Topic 3 Discussion 1

Operating a global company can have its challenges, especially complying with many laws and regulations across the globe. There are the Sarbanes–Oxley Act of 2002, the Markets in Financial Instruments Directive (MiFID) II, the General Data Protection Regulation (GDPR), the Fundamental Review of the Trading Book (FRTB), and the Australian Corporations Act 2001, to name a few. Discuss what approaches a company with cross-border operations can take to be compliant with mandates from national and international laws and regulations that relate to the protection against cyberattacks.

Hello Class,

While the GDPR is a great starting point, it's important to remember that other laws and regulations may apply depending on the specific context. For example, the Sarbanes–Oxley Act of 2002, the Markets in Financial Instruments Directive (MiFID) II, the Fundamental Review of the Trading Book (FRTB), and the Australian Corporations Act 2001 all have provisions related to cybersecurity(Team, 2025).

Navigating the landscape of national and international laws regarding cybersecurity can be quite challenging for companies with cross-border operations. To ensure compliance and protect against cyberattacks, organizations can adopt several strategic approaches:

Restructuring Data Policies - Companies should develop comprehensive data governance frameworks that align with the specific legal requirements of each jurisdiction they operate in(Fourrage, 2024). This includes understanding local data protection laws, such as the General Data Protection Regulation (GDPR) in Europe, and adapting policies accordingly.

Implementing Security Protocols - Adopting robust cybersecurity measures is essential. This can involve implementing multi-tiered security protocols that are flexible enough to meet varying regulatory standards across different regions(Sage, 2020). For instance, using encryption and secure access controls can help safeguard sensitive data.

Training and Awareness Programs - Regular training for employees on cybersecurity best practices and legal obligations is crucial(Hall, 2024). This not only helps in fostering a culture of security but also ensures that staff are aware of the specific compliance requirements relevant to their roles.

Increasing Transparency and Responsibility - Companies should enhance transparency in their operations, particularly regarding data handling and incident response. Establishing clear accountability structures can help in managing compliance effectively.

Cross-Border Data Transfers - Understanding the regulations surrounding cross-border data transfers is vital. Companies should ensure that they have the necessary safeguards in place, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), to facilitate legal data transfers while maintaining compliance(Global Data Alliance, 2023).

Collaboration and Information Sharing - Engaging in partnerships with other organizations and participating in industry forums can provide valuable insights into best practices and emerging threats. This collaborative approach can enhance overall cybersecurity resilience.

References:

*Cross-Border Data Transfers & Cybersecurity - Global Data Alliance*. (2023, February 9). Global Data Alliance. https://globaldataalliance.org/issues/cybersecurity/

Fourrage, L. (2024). *FAQ for How do international cybersecurity laws impact businesses?* Nucamp. https://www.nucamp.co/blog/coding-bootcamp-cybersecurity-how-do-international-cybersecurity-laws-impact-businesses

Hall, P. (2024, August 7). *Navigating Cross-Border E-commerce Cybersecurity Challenges - Secarma Website*. Secarma Ltd. https://secarma.com/cross-border-e-commerce-cybersecurity-challenges

Sage, J. (2020, November 11). *To combat cross-border cyber threats, cooperation is key*. IBM Policy. https://www.ibm.com/policy/to-combat-cross-border-cyber-threats-cooperation-is-key/

Team, T. A. (2025, February 8). *Cybersecurity Compliance: The Complete Guide for Businesses*. Atlassystems.com; Atlas Systems. https://www.atlassystems.com/blog/cybersecurity-compliance