GRC Recommendations for Leviton Financial Corporation

Sam Anderson
Divya Bhattarai
Gabrielle Drakh
Derek deLeyser
Max Kramer

Applicable Regulations – Current – Domestic

Marvel Consulting

- COPPA - Protects personal information of minors
- GLBA - Financial law that includes protections of personal information
- Right to Financial Privacy Act
- FCRA - Credit Report regulations that require secure handling of consumer information
- Bank Secrecy Act - Financial institutions must hold records for 6 years and report suspicious transactions
- FDCPA - Protects consumer information regarding debt
- Electronic Funds Transfer Act - banks have to notify consumers of policies for electronic transfer of funds
- Dodd-Frank Wall Street Reform and Consumer Protection Act - Established the Consumer Financial Protection Bureau

Applicable Regulations – Current – Foreign

Marvel Consulting

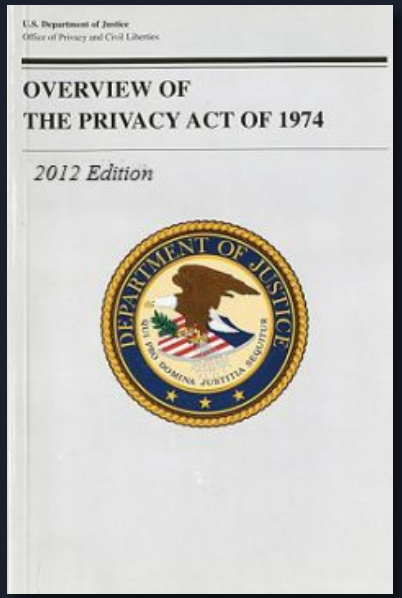
- Data Protection Law No. 25.326 for Argentina
- DPA 2018 and UK GDPR - United Kingdom
- Data Protection Act of 2012 - Singapore
- EU GDPR - France

Applicable Regulations – Future

- FERPA - Protects student information
- Privacy Act of 1974 - Provides protections for the release of records from federal agencies that contain personally identifiable information
- Freedom of Information Act - allows public to request access to various federal records

FERPA

Family Educational Rights & Privacy Act



Assessing CIA Using NIST SP 800-53

Marvel Consulting

Confidentiality: To maintain Confidentiality, the Data Center must be secure and only open to those with the proper authorization.

Integrity: The facility must be in a location with reliable internet access and adequate energy supplies to maintain reliable security at all times.

Availability: Facility must be designed in such a way that resources provided by the Data Center are available at all times

Control Families

- Access Control
- Personnel Security
- Risk Assessment
- Security Assessment

Physical, Logical, and Administrative Controls

- Physical - Key cards or biometrics, backup servers/generators, and on site security guards

- Logical - 90 day password renewal rule, minimum/maximum character count for employees username and password, and cat cards for higher ups

- Administrative - Media protection and trainings

Privacy Laws

- The Gramm Leach Bliley Act
- EU’s GDPR (European Union’s General Data Protection Regulations)
- CCPA (California Consumer Policy Act)

The Gramm Leach Bliley Act

- The Gramm Leach Bliley Act requires financial institutions (banks, insurance companies) to justify how data is being shared and how customers private information is being protected. In order to comply with the act, you must communicate with your customers on how their data is being shared, right to opt out if they prefer not sharing data and apply protective measures to secure their sensitive data

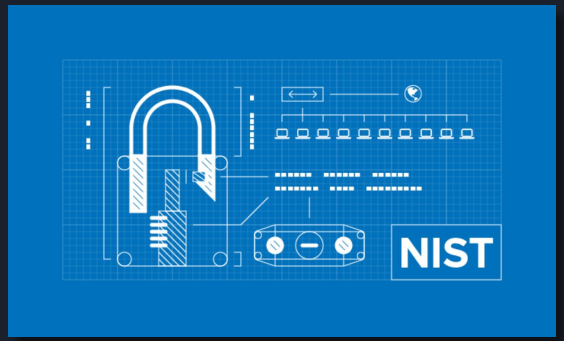
- NIST 800-100
- NIST 800-12

EU’s GDPR (General Data Protection Regulations)

- EU’s GDPR is set of regulations by the european union on data privacy and security. Since, it applies all around the world. Various different frameworks of NIST provides valuable insights and guidelines that meets the requirements for GDPR and access control strategies.

- NIST SP 800-100

- NIST SP 800-53



CCPA (California Consumer Policy Act)

- CCPA aims to enhance privacy laws and consumers protection for residents in california. They have the right to know, right to say no and right to protection when it comes to their data. Your california consumers are the reason you must comply with this law and NIST can help with its access control strategies.

- NIST SP 800-47

Data Center - Salt Lake City, UT

Marvel Consulting

- Superior networking infrastructure
- Little to no major natural disasters
- ISO 22301, ISO 24762, NIST SP 800-34
- BCDR Strategy:
    1. Strive for level 2N+1 Redundancy
    2. Data Backup Procedures
    3. Equipment Protection Procedures
    4. Service Restoration Procedures
    5. Communications Plan
    6. Asset Inventory
    7. Emergency Drills
    8. Regular Evaluations and Updates

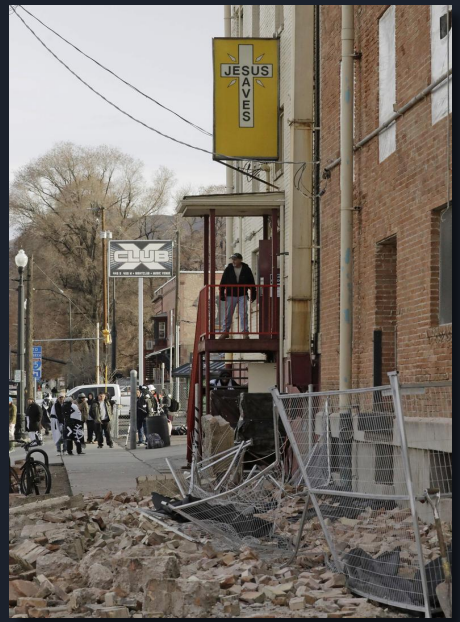
DDOS Attack

- Cyber Incident Response Plan (NIST 800-34)
  1. Detect
  2. Respond
     - Filter + Reroute Traffic
     - Have backup site available
  3. Adapt

Natural Disaster: Earthquake

Marvel Consulting

- Most Likely Natural Disaster to Occur
- Seismic Damping
- Quarterly Earthquake Training/Drills
- Offsite Data Storage (Cloud Computing Technology)
- Fire Suppression Systems: Oxygen Replacement (3M Novec, Carbon Dioxide)
- Positive Pressure Ventilation



Data Loss Prevention

Marvel Consulting

- What is it and why do we need it?
- Cost
- Physical Theft vs Information Theft

Regulations to Consider:

- GLBA
- Privacy Act of 1974
- California Consumer Privacy Act (CCPA)
- Argentina – General Data Protection Law (LGPD)
- Singapore – Personal Data Protection Act 2012 (PDPA)
- France – GDPR/French Data Protection Act
- EU – General Data Protection Regulation (GDPR)
- Payment Card Industry Data Security Standard (PCI DSS)
- 1978 Right to Financial Privacy Act (RFPA)
- UK – GDPR

Data Loss Prevention – Continued

- No Removable Devices
- Security Breach Notification
- No Devices Leave the Premises
- Network Encryption/Access Control/ Session Lock
- NDA/Employee Confidentiality Agreements/Non Compete Agreements
- Intellectual Property Ownership
- DLP Software
- Communication Limitation

THANK YOU!

References

Access Control Policy and Procedures. (n.d.). Retrieved from https://nvd.nist.gov/download/800-53/800-53-controls.xml.

Chalmers, A. (2019, October 11). Why some buildings fall and others stay standing during a quake. Retrieved January 23, 2021, from https://www.king5.com/article/weather/earthquakes/seismic-retrofit-withstand-earthquake/283-a8e8cfb1-4813-4f24-82ed-77efe07f953c

Cramer, M., & Diaz, J. (2020, March 18). 5.7-Magnitude Earthquake Hits Near Salt Lake City: 'The Last Thing We Need Right Now'. Retrieved January 23, 2021, from https://www.nytimes.com/2020/03/18/us/earthquake-utah-salt-lake-city.html

Financial privacy laws in the United States. (2020, December 15). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Financial_privacy_laws_in_the_United_States

Funaro, G. F. (2020, February 26). *Digital Guardian Wins Best Data Loss Prevention (DLP) Solution at SC Awards 2020!* Digital Guardian. https://digitalguardian.com/blog/digital-guardian-wins-best-data-loss-prevention-dlp-solution-sc-awards-2020

Furman, A. F., & Zappa, F. Z. (2019, October 1). *Argentina - The Privacy, Data Protection and Cybersecurity Law Review - Edition 6 - TLR - The Law Reviews*. The Law Reviews. https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1209995/argentina

Green, A. (2020, March 29). *Complete Guide to Privacy Laws in the US*. Retrieved from Varonis: https://www.varonis.com/blog/us-privacy-laws/#:~:text=Contrary%20to%20conventional%20wisdom%2C%20the,laws%20coming%20from%20the%20states.

Irwin, L. (2019, December 16). Data breach notification requirements. IT Governance USA Blog. https://www.itgovernanceusa.com/blog/when-should-an-organization-report-a-data-breach#:%7E:text=There%20is%20currently%20no%20federal,public%20of%20data%20breach%20alerts.&text=The%20GLBA%20(Gramm%E2%80%93Leach%E2%80%93,%E2%80%9Cas%20soon%20as%20possible.%E2%80%9D

Kerner, S. M. K. (2020, February 12). Top Data Loss Prevention (DLP) Solutions. ESecurity Planet. https://www.esecurityplanet.com/products/top-dlp-solutions.html

References

Long, W. R. M. L., Scali, G. S., Blythe, F. B., & Raul, A. C. R. (2019, October 1). Editors Preface - The Privacy, Data Protection and Cybersecurity Law Review - Edition 6 - The Law Reviews. The Law Reviews. https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1209988/european-union-overview

PRIVACY ACT OF 1974. (2020, January 15). Retrieved from justice.gov: https://www.justice.gov/opcl/privacy-act-1974#:~:text=The%20Privacy%20Act%20of%201974,of%20records%20by%20federal%20agencies.

Privacy, policies, and legal information. (2020, April 30). Retrieved from US Department of Veteran Affairs: https://www.va.gov/privacy-policy/

Protection, O. (n.d.). Fire Protection in Data Centers & IT: ORR Protection Systems. Retrieved January 23, 2021, from https://www.orrprotection.com/applications/data-centers

Rana, K. (2019, August 30). 5 Best Practices for Data Center Disaster Recovery. Retrieved January 06, 2021, from https://www.vxchnge.com/blog/data-center-disaster-recovery

Swinnen, E. (2020, April). The Ultimate Data Privacy Guide for Banks and Financial Institutions. Retrieved from https://www.ngdata.com/data-privacy-guide-for-banks-and-financial-institutions/

Tham, Y. U. T. (2019, October 1). *Singapore - The Privacy, Data Protection and Cybersecurity Law Review - Edition 6 - TLR - The Law Reviews*. The Law Reviews. https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1210086/singapore