WAR STORIES: A GUIDE TO PCI DSS FROM THE FRONT LINE

KEEP CALM AND CARRY ON
How to respond effectively when bad things happen
LOOSE LIPS
SINK CHIPS
What policies should look like to improve security
YOUR COMPANY
NEEDS YOU
nce of engaging with the whole organisation to protect you

THE BUNKER

Arcturus

Part of the CYBERFORT group

THE CURRENT LANDSCAPE

In 2004, major payment card companies including Visa, MasterCard, American Express, and Discover came together to combat credit card fraud. The result was one set of guidelines dedicated to protecting cardholder data – and the Payment Card Industry Data Security Standard (PCI DSS) was born.

Over 14 years and eight versions later, PCI DSS compliance is now mandatory for any organisation around the world that transmits, processes or stores payment card data – including financial institutions, merchants, point-of-sale vendors, and hardware and software developers involved in developing payment processing technologies.

However, the idea of compliance and the reality of putting this into practice don't always go hand in hand.

The complex minefield

Although PCI DSS has been around for many years, a true understanding of how the standard is effectively implemented still evades many businesses. Verizon's 2018 Payment Security Report revealed a drop in PCI DSS compliance, with just 52.5% of organisations compliant with PCI DSS, compared with 55.4% in 2017. This decrease is particularly worrying when compared to the 2015 report, which showed that the level of compliance was on an upwards trajectory for the previous three years – highlighting that compliance has become more difficult with the advent of increasingly complex payment technologies.

52.5%
of organisations were compliant with PCI DSS in 2018

Maintaining compliance is often another challenge. In fact, according to Verizon, nearly half (47.5%) of organisations assessed in Europe for interim PCI DSS compliance validation had not maintained all of their controls, putting sensitive information at risk.

The reasons behind this declining trend could be as complex as the standard itself, because it's not a failure of one single aspect. Some organisations still also see PCI DSS as a 'tick-box' exercise rather than an ongoing process, requiring continual improvement in order to safeguard against evolving threats.

What is clear is that many of the finer points of the standard are not understood – and, it would seem, neither are some of the fundamental aspects.

Some would argue that taking security seriously should mean that you are automatically compliant with PCI DSS – something that has become increasingly important over recent years with the emergence of the General Data Protection Regulation (GDPR).

This regulation has rejuvenated interest in the protection of personal data. However, if a focus on GDPR has led to this decrease in PCI DSS compliance it could point to a dangerous and fundamental lack of understanding of what security is all about.

SOME ORGANISATIONS STILL ALSO SEE PCI DSS AS A 'TICK-BOX' EXERCISE RATHER THAN AN ONGOING PROCESS

THE COST OF NON-COMPLIANCE

It is a merchant's responsibility to demonstrate compliance with PCI DSS and it can incur monthly ongoing costs equating to hundreds of pounds if it is unable to do so. If a data breach is traced back to an organisation that handles cardholder data, costs could run into the thousands of pounds.

Evidence also shows that consumers often stop spending with a business in the aftermath of a breach, as well as many spending less with firms that they perceive as having weaker data controls.

When combined with fines under GDPR – which can reach up to €20 million, or 4% of annual global turnover – the inevitable financial loss and reputational damage resulting from a data breach can have an enormous negative impact on any business There is simply nowhere to hide.

Our research

In an analysis of all non marketing-related ICO fines issued from 2015 to 2018, we discovered that 21% were related to payment card data or financial information that wasn't sufficiently secured.

These fines ranged from £55,000 to £500,000, which could amount to almost £2 million or £18 million respectively under GDPR. In total, these fines could have amounted to over £800 million under GDPR* – a staggering cost, particularly when compared to that of implementing sufficient security controls.

Over three quarters of these breaches were due to issues at the application layer, often related to out-of-date software, third-party payment systems or inadequate scanning. In one case, issues in the code supporting the login page of a third-party payment system ultimately enabled an attacker to access over 26,000 cardholder details.

Almost a third of these breaches were down to organisations neglecting simple security hygiene. After all, rigorous testing becomes meaningless if 30-40 employees know the password to the server, and have full admin rights – a factor that played a major part in one breach.

All of these factors are considered and outlined in the PCI DSS guidance – from antivirus to testing systems and encrypting data. When it comes down to the details, however, organisations can struggle with focusing their attention in the right areas.

Despite the bleak outlook for those that neglect data protection, becoming compliant with PCI DSS can go a long way towards meeting the requirements of GDPR as well. Other compliance standards can also significantly help with this, including ISO 27001 and Cyber Essentials.

Equifax

When: **July 2017**

Fine: **£500,000**

Fine under GDPR: **£102,000,000**

What went wrong?
Despite the company scanning its network for issues, attackers were able to exploit a vulnerability in the Apache Struts 2 web application framework used to support an online portal.

TalkTalk

When: **October 2015**

Fine: **£400,000**

Fine under GDPR: **£71,320,000**

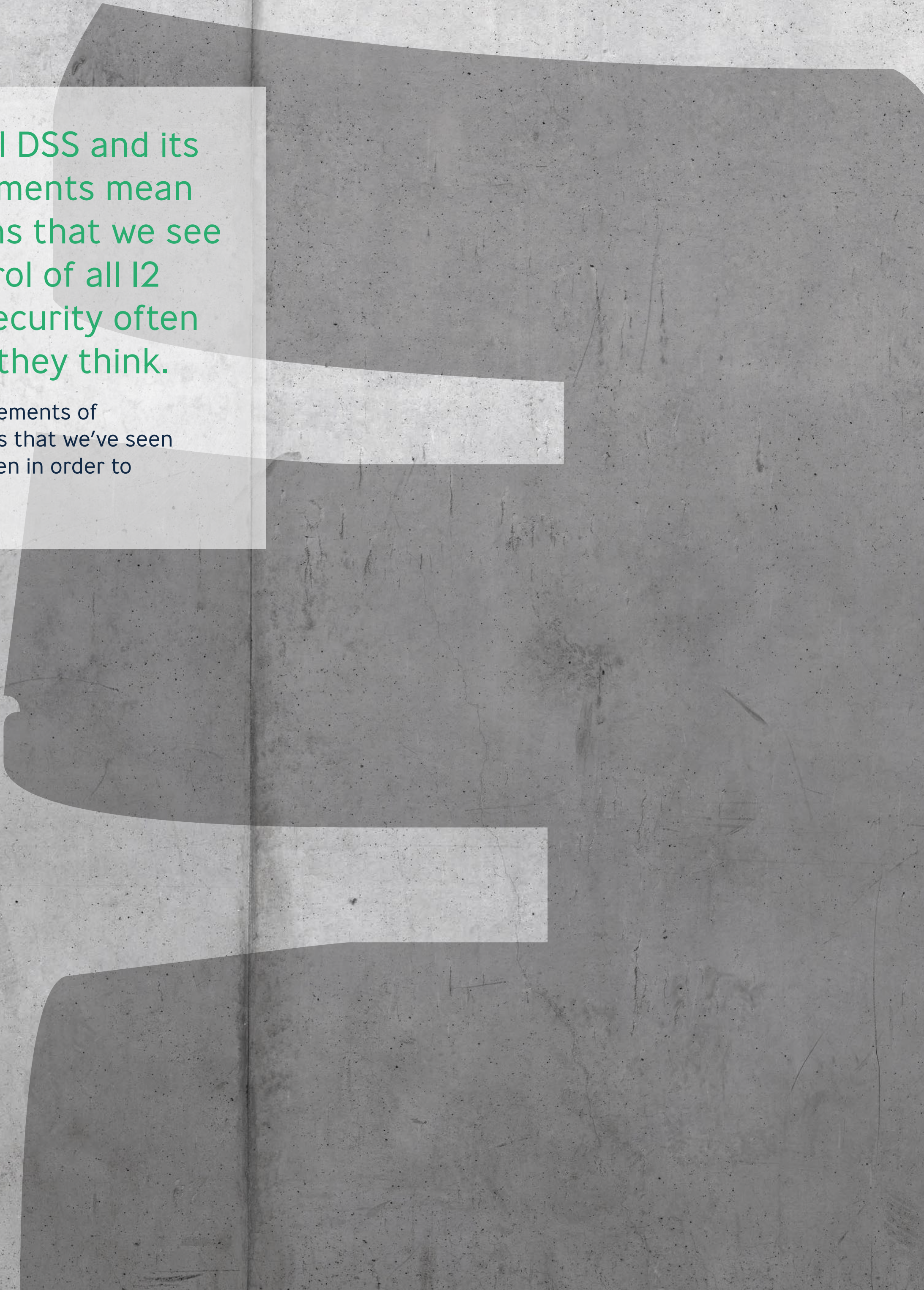
What went wrong?
The main cause of the breach was outdated database software – the solution was simply to update this.

*Calculated highest fine approximately by calculating the proportion of pre-GDPR fine as 4% of turnover or €20 million using the exchange rate of 1 Euro to £0.9. Exchange rate correct at 21st December 2018.

ONCE MORE UNTO THE BREACH: COMPLIANCE LESSONS FROM THE FIELD

The complexity of PCI DSS and its wide-ranging requirements mean that few organisations that we see are in complete control of all 12 requirements, with security often not as watertight as they think.

Here is a breakdown of the requirements of PCI DSS, alongside some scenarios that we've seen and the learnings that can be taken in order to maintain compliance.



Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Choosing an effective solution can be difficult. Many organisations also quickly discover that while having a firewall and perimeter defences is one thing, knowing how they are configured and managed is another. We worked with one organisation that said they had a firewall, and despite scanning for it across the network it couldn't be found. Eventually we found it in the server room... still in its box.

- ✓ **Choose a solution that spans your whole IT estate:** A firewall must be far-reaching in order to be compliant. This means examining all network traffic – including seemingly insignificant paths to and from e-commerce sites, third-parties and wireless networks – and blocking any transmissions that don't meet specified security criteria.
- ✓ **Keep track of your changes:** Under PCI DSS, a log of all changes made to the firewall is required for a mandatory six-monthly check.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

BUSINESSES OFTEN PUT THEIR FAITH IN VENDOR-SUPPLIED PRODUCTS, BUT, IN REALITY, VENDORS PUT THEIR FAITH IN ORGANISATIONS TO CARRY OUT BASIC CHECKS

We often work with businesses that think they have locked down their systems, yet we frequently uncover obvious admin passwords. We once worked with pen testers who were able to access the directors' shared wireless access point within a large financial institute while sitting in the car park. The team then discovered unencrypted cardholder data by simply trying the default password.

- ✓ **Change passwords upon installation:** Vendor passwords form an open door for attackers and are easily accessible online, so should be changed straight away.
- ✓ **Audit your attack surface:** If you haven't got around to changing your password, should you? Or do you even really need the software?

Requirement 3: Protect stored cardholder data

This is about process, and ensuring that cardholder data is stored, transferred and processed securely at every stage. While auditing one private school, we were impressed to discover a robust process for managing term payments, using secure third-party vendors. Then we found a full spreadsheet containing card payment details. The financial clerk said she was "taught to do it that way" when she started at the school ten years ago.

- ✓ **Minimise risk:** Cardholder data should not be stored unless it is absolutely necessary. If it is, the system used to process this information should mask the Primary Account Number (PAN) when it is displayed.
- ✓ **Understand your data landscape:** Organisations should commit to carrying out an audit of all data processing practices, including both digital and physical records, in order to understand where changes need to be made.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

We've worked with many organisations that believe that using an approved encryption standard – today, TLS I.I or higher – is enough to keep cardholder data safe in transmission, but this only applies to one point in time. To be truly secure, there is far more that should be done.

- ✓ **Map your data flow:** Understanding the entry and exit points for cardholder data in your organisation, externally, and throughout your supply chain, is the first step towards implementing robust data transmission practices.
- ✓ **Enforce good practices:** It's vital that employees only send cardholder data and other sensitive information over encrypted email, rather than using public or open networks. All devices should also use some form of VPN to transmit data.

Requirement 5: Use and regularly update antivirus software or programs

With new threats emerging every day, it is crucial to ensure malware and antivirus updates are regularly applied and tested. We once met an IT manager who was proud to have deployed malware protection across his network. However, we quickly discovered that regular patching and updating of the software did not take place, making this investment in security systems redundant.

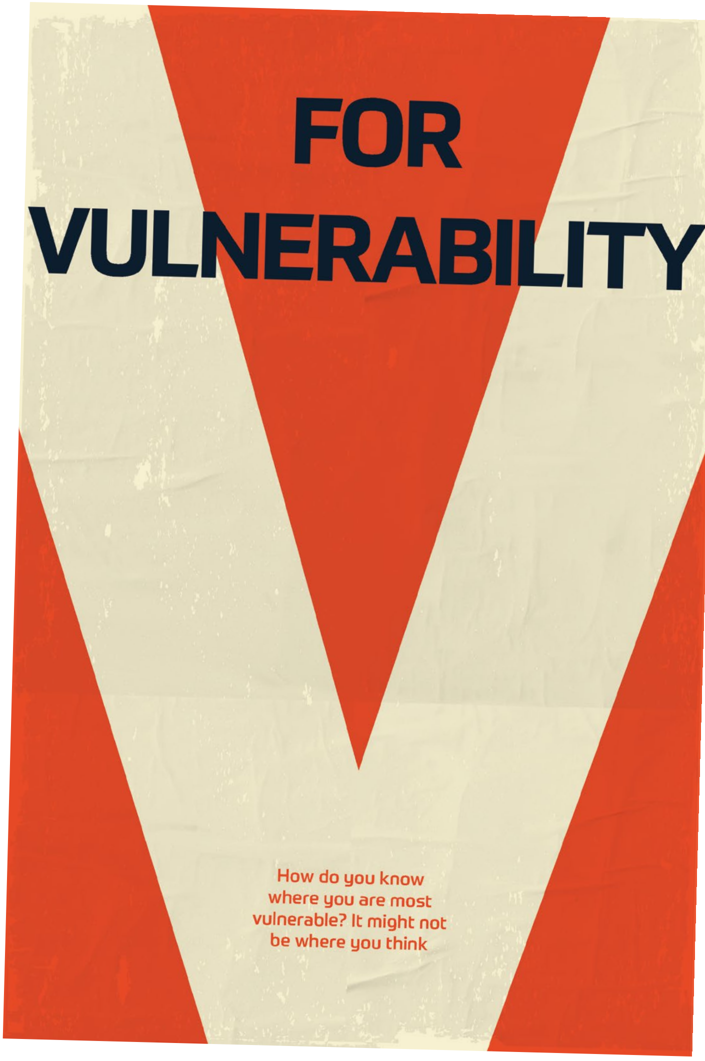
SYSTEMS SHOULD BE REGULARLY ASSESSED AND INTEGRATED WITH YOUR CHOSEN SOFTWARE.

- ✓ **Identify your attack surface:** Business-approved activities are often areas where malware can slip through the net, including e-mails and internet use, or via mobile and storage devices. Knowing these points of entry will highlight where antivirus is needed.
- ✓ **Stay on top of threats:** Proactivity is required to keep antivirus solutions working as they should be. This should include patch management, routine system maintenance and keeping up-to-date with cyber threats.

Requirement 6: Develop and maintain secure systems and applications

We often find that definitions of "secure" differ significantly from one organisation to another – the main reason is a lack of senior level support and investment, with board members often unaware of, and not invested in, security procedures.

- ✓ **Understand new vulnerabilities:** Establish processes to identify and assess security vulnerabilities with a risk ranking such as high, medium, or low.
- ✓ **Check your code:** Developers should carry out regular security reviews of code to expose any vulnerabilities, and testing should be baked into the software development life cycle, using Open Web Application Security Project (OWASP) as a resource.
- ✓ **Have a robust change control process:** Ensure that any changes to systems are documented, with a well-established audit trail available for compliance and forensic purposes.


FOR
VULNERABILITY
How do you know where you are most vulnerable? It might not be where you think

Requirement 7: Restrict access to cardholder data by business need-to-know

SYSTEMS SHOULD BE REGULARLY AUDITED TO ENSURE THAT ACCESS LEVELS ARE CORRECT.

Individuals shouldn't be allowed access to any sensitive data unless they specifically need it to perform a task that relates to their job role. While helping a retailer investigate several credit card fraud incidents, we discovered that some people in the organisation had access to the Cardholder Data Environment (CDE) merely because they had worked there for a long time. There was also no logging of how information was being accessed, making it clear how the fraud could have occurred.

- ✓ **Implement Role Based Access Control (RBAC):** RBAC is a clear process which ensures that access to cardholder information is determined by an individual's role, meaning people don't have access to any sensitive details unnecessarily.

Requirement 8: Assign a unique ID to each person with computer access

The problems associated with this were highlighted one Saturday when we received a call from a distressed director. A database containing more than 1,200 financial details had been stolen by an ex-employee and was being used by a competitor. We discovered that all 200 employees had access to this database without unique IDs or passwords, making it impossible to identify the culprit.

- ✓ **Keep it simple:** Many organisations are wary of impacting productivity when reducing employee access, but this doesn't have to be the case. Developing and maintaining secure policies and procedures promotes best practice across an organisation.
- ✓ **Create a solid perimeter:** Employing a robust password strategy, which requires passwords to be changed every 90 days, as well as providing unique access codes for any third-party suppliers, should be seen as best practice. Two-factor authentication is also worth considering to ensure that data remains as secure as possible.

Requirement 9: Restrict physical access to cardholder data

This stage is a common afterthought. One organisation we engaged with introduced ID cards after a polite employee held the door open for a potential client, allowing them to freely enter the building. Within minutes the potential client was sitting near the finance team, with cardholder data left in clear view on a desk. An uncomfortable meeting followed, and ultimately a lost opportunity, as the client had major concerns surrounding the storage of data.

- ✓ **Know your pain points:** Start with a full audit of where cardholder data is physically held, and how it is handled transferred and destroyed, including back-up devices such as USBs.
- ✓ **Move your data if necessary:** Physical security can be difficult to maintain, so it's worth investing in dedicated, secure suites to ensure that sensitive information is stored securely.
- ✓ **Get everyone involved:** Controlling physical devices in particular requires an understanding from everyone in an organisation. Make sure that everyone knows the rules.

YOUR COMPANY
NEEDS YOU
Importance of engaging with the whole organisation to protect you

Requirement 10: Track and monitor all access to network resources and cardholder data

Tracking access to network resources isn't enough – it's important to analyse this as well. Upon exploring how audit logs were monitored and tracked by one of our clients, we discovered that the company enabled logging but hadn't the time nor resource to review them. We then identified a user with administrative rights who was copying large quantities of data, included cardholder data, to a secure 'holding area' and looking for confidential information to sell to competitors.

- ✓ **Have a process to review data:** Once the size and complexity of the corporate network has been considered in order to track activity, identifying and responding to issues should then be tackled through dedicated analysis or automated Security Information and Event Management (SIEM) systems.
- ✓ **One solution doesn't fit all:** It's important to upgrade and tweak any monitoring systems as a business changes, to properly safeguard the entire network.

Requirement 11: Regularly test security systems and processes

This is all about having the knowledge and skills to thoroughly test systems for security weaknesses. For most businesses, the increasing complexity of legacy systems combined with new assets quickly compounds weaknesses, making spotting issues extremely difficult. Testing the security of one supermarket, we discovered a till that provided access to the local outlet network and central head office systems – all with the help of circuitry bought on eBay for under £10.

- ✓ **Regular means regular:** PCI DSS clearly outlines what it expects from the testing of security systems, with "regular" meaning at least quarterly external and internal vulnerability scans, and penetration tests annually at a minimum, as well as following any significant network changes.
- ✓ **Know how to respond:** It's crucial to ensure that an escalation process is in place, so that those responsible are clear on what to do upon discovery of any vulnerabilities or issues.

Requirement 12: Maintain a policy that addresses information security for employees and contractors

We've seen the most robust of security policies offset by one individual failing to follow procedures, whether that's transmitting information across public WiFi, or working on their own, insecure device. There's no magical policy to prevent this – it's about minimising the risk, and crucially, setting the example from the top down.

- ✓ **Awareness is key:** It's vital that everyone – including full-time, part-time and temporary employees, contractors, and consultants that have access to cardholder data - fully understands the sensitivity of company data and their responsibilities for protecting it.
- ✓ **Look to other compliance standards:** ISO27005 is mentioned in PCI DSS, but organisations should also assess their measures against ISO27001 when creating a security policy, as this sets out a framework to ensure all personnel properly understand information security.

THE FIVE P'S: CONSIDER SECURITY POLICIES THAT ARE FOCUSED ON PEOPLE, PREMISES, PROCESSES, PCS, AND PROVIDERS.

WE CAN
DO IT
Why IT is important, but not the whole story in your PCI DSS armoury

In a world that is becoming more technologically advanced and connected by the day, information security is an ongoing challenge. But standards like PCI DSS bring clarity to what needs to happen in order to demonstrate the protection of cardholder data, and that security is taken seriously.

Our PCI DSS experts are on-hand to discuss your requirements and assess your organisation's health and readiness with regards to the standard.

To find out more, get in touch to speak directly with a member of our team.

THE BUNKER

Arcturus

The Bunker
www.thebunker.net
info@thebunker.net
01304 814 800

Arcturus
www.arcturussecurity.com
info@arcturussecurity.com
01635 015 635

Part of the CYBERFORT group