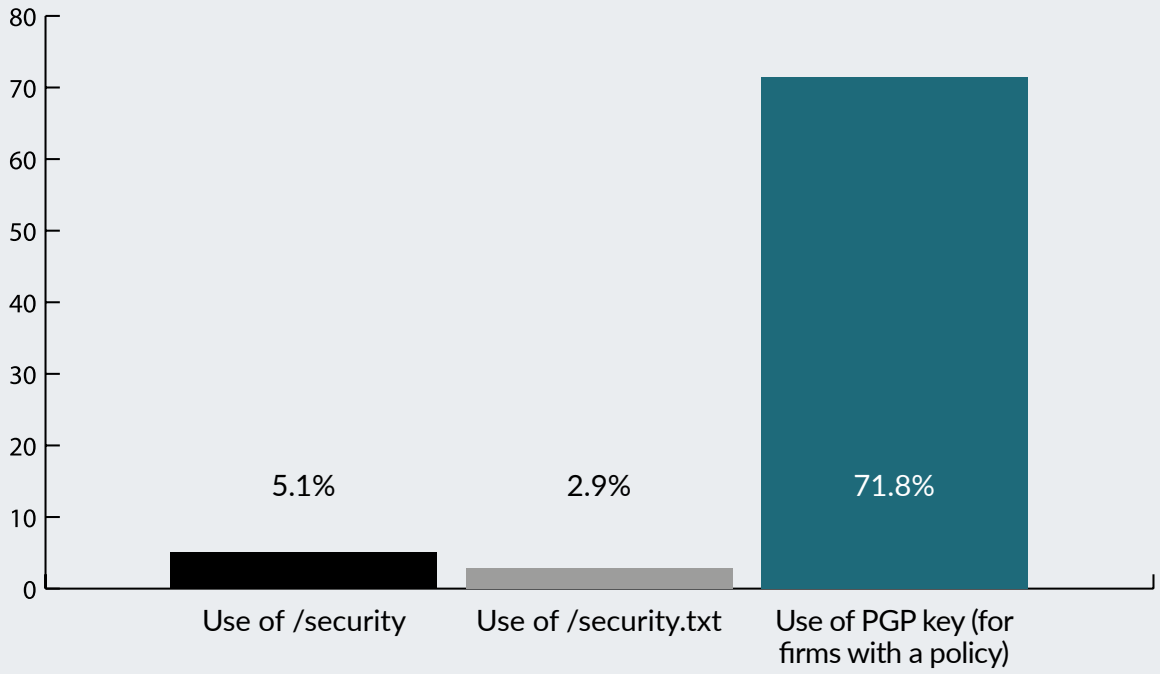
The feature, proposed in 2018, allows organisations to describe their vulnerability disclosure practices in a machine-parsable format so that the information can be found quickly by security researchers. However, the ease in which this information discovery can be automated carries a downside. There is some evidence[25] that security.txt files are being misused to tout for security work, or to deposit generic security reports that consist of nothing more than canned results created at the touch of a button (so-called 'drive-by reporting'). Dealing with these activities adds to the burden on security teams and could dent the appeal of the initiative if they become widespread.

As with bug bounty programs, the challenge is being able to separate reports of genuine security problems from a stream of low-value information, including spam, false positives and out-of-scope issues, which can soon overwhelm in-house resources[26]. Furthermore, depending on the mechanisms that are applied, there can be a fine line between reducing the numbers of invalid submissions and deterring useful participation in security programs.

Confidential Reporting: PGP Key

Of the firms that offered a formal reporting system, the majority – 71.8% (51/71) - provided a PGP key to encrypt the communication of vulnerability details. This continues to rise as in prior years – last year the number was 45.

Disclosure Methods



Companies no Longer Operating

As in our 2020 survey, we noted that several companies (21 in 2021 and 38 in 2020) are either no longer operating or no longer provide the product via the link (or a redirect) listed in the study.

In many cases, it's unclear why firms in our list have gone out of business, but one IoT camera provider no longer operating in the 'smart home, security' category has pointed to the current economic conditions as an explanation for their departure. It is certainly true that in many countries burglary rates have dropped during the global pandemic as people spend a greater proportion of time at home - a trend that could negatively affect the market for remote home security solutions, at least until travel and office life resumes.

There are signs that some firms have chosen to pivot out of the IoT sector – for example, one company has moved away from listing smart hubs on its Amazon page and now provides balloons and party supplies, which for customers looking for tech support may not be cause for celebration. Also, among the companies lost this year were some manufacturers making the more novel IoT products; devices that were traditionally "dumb", given a connection to the internet to expand their functionality (and price). This year we saw companies that sold a set of smart body scales, WI-FI slow cooker, smart pet feeder & pet bowl, and a connected kettle, no longer operating or making those products.

25 https://news.ycombinator.com/item?id=19151213
26 https://www.aronlaszka.com/papers/laszka2016banishing.pdf

Business to Business (B2B)

As mentioned in the methodology, this year we have included a supplementary list of 49 B2B IoT providers in our target data. These are companies that are primarily selling business products, rather than targeting the consumer (B2C) market, different to our 'workplace' category. The list was collated by the research team from various sources to give an indicative market representation, whilst not being exhaustive, does represent a sample of the activity that allows us to examine how the vulnerability disclosure practices of firms selling products to companies compares with the business to consumer market.

Of the companies in the B2B list, 71.4% (35/49) have some form of vulnerability disclosure policy – this compares with just 21.6% (68/ 315) of IoT providers in the B2C list (see Talking Points section for a discussion on potential reasons for this large difference in policy adoption). Curiously, B2B IoT providers with a policy appear to have less of an appetite for features such as PGP keys, /security pages, bug bounties and security.txt information, in comparison with the B2C sector. Also, we should note that the Workplace category in our main data set (which includes companies supplying products to both consumers and businesses, including oddities such as smart pens) suggests that work is still to be done on making vulnerability disclosure policies more widespread.

Of the 35 companies in the B2B list with a policy, we found 6 occasions (17.1%) where the text referred to the ISO 29147 vulnerability disclosure standard either directly on the page or, in one case, in the site's metadata.

Talking Points

Overall Trend and International Responses

While the number of IoT providers offering a public channel for vulnerability disclosure continues to increase, the proportion remains low – just over 1 in 5 companies surveyed. And this is in an environment where IoT related best practice has been freely available for anyone with an internet connection since 2017.

In April 2021, the UK Government noted[27] that the practice of vulnerability disclosure '*remains uncommon for manufacturers of consumer connected products*' whilst noting that it '*is an essential mechanism to identify and address security shortcomings, and to aid security innovation in the sector.*'

To protect consumers from insecure connected products, regulation will be applied with penalties for IoT providers who fail to comply. This includes the creation of an enforcement authority, whose role will be to '*investigate non-compliance, take action in relation to any non-compliance, and provide support to relevant economic actors to enable them to comply with their obligations.*'

It's not just the UK that's acting – noting the power of vulnerability disclosure to raise the security baseline. In the US, in addition to the 2020 IoT Cybersecurity Improvement Act mentioned above, it became a requirement under CISA Binding Operational Directive 20-01[28] that all federal civilian executive branch agencies publish a vulnerability disclose policy by March 2021 (six months from when the directive was passed). At the time of writing, there are more than 70 entities that have complied[29].

Possessing a vulnerability disclosure policy is also mandatory for participants in Singapore's Cybersecurity Labelling System[30], which in the beginning applied only to Wi-Fi routers and smart home hubs, but now includes all categories of IoT devices.

Hopefully, regulatory actions such as those in the UK and elsewhere will be sufficient to accelerate the adoption of vulnerability disclosure more widely and persuade companies that have dropped existing policies to re-instate them. For IoT providers that remain unaware of the need for vulnerability disclosure, legislation could provide a timely education.

Knowledge Gaps

It's plausible that non-traditional IT businesses entering the IoT market for the first time – for example, a fashion brand launching a connected product or a white goods manufacturer adding smart features to its products – will not have been exposed to the concept of a vulnerability disclosure policy. However, as noted earlier, data from proxy disclosure providers shows that companies from a range of sectors, not just computer software and hardware, are making use of their services. Also, in 2021 numerous resources have been made available, many of which are highlighted in this report, to help firms with vulnerability reporting. The need and requirements appear to be spreading – but only gradually.

27 https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation
28 https://cyber.dhs.gov/bod/20-01/
29 https://github.com/cisagov/vdp-in-fceb
30 https://www.csa.gov.sg/Programmes/cybersecurity-labelling/about-cls

Bug Hunting is good for Business

Two of the companies that were highlighted for their strong vulnerability disclosure performance in our 2020 analysis – Google and Xiaomi – continue to march forwards. Rather than rest on their laurels, Google have created a bug hunting community site[31], whilst Xiaomi has expanded its rewards program (hosted via a proxy service) after first dipping their toe in the water in May 2020. The Xiaomi program[32] now includes a 'Special breakthrough contribution award' for submissions determined to be of critical severity, and a monthly leader board prize to acknowledge regular contributors. Both examples are positive steps for vulnerability disclosure and recognise that embracing the desire of security researchers to make products safer is good for business.

HackerOne provides a breakdown of the growth in bug bounty programs by region in its annual security report[33], which puts APAC ahead (with a 97% expansion year-on-year) over North America (72%), EMEA (41%) and Latin America (29%). The figures suggest that the number of companies (across all business sectors, not just IoT providers) participating in the provision of bug bounties is on the rise, at least through the HackerOne service.

Knowing is Not the Same as Doing

One of the strangest findings from our research was a company that had posted a detailed blog[34] acknowledging the benefits of vulnerability reporting (referencing our 2020 report), but had then failed to publish a policy on its own site. However, navigating away from the .uk to the .com version (discussed further below) and scrolling down to the bottom of the page did reveal a small 'Bug reporting' link that opened up a reporting window.

Sadly, we also found two cases where firms had removed their vulnerability disclosure information over the past 12 months. Possibly this had occurred as part of a website refresh, but clearly this behaviour – whether intentional or not – represents a backwards step in the security of IoT devices.

Local Domains, Departmental and Licensing Issues

As touched on above, we have noticed issues with some multinational companies where the .com site will carry a vulnerability disclosure policy, including details for bug reporting, but the local sites – for example, with .uk, .de, and .fr suffixes – do not replicate or re-direct to the necessary information. Conversely, there was also a case where a local site carried the bulk of the information, although in this case a redirect did appear to be in place for visitors to the main website.

Large corporations making a wide range of products across different business groups can also be a source of confusion when it comes to reporting security issues. In some cases, we found that certain product categories were missing vulnerability disclosure information – for example, where the firm operated across a number of divisions and had no obvious central policy.

On a related theme, as we have highlighted in previous reports, brand licensing can also lead to uncertainty as to the correct contact point for security researchers where the brand is simply a wrapper and has no other involvement with the product on sale. Ideally, licensing agreements should contain a provision that makes clear the responsibility for vulnerability disclosure. For example, HMD Global makes Nokia-branded mobile phones, but doesn't carry its own vulnerability disclosure policy details, or at least none that were straightforward to find.

Terms of Use Restrictions, Safe Harbor and VDP Databases

Several IoT providers continue to apply terms of use restrictions to their products which prohibit, or at least discourage, activities such as disassembly and tampering. It's not clear how firms would enforce these restrictions placed on owners and raises issues in terms of a user's 'right to repair'[35]. From a security perspective, such terms of use provide no protection from potential attackers and instead simply frustrate or create a 'chill effect' on the efforts of legitimate researchers who could face legal hurdles.

In 2018, proxy service BugCrowd launched the website disclose.io to provide security researchers with a safe harbor framework so that people acting in good faith can report vulnerabilities without fear of legal repercussions. For companies and organisations, the initiative provides boilerplate vulnerability disclosure policies and gives them a starting point for initiating safe harbor. It also features a searchable list[36] of all known vulnerability disclosure programs (generated by the disclose.io community), which as of August 2021 contained 2294 entries.

31 https://bughunters.google.com/about
32 https://hackerone.com/xiaomi/updates?type=team
33 https://www.hackerone.com/resources/reporting/the-4th-hacker-powered-security-report
34 https://www.adt.co.uk/blog/are-diy-security-systems-vulnerable-to-hackers
35 https://en.wikipedia.org/wiki/Electronics_right_to_repair
36 https://disclose.io/programs/

Pulling this and other reporting information together opens the door to a rating system for companies and organisations, as Casey John Ellis - founder of BugCrowd, discussed in his presentation[37] at the 2021 HackerCon event.

There are other resources too, aiming to fill the information gap. FireBounty.com[38] features a searchable list of 20117 vulnerability disclosure policies, gathered using a mix of web crawling and direct submissions.

Policy Generation Tools

Advocates for vulnerability disclosure want to make the setup process as easy as possible to encourage more companies and organisations to participate. This includes not just boilerplate text for copy and pasting (as mentioned above), but also making tools available that reduce the friction of creating and updating a policy.

Currently available as a Beta-version, the Disclose.io community has launched its 'Policymaker' tool[39] - described by its creators as a "one-stop-shop" vulnerability disclosure policy generator. The target audience includes anyone launching a program for the first time, looking to update their information, or wanting to add features to their policy.

Users are guided through the process, entering their details via a web-based form, and once completed the application provides -

- A full vulnerability disclosure program policy,
- A safe harbor clause,
- security.txt files, and
- DNS Security TXT records[40].

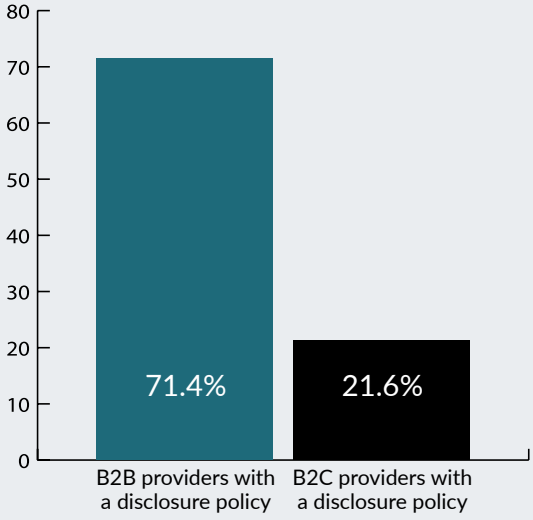
The generation of DNS Security txt records is a new initiative aimed at making security reporting information more accessible and more authoritative. It extends the security.txt standard (which has had its own tool[41] for some time) by placing the information in DNS zone files as a text record.

Gulf Between Consumer and Enterprise Adoption

As per our stated intentions, this year's survey has highlighted notable differences in the adoption of vulnerability disclosure policies between consumer and enterprise segments. Whilst we have not conducted a comprehensive survey of enterprise vendors, our simple survey provides an initial indicator. Based on our survey, the B2B sector appears to be more mature – at least in terms of the basics – compared with providers of IoT to consumers. As a reminder, 71.4% of B2B firms were found to have implemented some form of vulnerability disclosure compared with just 21.6% of B2C providers.

These results are not conclusive however, and we acknowledge more in-depth research needs to be done in this area to give the true picture.

Disclosure Policy Adoption Rates in Enterprise and Consumer



37 https://www.youtube.com/watch?v=HJPLUqRT_yU
38 https://firebounty.com/
39 https://policymaker.disclose.io/policymaker/introduction
40 https://dnssecuritytxt.org/
41 https://securitytxt.org/

Contributing factors to this gulf in adoption could include the size of the organisation, if we assume that bigger companies are more likely to have larger, and more established security teams, and the depth of their experience in the technology sector. However, if B2B IoT providers really do know better than their consumer cousins then we would ask: *why isn't the figure much closer to 100%?* That is, where it should be.

Winds of Change

While the outlook may seem broadly unchanged in our IoT survey, some members of the community are more optimistic.

Security researcher Jack Cable has described 2020 as the year that vulnerability disclosure went viral. In a recent presentation[42] he notes the CISA 20-01 Directive and points to a change of heart in some quarters such as from manufacturers of voting machines[43]. His observation is based on the number of companies and organisations (from all industries, not just IoT) listed on the disclose.io database, which increased from 880 at the start of 2020 to 2286 by the end of the same year.

Of course, not all these companies are IoT providers. But it does show an increase in security awareness that will influence other developers or product types. Questions remain, however as to when and how quickly this will occur. As illustrated in our on-going analysis in the IoT sector, we are still only seeing a gradual increase of adoption in the consumer space despite significant efforts across governments and global institutions.

Recommendations from IoTSF

We started this report by asking *"What is a coordinated vulnerability disclosure policy and why should you be Interested?"*. Below, we make some simple recommendations for each of the key stakeholder groups we identified.

Governments

Mandate vulnerability reporting as part of your regulatory framework. Many[44] are already adopting the top 3 requirements of the ETSI EN 303 645 standard when commencing regulatory activity for consumer IoT products.

Mandate CVD as part of your Governmental procurement policy for connected products and services and validate vendor security claims.

Businesses

As a technology, product or services provider uphold your duty of care towards your customers - create and maintain a VDP. You will find many free resources on the iotsf.org website and/or you might consider using a proxy service.

Endeavour to work within the spirit of vulnerability disclosure; build a respectful relationship with reporters – specifically, it is essential to set expectations for communications and adhere to them.

Security Researchers

Keep finding vulnerabilities and report them!

Please remember that patience can be a virtue, and, in some cases, you may find opportunity to help vendors who do not have a Policy by pointing them to this report and to the free guidance on the IoTSF website.

If the situation dictates, consider using a safe harbor service as mentioned in this report.

Customers and Users

Check whether a company has a Policy before purchase.

We advise you not-to-buy products from vendors that do not have a VDP or think very carefully before doing so – a golden rule in the discipline of risk management is to 'never accept risks you do not understand'.

42 https://www.youtube.com/watch?v=16UbH5umOAw
43 https://electionline.org/wp-content/uploads/2019/08/Coordinated-Vulnerability-Disclosure-Program-White-Paper.pdf
44 https://cetome.com/panorama

Conclusions

The case for making the adoption of a vulnerability disclosure policy a mandatory requirement for IoT providers is clear.

In 2018, we discovered that the level of detectable vulnerability disclosure practice was low in the IoT sector and strongly advised that adopting the processes of Coordinated Vulnerability Disclosure should be a priority.

A year later, little had changed, and we pointed out that stronger influence would be needed to motivate companies to adopt basic IoT security hygiene practices.

In 2020, we reiterated the need for worldwide providers of consumer IoT products to place 'implementing vulnerability disclosure policies' on their priority agenda – pointing to freely available best practice guidance.

And now, in 2021, there are new tools that make the process as simple as it has ever been – yet the proportion of firms advertising a policy on their websites remains low. The benefits of vulnerability disclosure are also clear and there for the taking. While the needle has moved a little, it is evident that it will take legislative, regulatory and enforcement steps – such as those that have come into force in the US and are imminent in the UK – to drive home the message and effect real change.

We therefore see the introduction of international baseline regulation in this space as a welcome development. It will help to protect users at the point of purchase and whilst products are used, it will also help to build trust in the marketplace.

The IoT Security Foundation continues its efforts to 'make it safe to connect' by 'helping to secure the IoT' across many applications – vulnerability disclosure practice is a common priority area, and we recommend that all firms lagging in this area move quickly and responsibly to improve their security posture.

Appendix A – Vulnerability Disclosure Policy Situation by Company

As per our threshold test described in the report, we separate out companies into:

- Green list: met the extended threshold test
- Amber list: met the basic threshold test but did not meet the extended threshold test
- Red list: did not meet the basic threshold test

Green List

1. Bosch
2. BT
3. Canon
4. Ecobee
5. Google
6. LG
7. Microsoft
8. Motorola Mobility
9. Oculus
10. Panasonic
11. Philips
12. Siemens
13. Signify - Philips Lighting
14. SimpliSafe
15. SonicWall
16. Sonoff
17. TomTom
18. TP-Link
19. Western Digital
20. Wink
21. Xiaomi (MI)

Amber List

1. Amazon
2. Apple
3. ARLO
4. ASUS
5. Belkin
6. Bose
7. Buffalo
8. Dahua
9. Dell
10. D-Link
11. Draytek
12. Eero
13. FitBit
14. Garmin
15. GE Appliances
16. Hanwha, Wisenet
17. Hikvision
18. Honeywell Home (Resideo)
19. Honeywell International
20. HP
21. HTC
22. Huawei
23. JBL
24. Lenovo
25. Lexmark
26. Lifx
27. Linksys
28. Logitech
29. Lovense
30. Netgear
31. OnePlus
32. OPPO
33. Peloton
34. PetCube
35. Procter & Gamble, Oral B
36. Roku
37. Samsung (Mobile)
38. Samsung (Smart TV)
39. Samsung (SmartThings)
40. Sonos
41. Sony
42. Tapplock
43. Vivo
44. WyzeCam
45. Yale
46. ZTE
47. ZyXEL

Red List

1. ACEMAX
2. Acer
3. ACTi
4. AdhereTech
5. ADT
6. Aeon Labs, Aeotec
7. Airboxlab
8. Airthings
9. AISIRER
10. Aiwa
11. AliveCor
12. Amaryllo
13. Amazfit (Huami)
14. Amor Gummiwaren GmbH
15. Aniken
16. Anker, Eufy
17. Anoto
18. Anova
19. ANTCOOL
20. Apollo Tech USA
21. Apption Labs
22. Aramatix
23. Armani (Armani Exchange, Emporio Armani)
24. Arris (Commscope)
25. ASAKUKI
26. Atom Labs
27. Audio Pro
28. August
29. Awair
30. AWOS
31. B&O
32. Bawoo
33. Beeline
34. Behmor
35. Best Buy, Insignia
36. Beurer
37. Bizfeat
38. BLU Products

39. BlueAir
40. BlueStork
41. Breathometer
42. Brother Industries, Ltd
43. Buddy
44. Canary
45. Candy
46. Canon, IRIS
47. Casio
48. Catapult Sports
49. Chamberlain
50. Circle
51. Clever Dog
52. Click and Grow
53. Curb
54. Current Labs
55. Deeper
56. Delta Five
57. DENON
58. Devialet
59. Devolo
60. DigitalKeys
61. Doogee
62. Double Robotics
63. Drayton
64. Drop
65. Dyson
66. Edimax
67. Elecom
68. Elgato, Eve
69. Eminent
70. Energenie
71. eq-3
72. Estimote
73. Etekcity
74. Expower
75. EXTSUD
76. EZVIZ
77. FIBARO
78. FireAngel
79. FirstBuild
80. FLiR
81. Flux Smart
82. Foscam
83. Fossil
84. FREDI
85. Furbo
86. Garadget
87. Gardena
88. Genetic International, Ultralink
89. GeniCan
90. Genius Hub
91. Greater Goods
92. GresatekEU
93. Guardian Technologies
94. Hangzhou XiongMai Technology
95. Hank
96. Hatch Baby
97. Hidrate
98. HMD Global (Nokia Mobile)
99. Hoover
100. Horsky
101. Hunterfan
102. Husqvarna
103. Icontrol Networks Canada
104. iFAVINE
105. IFITech
106. iHealth
107. iku
108. ilumi
109. Infinix
110. Innr
111. Insteon
112. Intelbras
113. InteraXon Inc
114. Invoxia
115. Iris Ohyama
116. Jasco
117. JingDong
118. June
119. Keen Home
120. KeySmart
121. Kobo
122. Kolibree, Baracoda
123. Koogeek
124. Kwikset
125. Lampaous, LUMENMAX
126. Laurastar
127. LEAGOO
128. Lenbrook Industries, Bluesound
129. Leotec
130. LetsFit
131. LifeFitness
132. Lightwave
133. Lithe
134. Lockstate, smartLOCK, RemoteLOCK
135. Logitech, Ultimate Ears
136. Lohas
137. Lorex
138. Loxone
139. Ludia
140. Lutron
141. Marshall
142. Mattel, Fisher-Price
143. Mellow
144. Meross
145. Michael Kors
146. MIPOW
147. Misfit
148. Moen
149. MoKo
150. Moleskine
151. MSI
152. MySpool
153. NAIM
154. NanoLeaf
155. Neato
156. Neo
157. Nespresso
158. Netatmo
159. Neurio, Generac
160. Nima
161. Nologie
162. NordicTrack
163. Novostella, Ustellar
164. Nuki
165. Omron
166. ONKYO
167. Osram
168. Otio
169. Perfect Company
170. PicoBrew
171. Polar
172. Proform (ICON fitness)
173. Quardio
174. Rachio
175. Ratoc Systems
176. Remotec
177. RENPHO
178. Reolink Digital Technology
179. Ring
180. Roberts Radio
181. Roost
182. Ruark
183. SAINKO

184. Samsung (Galaxy Watch)
185. Schlage
186. Seiko Epson
187. Seneye
188. Sengled
189. Sensoria
190. Shenzhen Neo
191. Skybell
192. Sleep Number
193. Small
194. Smanos
195. Smarter Applications
196. SmartHalo
197. SmartPlate
198. SmartyPans
199. Sphero
200. StoryLink
201. SUUNTO
202. Tado
203. Tanita
204. TCL Corporation (Alcatel)
205. Teckin
206. Tefal
207. Tend Insights
208. Theatro
209. TIBO
210. Tile
211. Tomshine
212. Tracking Point
213. TrackR
214. Trane
215. TrendingObjects
216. TRENDnet
217. Trust
218. TVT
219. TytoCare
220. UBTECH
221. Ustellar
222. Vankyo
223. Vaultek
224. Veho
225. Velco
226. Venturer (RCA)
227. Vivint
228. Vivitar
229. Voxx International, Klipsch
230. Wallfire
231. Wattcost
232. Wearable X
233. Weber
234. Weenect
235. We-Vibe
236. Whirlpool
237. Whistle
238. Winix America
239. Withings
240. XOLO
241. Xoopar
242. Xperi, DTS
243. X-Sense
244. Yamaha Pro Audio, Yamaha Corporation
245. Yeelight
246. Zeeq
247. Zmodo Technology

IoT Security Foundation

HOME