of the things that shocked most people about Equifax was not that it was breached but that this company, that most people had never heard of, had their private information – lots of it. How does it happen?

Institutions that lend you money or provide credit want to know whether you are a reliable customer. They do this by passing the details they collect from you to a credit agency that does this on behalf of so many other institutions that between them they can provide some assurance as to whether you should or should not be lent money. What actually happens is that a company can pay these credit agencies to send them your data – about other borrowing, about address history; it's a large dataset. Even if you don't have a relationship with the end user, you can still buy this data.

The reasoning is sound enough, it is just the implementation that is very risky. We trust institutions like banks not to lose data but it is certainly not guaranteed that it is safe. And if it was stolen, would you know? If you don't like this arrangement then don't borrow anything – no credit cards, no mortgages, no loans and no mobile phones. This is basically not an option for most of us.

So how do we provide the needed outcome without the risk of data sharing? The solution is something we call 'inversion of responsibility' or 'inversion of control'. Rather than an organisation asking the credit agency to send it all of your information, it instead sends the credit agency the lending 'rule' that it will run on the data. The credit agency runs the rule itself and returns the result to the organisation without the latter ever having to see any private data.

This solution wouldn't have helped with the Equifax breach but if far fewer organisations need to see the private data, the risk of it being stolen is massively reduced. The same basic principle could and should be used with authentication as a service where, instead of collecting customer data yourself, you trust a specialist company to do it for you. It provides the information during a session, so you can get delivery addresses and so on. But as soon as the customer logs out, the information is deleted or anonymised and your risk is removed.

Perhaps you have other ideas? Make them happen, make sure they live in the correct domain – industry, legal, corporate – and let's try and make our industry slightly less hard.

About the author

Cyber-security expert Luke Briner has a strong white-hat hacker pedigree and a passion for electronics. CISSP certified with special expertise in software security, he is the CTO at PixelPin, a company that offers a personalised two-factor visual authentication solution.

VPN: from an obscure network to a widespread solution

James Longworth

James Longworth, Insight UK

Looking at the evolution of virtual private networks (VPNs), one can see a clear shift in their usage in the past decade or so. While VPNs used to be reserved for big companies and government authorities – proving a mystery or unjustifiable expense to most – today we see VPNs being implemented and talked about on a much wider scale. From organisations of all sizes to individuals, more and more people are turning to VPNs to safeguard their data and ensure privacy.

However, to understand what key benefits this technology provides its users, we must first look at how it works. In short, VPNs are used to protect data from being accessed or altered as it travels over another network (eg, the Internet). This is possible through the use of a wide variety of computer protocols that securely 'wrap' your data in a layer of encryption and ensure that the destination for that encrypted data is authenticated (ie: the person or system is who it says it is) and authorised (allowed) to 'unwrap' it. In other words, VPNs allow users to securely access a private network and also share data remotely.

The rise of VPNs

The rise of VPNs goes hand in hand with the rise of other technologies that require a higher level of cyber-security protection. For instance, the sudden rise in popularity of virtual private networks and their current ubiquity is down, in part, to the rise of technology trends such as the Internet of Things (IoT) and bring your own device (BYOD), as well as legislative changes that allow state bodies to require ISPs to monitor and log individuals' online activity.

With more and more entities using these technologies on a daily basis, an increasingly larger number of individuals and organisations have begun to turn their thoughts towards the benefits of VPNs.

Initially, virtual private networks were created to provide secure remote access to network resources. With time, however, the VPN industry has undergone a shift in its focus to allow the technology to accommodate modern necessities. One way of doing this was by making privacy its primary role and unique selling point.

"The VPN industry has undergone a shift in its focus to allow the technology to accommodate modern necessities. One way of doing this was by making privacy its primary role"

As a result, when it comes to new VPN technologies entering the market in the next few years or so, we are looking to see new encryption methods being incorporated so that the technology becomes increasingly robust. In line with this, there are a number of improvements that can be incorporated to facilitate this shift towards a more privacy-focused solution. For instance, the next generation of virtual private networks might see improvements in areas such as anonymous tokenised authentication or protocol obfuscation. As a result, we might soon discover a significant change in how online privacy and data privacy on the Internet is enforced.

Because of these potential changes and the technology's prospects on the market, it is easy to imagine a prosperous future for the industry as a whole. Looking at the past few years, the use of this technology has rapidly shifted from targeting specific organisations to becoming widespread. After all, the VPN industry has the potential to bolster Internet security against a number of cyberthreats.

Holding back

Of course, this sudden rise in the popularity of VPNs among Internet users is not inexplicable - we need merely to look back at the significant amount of cyber-security threats discovered last year and breaches that have made the headlines in recent months. The past few years have been marked by cyberthreats and questions around data security, with hundreds of companies of all sizes rushing to develop new solutions to combat online threats.

Similarly to how firewalls quickly rose in popularity, many industry experts predict that VPNs could become the newest trend in just a few years. Users and providers alike must understand and keep note of the fact that even VPNs cannot completely eradicate cyberthreats or ensure absolute privacy for online users but in spite of this, it is likely that VPNs are on the path to becoming omnipresent in the context of business and professional environments, where the need for increased privacy will only grow in the coming years.

In the past few years, we've seen a significant increase in the need for a secure connection, mainly fuelled by the rise of mobile and the increase in policies like BYOD. With BYOD policies in particular pushing for a more flexible approach to home and mobile working, it comes as no surprise that in many cases users may not even know they are using VPN technologies.

That means that while VPN technology itself hasn't changed much since its inception, the way it is managed has changed significantly. VPNs are now quickly entering the realm of mobile device management, providing secure access to corporate resources. Another benefit is the cut in the number of steps users have to follow to gain access to resources, as everything now happens in the background, making the technology much more accessible and easy to use for the wider public. Inevitably, this leads to a more efficient set-up, speedier on-boarding processes and less lost information.

In turn, this change has led to greater flexibility, particularly for those who frequently work remotely and it has the potential to improve productivity, particularly with the expansion of the gig economy and the increased workplace mobility it offers.

Traditionally, a VPN's main benefit is enhanced security. While some users choose from the multitude of email encryption services and software available on the market, increasingly more prefer to trust VPNs to guarantee their privacy.

More in the future

The VPN industry is now undergoing a shift in its focus to accommodate new user expectations, switching its primary role from providing remote access to network resources to guaranteed privacy. Further to this, many industry experts are expecting new encryptions to be incorporated into the new VPN technologies that will significantly change how online privacy is reinforced.

"VPNs are far from a magic pill against all cyberthreats, but they've certainly secured a firm place in the future of most security-conscious organisations"

As such, it is good to see that both organisations and individuals have increasingly better access to such software, but responsible Internet browsing and common sense must stay at the core of online activity. One aspect must be kept in mind: VPNs are far from a magic pill against all cyberthreats, but they've certainly secured a firm place in the future of most security-conscious organisations and privacy-focused individuals.

About the author

James Longworth is the head of solution architecture (modern workplace) at Insight, where he works on solutions that enable increased productivity for professionals in any business or role. In his previous roles at Insight, he helped clients define their strategy and create cross-architecture roadmaps for their IT environments based on business strategies and priorities.