Security Foundation

The State of Vulnerability Disclosure Policy (VDP) Usage in Global Consumer IoT in 2023

A report prepared by Copper Horse Ltd
Published October 2023

Authors
Rohan Panesar, Mark Neve & David Rogers

Supported by
hackerone

Contents

Introduction

When the notion of this research was first conceived, we had a very clear objective in mind; we wanted to understand the status of IoT security in the marketplace. No one on the expert team would feel comfortable buying or using an IoT product that was sourced from a company that does not maintain its security. We therefore selected the presence (or absence) of a vulnerability disclosure policy as our litmus test.

Staying true to that original intent, this year's research parameters have been adjusted to track the movements in the marketplace and the developing regulatory landscape – an ongoing 'recalibration'. These adjustments have been made explicit in the report and direct comparisons preserved.

This year is especially notable as the much-anticipated legislation is now imminent with the UK's PSTI Act taking full force from April 2024 and several prominent others following in quick succession. What has caught my attention – specifically in relation to the UK legislation – are the requirements for non-manufacturers who are responsible for introducing products into the (UK) market; importers and distributors. This report has therefore paid special attention to some of the more prominent retailers (implied as a distributor – 'making the product available') in key regions as they need to take heed.

As always, 'the report' draws out important and interesting nuances to complement the key findings. I encourage the reader to contrast the findings (performance) between mature product categories and new products, the consumer and B2B markets and the effect of white-label goods. And of course, take a look at those companies that fail to meet the regulatory 'threshold test' as they will soon be in the sights of enforcement.

As the home of IoT security, IoTSF is here to help – wherever you are on your journey – I hope you find this report as useful as it is insightful.

John Moor, Managing Director, IoT Security Foundation

This report marks the sixth in a series of reports that has been following the adoption of vulnerability disclosure and associated practices, among manufacturers of popular internet connected devices. Since 2018 Copper Horse researchers have been studying popular IoT device manufacturers and tracking whether these companies have a point of contact for researchers to report security concerns. The process via which this is performed is internationally standardised and widely viewed as good practice. The process is called vulnerability disclosure and the adoption of a policy can be seen as a basic indicator of an organisation's security posture. Governments have become increasingly aware of the importance of vulnerability disclosure, particularly Coordinated Vulnerability Disclosure (CVD) and have endorsed and recommended it across the world. The UK's Product Security and Telecommunications Infrastructure (PSTI) Act, Part 1 of which focuses on consumer IoT product security, mandates the use of Coordinated Vulnerability Disclosure. The regulations come into effect on April 29th 2024. In the EU, the Cyber Resilience Act (CRA) is progressing into its final stages in the EU Parliament and various cyber security recommendations in the USA recommend or mandate CVD, with NIST having produced standards for policy usage.

The research in this year's report added 121 new popular device manufacturers, over 95% of which do not have a vulnerability disclosure policy. Overall, the percentage of this widened dataset with a policy has slightly decreased on the 2022 figure of 27.11% to 23.99% in 2023. This means that 76.01% of IoT manufacturers in the 2023 dataset do not have a way for security researchers to contact them. This is the first time in this report series a percentage decrease has been captured over the previous year's figure, however this should be considered a refinement and re-calibration of the global picture. The widening of the dataset captures more of the 'long tail' of IoT, which appears to be even less secure. The data is reviewed annually and companies are usually lost from the dataset; this year saw 7 companies no longer operating or stop selling IoT devices. By taking the dataset from 2022 in isolation, the pre-existing, continued trend can be observed, with the percentage of companies with a point of contact for security researchers increased to 31.08%.

> 76.01% of IoT manufacturers in the 2023 dataset do not have a way for security researchers to contact them.

The focus of regulators and governments in the next year will switch towards those retailers that choose to stock insecure products. In this year's report, the researchers have reviewed to what extent retailers are stocking popular products that have not adopted vulnerability disclosure policies.

What is vulnerability disclosure?

The concept of vulnerability disclosure grew out of the hacking community to eventually become standardised and adopted as good practice by many in the technology world, including governments. The European Union Agency for Cybersecurity (ENISA) defines vulnerability disclosure as "the process of identifying, reporting and patching weaknesses of software, hardware or services that can be exploited."[1] Not only is this process important to avoid or rectify potentially critical issues in a product, but a clearly defined vulnerability disclosure scheme for a manufacturer can be an indicator of a positive general security posture[2].

Implementing a vulnerability disclosure policy is easier than ever and there are free resources and tools to get an organisation started. Below is a table with resources to get an organisation started:

Organisation	Resource	Link
UK NCSC	Vulnerability Disclosure Toolkit	https://www.ncsc.gov.uk/files/NCSC-Vulnerability-disclosure-Toolkit-v2.pdf
Security.txt	Security.txt	https://securitytxt.org/
IoTSF	Vulnerability Disclosure Best Practice Guidelines	https://iotsecurityfoundation.org/wp-content/uploads/2021/09/IoTSF-Vulnerability-Disclosure-Best-Practice-Guidelines-Release-2.0.pdf
	Consumer IoT Security Quick Guide: Manage Vulnerability Reports	https://iotsecurityfoundation.org/wp-content/uploads/2020/08/IoTSF-Vulnerability-QG_FINAL.pdf
Dutch NCSC	Coordinated Vulnerability Disclosure: the Guideline	https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline

IoT resources available online

[1] https://www.enisa.europa.eu/topics/vulnerability-disclosure

[2] https://www.ncsc.gov.uk/files/NCSC-Vulnerability-disclosure-Toolkit-v2.pdf

Regions retailing IoT products

The first time this research was conducted, the researchers generated a list of global, major consumer retailers to gather IoT device manufacturers from. This year it was decided that the list would be reviewed in order to maintain a representative sample. To do this, the team ensured that retailers across all the regions outlined below were included to allow for regional comparisons; as legislation is progressing around the world it is becoming clearer that retailers will have some responsibility for selling compliant devices. The acronyms below are often used by global organisations to group continents and regions for business activities.

- EMEA – Europe, Middle East, and Africa
- NA – North America
- LATAM – Latin America
- APAC – Asia-Pacific

Turkey has been included in the EMEA region as it is geographically in Europe and Asia but is usually categorised as a part of the EMEA business region.

Methodology

2023 marks the sixth year of this research. In 2018, Copper Horse started examining the adoption of vulnerability disclosure among manufacturers of popular consumer IoT devices as a way to measure whether companies were adopting best practices on IoT security.

Vulnerability disclosure policies are one of the few public indicators that give this information – they're either on a company's website or they're not. These are what are considered 'insecurity canaries'. With each year that passes and with each annual review of the data, companies are removed from the research dataset. The main reasons for this are because companies cease operation or stop selling connected products. This year the dataset lost seven companies.

The terms manufacturer and vendor are generally used interchangeably in this report and it should be noted that all the retailers captured in this report have an online sales platform.

When the research was initially conducted, a list of global retailers used to gather manufacturers was built. The research team captured the most popular IoT devices by reviewing listings on the retailers in this list and usually sorting by the "best seller" metric. In this year's report the retailer list was expanded again in order to get a truer picture of the global consumer IoT landscape. It was split evenly across the EMEA, APAC, NA, and LATAM regions. Using this expanded global retailer list, the team has gathered 121 additional consumer IoT manufacturers selling products globally. While this represents a large increase to the overall dataset, the researchers felt comfortable expanding the research to a greater global reach, because they were using the same methodology used in the previous reports. To achieve an accurate, representative sample of popular IoT devices manufacturers from around the world, a review of the retailer list and examination of the current popular devices on these retailers was also required.

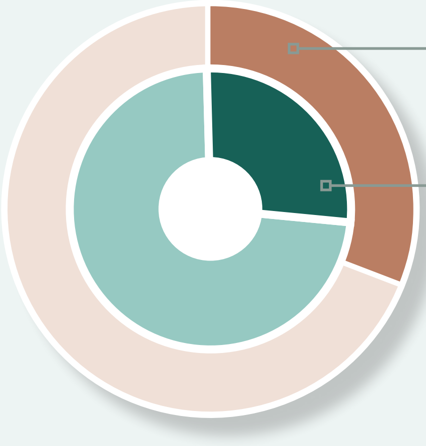
Some of the charts shown in the report this year track the 'core dataset' from 2022 in order to provide a comparison for the reader with the 'expanded' 2023 dataset. In addition, further analysis is provided on the products sold by retailers, which seeks to understand to what extent retailers are stocking products from manufacturers which adopt good security best practice in the form of vulnerability disclosure policies.

As with previous reports, the entire dataset is available as open data at copperhorse.co.uk.

Key Findings

The Headline Figure

🟩 Expanded dataset 🟫 Core Dataset



31.08% of the companies reviewed had a vulnerability disclosure policy

23.99% of the companies reviewed had a vulnerability disclosure policy

Figure 1

This year's widened dataset has brought to light an interesting change in the figures when incorporating the new additions. The net result is a re-calibration and refining of the global data such that it covers much more of the world's IoT product landscape. 2023's headline figure, the total number of manufacturers in the dataset with a vulnerability disclosure policy is 107/446 (23.99%). This means that the overall adoption of vulnerability disclosure mechanisms has reduced since last year, as 90/332 (27.11%) of companies had policies and / or contact points for disclosure. This means that this year, 76.01% of IoT manufacturers do not have a way for security researchers to report security issues representing a bleaker picture of the market than it already was. This may however be a reflection of the 'long-tail' of the market which may generally be expected to be of less quality than the suppliers that sell huge volumes of product.

Understanding and re-calibrating the data

For the first time in this series of reports the percentage of companies in the dataset providing a vulnerability disclosure contact mechanism for security researchers has not increased. This is because of the 121 new additions, only 6 (4.96%) have a policy, meaning for this additional new cohort of companies 115 of the 121 (95.04%) have not adopted vulnerability disclosure. These companies were: AVM, Hive, HONOR, iRobot, Phyn, and Tuya. Having added companies regularly in the past without disturbing overall trends, it is concerning to have new additions which, overwhelmingly, do not have a publicly accessible disclosure policy. This has resulted in 2023 being the first report in the series where the percentages for most datapoints have not trended upwards towards greater adoption (and therefore a more positive security picture).

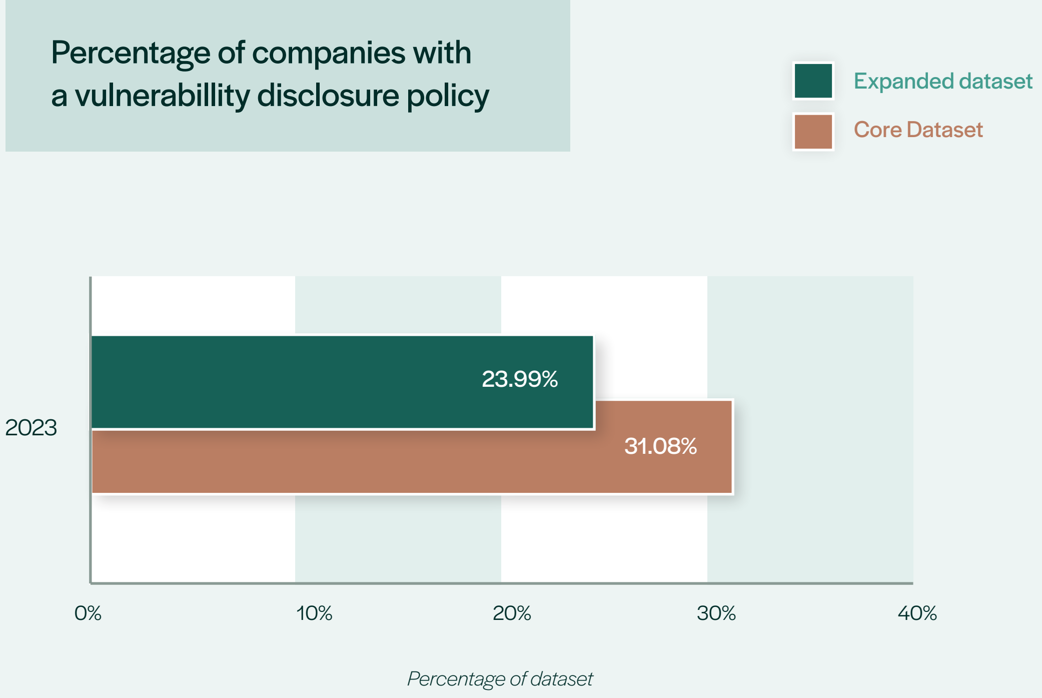

Percentage of companies with a vulnerabillity disclosure policy

Figure 2

What does the original overall trend look like?

While in many places the actual number of companies has increased, many of the percentages for datapoints captured in this research have remained similar or decreased due to the new additions. If the dataset from 2022 (carried over from the research conducted for the 2022 report) is isolated and examined the original trend continues: there is an approximate 4% increase in the percentage of organisations in the dataset adopting vulnerability disclosure – from 90 (27.11%) with a publicly accessible policy in 2022 to 101 (31.08%) in 2023.

Vulnerability Disclosure in Practice Trend

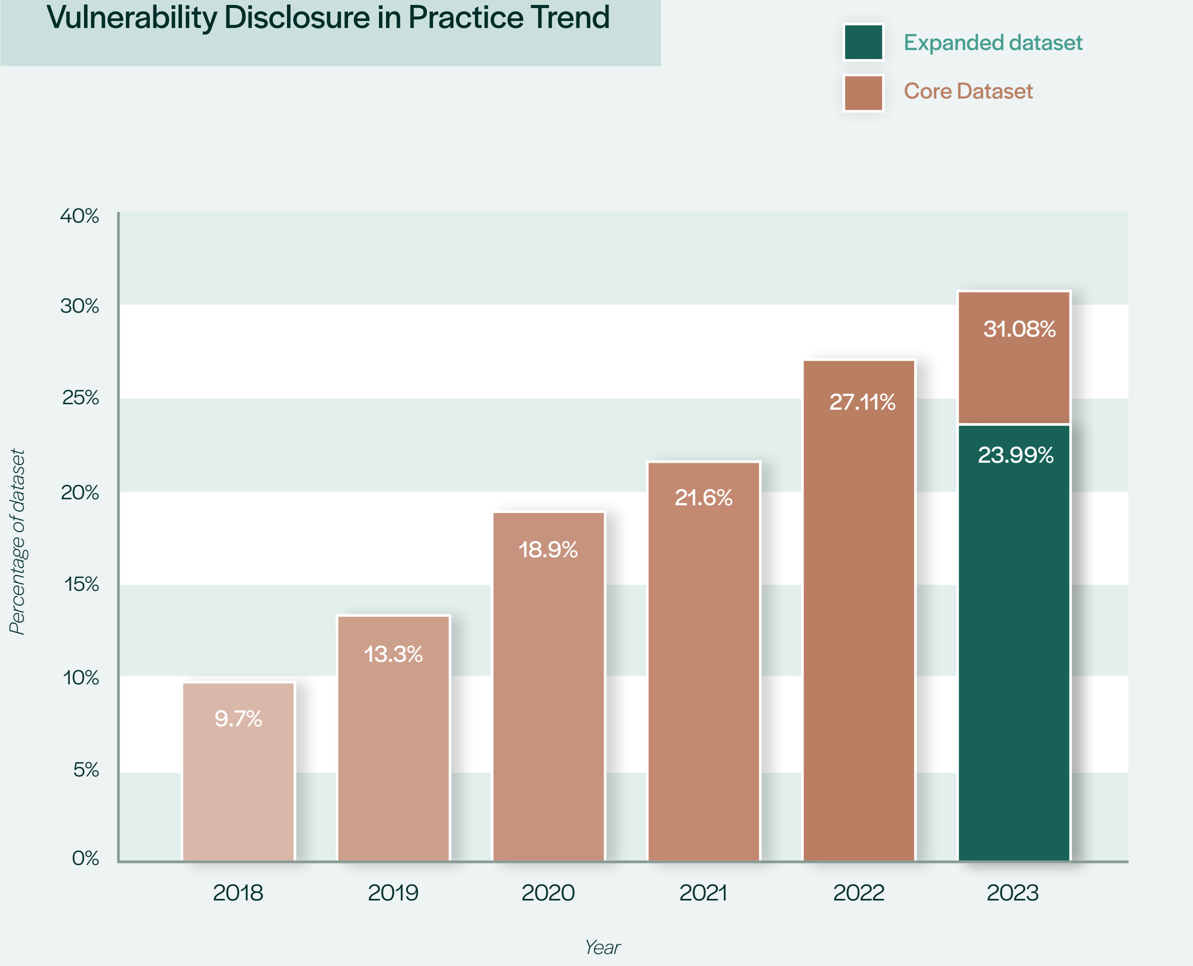


Figure 3

What does the original overall trend look like? (cont.)

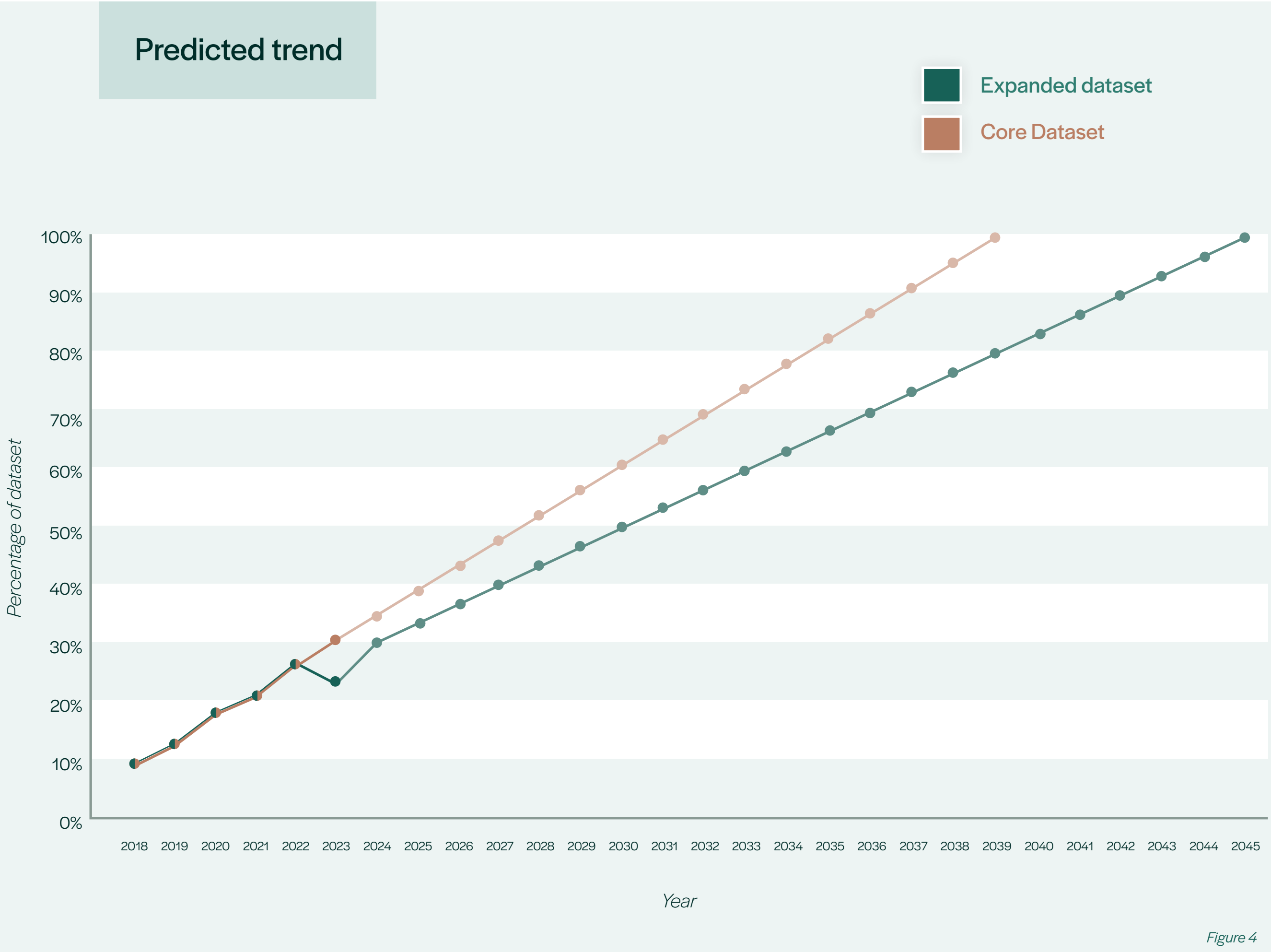


Figure 4

Taking more account of retailers

The research stage for this report is conducted annually and new manufacturers have been captured and added to almost every report, both to account for companies no longer operating or selling connected devices and to ensure the dataset remains representative of the current popular IoT manufacturers. However, the 2023 research data is the first time these new companies have impacted the entire percentage so greatly. All of the retailers Copper Horse researched to gather new manufacturers saw similar levels when it came to stocking products from IoT manufacturers that supported vulnerability disclosure policies or not; the vast majority of new IoT manufacturer additions did not have a point of contact for security researchers. Isolating the new vendor dataset - of the 20

Taking more account of retailers (cont.)

retailers used to gather data, only 6 of them (Best Buy, Currys, John Lewis, Jumia, Media Markt, and Walmart) had vendors that supported vulnerability disclosure policies. As action on IoT security grows across the world, retailers in countries where action is being taken should be concerned as they may be liable for stocking non-compliant and insecure products.

The vast majority of new IoT manufacturer additions did not have a point of contact for security researchers.

A portion of the research conducted in 2023 involved examining retailers from the EU, UK and US and comparing the results. This report found that EU and UK retailers both had similar levels of compliance among manufacturers of popular products on the platforms, with 38/67 (56.72%) and 23/41 (56.10%) respectively. US retailers saw 22/58 (37.93%) of manufacturers of the popular IoT devices with a vulnerability disclosure policy. In the legislation section this data is explored further.

Legislation

The UK government created the Product Security and Telecommunications Infrastructure (PSTI) Act, which received Royal Assent in 2022. Part 1 of this legislation mandates three requirements, one of which is the use of vulnerability disclosure by manufacturers of connected devices. Additionally, manufacturers need to include timeline information in the policy. The regulations were approved in parliament in September 2023. Manufacturers have until the 29th of April 2024 to comply with this legislation, with a penalty for non-compliance of up to a maximum of £10,000,000 or 4% of a manufacturer's worldwide turnover as well as heavy daily penalties for continued non-compliance.

Retailers of IoT products will come under 'Distributors', which are defined in the Act as 'someone who makes the product available in the United Kingdom, and.. ..is not a manufacturer or an importer of the product'. They have duties to check that products provided to them by manufacturers are compliant e.g. by being provided with a Statement of Compliance. One of the actions that could be taken against them is for a Court to order 'forfeiture' – i.e. that the IoT devices are seized by the enforcement agency to prevent them being sold.

The threshold test

The PSTI Act regulatory requirement for vulnerability disclosure is the basis of the threshold test. This test was created for this report in 2020 based on what the research team expected regulations to look like around the world.

The threshold test consists of two parts:

1. Have a vulnerability disclosure policy &;
2. Provide some kind of information on expected timelines

The researchers examined the data and found that the number of companies that pass both parts of the threshold test has increased to 42 (42/446 – 9.42%), up (in numbers) from 34/332 (10.24%) in 2022. Additionally, the number of companies that only pass the first part of the test has increased from 56/332 (16.87%) captured in 2022 to 65/446 (14.57%) in 2023. Regardless of an increase in the number of companies passing both parts of the test, a percentage decrease has been captured across the threshold test, due to the increase in participating manufacturers that do not have a vulnerability disclosure policy. This decrease is of concern, considering that regulation for the connected consumer product (consumer IoT) space is imminent in different places around the world.

Over 95% of new additions gathered in 2023 and over 75% the dataset as a whole do not have a vulnerability disclosure policy at all. Compliance for these manufacturers seems a distant prospect given that this subject has been talked about as good practice for many years now.

Threshold Test

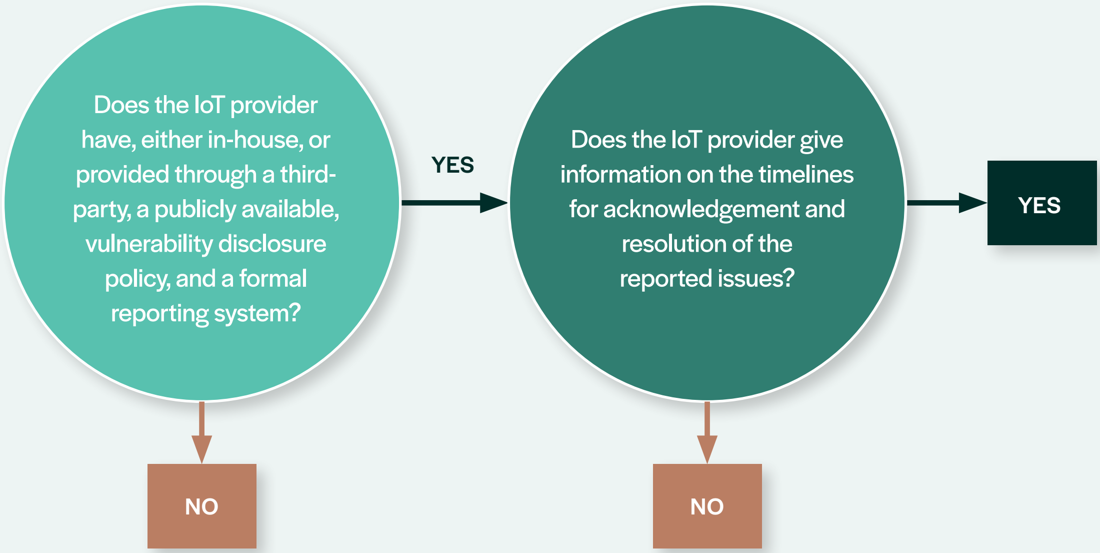

Does the IoT provider have, either in-house, or provided through a third-party, a publicly available, vulnerability disclosure policy, and a formal reporting system?
YES
Does the IoT provider give information on the timelines for acknowledgement and resolution of the reported issues?
YES
NO
NO

Figure 5

Europe

In the European Union, the Cyber Resilience Act (CRA) has been progressing. On the 19th of July 2023 it had its latest update. It has now entered the late stages where the final version of the draft Act will be negotiated within the European Parliament. The CRA specifically mandates the use of Coordinated Vulnerability Disclosure. Manufacturers wishing to sell products in the EU must complete a conformity assessment, either self-assessed or using a third-party assessor, that will determine whether the requirements of CRA have been met. EU member states will appoint "market surveillance authorities" who are responsible for enforcing CRA requirement obligations[3]. However, it is currently unclear how this will be assessed by whichever authority in each country is responsible for enforcement as the legislation annex text available at present is very high-level and does not provide detailed expectations of what it means by Coordinated Vulnerability Disclosure, for example the timescales involved. Also unclear is what the punishment for non-compliance will be, as well as how this will be enforced across all the countries in the EU. The CRA mentions the use of bug bounty schemes by manufacturers to incentivise the reporting of vulnerabilities, however this is not a requirement of the proposed legislation.

USA

In the US, work has been taking place on various pieces of legislation. At a state level, both California and Oregon have already enacted IoT security legislation and at a federal level, Congress introduced the Cybersecurity Improvement Act of 2020. This legislation required the National Institute of Standards and Technology (NIST) to publish standards and guidelines for the procurement and usage of IoT devices by federal agencies. Following this, in 2021, President Biden issued an Executive Order with the purpose of improving the nation's cybersecurity. The Executive Order charged NIST with producing various recommendations related to IoT security[4]. As a result, one of these outputs is the recommended criteria for a cyber security labelling scheme as well as NIST IR 8425, Profile of the IoT Core Baseline for Consumer Products, a standard which builds upon the NIST IR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers. NIST IR 8425 outlines basic vulnerability disclosure requirements – it requires device manufacturers to have the ability to receive and respond to queries, including having a point of contact where maintenance reports and vulnerability information can be sent. The document also uses bug bounty schemes as an example.

3. https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5375

4. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Examining retailer prospective compliance

It is increasingly apparent that retailers of connected devices will have some measure of responsibility for the products sold on their platforms, not only manufacturers. The UK's PSTI Act states that the security requirements it contains must be complied with by retailers of connected devices. For the 2023 report, the Copper Horse team examined retailer prospective compliance based on the existing popular connected products listed. It was decided that the three regions the researchers would investigate were the EU, UK and US because, as stated earlier, intended regulation in these areas is currently the most mature.

This subset of research was conducted following a similar methodology to the main dataset. The researchers captured the manufacturers of popular IoT devices, at the time of research, listed on retailers from the EU, UK, and US. The retailers below were selected as they offer a representative sample of major retailers within the three identified regions.

Region / Country (Number of Retailers)	Retailers	Stocked Manufacturers Using Vulnerability Disclosure
European Union (5)	CDiscount, France	5/12 (41.67%)
	El Corte Ingles, Spain	12/17 (70.59%)
	EPrice, Italy	5/10 (50%)
	Media Markt, Germany	7/8 (87.5%)
	Otto, Germany	9/20 (45%)
United Kingdom (3)	Amazon UK	3/14 (21.43%)
	Currys	11/17 (64.71%)
	John Lewis	9/10 (90%)
United States of America (3)	Best Buy	8/18 (44.44%)
	Target	8/10 (80%)
	Walmart	6/30 (20%)

Table showing retailers and the manufacturers they stock that use vulnerability disclosure

The UK and EU retailers are very close in terms of the percentage of popular IoT device manufacturers listed on the platforms, that have adopted vulnerability disclosure. EU retailers saw 38/67 (56.72%) of the vendors of popular IoT devices have implemented a vulnerability disclosure policy, while UK retailers had 23/41 (56.10%). The US retailers lagged behind the EU and UK with 22/58 (37.93%) of vendors engaging in vulnerability disclosure.

Delving deeper into this data allows a comparison between retailers. In the EU the retailer with the highest percentage of popular IoT device manufacturers with a vulnerability disclosure policy was Media Markt with 7/8 (87.50%), followed by El Corte Ingles with 12/17 (70.59%), ePrice with 5/10 (50.00%), Otto with 9/20 (45.00%), with the lowest being CDiscount at 5/12 (41.67%). The UK retailer John Lewis leads this entire list of retailers, across all 3 regions, with 9/10 (90.00%) of vendors of popular connected products having a vulnerability disclosure policy; the other UK retailers were captured as Currys with 11/17 (64.71%) and Amazon UK at 3/14 (21.43%). US retailers performed slightly worse than EU and UK retailers, with 8/10

Examining retailer prospective compliance (cont.)

(80.00%) of popular IoT device manufacturers listed on Target, Best Buy followed with 8/18 (44.44%) and Walmart with the lowest percentage, at 6/30 (20.00%).

This portion of data analysis has allowed the research team to identify commonalities between retailers. With the data gathered, popular manufacturers listed across multiple retailers (EU, UK, US) could be examined. Of the popular devices on these retailers at the time of research, it was found that Google and Philips were listed on the websites of 7 of the 11 retailers explored for this section. Additionally, Apple and Amazon were listed on the sites of 5 retailers. This indicates that these are popular connected device manufacturers in the markets where regulation is imminent, being listed across retailers in the EU, UK and US.

Types of Vulnerability Disclosure

Coordinated Vulnerability Disclosure (CVD) is the industry recognised and internationally standardised, best practice for vulnerability disclosure. The security researcher and vendor work together to identify, rectify and issue a patch; then finally the vulnerability can be disclosed to the public by the security researcher. Data from previous years showed a majority of organisations that have a vulnerability disclosure policy use CVD as the preferred method. The story is similar in 2023, with 70/107 (65.42%) of the companies with a policy indicating they have CVD – 70/446 (15.70%) of the entire dataset. A small number 4/107 (3.74%) of companies with a policy or 4/446 (0.90%) of the overall number of companies, have a non-disclosure policy where researchers are bound to not disclose found vulnerabilities publicly. The remainder 33/107 (30.84%) or 33/446 (7.40%) of the overall dataset, do not indicate either way. Previous reports have captured a minimal increase year-on-year, however the 2023 report has captured a small decrease in companies using CVD. In 2022 this report found that 62/90 (68.88%) of manufacturers with a policy used CVD and that there was a small increase in companies that do not indicate either way.

Regional differences

Most of the manufacturers in the report's dataset are headquartered in either North America, Europe, or Asia. None of the relatively small number of vendors based in Oceania, Africa or South America have adopted vulnerability disclosure policies.

The number of vendors in Europe, North America, and Asia adopting vulnerability disclosure has increased on the 2022 figures. However, due to the new companies added to the dataset in 2023, many of which have no direct way for security researchers to contact them, the percentages have decreased. Europe has increased from 11 (14.47%) in 2022 to 19/101 (18.81%), North America has changed from 35 (32.61%) to 50/172 (29.07%), and Asia from 34 (34.69%) to 38/153 (24.84%) with the current research, conducted in 2023.

Manufacturer adoption of vulnerability disclosure across the world

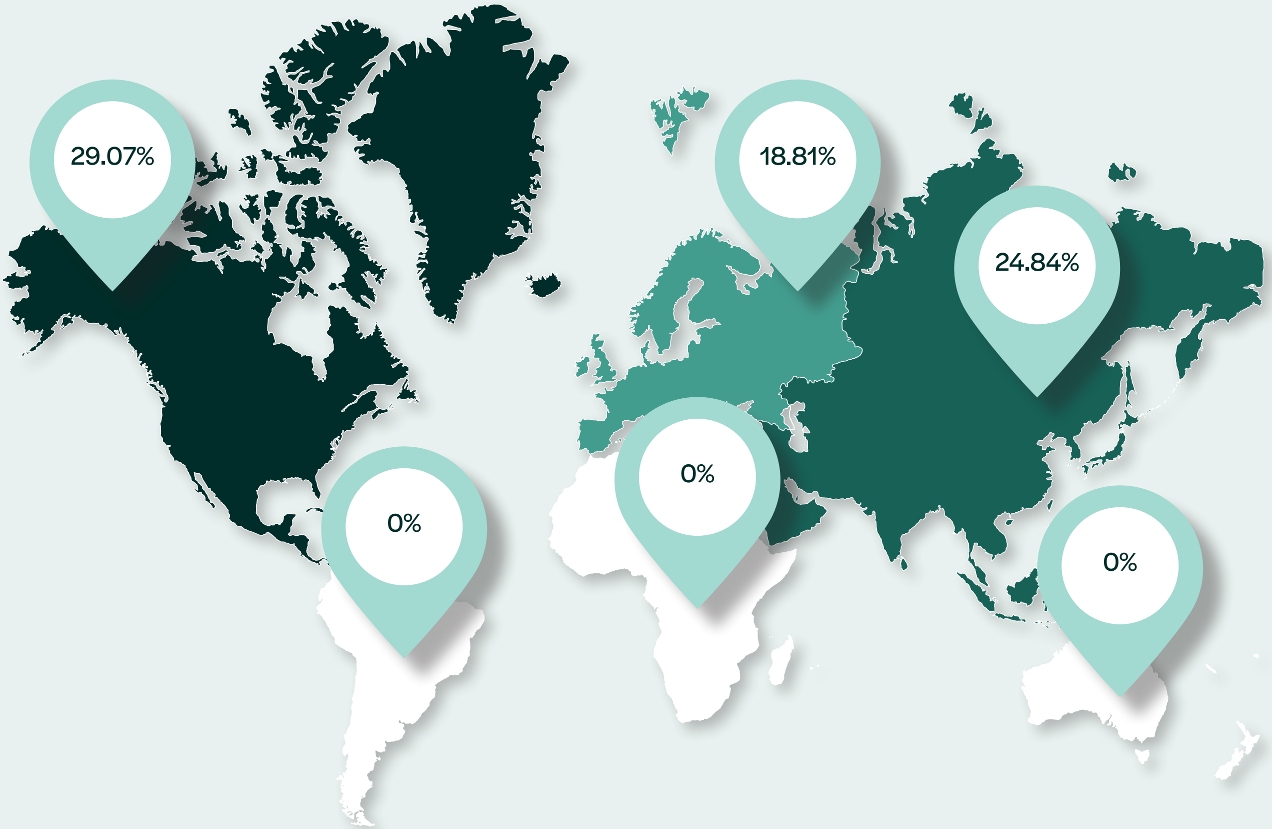


Figure 6

Product categories

Product categories are the main type of product a consumer IoT manufacturer produces, targeted at a particular domain. It allows a breakdown of the data of how different manufacturers of connected consumer devices perform within the category of the type of device they offer. The narrative observed in previous reports continues with the 2023 research. More mature product categories like TVs 6/6 (100%), Wi-Fi and Networking 11/14 (78.57%), and Mobile 11/16 (68.75%) consistently outperform less well-established categories such as Wearables. Of the 49 wearable device manufacturers, only 8 (16.33%) have adopted vulnerability disclosure, however this number is a minor increase on the 4 (13.33%) in 2022. Leisure & Hobbies still sits with 0/7 (0%) of the vendors with a policy, followed by Health, Fitness and Wellbeing at 6/46 (13.04%) and Lighting at 5/46 (10.87%). These three product categories are some of the most popular connected device types yet continue to see poor levels of adoption of vulnerability disclosure policies.

When searching for manufacturers and vulnerability disclosure, Copper Horse staff found public information on disclosed vulnerabilities in certain products, but no policy with contact information on the manufacturer's site, even when the issues with the products are being discussed publicly. After finding a publicly disclosed vulnerability in a product, as discussed above, it is often difficult to know whether a manufacturer has rectified the issue unless they explicitly communicate this; this is not a problem with coordinated vulnerability disclosure, where vulnerabilities are disclosed at the end of the process. An example of this is Ruveno, which has produced a smart lock and has no vulnerability disclosure policy, but its product was included in a Cambridge student's dissertation[5] where vulnerabilities in one of their products was revealed. Other manufacturers were found in the dataset such as Meross[6] and EZVIZ[7] which have no publicly available contact point for reporting issues, but both had articles publicly disclosing vulnerabilities in devices manufactured by these organisations.

[5] https://www.cl.cam.ac.uk/~kst36/documents/meng-dissertation.pdf

[6] https://www.which.co.uk/news/article/cheap-smart-plugs-could-expose-you-to-hackers-or-even-cause-a-fire-aMuck9K2OSYx

[7] https://www.bitdefender.co.uk/blog/labs/vulnerabilities-identified-in-ezviz-smart-cams/

Product categories (cont.)

Below are all the product categories captured in this research and the percentage of the category employing vulnerability disclosure.

Percentage of Companies in a Segment with a Policy

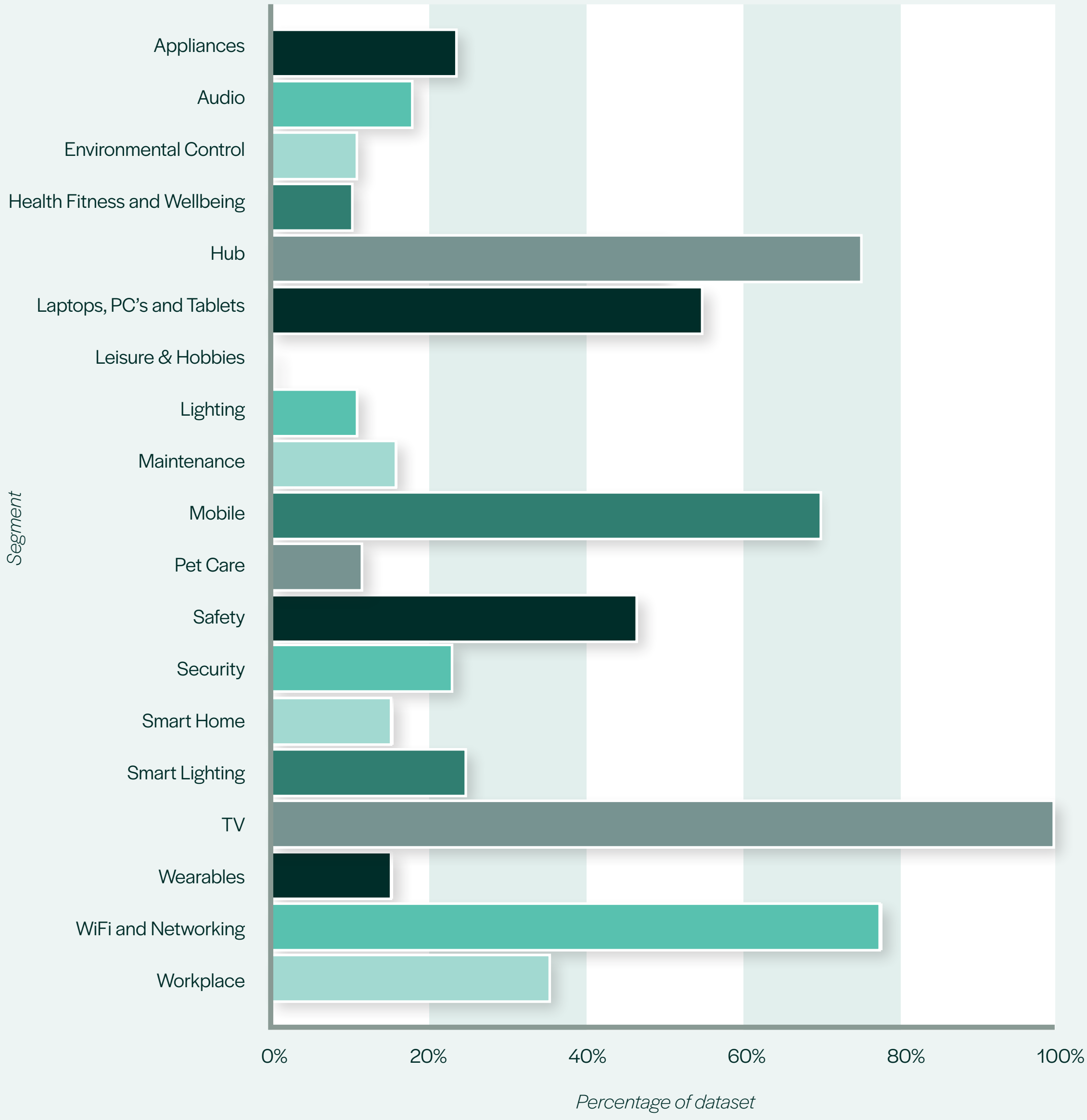


Figure 7

Enterprise

In 2021, the researchers examined a small group of enterprise or business-to-business (B2B) manufacturers. This dataset continually outperforms the core dataset of this report. The research carried out in 2023 found that 42/48 (87.5%), well over triple the core dataset figure of 23.99%. This may be due to the maturity of the enterprise sector and the fact that many of the organisations are long-standing, large brands. There was a discussion amongst the research team, before the 2023 research started, whether to incorporate this enterprise list into the core dataset. The decision was made to keep the two separate, but to continue reviewing the status of the enterprise companies in each report, as the findings are still relevant. This decision was made as the enterprise company list was gathered from various sources and was intended to be a representative sample of B2B organisations, not a comprehensive study gathered using the same methodology as the core consumer dataset.

Proxy Disclosure & Bug Bounties

Organisations which do not have the capacity to operate a vulnerability disclosure programme or simply want to outsource it can do so by utilising proxy disclosure organisations, which will host the company's desired policy on the proxy platform. Proxy disclosure usage in the previous reports has trended upwards; 2023 is an exception, with the large number of new additions without any policy reducing the overall percentage. The research has found that 27/446 (6.05%) of vendors now use a proxy disclosure organisation for vulnerability disclosure, a marginal change on the 2022 figure of 21/332 (6.33%). Previously the two proxy disclosure companies captured in this research were BugCrowd and HackerOne, however this year saw the addition of 3 new organisations. These are Intigriti, Yes We Hack, and BugBase. While the newly added proxy disclosure organisations are only captured as being used by one manufacturer each, making up a total of only 3 of the 27 companies in the dataset to utilise proxy disclosure (Nespresso (Nestlé), Withings, and boat), it is positive to see new participants in the market.

Some manufacturers choose to offer bug bounties alongside a vulnerability disclosure scheme. A bug bounty is simply a mechanism for offering a financial reward to encourage security researchers to submit vulnerabilities to a manufacturer, as a way of incentivising and rewarding participation. These bug bounty schemes typically include a scope which outlines the products and services a manufacturer makes available to test, and the financial reward a researcher can receive for each category of bug. The research in 2023 observed that 29/446 (6.50%) of vendors in the dataset used this method for engaging with researchers, the figure captured in 2022 was 23/332 (6.93%). The number of organisations offering financial rewards has increased, but the overall percentage has decreased due to the newly added companies to the dataset. It is therefore difficult to draw meaningful conclusions, however it will continue to be monitored in the next report.

Use of /security pages & Use of security.txt

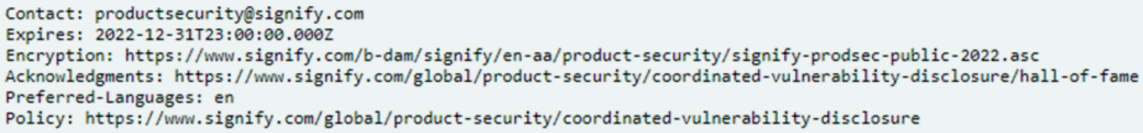
The research conducted in 2023 found for the first time, that the number of organisations using security.txt files (located at /.well-known/security.txt) was higher than the number of organisations placing its vulnerability disclosure policy on a /security page. In 2022, 25 or 7.53% of vendors were using a /security page and 19 or 5.72% using security.txt – this report has seen the actual number of companies using both /security and security.txt rise, but the overall percentage of the dataset using both of these methods for hosting a policy has decreased. In 2023, the research captured 28/446 (6.28%) using a /security page and 29/446 (6.50%) using security.txt. The relative overall change to this data is however fairly static.

/security web pages have been captured as a location for storing a vulnerability disclosure policy throughout these reports, being recommended in the IoTSF's publication Vulnerability Disclosure Best Practice Guidelines[8]. However, they aren't as universally applicable or specifically usage-reserved as a security.txt file would be. The location '/security' on a manufacturer's site may already be used for other purposes – to hold information about security related products, for example. security.txt offers a standardised location, as well as a defined format for information about a vulnerability disclosure policy. There is much progress to be made in this area and in vulnerability disclosure more broadly and it may be that guidance on vulnerability disclosure by recommendations and standards bodies should by reviewed in order to take into account the standardised location of security.txt. The security.txt standard is a universally applicable location, however the number of companies adopting it remains very low.

In the 2022 report there was a discussion on the expiration dates of security.txt files. The Internet Engineering Task Force (IETF) outlines the required elements of security.txt file in RFC 9116[9], one of which is an expiration date. The RFC states that an expiration date indicates the date after which the policy is stale; it also recommends that when creating a security.txt file, the expiration date be less than one year in the future to avoid staleness. In reality, it is unlikely that an expired security.txt (or ones beyond one year in the future) is entirely abandoned, but the lack of clarity can cause confusion in the vulnerability disclosure process.

Below are two examples of improperly formatted security.txt files.

Firstly, is the Signify security.txt – which expired 7 months before the research was conducted.



```
Contact: productsecurity@signify.com
Expires: 2022-12-31T23:00:00.000Z
Encryption: https://www.signify.com/b-dam/signify/en-aa/product-security/signify-prodsec-public-2022.asc
Acknowledgments: https://www.signify.com/global/product-security/coordinated-vulnerability-disclosure/hall-of-fame
Preferred-Languages: en
Policy: https://www.signify.com/global/product-security/coordinated-vulnerability-disclosure
```

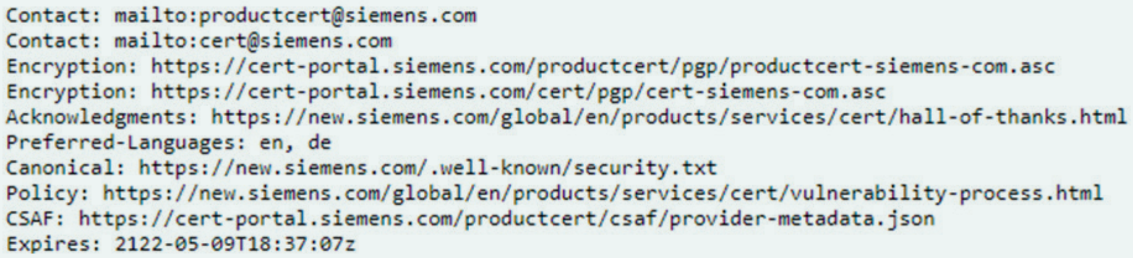
Figure 8

[8] https://iotsecurityfoundation.org/wp-content/uploads/2021/09/IoTSF-Vulnerability-Disclosure-Best-Practice-Guidelines-Release-2.0.pdf

[9] https://www.rfc-editor.org/rfc/rfc9116

Use of /security pages & Use of security.txt (cont.)

Secondly, is Siemens' security.txt which has an expiration date nearly 100 years in the future.



```
Contact: mailto:productcert@siemens.com
Contact: mailto:cert@siemens.com
Encryption: https://cert-portal.siemens.com/productcert/pgp/productcert-siemens-com.asc
Encryption: https://cert-portal.siemens.com/cert/pgp/cert-siemens-com.asc
Acknowledgments: https://new.siemens.com/global/en/products/services/cert/hall-of-thanks.html
Preferred-Languages: en, de
Canonical: https://new.siemens.com/.well-known/security.txt
Policy: https://new.siemens.com/global/en/products/services/cert/vulnerability-process.html
CSAF: https://cert-portal.siemens.com/productcert/csaf/provider-metadata.json
Expires: 2122-05-09T18:37:07z
```

Figure 9

PGP keys

The previous report in this series captured an approximately 14% decrease in the usage of PGP keys to encrypt vulnerability reports, with 52/332 (15.66%) of the manufacturers offering it in 2022. 2023 saw 57/446 (12.78%) using PGP. While the manufacturer numbers have slightly increased, the percentage has decreased once again with the larger dataset. The research conducted in 2023 saw 7 new organisations offering PGP as an option to encrypt submissions. Furthermore, 2 of those 7 companies previously had a vulnerability disclosure policy without a PGP key, and have adopted the use of encryption keys since the previous review. These were Devolo and Hikvision. Two companies, Ultimate Ears and Fitbit both appeared to have removed PGP as an option for submissions. The decrease in usage may reflect IT departments' reluctance to allow PGP usage in the business; the risk of malware infiltration into the business via this route may outweigh the benefit of providing the option. The other consideration is that PGP is fundamentally difficult to use for some and may introduce friction that is unacceptable to the business when a web form may address the encrypted submission requirements to an adequate level.

Disappearing manufacturers

In the methodology section of this report, the number of companies lost from the dataset was briefly discussed. The number lost in 2023 was marginally less than in previous reports, with 7 companies being removed (whereas 18 were lost in 2022). Usually when companies are lost, the researchers are unable to identify the specific reasons why. This may be because websites no longer load, or products are no longer being sold on a specific retailer, beyond this unfortunately, there is often no more information to be found. The company may have gone out of business, but definitive statements are generally unable to be made about their operational statuses.

One of the companies lost in 2023 put out a press statement on its departure from the market and it raises some interesting questions. PicoBrew was a home brewing system that allowed users to brew beer from their kitchen counters. The brand was in financial trouble and was acquired by new owners. However, an update on the company's website indicated that the brand would not be continuing: the post stated that products would remain operational, but the forums would be closed. News about the company from Forbes concludes[10] with questions about continued device operation and whether the servers will stay online. With forums being discontinued and little information about the new owners, what is a researcher to do if they find a vulnerability in a product, for a company that, for all intents and purposes, are out of business? This situation reflects end-of-life and support issues for IoT products that concern many in industry and in governments.

[10] *https://www.forbes.com/sites/katedingwall/2020/05/11/whats-going-on-at-picobrew/#3b840c3430f1*

Talking Points and Observations

This section includes some observations and talking points derived from things that have been seen when researching the companies in the report.

Manufacturers without their own online presence

Many manufacturers encountered during the research do not have contact information, location, or a website available and are only sold via other online retailers.

Each year during the research phase of this annual report, the researchers regularly encounter device manufacturers for which finding contact information is very difficult. In some cases, it isn't possible to find a company website, location information or a contact email address. The devices these manufacturers produce are commonly sold across a broad range of the retailers reviewed. They are especially common at retailers such as Amazon and AliExpress and often list security cameras, smart plugs, lights or similar connected devices. It is almost impossible to ascertain these organisations' vulnerability disclosure status. When the regulation for legislation, such as the UK's PSTI Act comes into force, the enforcement authorities will need to discover who and where these manufacturers really are, perhaps with the help of the distributors and retailers.

Maintenance: Bose

In the 2022 report Bose's /security page redirected to a URL that indicated a vulnerability disclosure policy was once hosted on that page

In 2022 the research team captured Bose's /security page. At the time of research in 2022, this returned a 404 (an error code indicating a web page does not exist, has been moved, or is broken), but the URL indicated some form of vulnerability response policy used to be located at this domain. The researchers have followed up on this observation in 2023 and it appears that this has been fixed, as the URL no longer contains the text indicating a policy was hosted there. Bose still does not have a vulnerability disclosure policy located at either the /security page, or /.well-known/security.txt. This illustrates a general need for companies to maintain their websites and or vulnerability disclosure policies as in the future it could impact their ability to sell their products due to regulation in this area. It also demonstrates that situations can change over time and this presents a risk of change in the gap between a testing or self-declaration process and the product actually being sold on the market.

Acquisition: Fitbit

Fitbit is now owned by Google and covered under the Google Bug Hunters programme. When the researchers looked at the company in the last report, Fitbit appeared to be in a state of limbo, no longer with its own active policy but not yet supported by Google.

Google acquired Fitbit in 2021 and during the company transition period (in the research window for the 2022 report), Fitbit's listed vulnerability disclosure scheme was no longer operating. This was seemingly due to them transitioning to Google's Bug Hunters scheme. It was captured during the 2022 report-writing period and reviewed in the 2023 research window, that this was in fact the case. Fitbit's /security page now directs researchers to Google Bug Hunters, and this has been reflected in the data for 2023.

End-of-life risks: Walmart

During the research phase, it was discovered that Walmart were selling an IoT product that research indicates is no longer functional.

During the research phase of this report, the research team reviewed the popular connected devices sold by Walmart. One of these was Fox&Summit, a company with a window and door sensor listed on Walmart's website. The researchers looked into the manufacturer, Fox&Summit and found multiple reviews claiming that the products had stopped operating. It was discovered that the manufacturer's site was not functioning, and the company had not posted on social media since 2020. Additional research was unable to find the company's developer profile on the Google Play Store, and the connected app has not received an update since 2019 on the Apple App Store. Google reviews also paint a picture of inoperable devices; 18 of 19 reviews rate the company 1 star with most writing about issues with the products no longer operating.

The researchers made the decision to not include this product and manufacturer in the new additions to the 2023 dataset.

Multiple routes for disclosure: Qardio

Qardio is a member of the medical device cyber consortium MedISAO that manages CVD submissions for members.

Qardio are a manufacturer of heart health monitoring devices. The company itself has a Coordinated Vulnerability Disclosure policy on its site. However, additionally, it is a member of MedISAO, a medical device manufacturer consortium focusing on device security. This consortium has its own vulnerability disclosure policy, which accepts reports on member company devices. The policy even lays out a scope, which does not allow testing of devices used by a patient or in a clinical setting, provides timeline information, and both a secure web form and PGP key for submissions. MediSAO's policy does not require a researcher to attempt contact with the manufacturer before submitting a report to them, only requiring that researchers comply with all relevant laws and regulations as well as the above stated patient safety testing rules. It is uncommon to see a company with two disclosure channels available and this may cause confusion in the disclosure process.

Disclosure scheme that doesn't cover the product: Withings

Withings has started a public bug bounty scheme, but the current scope does not include its products

In previous reports, it was captured that Withings, the French electronics manufacturer, did not have a vulnerability disclosure policy. In the research phase of the 2023 report, the researchers observed that Withings had created and published a policy. This policy is hosted with a proxy disclosure organisation, 'Yes We Hack' and contains all the relevant information. While it is always a positive when a vendor in the dataset adopts vulnerability disclosure, the scope for Withings' policy is limited. The company's bug bounty scope does not offer rewards for anything related to its physical products, only offering rewards for vulnerabilities found in its APIs and web applications. This limitation may discourage a researcher from submitting their findings to Withings.

Providing books about disclosure, but not delivering it: Kobo

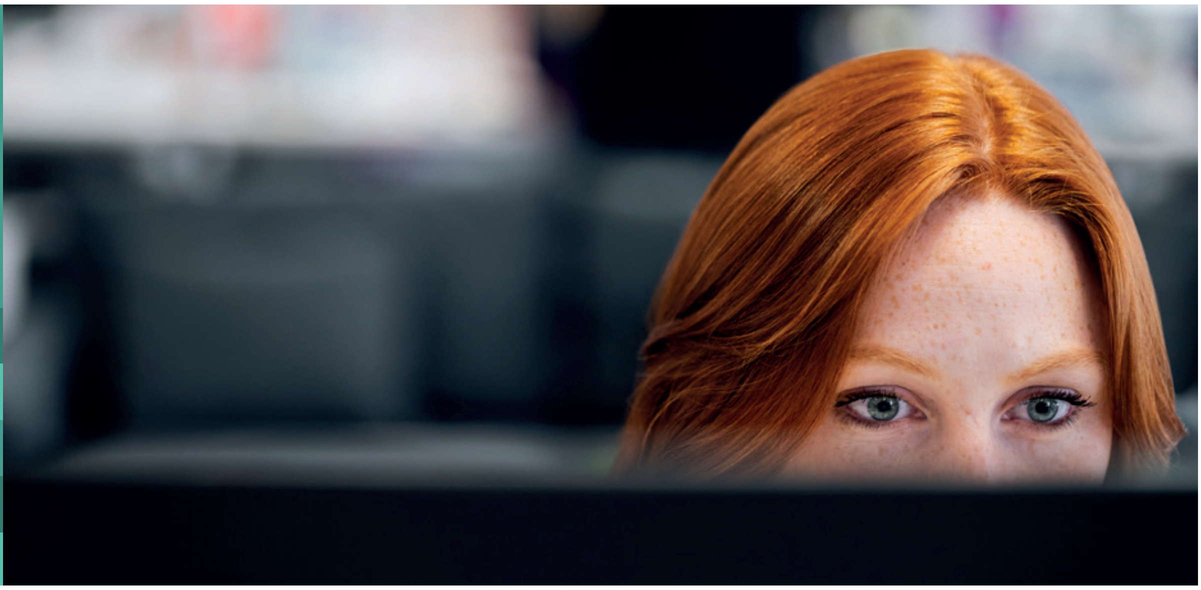
Rakuten Kobo (eBook device and book seller) sells a book on adopting vulnerability disclosure, yet does not have its own policy.

Rakuten Kobo sells eBooks and eBook readers among other related products. The company was added to the dataset because it offers internet connected eReaders. During the research phase, it was discovered that Kobo has no publicly available contact point for submitting vulnerability reports. The webstore for eBooks offers multiple books related to vulnerability disclosure – one of which is 'The Vulnerability Researcher's Handbook: A comprehensive guide to discovering, reporting, and publishing security vulnerabilities'. While it is obvious that the Kobo staff won't read every book on the platform, it is somewhat ironic that it does not have a policy but sells a book outlining the vulnerability disclosure process.

Progress: Fossil

Fossil is a fashion brand offering products including watches and jewellery. The company has been in the dataset without a policy in multiple of these reports. However, this report, Fossil had adopted vulnerability disclosure, utilising a proxy disclosure organisation.

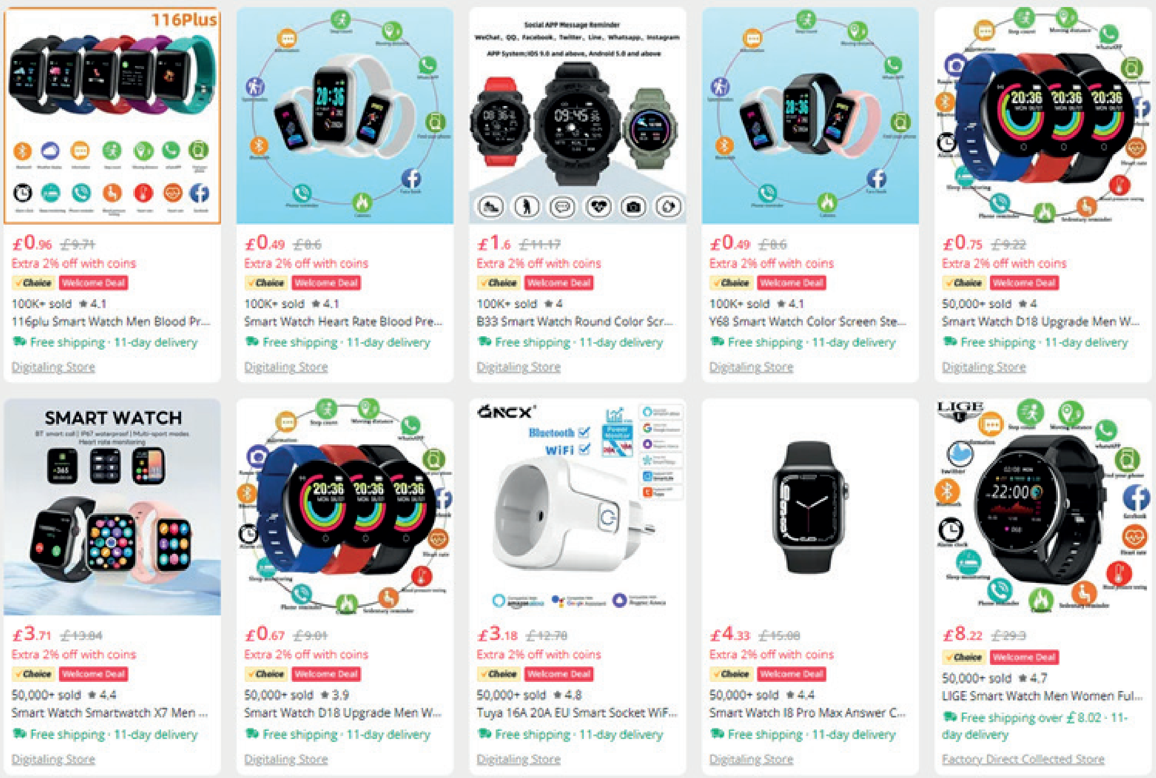
In 2023, Fossil introduced a vulnerability disclosure policy via HackerOne's proxy disclosure platform. Proxy disclosure organisations have helped to reduce the barriers of entry for vendors to engage in vulnerability disclosure.



White-labelled and confusing brand ownership: AliExpress

> *9/10 of the popular smart devices on AliExpress were cheap smartwatches, the majority of which were purportedly manufactured by the same company.*

The vast majority of the new additions to the dataset in 2023 do not have a vulnerability disclosure policy. A portion of the popular IoT devices added to the dataset in 2023 are what appear to be the same line of generic, white-labelled smartwatches, with different brands attached. Of the retailers the researchers looked at, nowhere exemplifies this trend more than the retailer AliExpress. When conducting the research for this report, it was observed that 9/10 of the top products on its store, when sorting by number of orders, were these generic smartwatches. Additionally, it was discovered that 9/10 of these top products were sold by the same seller to the retail platform, 'Digitaling Store'. Furthermore, many of these watches were listed as manufactured by a brand already captured in this dataset: YP – indicating that these are white-labelled watches, listed under different brand names.



£0.96 ~~£9.71~~
Extra 2% off with coins
Choice Welcome Deal
100K+ sold ★4.1
116plu Smart Watch Men Blood Pr...
Free shipping · 11-day delivery
Digitaling Store

£0.49 ~~£8.6~~
Extra 2% off with coins
Choice Welcome Deal
100K+ sold ★4.1
Smart Watch Heart Rate Blood Pre...
Free shipping · 11-day delivery
Digitaling Store

£1.6 ~~£11.17~~
Extra 2% off with coins
Choice Welcome Deal
100K+ sold ★4
B33 Smart Watch Round Color Scr...
Free shipping · 11-day delivery
Digitaling Store

£0.49 ~~£8.6~~
Extra 2% off with coins
Choice Welcome Deal
100K+ sold ★4.1
Y68 Smart Watch Color Screen Ste...
Free shipping · 11-day delivery
Digitaling Store

£0.75 ~~£9.22~~
Extra 2% off with coins
Choice Welcome Deal
50,000+ sold ★4
Smart Watch D18 Upgrade Men W...
Free shipping · 11-day delivery
Digitaling Store

£3.71 ~~£13.84~~
Extra 2% off with coins
Choice Welcome Deal
50,000+ sold ★4.4
Smart Watch Smartwatch X7 Men ...
Free shipping · 11-day delivery
Digitaling Store

£0.67 ~~£9.01~~
Extra 2% off with coins
Choice Welcome Deal
50,000+ sold ★3.9
Smart Watch D18 Upgrade Men W...
Free shipping · 11-day delivery
Digitaling Store

£3.18 ~~£12.70~~
Extra 2% off with coins
Choice Welcome Deal
50,000+ sold ★4.8
Tuya 16A 20A EU Smart Socket WiF...
Free shipping · 11-day delivery
Digitaling Store

£4.33 ~~£15.08~~
Extra 2% off with coins
Choice Welcome Deal
50,000+ sold ★4.4
Smart Watch I8 Pro Max Answer C...
Free shipping · 11-day delivery
Digitaling Store

£8.22 ~~£29.3~~
Choice Welcome Deal
50,000+ sold ★4.7
LIGE Smart Watch Men Women Ful...
Free shipping over £8.02 · 11-day delivery
Factory Direct Collected Store

Screenshot of the AliExpress store front displaying the 10 popular devices

Mixed disclosure responsibilities: Connex Connect

Connex Connect uses Tuya's platform for its connected app. Where does responsibility lie?

It can sometimes be complicated to discover who is really responsible for receiving reports of vulnerabilities found in a product or its associated technologies. If an IoT product is produced by a now-defunct company, but still being sold through a retailer, should the retailer still be selling it? What about when a company's product is controlled using another organisation's connected application? This second situation is what was observed with Connex Connect, owned by SMD Technologies. A press release[11] stated that "Tuya and SMD Technologies collaborate to power Smart Home Products on the Connex Connect App". Tuya provides cloud platform solutions to many companies, offering Platform as a Service (PaaS) and has adopted vulnerability disclosure. In this case, the application is branded as Connex Connect, and without research it would be difficult to identify that Tuya collaborated on the platform. Depending on where the vulnerability is found, whether it be in the application or the Tuya service, a researcher may find it difficult to contact the companies involved. Tuya has a vulnerability disclosure policy but Connex Connect does not.

Security requires maintenance: Spacetalk

Spacetalk has a report on its website about the security of its products. However, research found the company does not have a vulnerability disclosure policy.

Spacetalk is a manufacturer of smart watches. In a demonstration that it has taken a proactive approach to security, the company has information on its website related to an audit that a security researcher had conducted on its products. The audit concludes with "The Spacetalk watch has been designed with great consideration into the security of the device and the user's data". While taking this action was a positive sign, it took place in 2018 and since then the company has not publicly released any additional reports that would indicate that this type of product testing occurs regularly. Additionally, the company has not adopted vulnerability disclosure.

[11] https://www.prnewswire.co.uk/news-releases/tuya-and-smd-technologies-collaborate-to-power-smart-home-products-on-the-connex-connect-app-810449569.html

Conclusions

This report is the first in the six reports produced so far where the percentages of companies using vulnerability disclosure, as well as the other related datapoints, have not all generally increased, they decreased.

In 2023 the dataset saw 121 new additional popular device manufacturers, which overwhelmingly (95.04%) did not engage in vulnerability disclosure. While this represents a large increase to the overall dataset, Copper Horse researchers felt comfortable expanding the research to a greater global reach, because they were using the same methodology used in the previous reports. To achieve an accurate, representative sample of popular IoT devices manufacturers from around the world, a review of the retailer list and examination of the current popular devices on these retailers was also required.

It is important to note that the reports do not measure volume in the market (as this is not possible for the researchers to measure), they measure the breadth of manufacturers retailing into popular retailers and then also the popular devices sold by those retailers. Had the research team not added this dataset, the trend would have tracked the previous trends – a slight increase, but not one that matches the urgency of the requirement from governments across the world for manufacturers to adopt coordinated vulnerability disclosure policies.

This broadening of the consumer IoT landscape picture across the world refines the overall data to give a truer picture of the situation in the market, while retaining the methodology used in all the previous reports.

The research captured small increases in the number of companies with policies, utilisation of proxy disclosure and the other categories measured, across the board the percentages have decreased. Considering the original 2022 dataset in isolation without the new additions, the figures remain very low. With manufacturers wishing to sell into the UK needing to become compliant with the PSTI Act regulations by April 29th 2024, consumer IoT device manufacturers are still a long way off.

> With manufacturers wishing to sell into the UK needing to become compliant with the PSTI Act regulations by April 29th 2024, consumer IoT device manufacturers are still a long way off

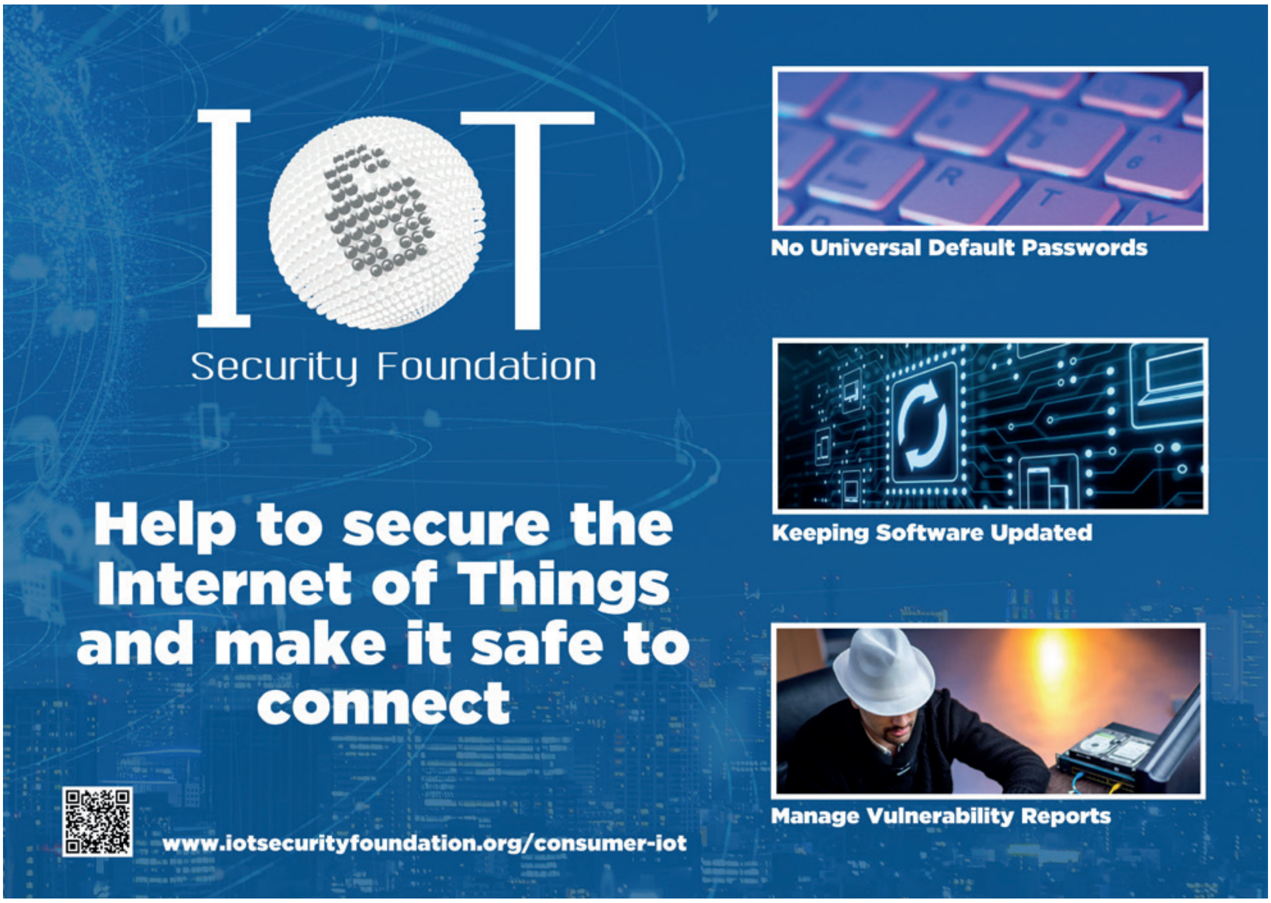
The new additions gathered in 2023 are also worrying, only 6 of 121 popular device manufacturers engage in vulnerability disclosure. While it is unlikely 100% compliance will ever be achieved, 4.96% is extremely low. What this may illustrate is a 'long-tail' of market volume but it should be noted that consumers buy these products and they are popular. An analysis of product price alone is not enough to elicit whether these devices are at the lower-end of the market, as some high-end products are often sold quite cheaply or as a 'loss-leader' in order to get the user to buy-in to other services online services.

The overall dataset in 2023, including the new additions captured 107 of 446 (or 23.99% of companies) having a publicly available point of contact for security researchers. Additionally, the threshold test indicates that only 42/107 companies with a policy would be compliant to the UK's PSTI Act requirements. It is positive that this number has increased on the 2022 threshold test, but with less than 12 months left until the Act comes into effect, this number will need to rise rapidly. By the time the next report in this series is published, unless there is a significant shift, many companies will be in breach of UK law.

A similar story has been captured in the product categories section. Previous reports have captured certain categories massively outperforming others. TV, Wi-Fi and Networking, and Mobile consistently perform better than others like Wearables, Leisure and Hobbies, and Health, Fitness and Wellbeing. Sector maturity may be the cause of this observation, as the categories performing the best often are more mature and are more comfortable engaging with security best practices. Enterprise or B2B companies exemplify this, massively outperforming the core dataset with over triple the levels of adoption.

With upcoming legislation and regulation in the consumer IoT space, especially in the UK, EU and US, the researchers took a deeper look at retailers from these 3 regions. Regulations are increasingly indicating that retailers will share some responsibility in the companies that list products for sale if they aren't compliant with requirements. Looking at 11 retailers, 5 EU, 3 UK, and 3 US, to evaluate the popular IoT device manufacturers listed on them. The UK and EU retailers had similar levels of companies with policies, with 56.10% and 56.72%, respectively, and the US lagged slightly behind with 37.93%. In terms of specific retailers, John Lewis outperformed the others with 9/10 (90%) of popular IoT device manufacturers with a publicly available policy, which contrasts with Walmart which was captured at 6/30 (20%).

This situation may change in the next year as the first regulatory deadlines for compliance are reached and it will be interesting to see how next year's data will or won't change. The general lag in adoption of vulnerability disclosure policies is compounded by the extraordinary and unprecedented global situation in the past few years both because of geopolitics, the COVID-19 pandemic and its economic fallout in the past couple of years as well as the war in Ukraine. These factors have all been damaging to businesses globally and will have likely delayed adoption of cyber security measures, when business survival has most likely been the priority. Sadly, this doesn't change security realities on the ground and attackers are not going to stop; their capabilities are only growing.


IoT
Security Foundation
Help to secure the Internet of Things and make it safe to connect
www.iotsecurityfoundation.org/consumer-iot
No Universal Default Passwords
Keeping Software Updated
Manage Vulnerability Reports

Annex

This annex represents the output of the threshold test.

- **Companies highlighted in green pass both test 1 & 2 of the threshold test:**
  Has a vulnerability disclosure policy and provides information on expected timelines
- **Companies highlighted in amber pass only the first part of the test:**
  Has a vulnerability disclosure policy but no timeline information
- **Companies highlighted in red do not pass either part of the test, meaning:**
  Has no vulnerability disclosure policy or timeline information

Bosch
Philips
Wink
Western Digital
Siemens
Ecobee
Microsoft
Xiaomi (MI)
SimpliSafe
Sonoff
Panasonic
LG
Meta
TP-Link
BT
SonicWall
Canon
Logitech
Peloton
Procter & Gamble, Oral B
Lenovo
OPPO
HTC
Huawei
WyzeCam
Samsung (Smart TV)
HP
June
Logitech, Ultimate Ears
Qardio
Anker, Eufy
Sengled
HMD Global (Nokia Mobile)
Foscam
BroadLink
Qnap
Synology
Netatmo
FIBARO
Fossil
Pico
iRobot

Signify - Philips Lighting
Google
Motorola Mobility
GE Appliances
Sonos
Lovense
Amazon
Dell
Garmin
Belkin
Lexmark
Bose
JBL
ASUS
Lifx
OnePlus
Vivo
ZTE
Samsung (Mobile)
Apple
PetCube
Honeywell Home (Resideo)
Dahua
Hikvision
Yale
ARLO
D-Link
Tapplock
Hanwha, Wisenet
Samsung (SmartThings)
Sony
Roku
Buffalo
Draytek
Eero
Linksys
Netgear
ZyXEL
Canary
Ring
Best Buy, Insignia
Devolo
Acer
Nuki
August
FLiR
Schlage, Allegion
TVT
Samsung (Galaxy Watch)
Arris (Commscope)
WiZ (Signify)
boAt
FitBit
Nespresso
Omron
Withings
Loxone
NanoLeaf
Airthings
Hangzhou XiongMai Technology
Hive
AVM
Tuya
Phyn
HONOR

Annex (cont.)

Vivint
TomTom
Anova
Apption Labs
Behmor
Candy
Hoover
iFAVINE
Laurastar
Perfect Company
Smarter Applications
SmartyPans
Tefal
Weber
Whirlpool
Aiwa
Audio Pro
B&O
DENON
Devialet
Lenbrook Industries, Bluesound
Lithe
Marshall
NAIM
Roberts Radio
Ruark
Small
TIBO
Voxx International, Klipsch
Xoopar
Xperi, DTS
Yamaha Pro Audio, Yamaha Corporation
Airboxlab
Awair
Drayton
eq-3
Genius Hub
Insteon
Iris Ohyama
Keen Home
Koogeek
Leotec
Tado
Trane
Winix America
Dyson
AdhereTech
AliveCor
Amor Gummiwaren GmbH
ASAKUKI
Beeline
BlueAir
Breathometer
Delta Five
Etekcity
Greater Goods
Guardian Technologies (Lasko)
Hatch Baby
Hidrate
iHealth
InteraXon Inc
Kolibree, Baracoda
LifeFitness
Misfit
Nima
NordicTrack
Proform (ICON fitness)
RENPHO
Sleep Number
SmartPlate
Tanita
TytoCare
Velco
We-Vibe
Zeeq
Ratoc Systems
Kobo
MSI
Vankyo
Venturer (RCA)
Deeper
Mattel, Fisher-Price
Sphero
Tracking Point
UBTECH
ACEMAX
Aeon Labs, Aeotec
EGLO
Bawoo
Elgato, Eve
Energenie
Flux Smart
Hunterfan
IFITech
iku
ilumi
Innr
Jasco
Lampaous, LUMENMAX
Lightwave
Lohas
Lutron
Meross
MIPOW
Novostella, Ustellar
Osram
Otio
Tomshine
Ustellar
Veho
Vivitar
Wallfire
Yeelight
Curb (Powered By Elevation)
Gardena
Neato
Roost
BLU Products
Doogee
Infinix
TCL Corporation (Alcatel)
XOLO
Current Labs
Furbo
Seneye
Whistle
MoKo
MySpool
X-Sense
ACTi
ADT
Amaryllo
Apollo Tech USA
Atom Labs
Bizfeat
Chamberlain
Clever Dog
DigitalKeys
Edimax
Eminent
EZVIZ

Annex (cont.)

FREDI
Intelbras
KeySmart
Kwikset
Lockstate, smartLOCK, RemoteLOCK
Lorex
Reolink Digital Technology
Shenzhen Neo
Skybell
Smanos
Tend Insights
Tile
Trust
Vaultek
Weenect
Zmodo Technology
AISIRER
Circle
Click and Grow
FireAngel
Garadget
Hank
Husqvarna
Moen
Neurio, Generac
Rachio
Remotec
StoryLink
Teckin
Wattcost
Amazfit (Huami)
Armani (Armani Exchange, Emporio Armani)
Beurer
Casio
Catapult Sports
LetsFit
Michael Kors
Polar
Sensoria
SUUNTO
Wearable X
Elecom
TRENDnet
Anoto
Brother Industries, Ltd
Canon, IRIS
Double Robotics
Estimote
Moleskine
Neo
Seiko Epson
Theatro
Weight Gurus (Greater Goods)
Night Owl
Kidde
HeimVision
Gosund
ELAiCE
EMOOR
BELLABEAT
Enabot
Wimius
116 Plus
YP
LIGE
Haylou
BeBird
Tado
Eve
IglooHome
Kickstart
Sacramento
HAVIT
AKILII
Hoco
F22
Noise
ApnaCam
Segway
Sensibo
Tzumi
Merkury Innovations
ONKYO
FITPRO
Ation
Hyiear
WEBCATLY
Yoosee
Midea
SOSAFE
NEXXT SOLUTIONS
ARKIFI
2NLF
UanTii
Baytion
Razuvious
Moes House
Promate
Hama
NGTeco
Aqara
Echel
iReader
CP Plus
CTRZQ
SNARIYOVSN
SKY HUB
Lifesense
360
Yunmai
Xiangshan
Hatch
TopVision
iHuniu
Luckwolf
Gavdhe
lulshou
Kangaroo
Merkury Innovations
Daybetter
Xueyu
Feit Electric
Topesel
DEWENWILS
iFanze
Mingwear
Vine
XODO (Contixo)
First alert
SPT Security
X10
Amped Wireless
Yummly
Vitamix
Jura
ThermoPro
Café
Govee
Whisker
PetLibro
Cube

Annex (cont.)

WeeKett
ANTELA
SwitchBot
Ruveno
SWAN
TEKXDD
Popglory
Blackview
GNCC
Aura
COA
InBody
Home Cam
Bangtan
Hyrican
Klarstein
Diyarts
XCOAST
SSC-LUXon
NAIXUES
KIQULOV
Teckin
Anmossi
Einhell
Groove
Neutron
Smartbell
SMD Technologies branded as Connex Connect
Aubess
POLAROID
SpaceTalk
Goldair
Frameo
Pixbee
SLD
CHRONUS
JUSTGREENBOX
SWANN
Therabody
VEHO
Cresta
Avidsen
Muvit
Nivian
DCU
SIXPAD (MTG)
Qrio
Arugo
Maxevis
Plus Style (+Style)
Aranet
Laresar
Geekee
Simpled
Oyajia
Overmax
HTN

IoT Security Foundation

www.iotsecurityfoundation.org

COPPER
HORSE

www.copperhorse.co.uk

59-60 Thames Street, Windsor, Berkshire, UK, SL4 1TX
+44 (0) 208 1337 7337 @copperhorseuk