IT Governance

Cyber Security Audit

Sample report

Protect • Comply • Thrive

Cyber Security Audit Report
Prepared for
Evelyn M.,
Chief Information Officer,
Lannister PLC

Table of Contents

1.0 Executive summary

IT Governance Ltd was invited to conduct a cyber security audit and review at Lannister's Manchester offices on the 18th June 2017 following a data breach that affected 50,000 customer accounts. **The purpose of the audit was to assist the executive team in developing a strategy for managing cyber security**.

A summary of the recommendations made during the cyber security audit is detailed in Section 2. The recommendations can be categorised as Non-Technical (NT), Technical (T) and Physical (P).

2.0 Cyber Assessment Summary Recommendations

2.1 Governance Recommendations

- Assign accountability and responsibility for security to an individual or individuals. (NT)

2.2 Asset Recommendations

- Compile an asset register with sections for hardware, software, data, people, processes, intangibles and third parties etc. (NT)
- Implement an information classification policy and labelling. (NT)

2.3 Risk Management Recommendations

- Conduct a risk assessment at regular intervals the organisations assets and apply controls applied where applicable. (NT)

2.4 Training and Awareness Recommendations

- Provide security awareness training to all staff on induction and communicate security updates at regular intervals. (NT)

2.5 Policies and Procedure Recommendations

- Document security policies, procedures, internal processes and technical work instructions. (NT)

2.6 Physical Security Recommendations

- Secure unattended offices, server rooms and filing cabinets. (P)
- Implement a clear desk and clear screen policy. (P)

2.7 Incident Response Management Recommendations

- Document an incident response management process. (T)

2.8 Business Continuity Management Recommendations

- Test the business continuity plan or arrangements. (T)

2.9 Third Party Recommendations

- Carry out third party supplier risk assessments. (NT)

2.10 Legal, Regulatory and Contractual Recommendations

- Prepare for the EU GDPR regulations. (NT)

2.11 Secure configuration

- Implement a standard build and roll out across all devices. (T)

2.12 Network security

- Implement regular vulnerability scanning and monitoring e.g. SolarWinds, Nessus. (T)

2.13 Anti-Malware

- Document and implement a patching policy for all hardware and applications. (T)

2.14 User Access and User Privileges

- Document an access control policy. (T)

2.15 Mobile devices, mobile working and removable media

- Document a BYOD policy for internal and external users.
- Enable remote wiping on mobile devices. (T)

2.16 Data storage

- Introduce a data retention policy. (NT)
- Encrypt all data in storage and transit. (T)
- Introduce a data and device disposal policy. (P)

2.17 Development

- Avoid using live data for development testing. (NT)
- Document the development process. (NT)

2.18 Security Monitoring

- Introduce network and device monitoring. (T)
- Introduce an IDS (intrusion detection solution). (T)

3.0 Conclusion

The UK government's National Security Strategy acknowledges cyber threats as one of the four major risks to national security.

Lannister is in the process of developing a robust cyber security strategy to support its future requirements.

Twenty-five (25) recommendations were made following the high-level cyber security audit.

Implementation of the summary report recommendations was carried out over a period of twelve weeks. Lannister is happy to report that they have not been breached since carrying out the Cyber Security Audit. Furthermore, thanks to the recommendations of the summary report, Lannister has been able to detect and prevent potential malware attacks.

For more information on how IT Governance Ltd. can help you establish a solid IT security foundation with our **Cyber Security Audit**, please call **+44 (0) 333 800 7000** or email **servicecentre@itgovernance.co.uk**.

We, of course, practice what we preach:

(Disclaimer: The report is based on a real-life consultancy project carried out by IT Governance Ltd. Names have been changed to protect the identity of the clients.)