TO: IT Manager, Stakeholders
FROM: Temilola Allen-Ijewere
DATE: Thursday 24th August 2023
SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

Please review the following information regarding the Botium Toys internal audit scope, goals, critical findings, summary and recommendations.

Scope: Our internal audit scope was aimed at ensuring our existing systems, security tools and hardware/software were functioning properly to keep the assets of Botium Toys secure. We also want to ensure that we are complying with any international laws as we have seen extreme growth worldwide.

Goals: Our goals were to identify any vulnerabilities within our existing systems and update them whilst adhering to the National Institute of Standards and Technology of Cybersecurity Framework (NIST CSF)

Critical findings (must be addressed immediately):
Administrative findings include:

- Ensure third-part vendors and non-authorised staff only have access to the data they need to do their jobs
- Disaster recover plans to ensure business continuity and minimise the impact to our reputation
- Password policies - current passwords are too weak and could be easily compromised
- Lack of confidentiality and integrity of data (Access control policies)
- Lack of separation of duties - users currently have more access than needed and can abuse the system for personal gain
- Lack of compliance with NIS CSF and the E.U General Data Protection Regulation

Technical findings include:

- Lack of an intrusion detection system - slows down the responsiveness of the IT team when identifying possible intrusions on the network
- Lack of encryption - user's sensitive data can currently be read in plain text, so there is a lack of confidentiality.

- No password management system - users can be locked out of their account with no way to get back in
- Antivirus software - we can be attacked by malicious software and have our data held at ransom or have our data breached easily

Physical findings include:

- Lack of CCTV cameras nor locking cabinets - we currently have no way to monitor our building or the equipment room
- Lack of fire alarms - in the event of a fire, the team will be unaware of this which could lead to severe data loss and inventory damage.

Findings (should be addressed, but no immediate need):

- Regularly scheduled data backups
- For our older systems, we need manual monitoring and maintenance
- A time-controlled safe is required in the event of a physical break-in but not urgent
- Lack of Adequate lighting increases the chance of hiding places within the building but is not urgent.

Summary/Recommendations:

- We should enforce stricter password policies to minimise the risk of a compromised account as well as offer
- Start encrypting our files into secure ciphertext which means it cannot be decoded without the cipher which will be stored on our servers. This will drastically improve the confidentiality and safety of our data.
    - This encryption also ensures we comply with the GDPR laws of the E.U and avoid any fines
- We can update user permissions to ensure correct levels of access are distributed amongst the company, limiting any opportunities for the abuse of power, or in the unfortunate event, limit the overall impact of a disgruntled employee.
- Lastly, we can implement regular backups and disaster recovery plans to minimise the damage done to Bortium Toys' reputation and to ensure the business is still able to run despite the incident.