



“The experts at Gradeon were able to meet a worldwide standard to protect card payments securely and reduce card fraud. They did this through tight controls surrounding storage, transmission and processing of cardholder data that the building society handle, mitigating any risks across the entire organisation”

Craig Marston, Director at Gradeon

“Protecting card holder data for one of the world’s largest building societies”

Client Benefits

- ✓ Mitigating risk across the entire organisation including branches nationwide.
- ✓ Protecting card holder data as per the latest PCI DSS requirements.
- ✓ Reducing card holder data from 18 million to 3 million.

Background

Organisations such as building societies, banks, insurers and investment firms are increasingly heavily regulated.

Privileged account abuse presents one of today’s most critical security challenges. One of the world’s largest building societies with millions of members and several hundred branches across the UK were looking to meet PCI DSS requirement around protecting card holder data.

Also as a major mortgage provider and one of the UK’s largest savings providers, security for its members was paramount.



The Challenges

The building society offers internet based and mobile banking services and faced increasing pressure to provide enhanced consumer protection against phishing, sophisticated malware and fraudulent activities.

The IT infrastructure was managed by users who are given passwords to ensure that the performance, resources and security of all computers including desk tops and drives to meet the needs of the business. Misuse of users has become one of the most critical security challenges and in line with the latest PCI DSS requirement all card holder data must be protected. Another challenge was assigning data ownership, identifying which department should own the data and therefore ensure the security of that data.

Solution

Gradeon firstly carried out a full audit to scope where all card data was held and the ongoing security processes surrounding it. This allowed ownership to be assigned to each department to help make the data secure.

Macros were created to reduce the workload associated with managing the process and the data discovery tool was tuned in order that algorithm was applied to identify all card hold data. This successfully stripped out phone numbers and other numbers that could be mistaken for card holder information. This gave Gradeon the ability to provide as dashboard that clearly showed what the organisational wide risk. It also provided a view of cardholder data held in each department.

Gradeon were then able to put processes in place, recruit and train permanent members of staff to carry out the formal daily reporting required and change the culture of the organisation.

Results

- ✓ Successfully reducing cardholder data held from 18 million to 3 million.
- ✓ Changing the culture and ensuring the 100's of departments and branches met compliance.
- ✓ Ensuring all levels from directors to bank clerks were aware of their responsibilities in meeting compliance.
- ✓ Ensured that cardholder data could not leak into applications such as SharePoint, end user computing such as laptops and hardware such as email servers.

“

Gradeon were able to offer added value such as helping to identify which departments should have data ownership and put the necessary training and security in place.

Craig Marston, Director at Gradeon

”