DATA SECURITY IN PRACTICE

How businesses can combat complacency and take practical action to protect customer data.

semafone®
securing data · protecting reputations

Foreword

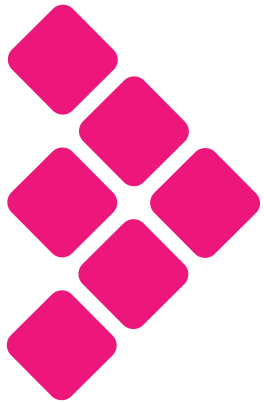
Data breaches, small, large or catastrophically huge, have a knack of making their way into the headlines, but their place in the media has been shared in recent months by alarmist stories about the consequences of failing to meet data protection regulations. A bombardment of contradictory advice and scary stories about failure to protect personal data adequately has driven many organisations into a state of paralysed panic. Instead of taking decisive action, they are still hesitating, unsure of the best way to proceed. It's like being warned that a change in lifestyle is needed to stave off a fatal heart attack – scary, but difficult to know where to begin.

It's time to take a different approach. At Semafone, our own customers have by definition put preventative measures in place before a disaster, not after. We asked them to share some of these actions; not simply in our own specialist area of card payments and PCI DSS compliance, but for customer data more widely. From our discussions with them, we have compiled this brief report.

It includes the practices and experience of three of Semafone's customers; online electronics retailer AO.com, touring membership community the Caravan and Motorhome Club, and regulator HCPC. Our own data security specialists have also added their advice to the mix.

We have distilled this information into five areas of focus and concluded with ten practical steps that companies can take right away. We hope that you will find it helpful in your own journey towards a more secure environment for your customers' data.

Your organisation will be breached: don't sit and wait for it to happen.

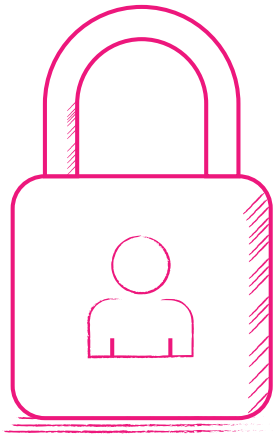


Introduction

When we set out to ask our customers about their overall approach to security, we expected their responses to focus on new technologies designed to defend them against cyber criminals. To some extent, they did. A theme that also came across strongly, however, was the struggle to overcome human fallibility in the fight against cybercrime. Whether it's accidental errors, duped staff or the occasional internal fraudster, dealing with the threat posed by humans should be high on the list of things to be addressed if you're trying to improve your corporate security. From simply establishing some clear procedures, to appointing security experts, people are at the heart of the solution as well as the problem. Below are some of the key conclusions, along with ten suggestions to help you along the path to improved security.

1

The Right Motivation: Customers Are People, Not Numbers



The companies making the biggest strides in security are not the ones racing to comply last-minute with a particular piece of legislation; they are those who genuinely care about keeping their customers' data safe. While regulations provide a helpful framework, they are unlikely to be effective if they are the only reason why a company is putting in place security measures. Two main drivers for change were mentioned by the companies we spoke to: protecting customers and protecting reputation.

Looking after the needs of customers is understood clearly by the Caravan and Motorhome Club, which is an organisation owned by its members.

> **"As a membership club, we are very conscious that doing the right thing by our members and looking after their data responsibly is critical. At the same time, we don't want to over-engineer data security in a way that will cause them problems. Putting the members' needs first, while protecting them is the ethos of the club."**
>
> **Jon Laws**
> **Financial Controller, The Caravan and Motorhome Club**

AO also places a strong emphasis on looking after customers and believes that an internal culture of care can help businesses build and maintain their reputation.

According to Carl Phillips, Group Director of IT at AO; ***"Simple compliance with requirements is not enough, the company culture needs to be that of protecting the customer, at all times and at all costs. Reputation is invaluable to organisations like AO and while it takes many years to build, it can be crippled overnight."***

He reports that the company never has objections from customers when additional security measures are implemented, adding; ***"Customers are asking more about security and we have a great story to tell."***

Guy Gaskins, Executive Director of Information Technology and Resources at HCPC, agrees on the importance of robust data policies and procedures in maintaining a strong reputation and gaining trust; ***"As a public sector organisation, HCPC must be open and transparent about its data processes to maintain its credibility and reputation."***

2

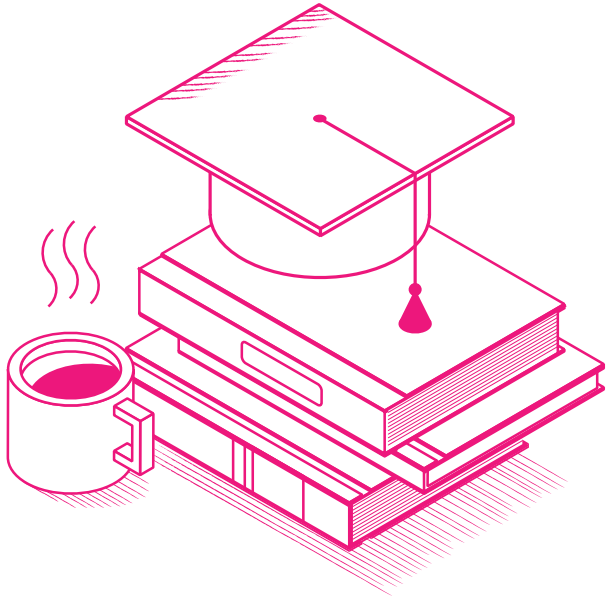
Look After Your Own People Too

This focus on people extends to the security measures themselves. Human error and insider crime are still at the top of the list of threats to a company's security, so a continuous cycle of education, processes, and monitoring is essential to mitigate this.

Education

At Semafone, all new employees take part in a rigorous security induction to guard against the most common threats. This helps them to be aware of the phishing tactics designed to entice them into clicking links or downloading software without checking with the security team. An internal security awareness tool delivers training and requires employees to complete tests to ensure knowledge remains current.

Shane Lewis, Information Security Manager at Semafone explains;
"It's not easy to keep security front of mind when staff have so many other preoccupations. The only way to succeed is through an iterative process; one training session a year won't do the trick. We require people to conduct online tests on a regular basis – but we call them "quizzes" to introduce an element of fun."



Access

Handling customer data comes with enormous responsibility. When staff are tasked with handling customer data, they themselves are exposed to a degree of risk; the risk of suspicion. Anyone who has worked in a clean room environment in a contact centre understands the implied assumption that having access to a mobile phone might make them a higher risk. To relieve employees of undergoing this level of scrutiny, following the principle of “least privilege” is a good approach – this means access to information is granted only when it is required, and should come as standard. AO applies this principle by starting with a blanket “deny-all” policy, selectively giving employees increased access over time.

HCPC chose to remove sensitive data from its contact centre altogether in order to provide its team with the best possible working environment.

> **“As an organisation, our values include transparency and openness, so we didn’t want to instigate clean rooms and require people to hand in their mobile phones, or only allow a proportion of people onto the registration floor because these approaches could create a negative working environment. We wanted technology that would allow us to maintain openness without arduous restrictions.”**

Guy Gaskins
Executive Director of Information Technology and Resources, HCPC

AO has adopted a continuous and heightened sense of security in all parts of its business, putting customer protection and data security at the heart of everything it does.

The company has added additional protection to its website so that shared customer information can only be deciphered internally; introducing a self-contained native app that makes purchases more secure and implementing protection against automated attacks using log-in details from other sites. The company has also outsourced its security testing.

Like Semafone, AO constantly screens its systems for cyber attacks and anomalies, applying geo intelligence to monitor, manage and block traffic from regions known to be potential threats.

“It is vital to keep awareness of cyber criminality high on your agenda. Attack vectors are getting more and more complex and using a security encyclopaedia just isn’t enough anymore. We need to track and trace millions of events and anomalies, so we’ve invested in pattern test technology which uses machine learning for anomaly mapping and is constantly looking for unusual activity. If people are hacked elsewhere, they may have used the same email and password on their AO account so we’ve had to take steps to detect fraudulent login attempts even where the username/password is correct, to deter the attacker and notify the customer that their details may have been compromised. Distributed denial of service attacks are also a growth area and even though we have flexible capacity and rate-limiting technology, these alone aren’t sufficient to mitigate against the most sophisticated attacks, so we challenge ourselves all the time to improve our defences.”

Carl Phillips
Group Director of IT, AO

4

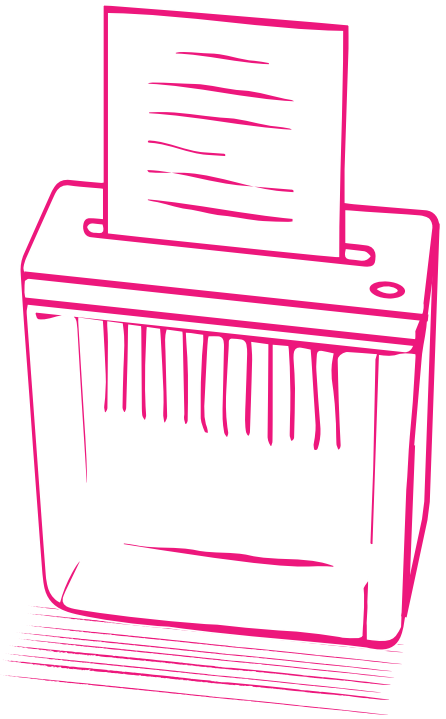
Only Store Data You Really Need

In light of the EU's General Data Protection Regulation (GDPR), all businesses must gain a clear understanding of the customer data they hold and what it is used for, ensuring they only store data they really need.

When the Caravan and Motorhome Club began working towards GDPR compliance in 2016, it undertook an extensive review of every part of the business, identifying any gaps in data processes and security, and developed recommendations to address these.

The company – which already uses Semafone's Cardprotect solution to avoid handling credit card details – is currently reviewing its approach to other financial data.

> **"We are considering taking bank details for direct debits out of scope. We're very conscious of changes that are happening in the payment industry with mobile payments and emerging fintech companies and are keeping an eye on that."**
>
> **Jon Laws**
> **Financial Controller, The Caravan and Motorhome Club**



AO also implements robust data classification procedures to determine what it needs to keep and as a result encrypts any data it does need to store. After company strategy and corporate account information, credit card details were the most valuable data the business handled, so it needed a special focus.

Carl Phillips advises; ***“One of the best things we did was to remove credit card details from our IT infrastructure. Don’t store data you don’t need to, then it can’t be stolen.”***

Semafone already undergoes regular data security audits due to the nature of the service it provides. As part of its payment service, for instance, Semafone processes details, such as addresses, names, telephone numbers, and dates of birth which are needed by the payment service provider for fraud checks. Semafone’s software removes all this personal data before it goes back to the merchant to avoid them having to store or encrypt it. By keeping sensitive data out of business infrastructures, organisations can dramatically reduce the impact of a data breach.

5

Be Prepared to Spend Some Money

It's too easy to see data security as the poor and unglamorous cousin of the IT family.

Allocating budget to it appears less attractive than other, more transformational projects – until a breach occurs, that is, when costs are disproportionately higher. To some extent, regulations have helped to address this, unlocking money for data security that was previously difficult for IT departments to obtain. The Caravan and Motorhome Club, for instance, spent £1.6 million over four years on PCI DSS compliance and is likely to spend another £1 million on GDPR compliance. But investing in customer data security isn't just about implementing the latest tools and technologies. Organisations must also be prepared to invest in people with the experience to protect customer information.

At Semafone, we practise what we preach. Our focus is security and in the past three years, as the massive increases in the rate and size of data breaches have become apparent, we have responded by appointing a certified Information Security Manager with a team that includes penetration testers to ensure that our own defences are constantly under scrutiny.

Part of the Caravan and Motorhome Club's investment was on personnel; including the appointment of a Data Protection Officer (DPO) 12 months prior to carrying out an internal data audit. It is now a legal requirement of the GDPR legislation for companies that deal with significant amounts data to appoint a Data Protection Officer.

"A project was running for two years but had stalled without a clear leader as we were just too busy to deal with our data. Appointing the DPO made it a priority; we now have a whole team reporting to her."

Jon Laws
Financial Controller, The Caravan and Motorhome Club

AO too has invested in people, with the full support of an enlightened senior management team. Carl Phillips says; ***"AO has a very supportive board who put the company's reputation first, so it has not had resistance to budgeting and resourcing for security. The business has invested in people and increased dedicated security staff by 100%. And that's without all the employees for whom security is not their main job."***

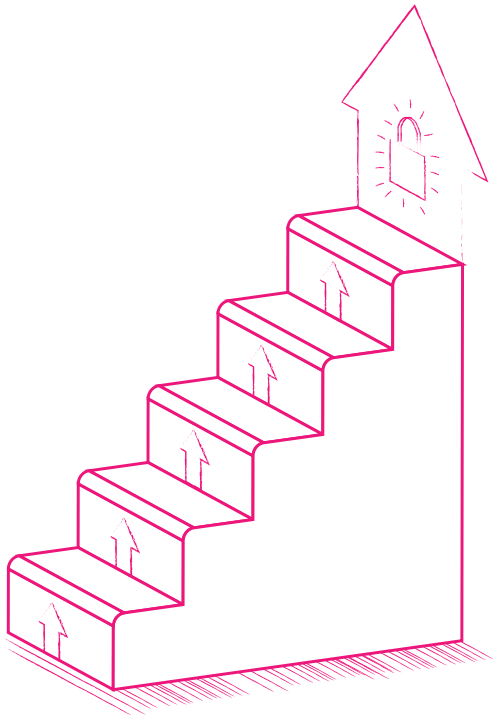
The experiences of these organisations clearly illustrate that the benefits of acting on data security in good time are enormous, allowing them to minimise the risk of a data breach, and handle valuable data in a responsible manner, which helps them build customer trust and a robust reputation.

Conclusion

The way in which you approach your own security challenge will depend on the size of your organisation and the amount of sensitive data that you handle. However, these ten tips are a good place to start, no matter the size of your business.

Ten Steps to Data Security

1. Make sure you are complying with the right security frameworks. From Cyber Essentials to ISO 27001 & PCI DSS, these will be a helpful guide. That said, remember why you are doing it. It's not to tick boxes – it's to protect your customers, your employees and your business.
2. Train EVERYONE in the company on how to stay secure. It's easy to forget, so implement regular "quizzes" to check that everyone stays up-to-date with procedures.
3. Invest in your data security team. It may not be the whole part of someone's job, but make sure that every aspect of security has an individual who is responsible for it.
4. Restrict data access using the principle of least privilege. Make "deny all" your starting point.
5. Don't store data unnecessarily. If the data isn't in your systems, it can't be hacked.
6. Look at your customer interfaces and take steps to address any weaknesses. Use native apps rather than mobile websites, and protect your main website using HTTPS.
7. See who's trying to get in. Invest in technology like Darktrace or AlienVault to monitor your systems for attacks. If you have the resources, employ human penetration testers as well.
8. Put up some sensible defences. You can't beat every hacker, but investing in anti-virus and anti-spyware software is just common sense.
8. Consider geo-blocking. If most of your business comes from the same area geographically, you may want to block access from countries outside this region.
10. Bite the bullet and spend some money. The improvements to customer service, employee morale and your own corporate reputation will be well worth the investment.



We would like to offer our thanks to the experts who have contributed to this guide:

Jon Laws
Financial Controller, The Caravan and Motorhome Club

Carl Phillips
Group Director of IT, AO

Guy Gaskins
Executive Director of Information Technology & Resources, HCPC

Shane Lewis
Information Security Manager, Semafone

About Semafone

We are contact centre data security and compliance experts, working closely with enterprises around the world to remove sensitive data from IT and business networks. Our aim is to protect your customers and your company's reputation and to help you comply with industry regulations such as PCI DSS and EU GDPR.

Our award-winning, patented data capture method allows contact centre agents to capture personal information securely over the phone using dual-tone multi-frequency (DTMF) masking technology. This data includes payment card and bank account details as well as digital ID such as social security or healthcare numbers. Unlike interactive voice response (IVR) systems, agents remain in full voice communication with the caller as they enter their numbers into their phone keypad, ensuring a positive customer experience.

Semafone was founded in 2009 and we now support customers in over 25 countries on five continents, including AO, AXA, The British Heart Foundation, Rogers Communications, Santander, Sky, TalkTalk and parts of the Virgin Group.

And we practise what we preach: Semafone has achieved the four-leading security and payment certifications: ISO 27001, and PA-DSS for Cardprotect our payment security solution, we are a PCI DSS Level 1 Service Provider and a registered Visa Europe Level 1 Merchant Agent.

If you'd like to talk to us about how to make your contact centre secure, as well as achieving compliance with EU GDPR and PCI DSS, please email us at emeasales@semafone.com, phone 0845 543 0822, or visit www.semafone.com.

semafone®

securing data · protecting reputations

+44 (0)845 543 0822

emeasales@semafone.com

www.semafone.com

@semafone

LinkedIn

Pannell House, Park Street, Guildford, Surrey GU1 4HN

DSP EB UK 04/19