Legal, Regulatory and Compliance Considerations

Legal, Regulatory and Compliance: The Real

According to IBM's 2020 Cost of a Data Breach Report, the average total cost of a data breach is $3.86 million. This increases to an average of $8.64 million for breaches in the United States.

A Cybersecurity and Data Privacy Study by NTEN reported that over 70% of donors are concerned about how nonprofits manage and use their personal data. Failure to comply with data protection regulations can lead to a loss of donor trust, which can directly impact donations and funding.

Legal, Regulatory and Compliance: The Truth

According to a study by Rapid7, organizations that have implemented a comprehensive compliance program, including regular audits and updates, have seen a reduction in data breaches by up to 50%.

According to a study by Deloitte, nonprofits that comply with cybersecurity regulations have increased operational resilience, enabling them to recover up to 30% faster from cyberattacks.

Legal, Regulatory and Compliance Considerations

Legal, regulatory, and compliance aspects are crucial to any cybersecurity program. The Knowledge House must comply with regulations such as PCI DSS, FERPA, COPPA, the NY SHIELD Act and GLBA, even though some of these regulations are not designed specifically for non-profits. Complying with these regulations will ensure the security and privacy of the donor, student, and other sensitive information.

Payment Card Industry Data Security Standard (PCI DSS)

The PCI DSS is a set of security standards to ensure secure handling of payment card information. It provides a comprehensive framework of requirements and best practices for organizations that handle, process, store, or transmit payment card data. Compliance with the PCI DSS demonstrates an organization's commitment to protecting sensitive cardholder data and reducing the risk of data breaches. It helps maintain customer trust, avoid financial penalties, and ensures a secure payment card environment.

Satisfying PCI DSS Regulatory Requirements and The Knowledge House

The Knowledge House, as an educational nonprofit, actively engages in online donation collections, often accepting credit card donations. Due to the nature of these transactions, compliance with the PCI DSS is crucial. To satisfy the regulatory requirements of the PCI DSS, The Knowledge House should focus on key areas including: scope identification, compliance assessment, data encryption, secure network infrastructure, access controls, and vulnerability management.

PCI DSS Violations: Examples and Consequences

PCI DSS violations can occur in various ways such as storing sensitive cardholder data unnecessarily, allowing weak passwords, not implementing robust network security measures, and failing to restrict access to cardholder data. Violating the PCI DSS can lead to fines, up to $100,000 per month, increased transaction fees, reputational damage, legal consequences, and termination of card processing privileges. Remediation costs are also a significant consequence of non-compliance.

The Family Educational Rights and Privacy Act (FERPA)

FERPA is a federal law that protects the privacy of student education records. While it isn't specifically designed for non-profit organizations, compliance with FERPA encourages such organizations to implement measures for the protection of student education records. FERPA's key components include Data Security, Monitoring and Auditing, and Training and Education, which are crucial for securing student information and protecting the organization against data breaches.

Children’s Online Privacy Protection Act (COPPA)

COPPA is a law that places parents in control over what information is collected from their young children online. Though The Knowledge House, as a non-profit, is not subjected to COPPA, it's recommended to protect COPPA’s protections to potential child visitors. Violation of COPPA can lead to significant penalties, with a court potentially holding operators who violate the Rule liable for civil penalties of up to $50.120 per violation.

Stop Hacks and Improve Electronic Data Security (SHIELD Act)

The SHIELD Act strengthens New York’s data security laws, and as The Knowledge House's main office is in New York, it is subject to this act. Penalties for violating this act include a civil penalty of up to $20 per instance of failed notification, not exceeding $250,000, and up to $5,000 per violation for failing to maintain reasonable safeguards.

Gramm-Leach-Bliley Act (GLBA)

The GLBA regulates how financial institutions deal with private information of individuals. It includes the Financial Privacy Rule, Safeguards Rule, and Pretexting provisions, designed to protect personally identifiable information, prevent false pretenses for information collection, and control how private financial data is collected and disclosed.

Gramm-Leach-Bliley Act (GLBA)

The GLBA primarily applies to financial institutions, but non-profit organizations like the The Knowledge House should implement appropriate data protection practices, maintain confidentiality, obtain consent where required, and ensure compliance with applicable data protection laws.

Compliance Monitoring and Auditing

Regular monitoring and auditing are essential to maintaining legal and regulatory compliance and ensuring that security controls remain effective. Internal audits should be carried out regularly to identify any vulnerabilities and assess the effectiveness of existing controls. External audits can be utilized to provide an independent assessment of the organization's security posture and compliance with laws and regulations.

Staff Training and Education

Staff training and education play a significant role in an organization's cybersecurity efforts. Training programs should cover all necessary security practices and legal requirements, ensuring that staff are well-versed in the laws and regulations applicable to The Knowledge House. Regular training updates can ensure that staff are informed about the latest threats and how to respond appropriately.

Legal, Regulatory and Compliance Considerations: The Next Steps

Data protection and security compliance are essential for any organization, whether in the educational sector, business sector, or non-profit sector like The Knowledge House.
Complying with relevant regulations like PCI DSS, FERPA and COPPA helps organizations to protect their reputation, maintain trust with stakeholders, and avoid costly penalties.