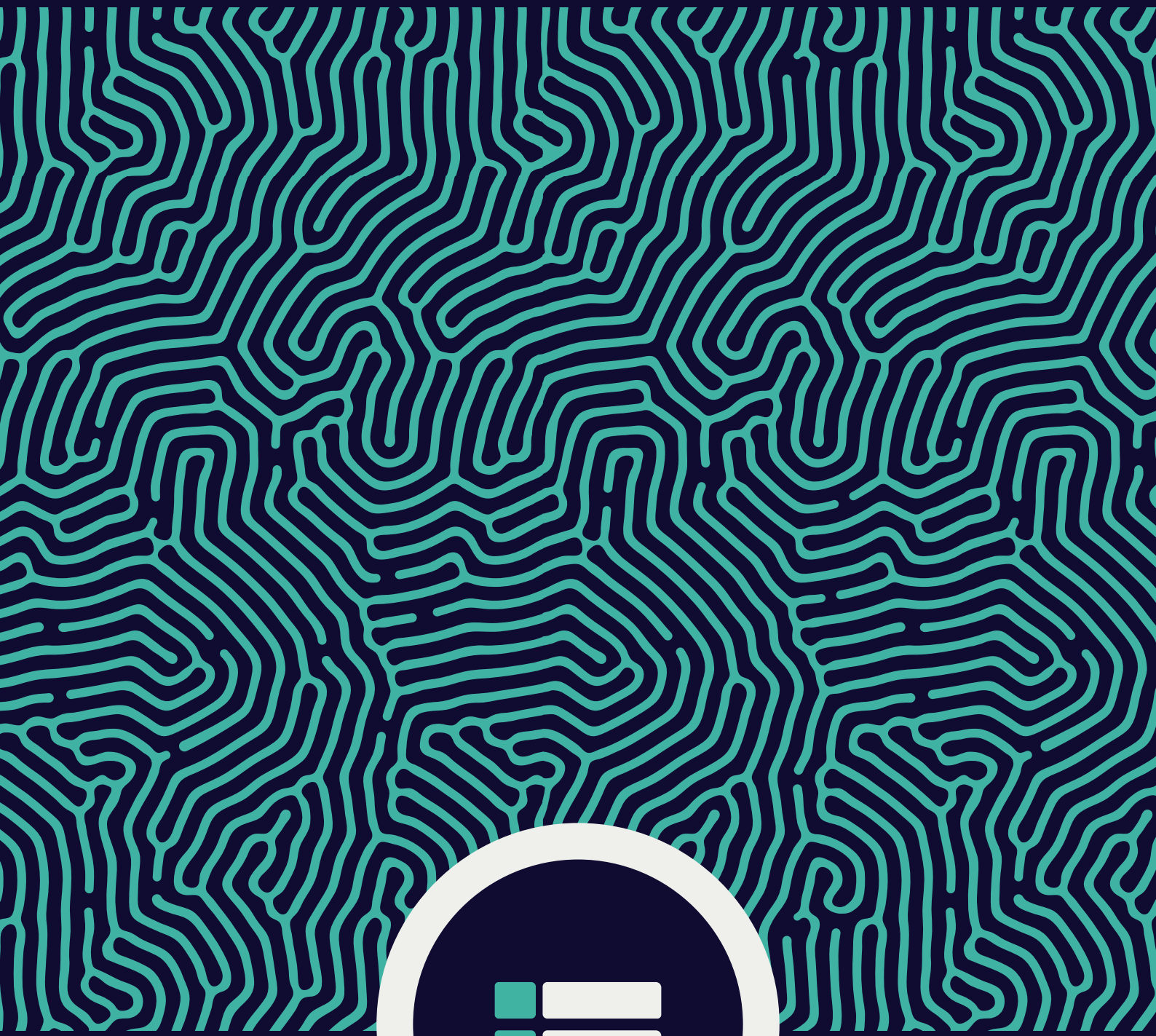
GLOBAL INTERNET REPORT 2016



Executive Summary

Introduction

Data breaches are on the rise. The impact of data breaches on users – consumers, employees and organisations is profound and lasting, including significant financial and non-financial costs. Even worse, in many cases the data breach could have been prevented. And, even if it could not have been prevented, the harm could have been mitigated.

So the issue at the heart of this report is, in some ways, a simple one.

Why are organisations not taking all available steps to protect those who entrust them with their personal information? Is it because they do not bear all the costs of the data breaches? Is it because there is not enough benefit to them in better protecting their users' data? The answer to both questions is yes.

While users bear the lasting costs of each breach, the ultimate casualty is trust in the Internet. The vision of the Internet Society is that the Internet is for everyone, everywhere. Trust in the Internet is at the core of that vision. Without trust, those online are less likely to entrust their personal information to the Internet, and, those who are not yet online will have a reason to stay offline. The Internet economy will not grow as fast as it could, and the UN Sustainable Development Goals (SDGs) will be that much harder to achieve.[1]

With this report, the Internet Society seeks to increase awareness on the topic of data breaches and our collective responsibility to help secure the data ecosystem. We make recommendations on how to reduce the number and impact of data breaches. Fundamentally, users should be at the centre of the discussion, as they are the ultimate victims of breaches. Their trust must be won and kept to help the Internet meet its full promise for everyone.

What is a data breach?

"A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service"

The Information Commissioner's Office (ICO) of the UK[2]

[1] As has been pointed out, data, like oil, has its downsides, and in this light, data breaches are the new oil spills. See the following article by the Internet Society's Technical Outreach for Identity and Privacy, Robin Wilton, at https://www.internetsociety.org/blog/tech-matters/2014/10/they-say-"personal-data-new-oil"-thats-good-thing.
[2] See https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/.

Data and Trends

Data breaches are trending upwards:

- A growing number of people are impacted by data breaches. Reported breaches are increasing, with a rising number of known records breached and even more that are unknown in number. The leading cause is outside attacks, mostly for financial gain. Most breaches appear to occur in the US, but that is likely because of data breach notification rules that lead to more disclosure.

- Surveys do not as yet indicate that reported data breaches are having a significant impact on non-users' willingness to go online. However, as more users are impacted by data breaches, such as by having their identity stolen for profit, more users will hesitate to use online services requiring personal information. They may also stop doing business with a company that has been breached. A widening breach of trust among users, in turn, could provide non-users with a reason not to go online.

- Organisations are spending more on prevention, but this has not yet noticeably lowered the number of breaches, or the impact and cost of breaches when they do occur. In turn, the cost of breaches, when calculated, typically only include the cost to the organisation, and not the full cost for the users who were the ultimate victims of the breaches.

These trends cannot be allowed to continue without significant harm to individuals' privacy and users' trust in the Internet, resulting in lower and more selective use of the Internet.

Case studies

The report highlights some leading causes of data breaches, and their impact on organisations and users. The numbers are staggering: Target had 40 million customers' credit card numbers stolen and put on sale online; Ashley Madison's records on 37 million married users and their personal affairs were taken and published online; and the US Office of Personnel Management had records on 21.5 million past, present, and potential employees, stolen.

The impact of these breaches on consumers, users, employees and third parties who did not even know the organisations had their data

is profound and lasting. Some users lost time and money protecting their finances and their identity from theft, some saw their marriages dissolve, and even committed suicide, and others may be subject to blackmail and exposure.

The case studies show how easy some attacks are, but also how difficult it is for organisations to protect against all threats. For users, the case studies highlight the increasing sense of insecurity online, requiring trust in organisations whose security users could not possibly assess. An ever increasing number of users have been directly or indirectly impacted by a data breach. The case studies make concrete the real and ultimate impact of these breaches on the users whose trust in organisations, as consumers or employees, is betrayed.

Issues

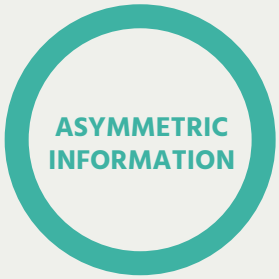
In the face of financial and non-financial costs highlighted by the data and case studies, it is puzzling that many of these breaches exploited **known vulnerabilities**, and were preventable. For some of these, there were patches available, but not used. Some involved social engineering attacks, in which employees were tricked into giving up their password or introducing an infection, typically in ways that could be prevented.

Of course, not all breaches result from attacks, and not all attacks are preventable. Some are the result of attacks using **zero-day exploits** not known before being employed. Others result from accidental disclosure of data, for example through the loss of a device containing sensitive data. While not preventable, given how common they are, such breaches are at least foreseeable. It is possible to mitigate the impact, by minimising the amount of data gathered, and encrypting the data that is stored and sent.

The question remains why, given the cost of breaches, more is not done by organisations to address the preventable ones, and to lower the cost and impact of foreseeable ones? This raises the issue of the economics of trust.

There is a **market failure** that governs investment in cybersecurity. First, data breaches have **externalities**; costs that are not accounted for by organisations. Second, even where investments are made, as a result of **asymmetric information**, it is difficult for organisations to convey the resulting level of cybersecurity to the rest of the ecosystem. As a result, the incentive to invest in cybersecurity is limited; organisations do not bear all the cost of failing to invest, and cannot fully benefit from having invested.

The breached organisation does not bear all of the costs of the breach – the cost borne by others is an externality that does not necessarily factor into its decisions on how to protect against data breaches. Further, the weight of data breaches impacts future trust, which is an externality, and from an economic perspective, there is no rational reason for organisations to account for this. However, this is an impact society cannot neglect.



Stakeholders do not have full information about the risks they may face online, making it difficult to take informed decisions. In particular, it is hard for organisations to benefit from taking the right steps to avoid data breaches, because they cannot convey their level of data security to customers. This limits the incentive to invest in data security.

Recommendations

The report highlights five recommendations for addressing the issues raised regarding the economics of data breaches.

R1 Put users at the centre of solutions; and include the costs to both users and organisations when assessing the costs of data breaches.

R2 Increase transparency through data breach notifications and disclosure.

R3 Data security must be a priority. Better tools and approaches should be made available. Organisations should be held to best practice standards when it comes to data security.

R4 Organisations should be accountable for their breaches. General rules regarding the assignment of liability and remediation of data breaches must be established up front.

R5 Increase incentives to invest in security by catalysing a market for trusted, independent assessment of data security measures.

The *first recommendation* is to put users at the centre of the solutions. As a way to kick-start this user-focused approach to data breaches, our *second recommendation* is to create increased transparency about the risk, incidence and impact of data breaches globally.

With increased awareness comes increased demand for better tools. Our *third recommendation* is that data security must be a priority. Better tools and approaches should be made available. Organisations should be held to best practice standards.

- **Prevention.** To avoid known vulnerabilities, security tools should be easier to use and update, including critical security patches. To prevent social engineering attacks, organisations should apply trusted tools and best practices to block phishing emails and embedded malware, and also train employees to help avoid these attacks

- **Mitigation.** Organisations should gather the minimal data needed to provide the desired services while preserving the rights and expectations of individuals. Organisations should also apply encryption for gathered and stored data that are in transit and at rest. Encryption must be made easy to use, and ideally implemented as a default, particularly for individuals.

Of course, as user-friendly as tools might become, they still cost time and money to implement, which not all organisations are willing to spend to prevent data breaches and to mitigate their impact when they cannot be prevented. The final two recommendations focus on how these market failures can be addressed through economic incentives, concerning both costs and benefits.

- *Fourth recommendation.* Increased accountability. By imposing more of the externalities of the data breach on the organisations holding the data, their costs will go up, leading organisations to increase efforts to prevent them and mitigate their impact.

- *Fifth recommendation.* Security signals. By enabling organisations to signal that they are less vulnerable, thereby reducing the asymmetry of information, organisations will be able to better compete for business, increasing the rewards of investing in preventing a data breach.

The five recommendations are summarised in the security circle.

Underpinning these five recommendations are two important principles: data stewardship and collective responsibility.

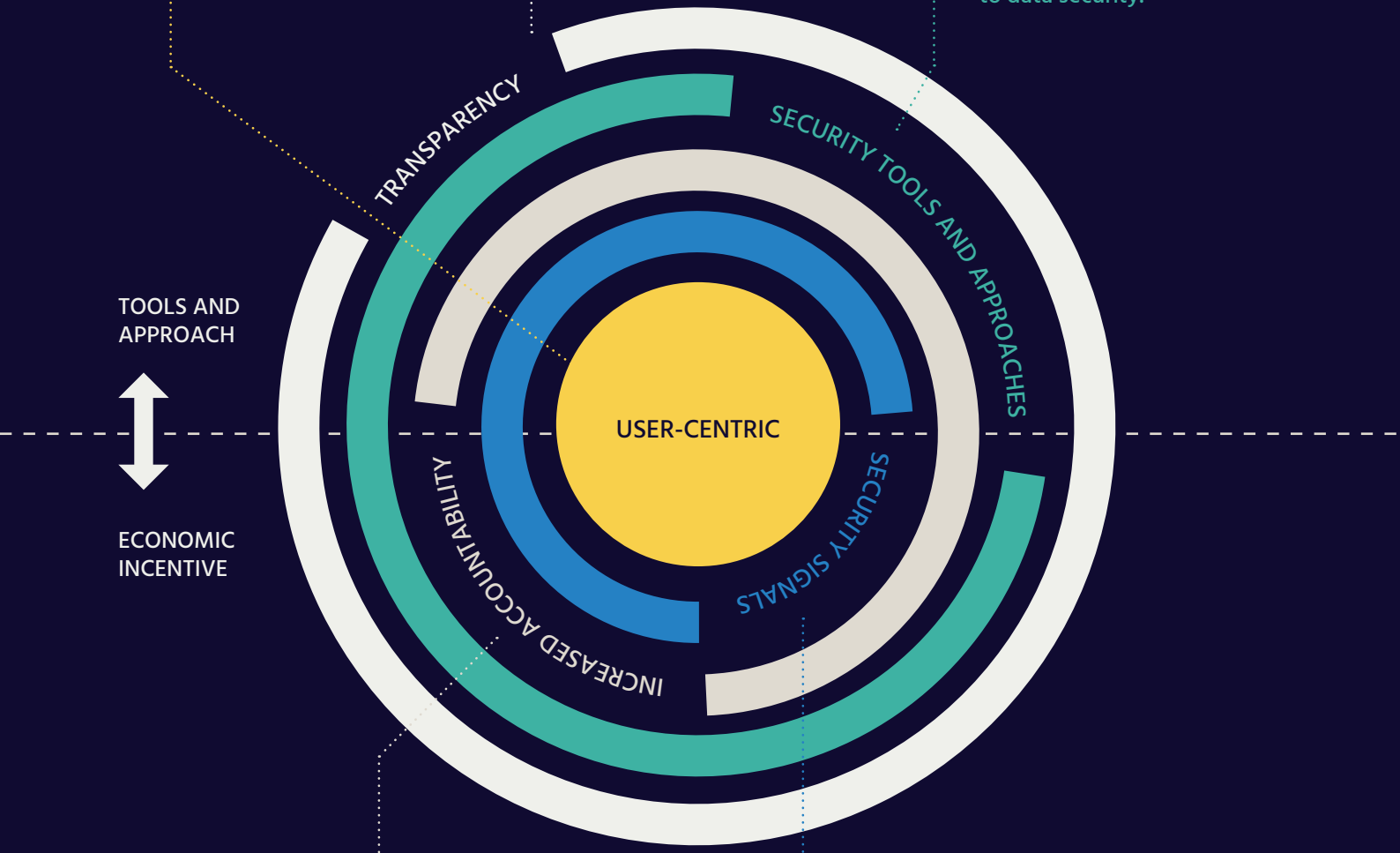
Data stewardship. Organisations should regard themselves as custodians of their users' data, protecting their data not only as a business necessity, but also on behalf of the individuals themselves. Organisations should apply an ethical approach to data handling, and understand that they can do well by doing good – protecting users should be a goal in its own right, which also protects the organisation.

Security Circle

1. Put users at the centre of solutions; and include both users *and* organisations when assessing the costs of data breaches.

2. Increase transparency through data breach notifications and disclosure.

3. Data security must be a priority. Better tools and approaches should be made available. Organisations should be held to best practice standards when it comes to data security.



4. Organisations should be accountable for their breaches. General rules regarding the assignment of liability and remediation of data breaches must be established up front.

5. Increase incentives to invest in security by catalysing a market for trusted, independent assessment of data security measures.

Collective responsibility. On the Internet, everyone is connected. One breach could lead to another (in other words, "your breach could be my breach"). Organisations have a responsibility to secure the data they hold. They also share a collective responsibility with other stakeholders to secure the data ecosystem as a whole. This includes vendors, employees, governments, and others. Should one of these links not function, the entire trust chain could be broken.

In summary, our message to organisations is:

- Personal data is precious and priceless – protect it!
- Collect only what is absolutely necessary and encrypt what you keep
- Restrict access to those who need to know
- Signal the level of data security you provide
- Destroy data when it is no longer in use
- Be more transparent about data breach incidents
- Be alert to breaches, prepare, notify and act immediately

Conclusion

Data breaches are a growing concern worldwide. To mitigate this problem and its economic impact, the report proposes a shift in the approach to data breaches, involving all stakeholders.

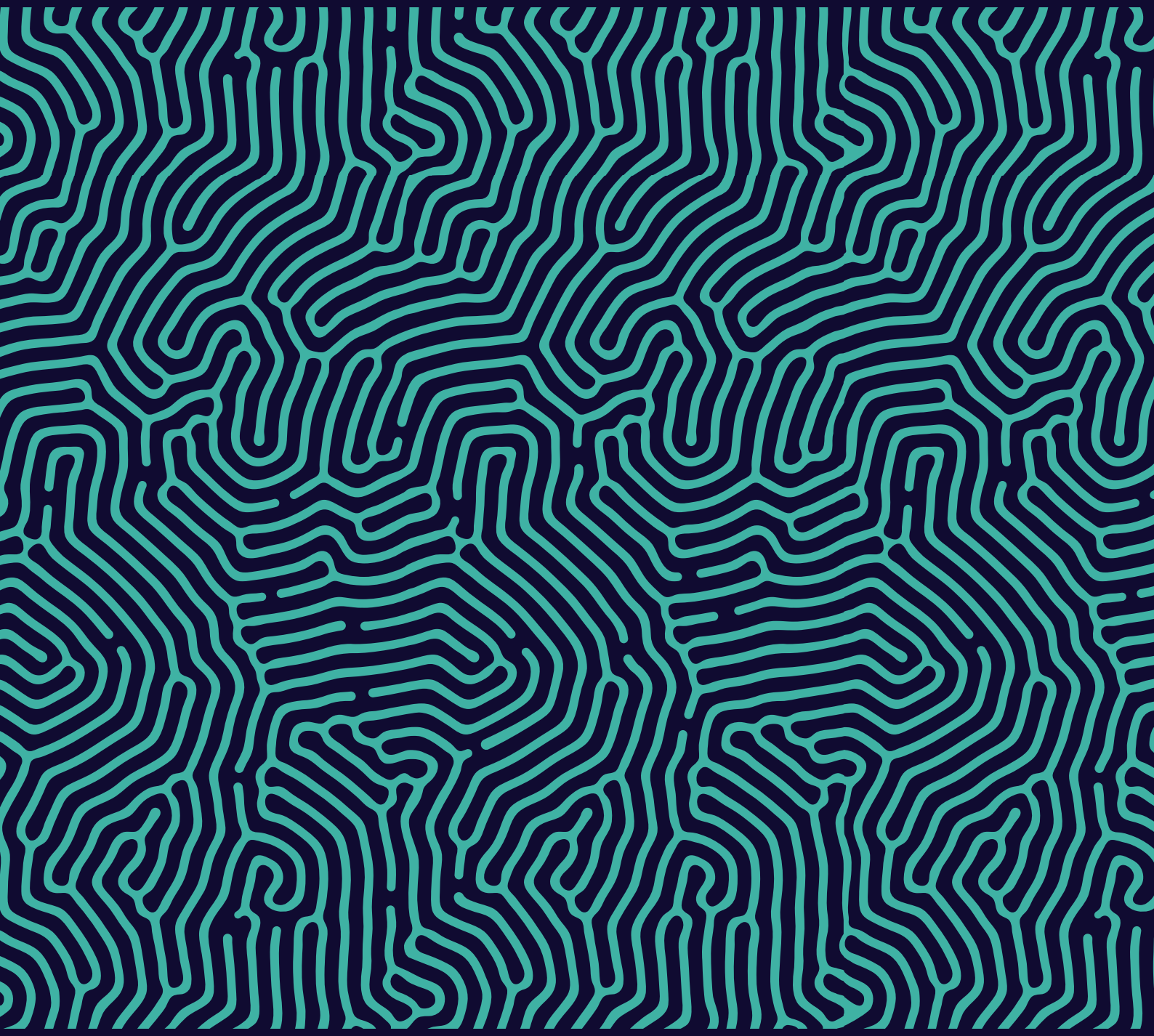
As users increasingly move their lives online, to achieve the full benefits of the Internet worldwide there must be user trust. That trust is dependent on how users' data is protected from breach. Each data breach creates a new group of users whose trust may have been betrayed, which spreads to their acquaintances through word of mouth, and more broadly through news reports, creating doubt, which undermines user trust at large.

With this report, the Internet Society's goal is to offer recommendations that will help to provide better data security. This, in turn, has the potential to increase use of the Internet, and raise the economic and social impact of the Internet on the broader economy and society. That, finally, will help meet the Internet Society vision that the Internet is for everyone, everywhere.

Internet of Things

Looking forward to a world of ubiquitous Internet of Things (IoT), vulnerabilities resulting in data breaches can also apply to IoT devices, with perhaps even greater impact on users. First, of course, connected devices such as baby monitors can contain sensors, including for video and audio, that can yield personal information about the owners. More broadly than a data breach, however, people may put their personal safety in the control of the connected devices, such as medical devices or connected cars. It is incredibly distressing to have one's health records stolen and sold. It is potentially fatal to have one's health devices hacked and overridden.

More broadly, many of our recommendations are valid for preventing or mitigating breaches of the full range IoT devices, not just for the data that they are gathering with their sensors, but also for a security breach that could lead to personal or public safety risks. As such, the Internet Society encourages the application of these findings to the range of relevant issues arising from the emerging IoT. While this is a broader issue than data breaches, the causes may be the same and should be considered in addressing the general security of these devices as a matter of priority.



Internet Society