Computer Fraud & Security
ISSN (online): 1873-7056

Consumer trust and perspectives on cyber security

CHRIS DIMITRIADIS
ISACA

Abstract: When your networks are breached, you may lose more than your data. Customers are increasingly wary of doing business with organisations that have been hacked. The reputational damage can last a long time – perhaps longer than the business itself.

Cyber security is commonly associated with major attacks on large organisations, and they are only becoming more frequent as cyber criminals adopt more-sophisticated technology and business operations are digitalised, widening the area of attack. This is particularly concerning for consumer-facing businesses whose customers are put at risk from attacks. Recent notable examples include a ransomware attack on Hackney Council that cost in excess of £12m; a data breach at Revolut that exposed the personal information of more than 50,000 customers; and more recently, a cyber incident at Royal Mail that prevented it from sending letters and parcels overseas.[1–3]

For these companies, cybercrime is not simply a matter of security – suffering from an attack is a serious reputational issue for the wider business that can create lasting damage to the bottom line.

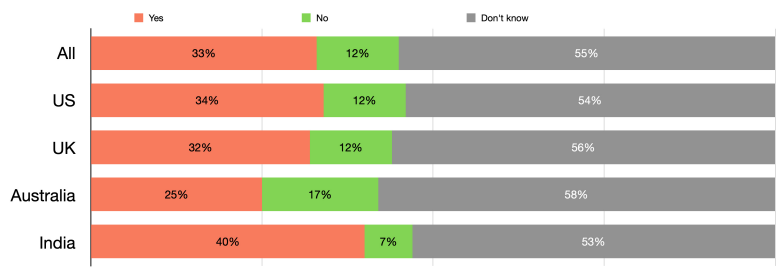
ISACA's report, 'Cyber security 2022 and Beyond: a consumer perspective', demonstrates that customers often rethink their relationships with businesses that have been attacked, or even neglect to buy into brands in the first place if they have a history of hacks and data breaches.4 This sentiment resonates on a global scale: 34% of North American consumers, 32% of UK consumers, 25% of Australian consumers and 40% of Indian consumers all claim to have stopped doing business with companies whose customer information has been compromised.

The lack of a strong cyber security team and framework can therefore hinder a business's wider strategic objectives if it cannot adequately protect itself and its customers. As businesses of all types become more reliant on digital processes, cyber security is increasingly becoming a key priority for enterprise leaders.

Cyber-conscious consumers

New research suggests that cyber attacks on UK businesses are becoming more frequent – and these aren't going unnoticed by consumers.5 ISACA's research reveals that – across all genders and age groups – 71% of UK consumers believe there has been a significant increase in cybercrime in the past year. As a result, consumer confidence is low, with 57% expressing concern that a company they do business with could be a victim of cybercrime within the next 12 months.

Figure: Percentage of consumers who stopped doing business with company whose customer information was compromised.



Source: ISACA.

There is a sense of helplessness among the consumer base: while people are aware that some of the companies they do business

with are likely to suffer from a cyber attack, 26% of consumers are not at all confident that these businesses can safely secure their personal identifiable information (PII). A further 27% of victims agree that there is nothing that they can do or use to protect themselves from cybercrimes.

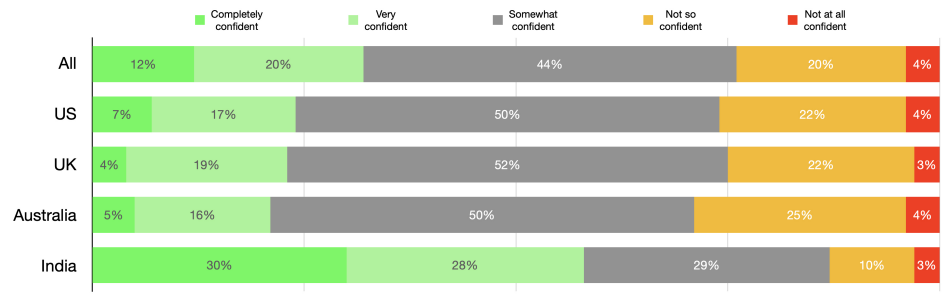
With growing awareness, consumers understand that cyber attacks are a reality and are looking at how businesses protect their data with a more critical eye. Retail banking offers a good example – in recent years several disruptor banks with significant market share have suffered security breaches. Without an in-person branch, consumers are expected to put all their trust in the digital capabilities of these banks, and failing to demonstrate these capabilities can quickly erode consumer confidence.

Transparency breeds trust

Consumers are right to demand more from suppliers. For businesses that are unable to demonstrate their ability to manage the threat landscape, there is a risk that customers may take their business elsewhere in a bid to obtain greater security. In fact, 32% of UK consumers report having severed ties with a company known to have experienced a breach.

Transparency is at the heart of any trusted relationship, yet the majority (66%) of UK consumers think businesses are under-reporting cybercrimes. While there has been progress in recent years, among some businesses there is still a tendency to view cyber attacks as a technology incident rather than a direct attack on the business with potentially serious implications for its customers and employees.

Figure: How confident consumers are that businesses can safely secure personal information.



Source: ISACA.

Some organisations have even been under attack without realising it, as they do not have the necessary detection controls in place to gather intelligence to raise the alarm. Many organisations neglect to consider the historical approach to data privacy of the businesses they partner with, leaving them vulnerable to attacks within the supply chain.

And this is not just smaller businesses. Large corporates and public sector organisations, such as the NHS, are burdened with legacy systems and may have massive gaps in their infrastructure. This gap in knowledge is preventing businesses from building trust with their consumers on the basis of their ability to protect their data and PII.

Companies should communicate with their customers from a place of transparency and education. The general public lacks knowledge about the threats themselves and the technology behind them. For example, companies that produce and use artificial intelligence and new technological capabilities that we use every day are often not transparent about how their algorithms work. While AI is beneficial, it introduces new risks, especially if it lands in the laps of bad actors. The responsibility lies with businesses that produce AI to educate the rest of the world on exactly how it works. At the same time, consumers need to demand more ethical principles and laws to protect them from the dangers of new technology – which includes placing more demands on the companies they do business with.

Invest in talent and tech

To close these gaps, investment is needed in both human capacity and talent, awareness, and expertise as better security is a fundamental part of a business's duty of care to its customer base. Studies have shown that 95% of cyber security breaches are caused by human error, which explains why 62% of UK consumers are more confident doing business with companies that hire certified cyber security professionals.6 Consumers are also calling on businesses to be independently graded on data security

practices, and for these scores to be made available to the public.

While cyber security is increasingly being prioritised at board level, businesses need to put the right talent in place to ensure that the implications of an attack can be explained to decision-makers in simple business terms. If active engagement with cyber security is demonstrated among business leaders, then it will trickle down throughout the company, and both the business and its customers will be better protected in the future.

Creating digital trust

Digital trust means having confidence in the integrity of relations, interactions and transactions among providers and consumers within an associated digital ecosystem. It is a driving factor in consumer decisions and enterprise resilience in a digital-dominated environment. Most businesses (84%) see digital trust as important, as reported by ISACA's latest digital trust survey. What's more, 65% say digital trust is relevant to their jobs and 86% say digital trust will be even more important in five years' time than it is today, as they prioritise digital transformation, customer confidence and business security.

Just one breach of digital trust can have a devastating impact on a business. Survey respondents recognise that organisations with low levels of digital trust suffer from reputational decline (66%), more privacy breaches (56%), more cyber attacks (54%), customer loss (54%), and unreliable data (47%) among other consequences. However, many have yet to grasp the steps needed to get to a mature state of digital trust, which could have serious reputational, regulatory and financial repercussions.

In fact, fewer than one in 10 (8%) of European organisations has a dedicated role for digital trust and only a quarter (27%) offer digital trust training to staff. Skills and training are just two of the reasons that businesses aren't making progress, but lack of alignment with business goals (42%), lack of leadership buy-in (37%), lack of budget (37%) and lack of technological resources (30%) are also having a significant impact.

Over three quarters (76%) of respondents see digital trust as important to digital transformation, which we know is a key priority for businesses. As a result, companies are making changes to their internal structures as only 29% say their organisation will likely have a senior staff role dedicated to digital trust in five years.

The top three components of digital trust are security, data integrity and privacy, according to respondents, but fewer than half agree that there is sufficient collaboration among professionals in these and other digital trust fields.

The top three roles for strengthening digital trust are IT strategy/governance (85%), security (82%) and IT (69%). Many organisations are still in the early stages of digital transformation, so the demand for digital trust provides an opportunity for professionals to step up, gain knowledge and lead a multi-disciplinary team.

Digital trust must be backed by every corner of an organisation. Every department must embed policies into its activity and determine how it can promote digital trust among both customers and employees. Those organisations that keep digital trust front of mind are far more likely to see their business go from strength to strength and see the value of their investments.

Given the evolving nature of cyberthreats, demonstrating robust cyber security will need to be a key priority to maintain customer trust moving forward. For this to be achieved, organisations need to take a holistic approach that combines cyber security with the adjacent domains of audit, risk, privacy and technology governance.

Figure: Chris Dimitriadis, ISACA

About the author

Chris Dimitriadis is the chief global strategy officer at ISACA, an international not-for-profit association with more than 220 chapters, serving more than 160,000 IT, cyber security, information security, audit, risk and compliance professionals.

References:

1.'Hackney Council spent over £12 million to restore operations following a 2020 ransomware attack'. Teiss, 19 Oct 2022. Accessed May 2023. www.teiss.co.uk/news/hackney-council-spent-over-12-million-to-restore-operations-following-a-2020-ransomware-attack-11035.

2.Moulds, Karen. '50k customers of Revolut affected by phishing data breach'. Intercede, 24 Nov 2022. Accessed May 2023. www.intercede.com/50k-customers-of-revolut-affected-by-phishing-data-breach/.

3.'Royal Mail ransomware attack timeline'. Cyber Management Alliance, 7 Mar 2023. Accessed May 2023. www.cm-alliance.com/cyber security-blog/royal-mail-ransomware-attack-timeline.

4.'Cyber security 2022 and Beyond: a consumer perspective'. ISACA. Accessed May 2023. www.isaca.org/resources/ebook/cyber security-2022-and-beyond-a-consumer-perspective.

5.Kelly, Ross. 'Cyber attacks on UK organisations surged 77% in 2022, new research finds'. IPPro, 6 Jan 2023. Accessed May 2023. www.itpro.com/security/369813/cyber attacks-on-uk-organisations-surged-77-in-2022-new-research-finds.

6.'After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk'. World Economic Forum, 17 Dec 2020. Accessed May 2023. www.weforum.org/agenda/2020/12/cyber-risk-cyber security-education.

Computer Fraud & Security
ISSN (online): 1873-7056

Are we smart enough for smart technology?

SAREENA HEER

SAMIAH ALGHAMDI

STEVEN FURNELL
University of Nottingham

Abstract: It's common to find any number of 'smart' devices in the modern home, with the most common being so-called smart speakers. Despite their huge popularity, people often view these devices with at least some degree of suspicion, with concerns about security and privacy. With this in mind, this article presents the details of a study conducted among current smart speaker users to examine their awareness and understanding of the security and privacy aspects of the devices that they are already using.

The smart device has become the public face of the technologies that represent the wider growth of the Internet of Things (IoT). Many familiar consumer-level devices now have a 'smart' counterpart, with televisions, vacuum cleaners, doorbells, lighting, refrigerators and other appliances now readily falling into the category, with all of them contributing to the wider notion of the smart home (while also acknowledging that some of the devices also get deployed in other contexts).

However, the most common incarnation of the smart device is smart speakers, which are now claimed to have a worldwide base of over 170 million units and are predicted to increase to over 300 million by 2027.1 Despite their popularity, however, prior research has determined that users are concerned about the privacy offered by these devices, although they often fail to do anything about it.2 Nonetheless, findings have highlighted issues around the privacy and permission settings of smart speaker devices, particularly in relation to the privacy paradox and the end-user's ability to manage the tension between privacy and personalisation.3

The prior findings have suggested that the ability to configure settings is variable and dependent on technological literacy. This implies that research needs to be conducted whereby the factors causing inequality in technological literacy are considered. Moreover, it can be acknowledged that demographic factors impact technological literacy. Many previous studies only considered young male participants, thus focusing on individuals with similar demographic characteristics. Therefore, there is a need for research to consider participants with a broader range of demographic characteristics.

The disparity between worries around privacy and the lack of action to minimise privacy-related threats is termed the 'privacy paradox'. A key reason for it is that users are concerned with the improved convenience and connectedness offered by a device and dislike taking too long on configuring settings, and this essentially outweighs the concern over privacy threats.4 It is also well recognised that users often lack the inclination to read the terms and conditions, and that those who do read them might be discouraged by the complexity of technical language, which end-users might misunderstand.5 Such misunderstanding may, in turn, lead to the misconfiguration of settings, such that they are not correctly aligned with the intention of the user.6 A final reason for failing to read the terms and conditions of privacy settings is that end-users may trust the manufacturer or service provider to safeguard their personal information.7

The user perspective

A prior study has evaluated the extent to which security- and privacy-related information is promoted to users at different stages of the purchase and ownership cycle.8 In this earlier work, we sought to benchmark what users could determine about the devices from different online sources, assessing whether there was coverage of security and privacy aspects as part of the manufacturer's product web page, the user manual, and a 'frequently asked questions' (FAQ) page or similar (noting that in the case of coverage on the product web page, it was not expected that such issues would be discussed in operational detail, and the assessment instead considered whether they were tangibly highlighted in some way as features or issues to consider with the devices).

The evaluation considered six categories of smart home device – TVs, speakers, thermostats, robotic vacuum cleaners, smart video doorbells and displays – with 2-4 example products then being considered in each case and encompassing a cross-section of manufacturers with large, medium and small market shares in smart homes. Table 1 summarises the overall findings. The ticks

and crosses denote whether security/privacy-related information was identified at each stage (a dash indicates that the associated element was not available for assessment).

Figure: Encountering security/privacy information at different stages.

Category	Device	Assessed Element		
		Product web page	User manual	FAQ page
Speaker	Echo Dot	×	×	✓
	HomePod	✓	✓	✓
	Nest	×	✓	-
Thermostat	Amazon	×	×	-
	Netatmo	×	×	×
Vacuum	Eufy	×	×	×
	Ecovacs	×	×	×
	Wyze	×	×	✓
	iRobot	×	×	×
Doorbell	Netatmo	×	×	✓
	Eufy	×	×	-
	Ring	×	×	×
Display	Nest Hub	×	×	-
	Echo Show	×	×	✓
	Portal	×	✓	✓
TV	Sony	×	×	✓
	Samsung	×	✓	-

The results as a whole clearly suggest a level of variability in whether users are likely to find themselves presented with security- and privacy-related information, which in turn may affect the extent to which this becomes a consideration in their mind when buying and installing their device. As seen in the table, smart speakers tended to fare better than most categories in terms of attention being highlighted, but this of course only represents the first step towards users actually being aware and taking any related actions.

The same study then sought to determine the ease (or otherwise) with which users may be able to perform a series of security/privacy-relevant tasks, with smart speaker platforms being selected as the target of analysis. The investigation considered tasks relating to controlling the devices' listening and recording capabilities, controlling purchases, location-based services, software updates and voice recognition. In the vast majority of cases, whether using the Amazon, Google or Apple smart speaker platform, users would find themselves in a multi-step activity in order to complete the task (eg, the task of 'deleting all recordings' involved an eight-step process in both the Amazon and Google apps used to manage the devices; and even this assumes that the user has selected all the options in the right order to reach the final step).

From these findings, it becomes clear that users may face challenges in becoming informed about the security and privacy aspects of their devices, as well as in putting related actions into practice. With this in mind, it was relevant to further investigate the experience from the user side and we sought resulting input from a series of established smart speaker users in order to get a sense of their perspective.

User attitudes and practices

The participants involved in the study are summarised in Table 1 and the participant numbers are used later in the discussion for attribution of interview quotes. Participants were selected based on owning Amazon and/or Google smart speakers, with a mix of genders, ages ranging from 18 to 56 years old, and variation in the level of self-declared technology literacy.

Data was collected via online semi-structured interviews to develop an in-depth understanding of participants' views, along with a short interactive exercise to determine their knowledge and understanding of smart speaker settings. Primary data collection occurred over two weeks in mid-2022 and involved a total of 15 interviews. This was considered a sufficient sample because previous studies have identified that data saturation is often reached beyond this point (ie, there is no additional benefit in conducting more interviews, as no more useful information will be found).9

Table 2: Overview of interview participants and smart speaker ownership.

Participant	Gender	Age category	Smart speaker brand(s) used	Total in household
1	Male	Teens	Amazon, Google	3
2	Female	Teens	Amazon, Google	3
3	Male	40s	Amazon	5

Participant	Gender	Age category	Smart speaker brand(s) used	Total in household
4	Male	50s	Amazon	1
5	Male	20s	Amazon	1
6	Female	20s	Amazon	1
7	Male	20s	Amazon	1
8	Female	20s	Amazon	5
9	Male	20s	Google	1
10	Female	40s	Amazon	2
11	Female	50s	Amazon	2
12	Female	20s	Amazon, Google	2
13	Female	20s	Google	6
14	Male	20s	Amazon	1
15	Female	20s	Amazon	4

Each of the interview sessions was structured as follows:

Smart speaker usage: A series of six questions that explored the participant's own understanding of what a smart speaker is, and their personal use of the devices (eg, how many they have, what brand(s), where they are located, and how many people use them).

Privacy aspects: A set of eight questions exploring the participant's perception and prioritisation of privacy issues and their awareness and assumptions about data collection by the smart speaker(s). Questions also investigated the extent to which participants were aware of privacy and permission settings and whether they had attempted to configure them (and, if so, their resulting experience).

Interactive tasks: An activity-based segment in which participants were asked to suggest how to perform certain privacy-related tasks via the user interfaces presented by two popular smart speaker brands.

Reflections: A final series of five questions, reflecting upon the interactive tasks and clarity of the information provided by the two platforms, as well as more general consideration of the participant's likely use of privacy and security settings in the future.

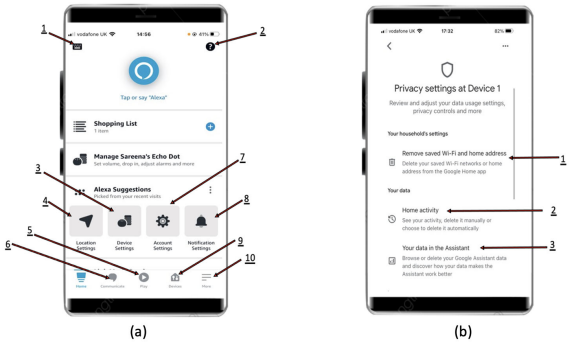
The interactive task phase involved the participants being presented with a series of privacy-related tasks on the Alexa and Google Home platforms (selected on the basis of being the two most popular brands). During the activity, the researchers shared their screen so that the participant could see mock-up screens of the Amazon Alexa and Google Home applications. In each case, a series of six Alexa and Google Home app interfaces were presented, and participants were then asked to identify the correct option to perform or progress a given task. The related tasks for each platform and the order in which they were presented, are listed in Table 3. Illustrative examples of the interfaces used in each task series are presented in Figure 1.

For each task, the researcher would ask the participant, “What option would you select to do [task]?”. The participants would then be given the chance to examine the presented interface and indicate the number corresponding to the labelled option that they would select. The participants were not able to seek help or guidance from the researcher, whose role was simply to present the task and collect the chosen response.

Table 3: Interactive tasks for Alexa and Google Home.

Alexa tasks	Google Home tasks
Accessing the privacy settings (two stages via different interfaces). Finding support on how to set up and edit the privacy preferences. Identifying the correct option to delete voice history. Identifying the correct option to set or edit different profiles. Add a voice ID for a personalised experience.	Accessing the privacy settings (two stages via different interfaces). Identifying the correct option to delete voice history. Finding help concerning privacy preferences (two stages via different interfaces). Identifying the route to start setting up ‘guest mode’.

Figure: Example interfaces presented for (a) identifying how to access Alexa privacy settings, and (b) identifying the route towards deleting voice history on Google Home.



With the inclusion of the discussion and interactive tasks, the interviews took an average of 15 minutes per participant.

Findings

The early background questions were used to both set the participants at ease and determine the basics of their smart speaker usage. The findings revealed that all had a good conceptual understanding of what smart speakers are and what differentiates them from normal speakers.

Across the group as a whole, there were variations in the number of devices they owned and whether they owned just one or both of the target brands. Devices tended to be placed in various locations, but users with a single device typically located it in the kitchen. In contrast, those with multiple devices found them spreading to lounges, family rooms and individual bedrooms.

The devices were generally used and accessible to multiple people across the household and the main reasons for adopting them related to convenience (especially evident where the purchase of one device had led to others) and curiosity, having heard about the technology from others.

Specific issues

When moving to the more specific discussions of privacy and permissions, one of the early questions explored the participants' prioritisation of privacy. The clear general view at this stage of the interviews was that it was something that mattered to them, as illustrated by the following quotes, each highlighting different perspectives:

"Yes, privacy is very important to me. I don't want my data to be collected and given to a third party whom I don't know about." (P2)

"I don't feel like enough light is shone onto the subject for people to actually have genuine concerns about it. Like there's a lack of representation of the privacy side of things, so people don't necessarily think it's an issue and I haven't thought it's an issue before." (P15)

At the same time, when it came to what their smart speakers were being used to do (and the data they required in order to do it), most participants were also well aware that a level of personal data was being collected was being used to profile them in terms of musical tastes. However, they were generally relaxed about this and indeed recognised it as a prerequisite for the smart speakers to offer some of the desired personalisation features:

"I think that that's part and parcel of having a smart speaker. You accept that that's gonna happen, but it makes your life easier." (P7)

"I'm happy for it to know where in the world it is and happy for it to know my email address etc … I don't particularly want it to know my daily routine, so I try not to let it." (P9)

"I'm aware that they can collect private data. And so I think the sort of information it collects would be like location, the time of day that you've been using it, the requests and responses that gives, and probably as well how long it's been turned on and that sort of thing and where in the house is. And all of those things don't really bother me. And yeah, not really fussed about that." (P13)

While this suggests a degree of comfort regarding trading privacy for features and convenience, multiple participants commented about related concerns. Chief among these was the potential for devices to be able to listen to conversations, with banking/financial data being a clear area of concern about what could be captured:

“The one piece of information that needs to be guarded on my behalf by that smart speaker is really just any banking information, any financial information, any other information … I'm not worried about the fact that the microphone's on all the time or anything like that … You know it can record what we're saying when we say it, but it's only from the banking point of view.” (P3)

“I'd like to know when it's listening and when it's not … Because you don't want it to pick up bank details or anything in the house” (P4).

“Like I hope it's not sort of recording the bank details.” (P7)

“They probably listen to what you talk about.” (P8)

“I Just found it a bit weird, that it was sort of listening in, but I think that it's OK … I understand they use for like target ads and stuff like that. But yeah, I think we've just sort of compromised on it.” (P12)

“I guess it is concerning when you hear about all the voice recognition stuff and how they take into account what you want for marketing but nah, nothing else. I don't think about it too much.” (P14)

Lack of understanding

Reflecting of the views expressed here, some comments perhaps suggest a lack of understanding about what the devices could really pick up from household discussions. If the devices *were* recording conversations, the likelihood is that most participants do not spend any time speaking about their bank account details anyway. Meanwhile, the smart speaker provider will typically have their customers’ bank/credit card details on file *already* as part of a subscription. By contrast, it is easy to imagine that if a smart speaker was being used as a general listening device, then all manner of personal insights could be gained that participants would not choose to divulge. As such, it would seem that participants’ instinctive concerns about their privacy tend to be misdirected.

It is also notable that the less IT-literate participants were unaware of both privacy settings and the fact that personal data was collected to some degree:

“It's not something I've ever thought about, I would rather have more privacy and less facilities … They don't have a photograph in there when I'm walking around naked in the kitchen do they?” (P11)

Having established a sense of their position on valuing privacy and protection, the discussion considered the extent to which participants had done something about it with the devices themselves. Here, there was a clear swing in support of the earlier-mentioned privacy paradox, with multiple participants indicating that they were *aware* of privacy and permission settings, but with few having *looked* at them or configured them beyond the defaults. Considering first the awareness of settings and having looked at them, the following quotes are typical:

“I would have assumed that they had them, but I've never really given it that much thought. I've never looked at the privacy settings. No.” (P2)

“I need to investigate more, I haven't looked at it enough at the moment.” (P4)

“I feel like I probably know that they have those settings, but I don't think I've ever looked them in great detail.” (P7)

“I trust that the speaker has kind of built-in settings. I don't necessarily look at them personally.” (P8)

“Yes, I know about them. And no, I haven't looked at them.” (P10)

“I haven't because I didn't know how to do it or I didn't know I needed to do it, and I didn't know it existed.” (P11)

“I'm aware of it. I've never looked into it.” (P14)

“I think I am aware … I knew there were privacy settings because when I set up the app, I think it mentions it, but I haven't properly looked at them, no.” (P15)

Default settings

Similarly, there was a clear level of inertia when going beyond the default setting. All the following quotes essentially amount to the same thing (ie, the defaults have not been changed), but the participants can offer a variety of reasons or justifications for the inactivity:

“You know, you just assume that everything is set up correctly out of the box. The way these devices are when you buy them as well. They are marketed to be plug and play and because of that we're less likely to look.” (P3)

“I think when you get the device you just want to get it up and running rather than looking at how everything works and all the settings involved. So perhaps a bit of naivety and overlooking things and thinking it would be OK. So I think it's a time thing and assuming that whatever it's set at, it should be OK when perhaps it's not.” (P5)

“I probably know the default settings could be improved in terms of security, but I can't say I've actually gone in and changed anything … it's more just in case I forget and I don't have the time to … it's probably due to laziness that while I'm aware there are issues with it, I can't really be bothered to change it.” (P6)

“As far as I'm aware, think I've kept it with the default settings. Obviously when I got it and turned it on and looked at it I'm sure I would have considered it at the time and whether those settings were good enough. But I think, to be honest, I've just, I've just kept them how they are, as how they come.” (P7)

“I know we just leave it with the default settings and just, yeah, I think that is enough.” (P12)

“I believe the default settings to be good enough, I guess I'm a bit naive.” (P14)

“I would presume that the default setting wasn't set so it would collect all of your data … I'd expect the default setting to be that it only collected the information that you asked once you used the command words.” (P15)

Several participants made an underlying assumption that because related settings are *provided*, they are likely to be set up appropriately (ie, they were reassured by the option to have control rather than have having *exercised* the option). Of the specific quotes listed, it is easy to sympathise with responses such as those of P3, P5 and P14, where the expectation is that they have bought a device and expect the standard settings to be appropriate. Moreover, the defaults may be appropriate. However, it is not possible for anyone to be sure they are appropriate to their individual needs and preferences unless they take the time to check.

Where participants could recall having looked at the settings, the result was not necessarily satisfaction. This is illustrated in the following two quotes, both highlighting a perceived complexity when trying to understand how the settings work and how to navigate them:

“I have configured the settings before and they are more complicated than necessary because there are two sets of privacy settings: there's the privacy settings for your Google account, and then there's privacy settings for your smart speaker itself.” (P9).

“I have gone into the settings and played around with them. It's not that easy on Google Home and because there's a few different places you can actually get into the settings and it's quite confusing whether it's to do with your Google account or the device. So it's not as straightforward as it probably could be.” (P13)

These observations can be considered to feed into the interactive tasks, where participants were required to put their understanding into practice and test their ability to correctly select or interpret the settings on offer to them. The results are summarised in Table 4, and the varied findings suggest that the interfaces are not sufficiently intuitive to ensure that users find a natural path to each setting they may be looking for. Indeed, no tasks were uniformly performed correctly and all participants made multiple incorrect assessments of the options they needed to choose.

Figure: Participant performance in the interactive tasks.

	Tasks	Participants														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	Accessing the privacy settings (2-stages, via different interfaces)	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	Finding support on how to set up and edit the privacy preferences	✓	✗	✓	✗	✗	✗	✓	✓	✗	✗	✗	✓	✓	✓	✗
	Identifying the correct option to delete voice history	✓	✓	✗	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✓	✗
	Identifying the correct option to set or edit different profiles	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗
	Add a voice ID for a personalised experience	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓
Google	Accessing the privacy settings (2-stages, via different interfaces)	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓
Google	Identifying the correct option to delete voice history	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓
Google	Finding help concerning privacy preferences (2-stages, via different interfaces)	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Google	Identifying the route to start setting up 'Guest mode'	✗	✓	✓	✗	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗

These levels of incorrect response suggest that participants would find difficulty performing the tasks in practice, potentially representing a further disincentive for users that had generally not tried to engage with the settings in the first place. Bearing in mind that in this exercise, the users were being given a specific task to perform (and therefore a particular setting/option that they were aiming to locate), it approximates a situation in which the user enters the settings with a security/privacy objective already in mind. The fact that even this seemed to prove challenging suggests that they might be even more confused if they were trying to more casually explore the settings to determine the options available to them (ie, potentially mirroring some of the comments about the complicated settings and the ability to navigate them).

From the platform perspective, there was no clear consensus over whether the participants had found the Alexa or Google interfaces easier to understand, and their opinions may have in any case been skewed by the interfaces they were more familiar with using. At the same time, the fact that users still made mistakes on their 'home' platform indicates that this is not a definitive advantage.

Settings for the future

At the end of the sessions, participants were asked to reflect upon how they would feel about reading and configuring privacy and security settings in the future. As the following quotes illustrate, a dominant theme was an apparent recognition that they ought to be more involved and take more responsibility:

"I think I should take time out and just have a look." (P3)

"I will definitely keep an eye out for it more." (P6)

"I should do it more often. I should look at it a bit more clearly and read everything." (P8)

"I think I'm going to have a look when I get off this call." (P10)

"I think it made me realise that I probably don't know very well how to reconfigure privacy and stuff as well as I thought I would be able to do. So yeah, I think maybe it should be made a bit clearer so that you are easily able to make adjustments if you want to." (P12)

"I feel like I'd be more wary in the future, and I will probably look more into it and have a proper look when I get new devices, as that's not necessarily something I do straight away. I usually go straight into playing and trying out the new device rather than actually checking the settings." (P15)

As such, it seems that many participants emerged from the interviews with a greater sense of interest and (in some cases) concern about investigating the settings available to them. Whether they acted upon this was beyond the scope of the study, but it was relevant to note that most clearly left with a greater level of awareness around the privacy and permissions aspects than they had held at the outset.

Discussion and conclusions

The main observations arising from the findings can be summarised as follows:

> The default position is that privacy and security settings are a low priority for end users (which aligns with findings from earlier surveys).

Trust in the smart speaker's brand and reputation influenced many participants in not configuring their privacy and permission settings.

Users expect a level of privacy from the default settings of their smart speakers.

Most participants were more concerned with maintaining privacy from third parties than other people in the home.

User experiences of configuring privacy and permission settings are varied, and concerns for privacy grow with greater exposure to the settings available.

Most participants seemed more concerned about managing their privacy settings following the interactive exercise.

It was clear from most responses that the users had taken little interest in the security and privacy settings, and even if they had looked at them at all, most had left things at the defaults. While there was no reason to assume that the participants had suffered problems or breaches as a result, it clearly illustrates that they are at the mercy of whatever the default settings happen to be.

Part of the assumption around defaults being 'good enough' appeared to be linked with participants' perception of brand reputation. Equally, it is interesting that the notion of a *big brand* is conflated with being *trustworthy*, especially given that these brands are often in the spotlight for collecting personal data. This to some extent mirrors the findings from other recent research, suggesting that users tend to assume that many of the risks are addressed by consumer protection regulation.10

In practical terms, the results point to the need for greater levels of user awareness, which could be more effectively supported and enabled by those providing the technology. Suppose the users' natural disposition is to generally leave the settings at the defaults (either because they assume they can be trusted or because they do not take the time to look). In that case, they need to be more directly aware of what these defaults are. This means greater clarity and transparency in the provision of the technologies. For example, work such as the IoT Security and Privacy label from researchers at Carnegie Mellon University and the University of Washington would offer a means of enabling consumers to see summary details of the security mechanisms and data practices of a device via a label that could appear on product packaging or websites (with a secondary, more detailed, level of information being accessed via a QR code or web link on the original).11

The intention would be to consistently provide such labels to allow consumers to make more-informed decisions. However, unless it becomes a requirement to take such steps, the decision over whether to do so is essentially left to the providers. While guidance and warnings about privacy can still be provided from other sources, the device provider has the direct ability to ensure that it reaches the user.

These overall findings are significant as they indicate that configuration of privacy and permission settings is low on the agenda for many people when considering the adoption of the smart speaker (a factor that could reasonably be assumed to generalise to smart technologies). Moreover, technological awareness does not seem to translate into knowledge of how to configure settings in practice, as illustrated by the results of the interactive exercise and the heightened concerns for privacy and permission settings that appeared to follow it. As such, the implications include a need to improve the ease of *accessibility* of the options to bridge the gap between those users who are technologically literate and those who are not, as well as the need to nudge and encourage users towards *looking* at the settings so that they are at least able to exercise the control available to them.

About the authors

Sareena Heer gained her MSc in computer science from the University of Nottingham and conducted 'Assessing the clarity user-facing security, privacy and permission settings of in-home smart speakers' as her dissertation project. She has an undergraduate degree in geography (BA Hons) from the University of Nottingham. When studying, she had an interest in human geography modules and therefore the interaction between humans and their environment. This prompted an interest in researching the interaction between humans and their technological environment.

Samiah Alghamdi is a PhD researcher within the Cyber Security Research Group at the University of Nottingham. She obtained her MSc in management of information technology from the University of Nottingham and her bachelor's degree in computer science-statistic from King Abdulaziz University in Saudi Arabia. She is interested in many topics in cyber security, such as Internet of Things security, smart homes security and privacy.

Prof Steven Furnell is a professor of cyber security at the University of Nottingham. He is also an honorary professor with Nelson

Mandela University in South Africa and an adjunct professor with Edith Cowan University in Western Australia. His research interests include usability of security and privacy, security awareness and culture, and technologies for user authentication and intrusion detection. He has authored over 360 papers in refereed international journals and conference proceedings, as well as various books, book chapters, and industry reports. Furnell is the UK representative to Technical Committee 11 (security and privacy) within the International Federation for Information Processing, and a board member of the Chartered Institute of Information Security.

References:

1.Laricchia, F. 'Smart speaker market volume worldwide from 2015 to 2027'. Statista, 2 Mar 2023. Accessed May 2023. www.statista.com/forecasts/1367982/smart-speaker-market-volume-worldwide.

2.Meng, N; Dkdulluoglu, D; Vaniea, K. 'Owning and Sharing: privacy perceptions of smart speaker users'. Proceedings of the ACM on Human-Computer Interaction, 2021, 5(45), pp.1-29.

3.Kokolakis, S. 'Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon'. Computers & Security, 2017, 64, pp.1-13.

4.Zheng, S; Apthorpe, N; Chetty, M; Feamster, N. 'User perceptions of smart home IoT privacy'. Proceedings of the ACM on Human-Computer Interaction, 2018, 2(200), pp.1-20.

5.Pilton, C; Faily, S; Henriksen-Bulmer, J. 'Evaluating privacy – determining user privacy expectations on the web'. Computers & Security, 2021, 105(102241), pp.1-36.

6.Madejski, M; Johnson, M; Bellovin, SM. 'A study of privacy settings errors in an online social network'. IEEE International Conference on Pervasive Computing and Communications Workshops, 2012, pp.340-345.

7.Vimalkumar, M; Sharma, SK; Singh, JB; Dwivedi, YK. 'Okay Google, what about my privacy?: User's privacy perceptions and acceptance of voice-based digital assistants'. Computers in Human Behaviour, 2021, 120(106763), pp.1-13.

8.Alghamdi, S Furnell, S. 'Assessing security and privacy insights for smart home users'. In Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023), 22-24 Feb 2023.

9.Francis, JJ; Johnston, M; Robertson, C; Glidewell, L; Entwistle, V; Eccles, MP; Grimshaw, JM. 'What is an adequate sample size? Operationalising data saturation for theory-based interview studies'. Psychology & Health, 25(10), 2009, pp.1229-1245.

10.Turner, S; Pattnaik, N; Nurse, JRC; Li, S. 'You just assume it is in there, I guess: understanding UK families' application and knowledge of smart home cyber security'. Proceedings of the ACM on Human Computer Interaction, vol.6, issue CSCW2, 2022, pp.1-34.

11.Emami-Naeini, P; Agarwal, Y; Cranor, LF. 'Specification for CMU IoT Security and Security Label (CISPL 1.0)'. IoT Security & Privacy Label, 17 Jan 2021. Accessed May 2023. www.iotsecurityprivacy.org/downloads/Privacy_and_Security_Specifications.pdf.

Computer Fraud & Security
ISSN (online): 1873-7056

Don't turn a blind eye to cyber security

FABIEN RECH
Trellix

Abstract: There's often a gap between security threats as understood by the C-suite and the day-to-day threats faced by security professionals. This can condemn the latter to working with outdated and inadequate solutions. Executives need to understand that cyber security is an area crying out for investment.

The global threat landscape is always expanding and evolving. Threat actors are improving their tools and growing more sophisticated in their approach to destabilising businesses' security systems. This means that security operation centres (SOCs) must also adapt and innovate to stay one step ahead of these cyber criminals. However, insights from recent research surveying cyber security experts offers a clear picture of the disparity between the C-suite and wider organisational security priorities.1

Many organisations still rely on disconnected and outdated security solutions that prevent them from implementing effective threat mitigation and response. This leads to some companies continuing to face challenges as cyber security professionals struggle to keep up with the increasingly dynamic security environment. The C-suite and decision-makers need to invest in cutting edge and innovative technology while focusing time and resources into building a robust security infrastructure.

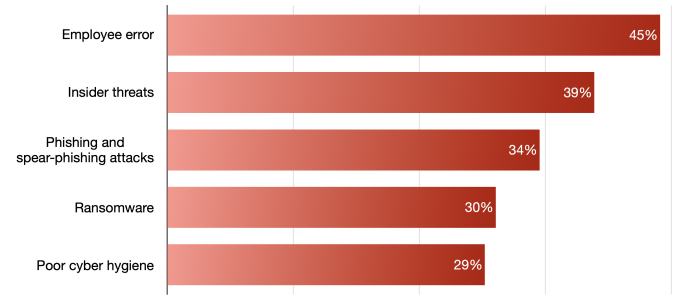
Tools such as artificial intelligence (AI) and machine learning (ML) that work in harmony with SOCs ensure that they have full visibility over operational functions, allowing for predictive and automated responses over a wider attack surface. This shift away from disjointed solutions towards intelligent, centralised ecosystems creates an adaptive cyber security environment that protects organisations on an ongoing basis.

One thing is clear – when the C-suite and security professionals are not on the same page when it comes to having a robust approach to security, it can have a detrimental impact on business operations. So, what can businesses do to bridge this gap and extend a strong security posture across the board?

Decoding the disconnect

Ownership of cyber risk needs to equate to prioritisation of security in order to avoid cyber security being treated as a tick-box exercise. Yet, the research found that while 94% of cyber security professionals agree that there is a well-defined ownership of cyber risk at a board level, an alarming one third (31%) feel that cyber security has been deprioritised when it comes to business objectives set by the C-suite and above. This points to a worrying trend that cyber security is not receiving the attention it should, which could lead to businesses becoming increasingly vulnerable to threats as there is not enough action being taken to remediate this.

Figure: The same cyber threats face all businesses.



Source: Trellix.

The impact of deprioritising cyber security in businesses can be damaging, with 84% of businesses reporting that their organisation lost as much as 10% in revenue from cyber attacks. Following Gartner's recent 2023 cyber security predictions estimating that the average number of annual data breaches per organisation will grow by 11% to 145 per year – it's clear that inadequate security controls can affect the bottom line.2 For small to medium-sized businesses, the fallout can be significantly more dangerous and can even affect their ability to continue operating.

Therefore, cyber security needs to be a priority from the top down. The tone from the board level must be conducive to strong cyber security management: only then can a culture of security be fostered across the organisation.

Obvious exposures and poor remediation

When observing the various tactics used by threat actors targeting businesses, the strategies used are not unique. For example, employee error (45%), insider threats (39%), phishing and spear-phishing (34%), ransomware (30%), and poor overarching cyber hygiene (29%) were the most relied-on attack vectors, illustrating that the 'tried and tested' techniques continue to be successful.

Having a robust cyber security policy in place to give the organisation – from the top down – a clear guide on responding to a cyber attack or an exposure is vital. However, it must be more than just posturing, especially when a breach could impact finances, operations and reputation.

Integrating these policies into ongoing activity to identify the threat, report to the board and respond in a timely fashion cannot be overlooked. Yet, a mere quarter of cyber security professionals (25%) report cyber security attacks to the board within one hour, and 26% have admitted that it can take at least a couple of days or longer to report to senior management.

During an ongoing incident, the impact of cyberthreats grows exponentially and taking one hour or several days can be the difference between successfully mitigating an attack or facing difficult consequences. Well-embedded and well-followed processes ensure that ownership, accountability and organisational integrity are maintained. Swiftness and decisiveness are the key elements to protecting businesses.

The right innovation and language

Bridging the disconnect between the C-suite and cyber security professionals will require them to find common, non-technical language to map cyber risks and discuss strategies on how to protect their business. Cyber security has a lot of moving parts, depending on an organisation's needs. Tools like endpoint, network, email and cloud protection all work independently. However, this can result in security infrastructures feeling like balancing spinning plates – sooner or later one will fall, and with it the entire system becomes compromised.

All facets of protection need to be centralised into one single solution, as opposed to managing multiple systems independently. Some 61% of organisations use up to 10 different tools to manage their organisational attack surface. This may be effective against rudimentary cyber attacks, but given the sophistication and aggression shown by current threat actors, organisations need to have better visibility to respond quickly in emergencies.

With 89% of cyber security professionals stating that their current security model is 'siloed', it's clear that organisations need to update their approach. Businesses need to implement a centralised security system that is able to learn from previous incidents, plot telemetry and identify patterns to facilitate predictive capabilities.

It is also important that the language is non-technical when communicating how this adaptive security infrastructure will help respond automatically to emerging situations – this helps decision-makers understand its importance.

Taking action now

Proactivity in cyber security is vital – anticipating threats, factoring-in learning and communicating them to decision-makers is integral to an adaptive security infrastructure. This involves evolving with each incident, creating a phalanx of cyber security as opposed to reacting to emerging risks as they take a hold.

Innovative technology is the helping hand needed to keep executives and cyber professionals up to speed with threat actors. It is key to have a centralised solution that can ease the monitoring of threats on an ongoing basis, while also allowing data and insights to be communicated in a clear and digestible way for the C-suite and board to make informed decisions.

All of this communicates the importance of preventative solutions when it comes to cyber security. Proactivity and clarity throughout the business is vital to limiting the effects of a potential compromise. Systems need to work behind the scenes to nip

threats in the bud before there can be any real impact on the organisation.

Figure: Fabien Rech, Trellix

About the author

As EMEA senior vice-president at Trellix, Fabien Rech is focused on building the business across Europe, the Middle East and Africa following its launch in January 2022. He joined McAfee Enterprise, now Trellix, in 2008. Prior to this, he held the role of GM at Netstaff – a company he founded at 25 years old. After graduating from university with an engineering degree and starting his career as an IT project manager, Rech and his team developed the computer network company, collaborating with well-known brands, before being bought by Lexsi (later acquired by Orange).

References:

1.'XDR: Redefining the future of cyber security'. Trellix. Accessed May 2023. www.trellix.com/en-us/assets/downloads/xdr-survey-ebook.pdf.

2.'The Gartner Top Cyber security Predictions for 2023'. Gartner. Accessed May 2023. www.gartner.com/en/webinar/440341/1040284.

Computer Fraud & Security
ISSN (online): 1873-7056

Looking back to the future

BERNARD MONTEL
Tenable

When we think of the modern attack surface it is a mix of on-premise and cloud-based infrastructure, complex identity and access management systems, and large numbers of web applications and microservices to accommodate modern working practices.

Tenable's Security Response Team reviewed the threats that impacted organisations in 2022 and found that more than 2.29 billion records were exposed, which accounted for 257TB of data. More than 3% of all data breaches identified were caused by unsecured databases, accounting for leaks of over 800 million records. In EMEA, over 300 million files were exposed, representing a total of 13% of exposed data worldwide. Digging a little deeper, France takes top spot with 8 million files exposed, which is about seven times more than the UK (1.2 million), 11 times more than Germany (746K), and 30 times more than the United Arab Emirates (290K).

When looking at how these attacks occurred, one theme that emerged was that threat actors continue to find success with known and proven exploitable vulnerabilities that organisations have failed to patch or remediate successfully, some of which dated as far back as 2017. The top exploited vulnerabilities within this group include several high-severity flaws in Microsoft Exchange, Zoho ManageEngine products and virtual private network solutions from Fortinet, Citrix and Pulse Secure. For the other four most commonly exploited vulnerabilities – including Log4Shell; Follina; an Atlassian Confluence Server and Data Centre flaw; and ProxyShell – patches and mitigations were highly publicised and readily available. In fact, four of the first five zero-day vulnerabilities exploited in the wild in 2022 were disclosed to the public on the same day that the vendor released patches and actionable mitigation guidance.

What matters most

However, given the volume of disclosed vulnerabilities, fixing every vulnerability just isn't feasible. Over a five-year period from 2018 through 2022, the number of reported CVEs increased at an average annual growth rate of 26.3%. There were 25,112 vulnerabilities reported in 2022 (as of January 9, 2023), which represents a 14.4% increase over the 21,957 reported in 2021 and a 287% increase over the 6,447 reported in 2016. Organisations need to reduce effort by focusing on what matters most.

Protecting everything is soul destroying given that it's almost an impossible task. Similarly, organisations are well beyond the point where vulnerability management can be performed in a vacuum. Alone, it only tells part of the story. By focusing resources on the vulnerabilities that are exploitable and understanding how attackers chain vulnerabilities and misconfigurations, security teams can design more complete strategies for reducing their overall risk exposure.

The truth is that successful security programmes must take a comprehensive approach, allowing security teams to understand where their most sensitive data and systems lay and what vulnerabilities or misconfigurations pose the greatest risk.

And that's where exposure management steps up to the plate. A relatively new concept, it's designed to transcend the limitations of siloed security programmes. Building an exposure-management programme involves bringing together data from tools associated with vulnerability management, web application security, cloud security, identity security, attack path analysis and attack surface management and analysing it within the context of an organisation's unique mix of users and IT, operational technology (OT) and Internet of things (IoT) assets. The goal? Having the contextual data needed to execute an ongoing, preventive security programme built on risk-based workflows.

Understanding attacker behaviour helps inform security programmes and prioritise security efforts to focus on areas of greatest risk and disrupt attack paths, ultimately reducing exposure to cyber incidents. Organisations that can anticipate cyber attacks and communicate those risks for decision support will be the ones best positioned to defend against emerging threats.

Bernard Montel is EMEA technical director and a cyber security strategist at Tenable.

Figure: Bernard Montel, Tenable

Vol: 2023 | Iss: 5 | 2023 | 10.12968/S1361-3723(23)70023-7 |

Computer Fraud & Security
ISSN (online): 1873-7056

Vol: 2023 | Iss: 5 | 2023 | 10.12968/S1361-3723(23)70023-7