NordVPN®

Your smart devices are a security risk

Table of contents

Background

The Internet of Things (IoT) is everywhere. But, with the number of privacy and security issues they can expose us to, is it really that “smart” to bring these devices into our homes? Do you always do everything you can to protect your IoT devices? Blame is often put on users, but they are only the final point of a long line of problems.

There is a strong community of cybersecurity researchers — both in academia and the industry, often working with government agencies — who are committed to finding vulnerabilities, making the risks known, and helping to fix them.

But what if you can’t find who to go to when you need to get something fixed? There are so many startups and other small IoT companies all over the world, and many of them don’t stand the test of time. But IoT devices need to be for life, not just for Christmas. It’s much harder to fix devices when the maker no longer exists. And even without explicit vulnerabilities, if the company goes under or is bought out, then support for users also disappears. This could mean we no longer have access to crucial updates or assurances over user data that has been collected and stored.

Method

To gain a better understanding of the user aspect of IoT, we conducted a survey via CINT. A total of 7,000 people were surveyed, with 1,000 people from each of the following countries: Australia, Canada, France, Germany, the Netherlands, the UK, and US. Participants formed representative samples across gender, age, family situation, and income levels. The questions revolved around which IoT devices people had in their homes, what measures they took to secure them, and whose responsibility they thought it was to ensure the security of IoT devices. The results were cross-referenced with a new user-focused taxonomy of the main vulnerabilities IoT devices are exposed to. The timeline and taxonomy were generated through a review of the key literature on IoT security and vulnerabilities, as well as looking at press coverages of major attacks.

Problems in the IoT

IoT devices, many of which are actually just Linux-based computers stuck into everyday household objects, from TVs to fridges, introduce problems that should have been solved decades ago, and in many cases were. But IoT devices are lightweight, so they often can't handle the levels of security that a conventional computer, laptop, or smartphone can. You would hope that a laptop would be sold with the latest security features and would automatically update itself (or prompt users to do the updates), but IoT makers aren't always so careful. So, one step we can all take is to think about the security and privacy of IoT devices more like we do for our more complex devices. This goes both for users and manufacturers.

This leads us to another major problem with IoT security. The market is so competitive that devices are often rushed onto the shelves and into our homes. Default passwords can be left in through careless programming or "commented out" of browser login interfaces without actually removing them from the underlying code. If you have investors and competitors breathing down your neck, you are likely to make mistakes. Added to the fact that device makers are unlikely to be security experts and might not hire a dedicated security team to keep costs down, this means that privacy and security tend to be afterthoughts (that is, if they are thought about at all).

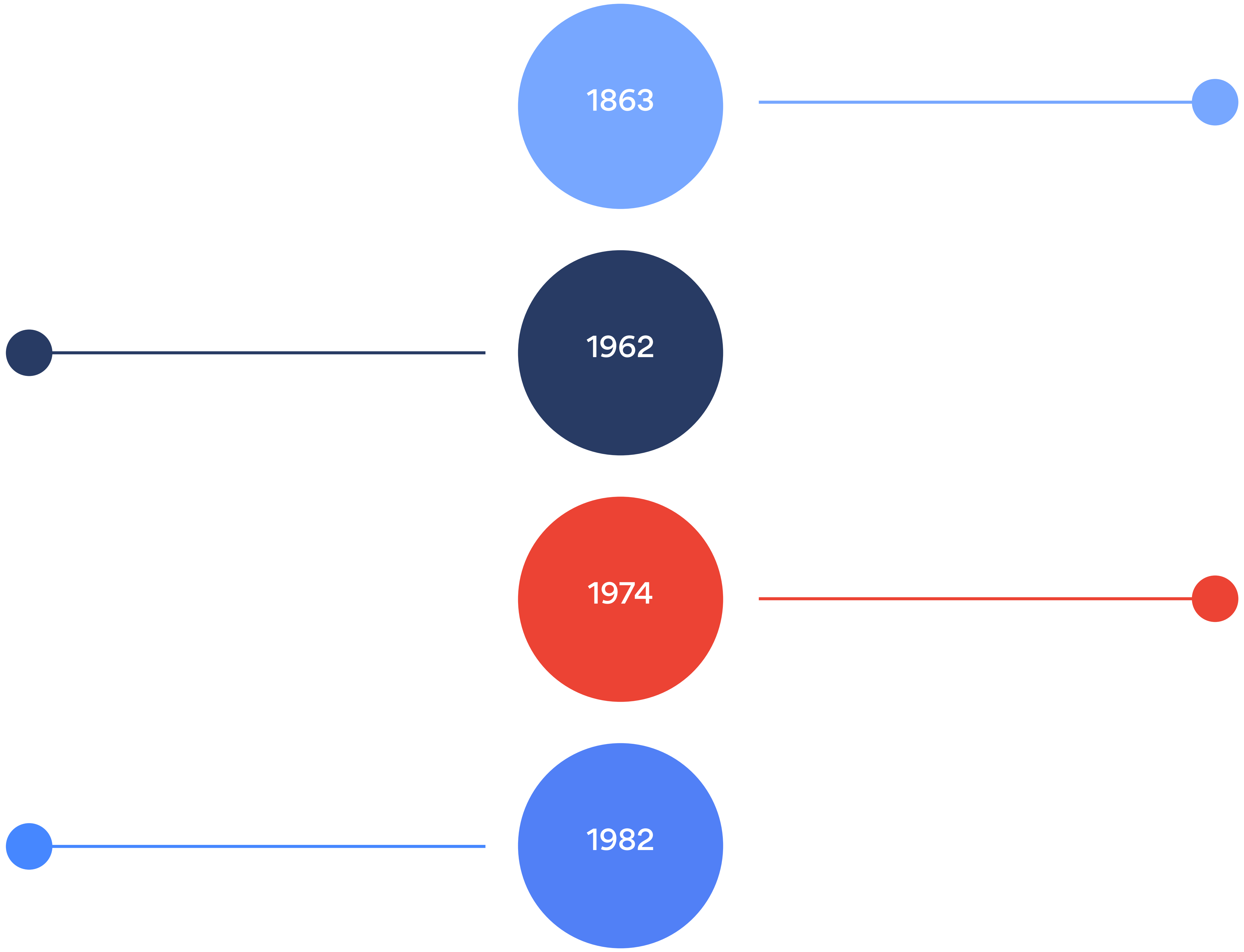
IoT devices by their very nature collect and send information. This might be done securely and for a specific purpose, such as an encrypted message to tell your heating to turn off. But it might also be leaky, either through bad encryption (or none at all) or through giving away extra information. For example, the internet-connected camera on your front door might let you know when a visitor or possible intruder is there, but, if someone else is watching, it can also reveal when the house is empty or when children are home alone.

There are also social problems with IoT devices that don't always have technical fixes. In a business situation, these types of problems might be called OpSec (operational security), and those include keeping things up to date and having strong passwords. But, for most of us, it's about personal relationships. Are you in a shared living arrangement where housemates might bring unknown devices into the network? Do you have a housemate or partner who has left but still has passwords and access? Yes, you can change the password, but will you remember to do that in the middle of a breakup? And what if the person who left is the only one who knows the passwords or how everything is set up? No one wants their ex messing with their heating or sharing camera images, so more effort needs to go into reducing the risks for users' security and privacy.

In light of all the technical and structural issues, user behavior is just one extra aspect of potential security vulnerabilities, but there are often simple steps we can all take to improve the security of our devices and networks in our homes or offices. Other aspects and responsibilities include manufacturers and governments, who should be ensuring the best practices and up-to-date information available to everyone. IoT is by its nature an ecosystem of networks, devices, and data, so it needs a holistic approach to keeping everyone safe.

Timeline of problems in the IoT

More and more “things” are on the internet each day, from cameras to fridges. But, although the boom in IoT devices seems relatively recent, there’s a long history of problems associated with connected and smart devices.



1863

Jules Verne writes Paris in the Twentieth Century, outlining early visions of smart technologies such as automated security systems. However, the publisher rejected the dystopian vision, and it wasn’t published until the 1990s.

Other works by Verne include An Ideal City (1875), featuring music sent live over wires from a performer’s piano to people’s homes, and In the Year 2889 (1889), featuring video conferencing. Verne’s fantastical inventions kick-started sci-fi imaginings of smart devices in our homes.

1962

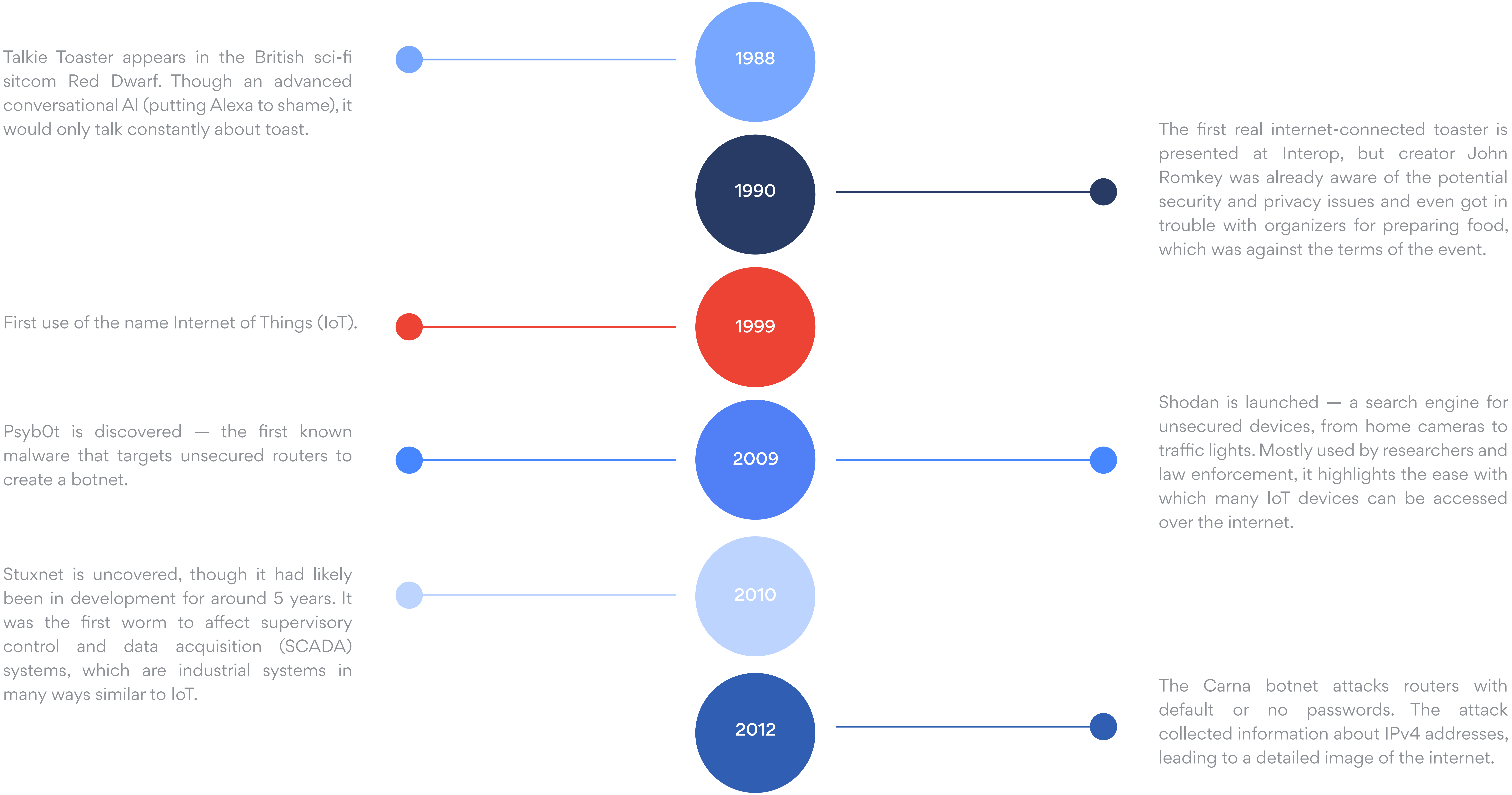
The Jetsons brought a home filled with “smart” devices like an automatic hoover to TV screens, although the devices were not without mishaps, like the pet dog swallowing a flying car toy and gaining the ability to fly.

1974

The Transmission Control Program (TCP) is published, including the first use of the term “internet”. While it was one of the key Internet Protocols (IP) and set the basis for a common internet, TCP/IP would later become a major target for vulnerabilities.

1982

The first internet-connected device became operational — a Coke machine connected to ARPANET at Carnegie Mellon so researchers could check without leaving their office whether the machine was stocked and the drinks were cold. Coke engineers weren’t happy about the tampered device.



1988

Talkie Toaster appears in the British sci-fi sitcom Red Dwarf. Though an advanced conversational AI (putting Alexa to shame), it would only talk constantly about toast.

1990

The first real internet-connected toaster is presented at Interop, but creator John Romkey was already aware of the potential security and privacy issues and even got in trouble with organizers for preparing food, which was against the terms of the event.

1999

First use of the name Internet of Things (IoT).

2009

Psyb0t is discovered — the first known malware that targets unsecured routers to create a botnet.

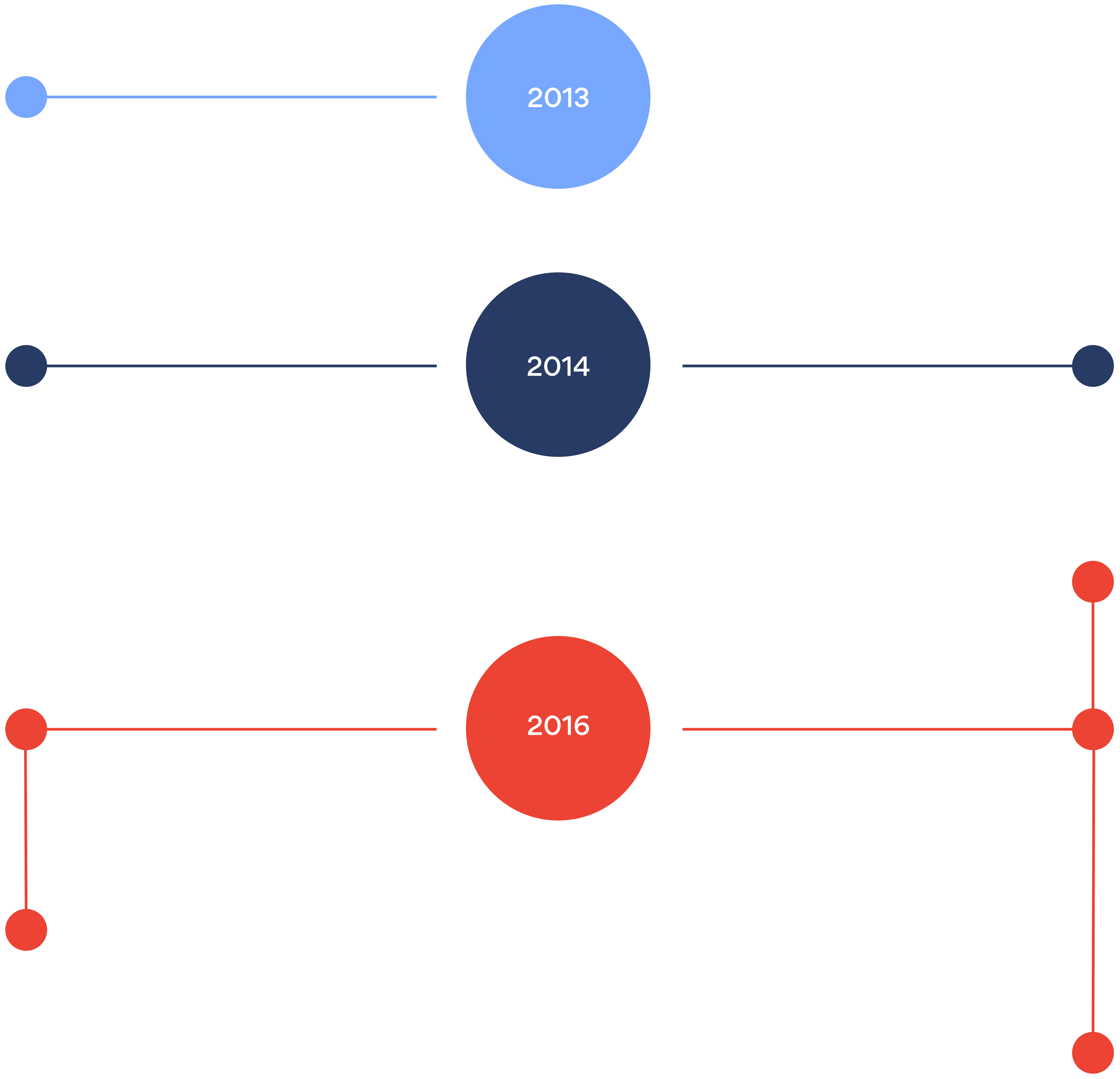
Shodan is launched — a search engine for unsecured devices, from home cameras to traffic lights. Mostly used by researchers and law enforcement, it highlights the ease with which many IoT devices can be accessed over the internet.

2010

Stuxnet is uncovered, though it had likely been in development for around 5 years. It was the first worm to affect supervisory control and data acquisition (SCADA) systems, which are industrial systems in many ways similar to IoT.

2012

The Carna botnet attacks routers with default or no passwords. The attack collected information about IPv4 addresses, leading to a detailed image of the internet.



2013

Linux. Darlloz infects IoT devices via a PHP vulnerability. It is later used for crypto mining.

2014

Linux. Wifatch is released. This “vigilante” malware actually removes other malware and reminds users to update their firmware and change default passwords.

BASHLITE (also known as LizardStressor and many other names) infects mostly IoT devices like cameras to create high-volume DDoS attacks. It is notable for being able to infect other devices on the local network.

2016

Ring doorbell cameras prove easy to hack and even enable attackers to steal users’ Wi-Fi passwords.

Muddy Waters Research reported vulnerabilities in connected heart implants made by St. Judes. While the company initially denied the findings, the next year the FDA confirmed the devices were vulnerable.

The Remaiten malware creates a botnet by testing commonly used passwords on routers and other devices.

The Mirai botnet uses thousands of co-opted IoT devices to create a string of huge DDoS attacks, including against the Dyn DNS servers, blocking many major websites. This is all despite the malware originating from competing Minecraft server hosts on a college campus.

Another “vigilante” white-hat malware called Hajime emerges, competing against Mirai by protecting devices.

2017

BrickerBot, which aims to permanently disable or “brick” IoT devices after brute forcing Telnet passwords, is discovered when it attacks a cybersecurity company’s honeypot. It was soon retired, but the creator claimed it was designed to stop devices infected with Mirai.

2019

In a series of revelations, it was reported that Amazon, Google, and Apple all sent smart assistant recordings to contractors to improve their speech recognition systems without users’ knowledge.

2020

A class action lawsuit is brought against Ring for weak security that enabled mass hacking of their cameras, including attackers being able to speak to users and their children (often with threats or racist messages).

2021

Name:Wreck exposes 100 million IoT devices. This is only one of the most recent in a long history of vulnerabilities.

Taxonomy of IoT vulnerabilities in context

Relevant literature provides different ways of classifying IoT vulnerabilities, including four broad categories with subtypes, eight categories with subtypes, or even nine categories spread across a multidimensional taxonomy. Here, we build on those taxonomies that divide vulnerabilities into categories more clear for users. We use the four main categories — physical, network, software, and encryption — slightly adjusted. Given the similarity and crossover in many of the attacks, we merge encryption and network, as most encryption issues come to light when information is shared across a network (either internally or over the internet). We also focus on the application layer instead of software specifically. This matches with the accepted structure of vulnerabilities in the IoT stack in the literature. We also add a further category of social vulnerabilities. Each category contains several main types of vulnerability, matched with those identified in other taxonomies.

Physical vulnerabilities have to do with the devices themselves and how they are constructed. They usually require an attacker to be there in person, so, most likely, they occur in external devices such as cameras.

- **Physical damage** to sensors to create malfunctions or false readings (also called node tampering);
- **Physical access** by taking a device apart or accessing a USB port could make devices easy to hack by injecting malicious code;
- **Interference** or jamming of wireless communication;
- **Power** supplies to devices can be attacked or batteries drained through keeping devices unnecessarily active;
- **Malicious devices** can be added to a network to interact with proper devices.

Network and encryption vulnerabilities

- Man-in-the-middle (**MITM**) attacks, in which information is intercepted by a hacker. This can include key exchange for encryption so each end thinks they are interacting with each other, when in fact it's the MITM interacting with both sides;
- Denial-of-service (**DoS**) attacks, in which excessive data is sent to devices to block legitimate data or cause the device to shut down. This is separate from turning IoT devices into botnets for a distributed-denial-of-service (DDoS) attack, which is generally targeted at internet infrastructure or major organizations;
- Radio Frequency Identification (**RFID**) attacks, including spoofing, cloning, or analyzing traffic, in which the wireless communication is intercepted, disrupted, or tricked;
- **Routing** attacks, including spoofing, looping, or creating "sinkholes" to suck up data or drop it into nowhere;
- Poor or no **encryption** on low-quality devices can make it easy for hackers to access or decrypt data. This can include reading plaintext (unencrypted data), working out encryption techniques if there is some known plaintext, or analyzing the cryptography in order to break it.

Application (software) vulnerabilities

- The broad category of **malware**, including viruses, worms, trojans, and others, can stop devices functioning, send data to attackers, or co-opt a device into a botnet;
- **Programming errors** can include poor implementation of accepted practices, leaving hardcoded passwords in firmware, not setting up upgrades properly, not storing keys or other information (like Wi-Fi network passwords) securely, and any other poor practices that can open up devices to a huge range of vulnerabilities;

- Various **authentication** attacks include escalating privileges, downgrading protocol versions, weak password protocols, attacking poorly coded browser-based login systems, or (a regular problem) unchanged default passwords;
- Other vulnerabilities, like DoS and phishing, can involve application and software elements, and different attacks can be combined. This may be particularly pronounced if support for a device stops, as **deprecation** can lead to out-of-date systems and vulnerabilities that have been fixed elsewhere.

Social vulnerabilities

- **Social engineering** attacks trick people into giving up information or access, which can be letting someone physically into your home to access devices or handing over passwords to phishing emails;
- Operational security (OpSec) falls into two further types: **User OpSec**, which includes setting up and maintaining devices (like changing default passwords or updating devices) and is mostly about simple but important steps to prevent vulnerabilities; and **System OpSec**, which includes the manufacturer and cloud services keeping updates available, following data retention and access practices, and other related ongoing processes that can create or stop vulnerabilities.
- **Privacy** issues can occur even when devices are working properly, including unnecessary data being collected, sent, and potentially exposed to other risks later on, or companies misusing or mishandling data they don't really need.

We now outline this taxonomy with an extra sociotechnical dimension, which combines countermeasures with issues of context and responsibility. To make a taxonomy that is useful not only for technical experts and abstract attack scenarios but also for real-world contexts and situations in which users and IoT devices exist, it is important to understand not only what countermeasures can be applied to certain vulnerability risks but also to emphasize who can and should be taking these measures.

We introduce four categories for this context/countermeasure dimension, which are all based on the literature as well as the social aspects of responsibility and user behaviors:

- **Manufacture**: What vulnerabilities must be mitigated when devices are designed and made?
- **Service:** What vulnerabilities are part of ongoing responsibilities of service providers (including, for example, updates, cloud access, and data storage)?
- **User:** What vulnerabilities can or must be mitigated in the setup and operation of devices within the home or other use context?
- **Ecosystem:** What vulnerabilities and measures cut across different contexts of the IoT ecosystem?

These are cross-referenced with the vulnerabilities to create an indicative (non-exhaustive) taxonomy not only of vulnerabilities but also of sociotechnical action and responsibility.

		Contexts and responsibilities			
Categories	Vulnerabilities	Manufacture	Service	User	Ecosystem
Physical	Damage	Security-conscious design		Check devices; stop using devices if necessary	Best practices Regulation Knowledge and skills Perceptions and social norms Open analysis Media and reviews
	Access	Advice to users		Check setup and access	
	Interference	Best practice and secure standards			
	Power				
	Malicious devices			Separate local networks for devices; change default passwords	
Network and encryption	MITM	Use proven standards; secure implementation	Prompt updates; secure and up-to-date systems	Change default passwords; VPN on router	
	DoS			VPN on router	
	RFID		Prompt updates	Change default passwords	
	Routing			Change default passwords; VPN on router	
	Encryption			Keep devices up to date; review before buying	
Application (software)	Malware	Follow best practices; seek external audit	Issue prompt patches and updates	Safe behaviors; change default passwords; update	
	Programming			Update; review before buying	
	Authentication		Maintain systems and practices	Change default passwords	
	Deprecation	Clear policies	Notify users	Stop using device	
Social	Social engineering		Notify users of common/new attacks and tips for action	Careful behaviors	
	User OpSec	Empower users with easy and granular configuration (e.g. changing passwords; admin accounts)		Careful behaviors; keeping up to date on information	
	System OpSec		Update policies and procedures; GDPR and other data protection compliance; regular audit		
	Privacy	Best practices for data systems		Check policies; make complaints to regulators	

User behaviors, attitudes, and vulnerabilities

How do we use our IoT devices? Do we do everything we can to protect ourselves? Our survey of 7,000 respondents, spread evenly across Australia, Canada, France, Germany, the Netherlands, UK, and US, revealed some predictable and some surprising differences between the habits of different groups.

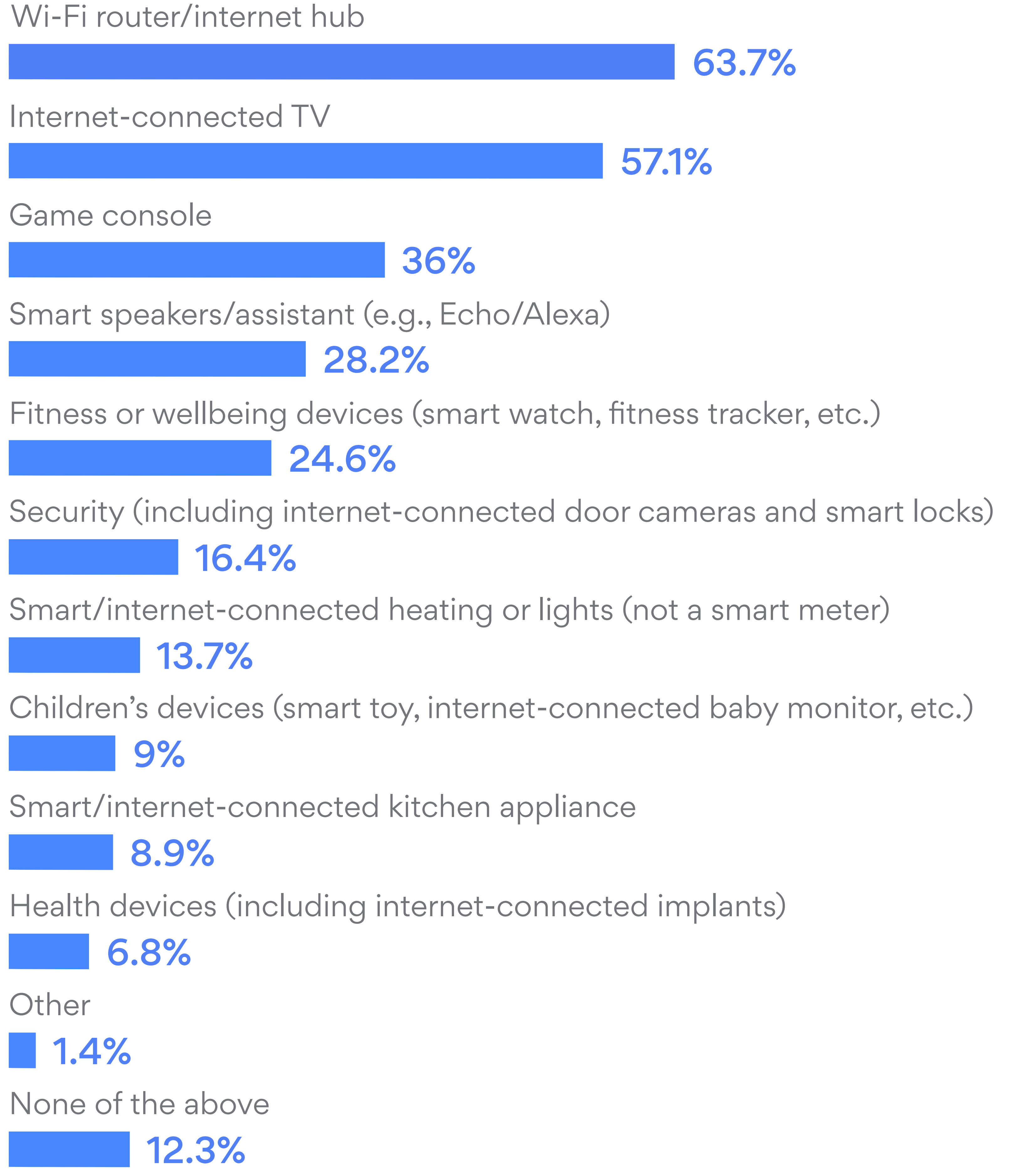
What devices are in our homes?

Overall, the vast majority of us have some kind of IoT or connected devices in our homes, even if it's just a router. In fact, only 12.3% of people surveyed did not have any of the listed devices. This highlights the importance of IoT security, which is worrying given the number of unsecured devices still online. Women were more likely not to have any IoT devices in their homes (14% vs. only 10% of men), and this was most pronounced in France (27% vs. 19% of men). The number of people without any devices was generally higher in France too (23% vs. the average of 12%) and also a bit in the Netherlands (16%). The UK and Canada saw the most prolific use of IoT devices, with only 5% (UK) and 8% (Canada) of people saying they had none of the devices in their homes.

Gender differences overall were not that pronounced. Men are slightly more likely to have IoT or connected devices, except for fitness and children's devices (including monitors and toys), although there were some minor variations between countries. In Australia, for example, men are significantly more likely to have most devices. For example, they are twice as likely to have connected security or heating/lighting and three times as likely to have connected health devices (like implants) or kitchen appliances. Another notable exception is that, in the Netherlands, women are more likely to have game consoles at home (29% vs. 20% of men in the Netherlands).

Factors of age were not surprising. Younger age groups (18-24 and 25-34) were more likely to have smart speakers, game consoles, and children's devices. Internet-connected TVs peaked for middle-age groups (35-44 and 45-54), perhaps due to younger groups being more likely to stream via other devices, like laptops or phones. The likelihood of someone

Which of the following IoT (Internet of Things) or "smart" devices do people have at home?



having no devices at home went up with age. Similarly, the number of devices also went up with income, and this was more pronounced with devices that were more part of the house itself, such as security or heating and lighting. But even in the least financially secure group, more than 1 in 5 had a smart speaker and almost a half had a smart TV.

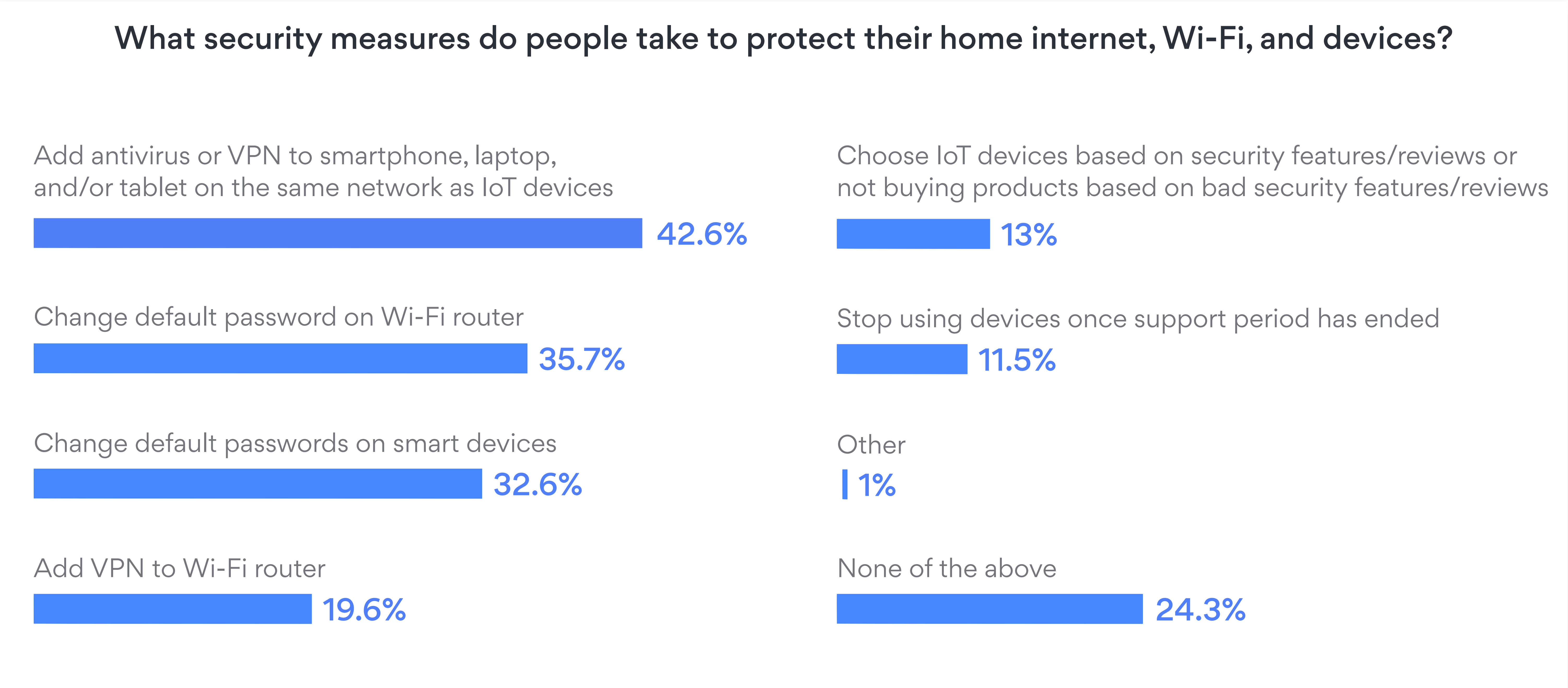
Canada, the UK, and Australia had an above average percentage of people with devices of different types. In Australia, there was a focus on health, fitness, and children's devices, while smart speakers were not as popular. Figures for the US were mostly close to average, while Germany, France, and the Netherlands had fewer devices. There were a few exceptions, such as connected heating or lighting being more common in the eco-conscious Netherlands. The only type of device that France had the most of was connected kitchen appliances — not surprising, perhaps, in a country famous for its cuisine.

An interesting difference emerged with how many people had Wi-Fi in their homes. Age was a less overt factor. Those in the 45-54 age group were most likely to have Wi-Fi devices in their homes, whereas younger and older groups were less likely to have those. This could be due to less connectivity in older groups, while younger groups would be more likely to have mobile data or shared living arrangements where devices weren't as clear.

When looking at Wi-Fi devices among countries, again the UK and Canada had more of those, along with Germany. In all three countries, around three-quarters of respondents had a Wi-Fi router or internet hub in their home. France stood out here, with only 35% of people saying they had a Wi-Fi router or internet hub in their home — this is despite France having notably good broadband coverage. This could be for a number of reasons. Many French users have "triple play" boxes, such as the Freebox, which acts not only as your own Wi-Fi box, TV box, and home data storage but also as a Wi-Fi hotspot for others subscribing to the network. This could also mean that French respondents didn't see any difference between devices.
take into account the number of people without any devices (roughly 12%). However, while making some results less extreme, the number of people with no devices doesn't significantly affect the overriding trends across gender, age, or financial situation. Breaking results down by country, however, is affected by this adjustment, and is discussed in more detail below.

The most common way of protecting devices was not actually protecting IoT devices at all. Antivirus and VPNs are already common ways of protecting laptops and smartphones, and this includes protecting them against compromised devices on the same network. If a hacker can get into an IoT device which has less security, it can give them a foothold in the network, so having extra protection on our more complex or sensitive devices is always a good measure.

How do we use our IoT devices? Do we do everything we can to protect ourselves? Our survey of 7,000 respondents, spread evenly across Australia, Canada, France, Germany, the Netherlands, UK, and US, revealed some predictable and some surprising differences between the habits of different groups.



How do we protect our devices and networks?

IoT devices are increasingly present in our homes and lives. But are the relevant security and privacy skills also there and being used? Our previous research highlighted the importance of thinking about devices in shared settings, and that goes for IoT devices on home networks as well. Having any vulnerable devices is a risk to everything on the network, including things like your phone or laptop, which may have very important data. So, instead of taking measures that protect individual devices, we need to take those that protect the whole network.

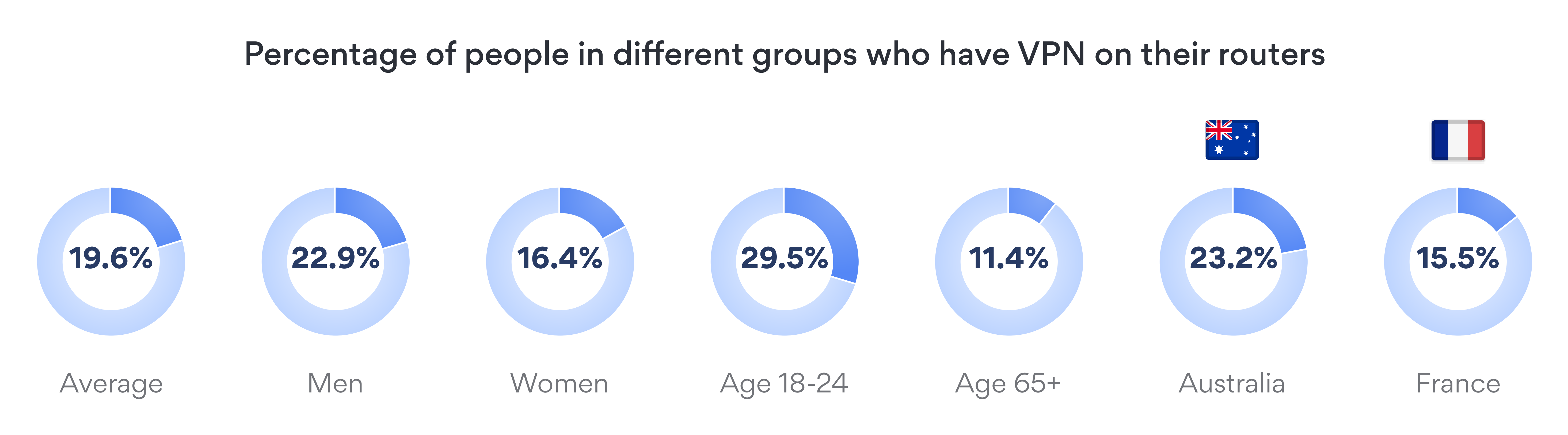
For the results of these questions, we need to take into account the number of people without any devices (roughly 12%). However, while making some results less extreme, the number of people with no devices doesn't significantly affect the overriding trends across gender, age, or financial situation. Breaking results down by country, however, is affected by this adjustment, and is discussed in more detail below.

The most common way of protecting devices was not actually protecting IoT devices at all. Antivirus and VPNs are already common ways of protecting laptops and smartphones, and this includes protecting them against compromised devices on the same network. If a hacker can get into an IoT device which has less security, it can give them a foothold in the network, so having extra protection on our more complex or sensitive devices is always a good measure.

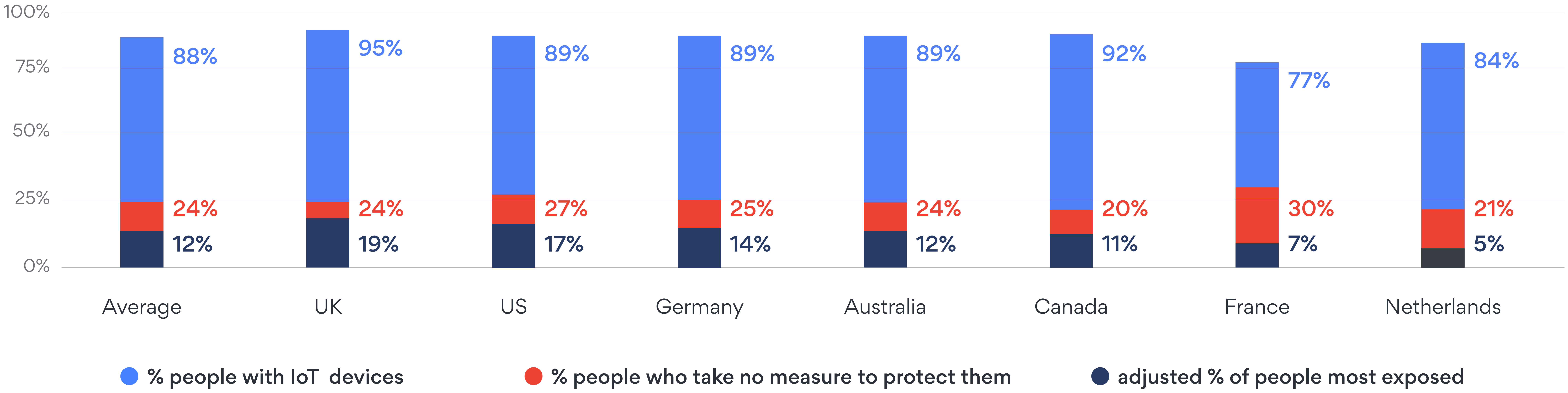
Around a third of people changed the default passwords on Wi-Fi routers and/or the smart devices. This number should be significantly higher, as it is an easy method of adding extra protection, particularly against some of the larger-scale attacks like botnets. It's something that should be recommended more clearly as an important part of setting up devices. The idea of "plug and play" might make devices seem easy to use, but, if changing the default password isn't part of the simple setup steps, then something needs to change.

Men were more likely to take precautions than women, consistently scoring at least 3% higher on whether they took each measure. This could be down to stereotypes of men being more likely to take charge of devices in the home, greater confidence in tackling IT issues, or greater access to skills and knowledge. In general, younger age groups were more likely to take measures, particularly the more involved ones, like adding VPN to routers (30% of 18-24-year-olds compared to only 11% of 65+). Similarly, those in more financially stable situations were more likely to take measures. We need to do more to make sure everyone is supported in protecting themselves and their devices.

Australians were the most likely to take several measures, including adding VPNs to their routers. They also scored highest in terms of taking security reviews into account before buying devices (18%) and stopping using devices after support finished (13.8%). France scored consistently under average among those surveyed. Besides, France (30.8%) and the US (27.1%) had the most people who took no measures. Once we adjust for respondents without devices, this drops to only 7% in France but is still 16.5% of people in the US. Using adjusted numbers, the Netherlands performed best, with only 4.6% of people taking no measures to protect their devices. Using the same adjusted numbers, the UK was surprising and worrying, with almost one in five people (18.5%) having devices but taking no measures to protect them. The UK has high device coverage but low behaviors, which could be why the UK government has recently been working on its own [recommendations for better IoT practices](). Other countries' results were mixed, suggesting that more needs to be done to promote the full range of behaviors across different contexts.

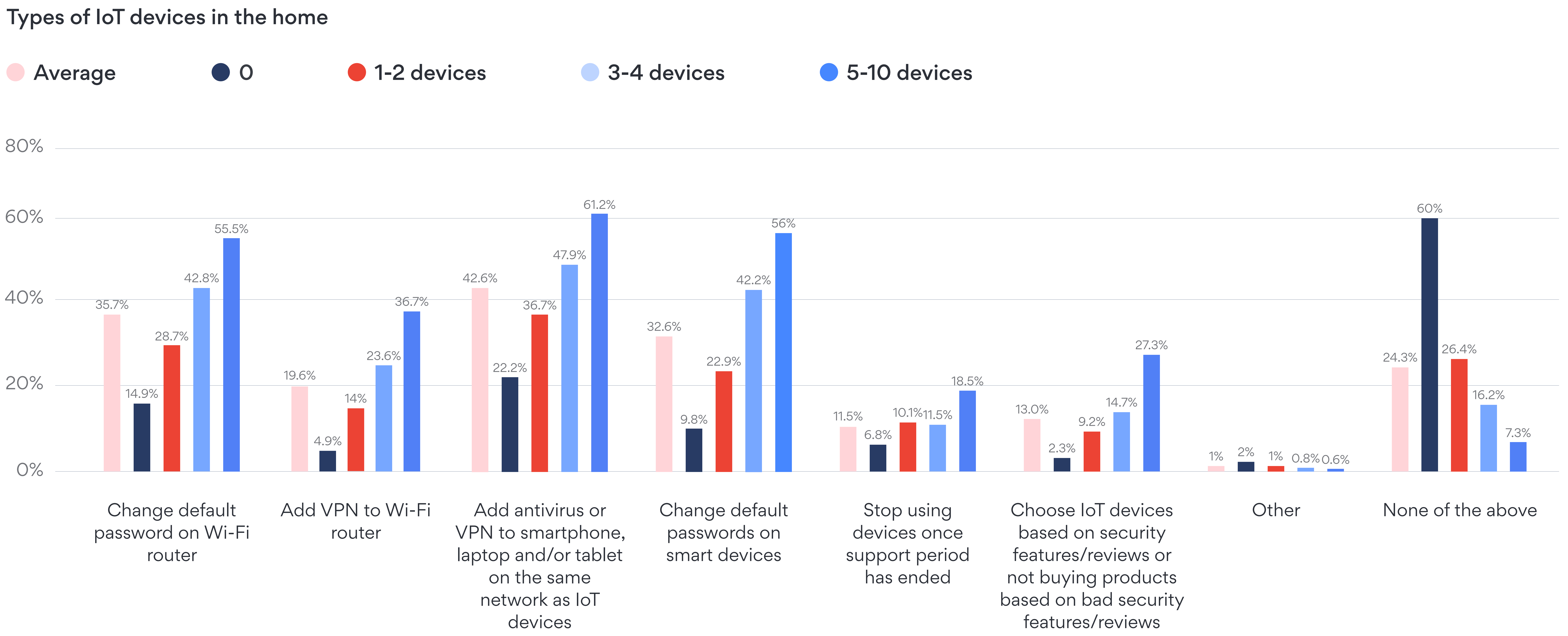


Percentage of people with IoT devices who take no measures to protect their IoT devices or home networks, and adjusted percentages of those most exposed (those taking no measures, not including those without any devices)



Does having more devices put people at more risk? On a technical level, the more devices you have, the greater the risk, and this also depends on what particular devices you have and how secure they are. But how does the number of devices in our homes relate to our behaviors? Our surveys showed that those with more devices took significantly more measures to protect them (only 7% took none, and they were well above average across all measures). But the largest group, making up over one-third of respondents, was those with only one or two types of IoT devices, and these people were more likely to take no measures (over 26% took none, and this group was below average on all measures). While this may be expected — the more into devices you are, then maybe the more likely you are to look after them — it still raises concerns. Particularly in countries like the UK, with many more people having at least some devices, this suggests that there are large numbers of more casual device users who may only have a few devices but take fewer measures to protect them. Depending on what type or make of device these users have, this could lead to significant security and/or privacy risks.

What security measures do you take to protect your home internet, Wi-Fi, and devices?



Breaking this issue down by types of devices, we see that those with smart TVs are the least likely to take measures (18% took none), followed by those with game consoles (15%), smart assistants (15%), and fitness trackers (13%). Given the potential security risks with smart TVs and the privacy risks with fitness trackers and smart assistants (which have come under a great deal of scrutiny for data practices), this is concerning.

People with connected health implants or children's devices, followed by those with security devices, tended to have better behaviors, which makes sense given the more critical nature of these devices. But having even one seemingly harmless unsecured device can lead to further problems, particularly if it allows an attacker to break into other devices on the network or gives away private information.

Overall, it is perhaps worrying that around a quarter of people surveyed (24%) took none of the listed steps to protect their devices and networks. Even taking into account those with no devices, who don't need to protect anything, this still leaves around 12% of people as highly vulnerable.

What attacks are people vulnerable to?

Based on our study, we can combine the user survey data and taxonomy of vulnerabilities in context to outline which vulnerabilities people are most exposed to. Focusing on the problems that users can mitigate, the vulnerabilities are cross-referenced with the average percentages of people in our survey who take those measures, adjusted for those without any devices. The table below shows these results.

Vulnerabilities	% of people exposed	Key measures
Malicious devices	52%	Change default passwords
MITM	52-68%	Change default passwords; VPN on router
DoS	68%	VPN on router
RFID	52%	Change default passwords
Routing	52-68%	Change default passwords; VPN on router
Encryption	75%	Review before buying
Malware	52%	Change default passwords (among others)
Programming	75%	Review before buying
Authentication	52%	Change default passwords (among others)
Deprecation	76%	Stop using device
Social engineering	12-76%	Careful behaviors (doing some or all)
User OpSec	12-76%	Careful behaviors (doing some or all)
Privacy	75%	Check policies (review before buying)

Attacks that are a particular concern include those introduced via deprecation. Once we have spent money on a device, we aren't as likely to abandon it even if the support period has ended. This is a particular concern for those with smart assistants, game consoles, smart TVs and fitness trackers. While smart assistants are likely to simply stop working once support has stopped (if the cloud services they rely on are withdrawn, for example), smart TVs and even fitness trackers can potentially carry on working for years, picking up more vulnerabilities over time if they are unsupported and, therefore, unpatched. And for fitness trackers that connect to a smartphone app this adds an extra layer of security risk.

People also need to increase the time they take looking into devices before buying. Many vulnerabilities stemming from poor security practices on the part of the manufacturer can be avoided by checking reviews for security and privacy features. Again, those with smart assistants, game consoles, smart TVs, and fitness trackers were least likely to check before they bought. Given the increasing ubiquity of these particular devices, more needs to be done to provide access to easy-to-understand reviews that take security and privacy into account. And, if we only buy devices with good security reviews, it may mean that we have to avoid cheaper devices, but it is likely better to have no device at all than one that puts your entire home network at risk.

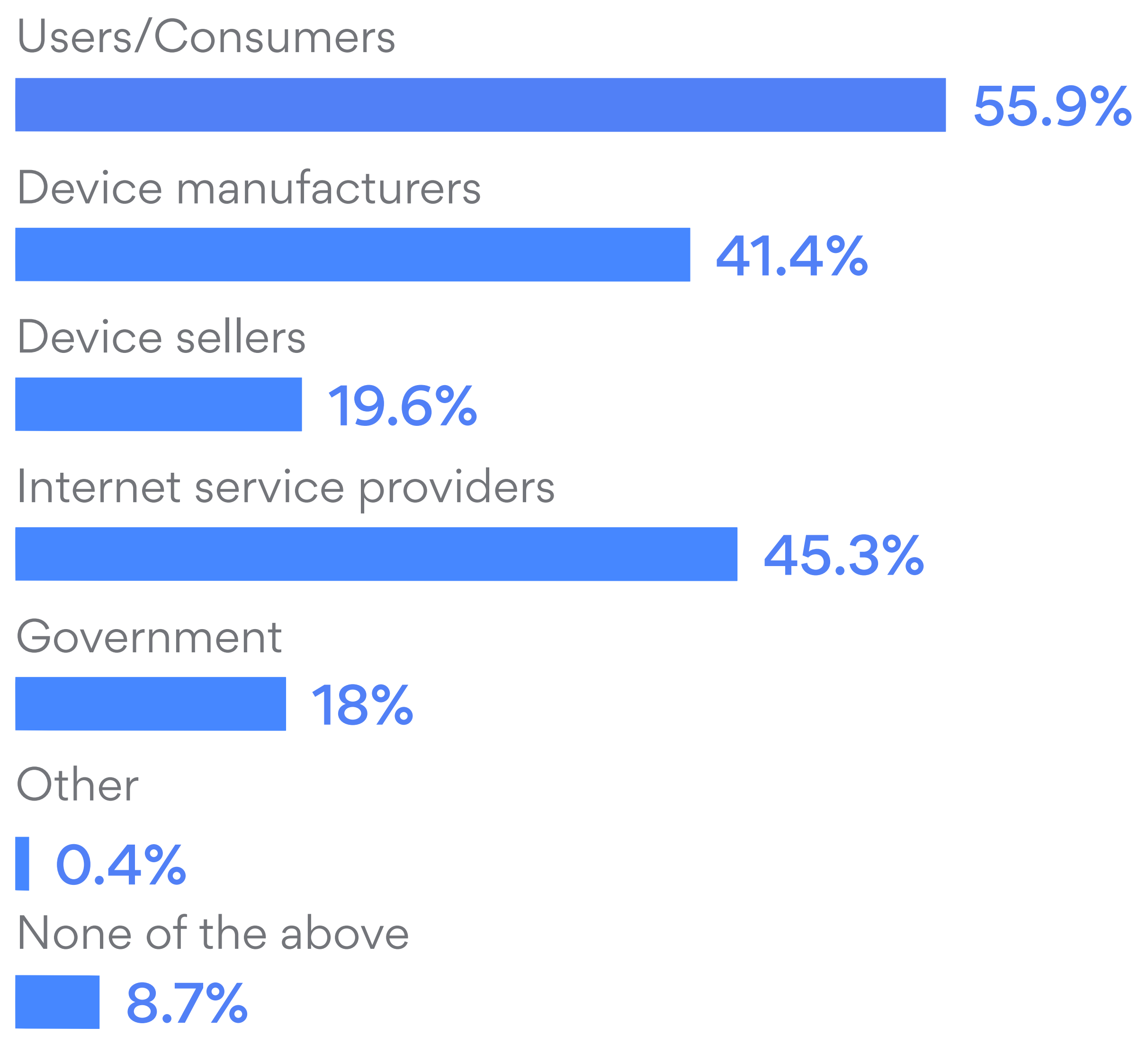
Another key area of concern are the potential problems even when the device is working as intended. IoT devices by their nature collect and send data. But what data are they collecting? Where are they sending it? Are they keeping it safe? Smart assistants, for example, could be listening at any time and might be sending that information to servers or contractors all over the world. Part of checking a device before buying it is looking into privacy policies and the data practices of the service. Considering how many of us have devices like smart speakers and voice assistants, this is creating potentially massive data breaches just waiting to happen.

Who should be responsible for IoT security?

We have looked at what users can and should do to protect their devices. But, if some vulnerabilities are there even when the devices are working properly, what do people think about the responsibility of different organizations when it comes to securing the Internet of Things?

56% of the people surveyed thought that users themselves were responsible for securing their IoT devices. This was as high as 61% in the 45-55 and 55-65 age groups, but much lower in younger (45% for 18-24-year-olds) and less financially secure (48% of those who lack money for some essentials) groups. It's true that there

Whose responsibility is it to protect the security of IoT and smart devices?



are steps users can and should take to protect themselves. Those with more devices (who also tended to have better behaviors) tended to place more responsibility on themselves (68% of people with 5+ types of devices). This was most pronounced in Canada and the Netherlands, where 74% and 72% respectively of this group put responsibility on users — significantly more than the responsibility they placed on others.

It is disconcerting that we tend to place so little responsibility on the people actually making the devices. Only 41% of the people surveyed thought device manufacturers were responsible. In fact, overall, more people (43%) thought Internet service providers (ISPs) were responsible. While possibly misplaced, this suggests that users understand the importance of secure networks to support their devices. But, if ISPs don't consider it their responsibility, then this is an area where tools such as VPNs can certainly make a difference.

There were some differences in terms of where people thought responsibility should lie. The UK, Canada, and US placed the highest responsibility on users (over 60% of people in each country), while Australians were more varied in who they held responsible, with more people placing the burden on device sellers (23%) and governments (24%). It might not be surprising that people in the US put low responsibility on the government (13%), but this was fractionally lower still in the highly regulated Germany.

Tech critics, researchers, and regulators often talk about a "privacy paradox" — a gap between our attitudes and behaviours. This means that we are aware of and concerned about privacy and security risks of technology, but we don't necessarily do anything about it. Sometimes this is pinned on a "third-person effect", when we assume attacks happen to other people, not us, so we don't make the effort to protect ourselves. Unless we have suffered a privacy breach ourselves, it can be difficult to persuade us to change our behaviors.

But this privacy paradox has recently come under criticism. The argument is that attitudes and behaviors occupy two different spaces. Our attitudes refer to concepts such as rights and responsibilities and apply to broader social contexts. Our behaviors are focused on the specific habits of our daily lives and things we feel we can personally control. Placing too much emphasis on converting attitudes into behaviors can lead to people feeling helpless and then not taking any action, like seeing news about surveillance and then using weaker passwords.

The issue at stake is locating the right kinds of responsibility in the right place so that the right people can take the right action. To do this, we need to rethink how we classify IoT vulnerabilities and remedies.

How to protect our IoT devices

With the number of IoT devices in our homes being on the rise, many of us are worried about them and are looking for ways to improve their security and privacy. Some behaviors should be our responsibility. Others are sensible things we can do to protect ourselves from privacy-invasive policies or substandard security design. There are a number of things we can do to our devices and routers that can help.

Devices

- Check before you buy. Do you look further than the number of stars a product receives? Many tech sites dig into privacy and security issues, so try to look for reviews that specifically mention these things, or buy devices certified by organizations like ioXt.

- Privacy policy and other terms and conditions are often long-winded and written in complex legal language, but it's worth checking them. Again, some tech or research sites help make these easier to understand.
- Change default passwords. Default passwords are a source of some of the biggest vulnerabilities. Creating stronger passwords for your devices is a great step to keeping them more secure.
- Keep devices patched and up to date. Don't fall victim to out-of-date vulnerabilities — check if your devices update automatically. If not, make sure they are running the latest firmware.
- Turn off features you don't use. Having unused features running in the background opens up unnecessary vulnerabilities or privacy issues.
- Check the support lifetime. How long will the manufacturer support updates for the device? Is the company likely to go under? What happens to your data and support afterwards?

Routers

- Change default passwords. Just like with devices, this is a major risk that can be easily fixed.
- Consider setting up separate local networks for your main devices (laptop, computer, phone), your IoT devices (TV, heating, cameras), and guests. This not only protects your devices from each other, but also helps if someone else on your network has problems.
- Install a VPN on your router. This is a great way to protect your network and devices. VPNs can help prevent man-in-the-middle attacks by encrypting your traffic and it covers many of the issues with poor encryption on IoT devices. VPNs can help prevent botnet and other attacks by hiding your location and making it more difficult for attackers to find your network or devices. Many people recommend VPNs as an easy measure to provide significant protection for IoT devices and networks.

Social measures

- Help others. We all need a bit of help sometimes. Sharing advice and knowledge means we can all be safer with our devices. If you visit a friend or family member and they have an unsecured Wi-Fi connection or similar issues, point them in the right direction to find the information they need.
- Put pressure on those responsible. Don't be afraid to make complaints, be it directly or on social media, to companies making devices and politicians writing regulations. IoT is a fast-moving area, and there is a lot of activity going on. But some organizations need a push to get up to speed.

Conclusion

Connected devices present vulnerabilities from the home all the way up to smart cities. It is essential that greater emphasis be placed on the specific security and privacy issues and needs for the IoT. Researchers have been pushing this for years, and there are trustworthy manufacturers out there (though even well-known brands often have problems). Regulators have also been starting to catch up. But the IoT is still full of holes, and there is a lot of work to be done.

There is a need to make the different roles and responsibilities clear to users, companies, and regulators. This includes, to **users**:

- What aspects of security and privacy are the responsibility of users and what behaviours they should adopt;
- What aspects of security and privacy are useful additions for users. It might not be their responsibility, but users can adopt additional

behaviors to protect against flaws by other parties;

- What pressure needs to be put on other parties to take responsibility and action, whether this is pressure on politicians for better regulation or pressure on companies to make better devices (which includes “voting with your wallet”).

To **device manufacturers:**

- What the responsibilities are to protect devices against vulnerabilities, especially known vulnerabilities with standard solutions;
- How to prioritize security and privacy by embedding best practices in their internal processes. This includes when off-the-shelf or standardized solutions are available;
- What the penalties are for failing to take these responsibilities seriously, whether that is market pressure or regulatory pressure.

To **regulators:**

- What the needs of manufacturers and users are to improve security. This includes access to information and support for skills;
- What best practices are needed and enforcing these standards;
- What sociotechnical considerations need to be considered when developing new standards and regulations. This includes engaging with users, manufacturers, and the research community to take a more holistic approach, as well as thinking carefully about how IoT security fits into other government aims such as digital economies, smart cities, and data-driven society.

Together, the security and privacy of IoT devices can be enhanced. It may likely never be fixed, existing as a loose set of practices and standards across global contexts. But, if everyone takes responsibility for the parts they can achieve, and if everyone has the information, skills, and tools they need to do this, then the IoT can certainly be made much safer than it is now.

What does the future look like for IoT?

The IoT boom is not likely to slow down any time soon. Statista reports that worldwide IoT spending may reach over $1 trillion by 2023. Devices are selling rapidly, and governments are keen to promote digital and data-driven societies. The biggest growth areas are connected industry and smart cities. The continued growth is likely to bring with it more vulnerabilities. This includes issues with specific devices but also larger vulnerabilities or attacks that are yet to be discovered. However, it’s not all doom and gloom. Here are some of our more positive predictions:

- Better standards, particularly as the bigger tech companies dominate the market;
- Better regulation, as governments start to catch up with technological developments;
- Better awareness, as researchers make issues known and users level up their skills.

We will still need to watch out for more systemic issues like privacy and monopolization. And we all need to watch our own behaviors to keep ourselves, our homes, and our data safe.