Bolsover District Council

Executive

16th September 2019

Payment Cards Industry Data Security Standards Compliance

Report of the Portfolio Holder – Corporate Governance

Purpose of the Report

- To raise Executive awareness of potential cost and service implications in progressing towards Payment Cards Industry Data Security Standards (PCI-DSS) compliance.
- For Executive to review options and seek approval for measures to facilitate progress towards compliance with the PCI-DSS.

1 Report Details

Background

1.1 The PCI Data Security Standard was originally formed by Visa and MasterCard to bring together their individual compliancy programs. Three other payment brands, American Express, Discover and JCB then joined up which lead to the PCI SSC (Payment Card Industry Security Standards Council) being formed as an independent industry standards body providing oversight of the development and management of Payment Card Industry Security Standards on a global basis.

1.2 The PCI DSS covers the security of all entities that store, process and/or transmit cardholder data including; merchants, processors, acquirers, issuers and service providers as well as all other entities that store, process or transmit cardholder data. The PCI DSS is intended to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. This is built upon 12 requirements as shown in the table below; each one consisting of over 240 individual requirements (v3.2).

Control Objectives		Requirements
Build and Maintain a Secure Network	1.	Install and maintain a firewall configuration to protect cardholder data.
	2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3.	Protect stored cardholder data.
	4.	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Programme	5.	Use and regularly update anti-virus software or programs
	6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7.	Restrict access to cardholder data by business need to know.
	8.	Assign a unique IT to each person with computer access.
Regularly Monitor and Test Networks	9.	Restrict physical access to cardholder data.
	10.	Track and monitor all access to network resources and cardholder data.
Maintain an Information Security Policy	11.	Regularly test security systems and processes
	12.	Maintain a policy that addresses information security for personnel.

1.3 A breach of compliance involving the loss of card holder data can result in:

- Significant financial penalties ranging from £1000's to £100,000's, enforced by the five payment card brands: Visa, MasterCard, American Express, JCB International and Discover.
- In addition, related data breaches enforced by GDPR legislation
- Damage to organisations reputation
- Loss of customer trust

1.4 In order to reduce the scope of PCI and therefore our exposure to risk, the Council should work towards ensuring all risks associated with card payments are reduced as far as is practical.

1.5 A risk management approach must be taken, key elements are:

- Identify all known risks and record them on a risk register
- Develop a risk management program to determine the risk and identify solutions to reduce risk
- Implement / work towards solutions to mitigate the risk
- Continue to monitor and review

1.6 The Council operates three different card payment channels; e-commerce, card-present and card-not-present. Approximate transactions over a 12 months period (1.4.18 – 31.3.19) is as follows:

- Automated Telephone transactions is approx. 12,693 per year,
- Operator Assisted Telephone transactions is approx. 20,681 per year,
- E-Commerce transactions is approx. 28,025 per year,- Pin Entry Device transactions (kiosks) is approx. 15,696 per year.

With the total number of card transactions being approx. 77,095 per year, the Council is classed as a level 3 merchant which means a self-assessment questionnaire is completed to certify compliance.

1.7 A PCI Working Group was convened to fully consider the implications to the Council. To date, this group has:

- Commissioned Sec-1 Ltd Security Testing to undertake a gap analysis to identify the key areas to address.
- Received presentations from payment providers to develop understanding possible solutions for card not present payments
- Undertook corporate assessment during 2018 to identifying all non-compliance areas
- Site visits have been undertaken with other Councils to establish how they are addressing compliance.

1.8 At this point in the journey towards compliance there are two key areas that require addressing by the Council:

- Future use of payment kiosks across the contact centres
- Risks inherent within the current cardholder not present payment processes

Payment Kiosks

1.9 As of 1st January 2020, regulations are changing in relation to cardholder present electronic payments. All point of sale (POS) terminals must offer contactless functionality. Therefore the existing payment machines are non-compliant.

1.10 In addition, the current supplier, Banking Automation, will no longer support the payment machines beyond 31st December. By continuing to take card payments through the payment machine after this date the authority would be at risk of non-compliance. Also, due to being unsupported, the machine will not be updated to receive the new £20 note in 2020.

The forecast cost is in the region of £15,000 for a compliant payment machine. Therefore, total forecast cost for replacement is £60,000.

1.11 The usage of the kiosks across the contact centres can be seen in the tables below:

Table 1: Number of transactions

Contact Centre	2016/17	2017/18	2018/19
Bolsover	16,434	14,812	13,498
Shirebrook	22,297	19,475	17,562
South Normanton	16,423	14,369	12,888
Clowne	18,689	16,062	13,702
Total	**73,843**	**64,718**	**57,862**

Table 2: Value by payment type:

Contact Centre	2016/17 £	2017/18 £	2018/19 £
Bolsover			
Cash	769,712.45	675,559.85	636,502.18
Cheque	135,894.54	125,704.92	127,249.41
Card	455,792.76	424,547.95	406,427.13
Shirebrook			
Cash	1,190,292.74	987,364.14	930,693.24
Cheque	156,530.67	122,475.53	59,815.16
Card	646,091.12	609,619.41	612,031.41
South Normanton			
Cash	948,972.68	846,738.11	766,190.07
Cheque	140,390.38	128,357.05	106,310.32
Card	485,623.27	473,407.10	463,521.62
Clowne			
Cash	754,127.66	678,269.92	632,246.68
Cheque	331,124.44	267,088.43	258,134.44
Card	456,246.30	432,516.27	429,825.46
Total	**6,470,799.01**	**5,771,648.68**	**5,428,947.12**

Average Contact Centre monthly value by type:

- Cash: £61,000 per month
- Cheque: £11,500 per month
- Card transactions: £40,000 per month

1.12 To address the compliance issue it is recommended that Executive considers three options:

Option 1 - Replace payment kiosks at the Contact Centres with a like for like kiosk taking cash and card payments.

- Cost of **£58,144** for four new kiosks and **£6,340** annually for support and maintenance.

Option 2 – Replace payment kiosks at the contact centres with card only payment devices

- Cost of **£47,824,** or **£41,416** (wall mounted) for four new kiosks and **£4,470** annually for support and maintenance.

Option 3 – Move to cashless operation at all Contact Centres

- Aligns with strategic transformation aims
- Avoids significant expenditure as with options 1 and 2
- Cost saving on cash handling of **£22,000** per annum

1.13 In addition to the payment kiosk, irrespective of Executive's preferred option, customers will continue to have access to alternative methods of payment such as:

- 24 hours a day via the website
- 24 hours a day automated telephone payment line (Council Tax, Rents, Sundry Debtors, NNDR, Overpayments only)
- At any Post Office or PayPoint outlet by cash or debit card using your Council Tax (This is an option that is not promoted and only for customers who do not live near a contact centre. Customers have a payment card and can only pay for council tax. It is an expensive method of payment.)
- Telephone card payments taken during opening times by the Customer Service Advisors
- Direct debits and Standing Order arranged through a bank with payment dates of the customer's choice

Customer Not Present payments

1.14 Our current telephone payments processes for Customer Not Present card payments are currently not PCI-DSS compliant. Currently an officer taking payments must enter the card details on behalf of the customer into our payments solution. To mitigate risks inherent in this process, it is necessary to remove the exposure of the officer from the customer's card details, and remove these details from our network

1.15 To address the compliance issue three options are proposed:

1. Civica, our payments solutions provider, have an 'off the shelf' end call solution called CallSafe, the revised process would be:

    a) Officer captures customer details up to the stage of the card detail entry, at which point:

    b) To help safeguard the customers card, the system provides a four digit number and the operator transfers the call to an automated service to take their card details

    c) The customer enters the four digit pin, the automated service finds the transaction details and speaks the amount to be paid. The card details (card number, start date etc.) are entered by the customer using a telephone keypad.

    d) The basics of this system is that the call is transferred to the Civica Hosted Data Centre where ATP completes the payment.

    e) The approximate cost of this solution is an initial £7,000 implementation fee, an application license fee of £18,000 and annual hosting charges of £4,000.

2. Civica also have a mid-call solution in partnership with PCI Pal which requires no changes to the current process and offers Contact Centre Advisor support to the customer throughout the process. This option is currently under discussion with both parties to ascertain ICT requirements, options available and costings. Indicative cost to date are initial £15,340 implementation fee, an application license fee of £18,000 and annual hosting charges of £17,745.

    Consideration needs to be given to ensure that all incoming calls that could take a payment come via a line that diverts to PCI Pal. The more numbers we divert to PCI Pal (for example council tax, MOT, etc), the more cost we will incur. Every call that goes through PCI pay will incur a charge. So, if we divert 2424 to PCI Pal, all calls to 2424 will have an associated charge, whether or not a payment is made.

3. An extension of the current Automated Telephone Payments (ATP) solution. Currently, the Council utilise an ATP to take telephone payments for a number of funds. This solution would involve engaging Civica to implement additional payment fund types and some work from ICT, Customer Services and Finance to implement. It is understood that this would provide a similar outcome as the Civica End call solution (1. above) but at less cost. The revised process would be similar to that outlined above. The advisor will then need to log into the reporting system to check the payment has successfully processed and obtain the reference number. This solution would require further testing from both a technical and customer service perspective but has the risk of being inefficient and increase the likelihood of human error.

Essential upgrade of current online payment provision

1.16 Not directly related to PCI compliance but a consideration to support secure and accessible online transactions, the current Webpay Public online solution (payments

via the Council website) has been in use for 8 years and Members should be aware that Civica have moved this solution to their 'end of service' phase. This product is based on technology that is 15 years old, and is not mobile friendly. The 'end of service' phase means that Civica will continue to provide support and critical security updates at the moment, but will not be investing any further development in it. The next stage will be the solution becoming unsupported and this presents unacceptable security risks.

1.17 The recommendation is to move to the latest mobile commerce solution (EStore Lite) that would improve the usability and accessibility to customers and is provided by Civica and compatible with existing systems. It is fully integrated with the CivicaPay solution and utilises existing validations and automated back office processing. It also allows mobile page rendering of web pages for all mobile devices and applications.

1.18 The approximate cost of the EStore Lite solution is £30,000 for the license application and implementation fee, together with annual hosting charges of £4,000.

2 Conclusions and Reasons for Recommendation

2.1 The report aims to raise Executive's awareness of an emerging compliance issue and related upgrades that could result in significant additional cost to the Council. Officers will continue to develop the solutions and will present a final proposal in a further report close to the end of the calendar year.

2.2 Whilst this work progresses, Executive should consider options to reduce the amount of cash taken in each Contact Centre, working with customers to encourage alternative methods of payment.

2.3 Resource will be committed to progress investigation with regards to the Civica 'PCI Pal' solution. Process changes may be required in relation to service areas outside of the Contact Centre taking card payments.

2.4 The recommendations seek to provide a practical and economical solution to ensure PCI DSS compliance, whilst maintaining or enhancing the customer experience and trust in the Council when it comes to personal and sensitive data.

3 Consultation and Equality Impact

3.1 Consultation has initially been undertaken with the relevant departments such as ICT, Finance and Customer Services.

3.2 Procurement and Legal will be engaged prior to any procurement exercise.

4 Alternative Options and Reasons for Rejection

4.1 At this time the alternative options whilst not being actively pursued have not been ruled out. A further report will be provided to present the implication and progress of driving down demand for kiosk usage and future Cardholder Not Present solutions.

5 Implications

5.1 Finance and Risk Implications

5.1.1 No funding is required at this stage to support the implementation of the recommendations.

5.2 Legal Implications including Data Protection

5.2.1 In order to reduce the scope of PCI, organisations should work towards ensuring all risks associated with card payments are reduced as far as is practical.

This reports demonstrates that we are working towards practical solutions however, a breach could result in:

- Significant financial penalties ranging from £1000's to £100,000's, enforced by the five payment card brands: Visa, MasterCard, American Express, JCB International and Discover.
- In addition, related data breaches enforced by GDPR legislation
- Damage to organisations reputation
- Loss of customer trust

5.3 Human Resources Implications

5.3.1 Depending on the option which Executive choose to pursue regarding the kiosks, there may be Job Evaluation implications through the removal of cash handling from some roles. Whilst this may trigger a review, 'Responsibility for Finance' is one factor in the process and it doesn't necessarily mean a change in pay grade. As with all HR matters of this type, any review will follow the relevant policy and Union consultation will be undertaken.

6 Recommendations

6.1 That Executive:

(i) note the content of the report and acknowledge potential cost implication outlined within the report.

(ii) consider the options in 1.12 and decide on a preferred option.

(iii) receive a further report on proposals for a future payment strategy.

7 Decision Information

Is the decision a Key Decision? A Key Decision is an executive decision which has a significant impact on two or more District wards or which results in income or expenditure to the Council above the following thresholds: *BDC: Revenue - £75,000* ☐ *Capital - £150,000* ☐ *NEDDC: Revenue - £100,000* ☐ *Capital - £250,000* ☐ ☑ *Please indicate which threshold applies*	No
Is the decision subject to Call-In? (Only Key Decisions are subject to Call-In)	No
Has the relevant Portfolio Holder been informed	Yes
District Wards Affected	All
Links to Corporate Plan priorities or Policy Framework	All

8 Document Information

Appendix No	**Title**
Background Papers (These are unpublished works which have been relied on to a material extent when preparing the report. They must be listed in the section below. If the report is going to Cabinet (NEDDC) or Executive (BDC) you must provide copies of the background papers)	
Sec-1 Ltd Report: Cardholder Data Environment Mapping – Oct 18	
Report Author	**Contact Number**
Head of Partnerships and Transformation	2210