HOGAN MARREN BABBO & ROSE, LTD

Requisitos sobre la Seguridad Cibernética para Instituciones Autorizadas Bajo Título IV

Dennis Cariello & Jay Rosselló

Septiembre 21, 2018

PRASFAA

Agenda

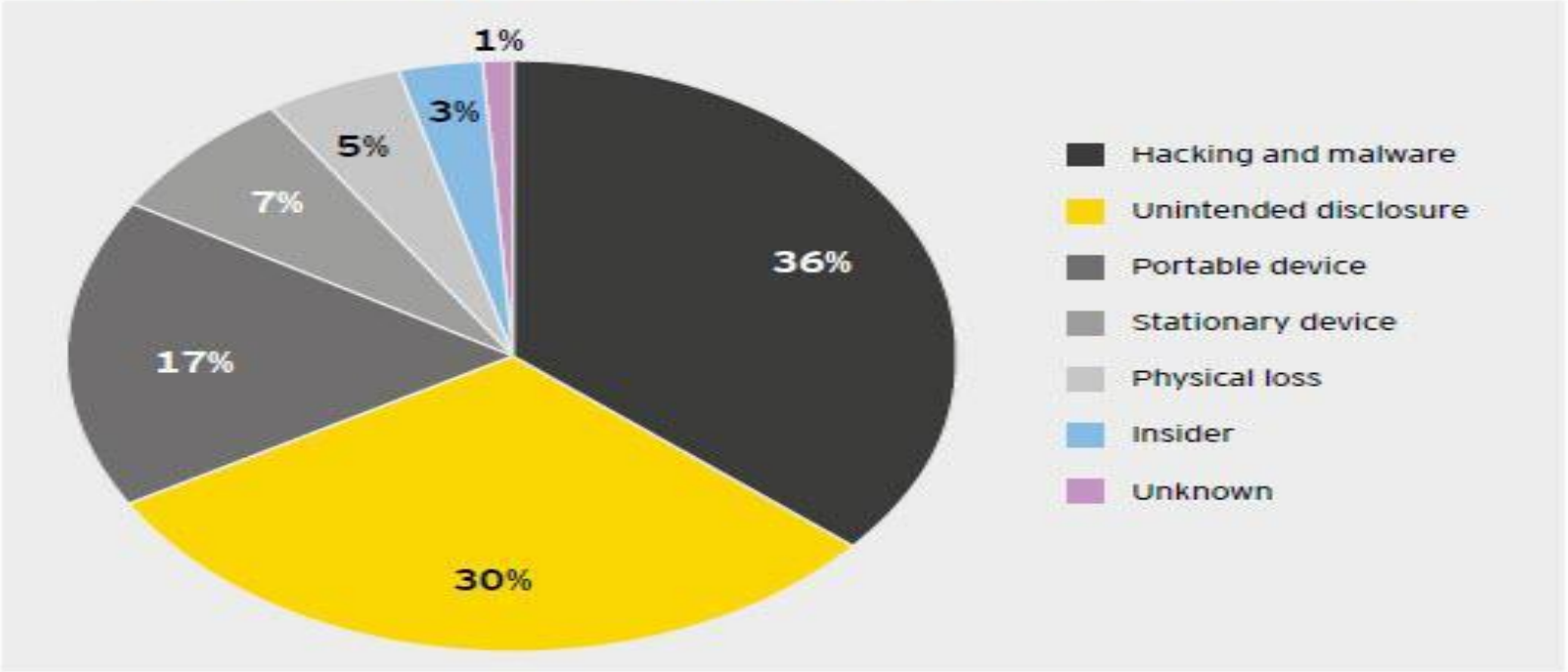
- La Importancia de la Seguridad Cibernética
- Leyes y Reglas sobre la Seguridad Cibernética
- Identificación de Brechas de Seguridad Cibernética
- Reportaje de Brechas de Seguridad Cibernética
- Recommendaciones y Sugerencias
- Preguntas

HM BR HOGAN MARREN BABBO & ROSE, LTD

La Importancia de la Seguridad Cibernética

- La frecuencia de ataques cibernéticos contra universidades y otras escuelas superiores continúa en ascenso – entre los primeros cinco sectores de la economia.

Figure 1. Types of data breaches impacting higher education institutions



La Importancia de la Seguridad Cibernética (cont.)

- Esta tendencia es debido a:
  - Poca atención a la seguridad.
  - Poca coordinación sobre la seguridad.
  - La complejidad de sistemas de información utilizados.
  - La cantidad de información/data recogida y guardada.
  - Redes abiertas y amplio aceso al público.

- Las motivaciones de los atacantes son influenciadas por el tipo de información y el valor que tiene. Por ejemplo, aquellas escuelas que guardan data de investigaciones (research) son más suceptibles a ataques por parte de organizaciones criminales y actores de estado, mientras que data personal tiende a atraer a "hackers" buscando causar daño financiero o de reputación.

La Importancia de la Seguridad Cibernética (cont.)

- Brechas cibernéticas pueden traer un sin número de consecuencias para la escuela, incluyendo:
  - Robo de identidad.
  - Daño al la reputación.
  - Pérdida de confianza por parte de estiudiantes, facultad y otros empleados.
  - Impacto negativo al estado financiero y operacional de la escuela.
  - Multas y otras consecuencias legales y regulatorias.

- Comenzando con el año fiscal 2018, auditorías de escuelas superiores van a incluir el nivel de seguridad de información estudiantil.

Gramm-Leach-Bliley Act (GLBA)

- El Departmento de Educación de los Estados Unidos (USDOE) had determinado que escuelas superiores autorizadas bajo Título IV son de ser consideradas “Instituciones Financieras” conforme al GLBA (15 U.S.C. § 6801).

- El GLBA requiere que instituciones financieras:
  - Adopten por escrito e implementen medidas para mantener segura información sobre clientes.
  - Designen empleados responsable por coordinar dichas medidas.
  - Identifiquen y evalúen riesgos a la información de clientes.
  - Diseñen e implementen un programa para proteger información de clientes.
  - Aseguren que afiliados y proveedores de servicios mantengan seguridad.
  - Revisen periódicamente el program de seguridad.

- De todas las leyes y reglas que aplican a este tema, el GLBA refleja los mas altos estándares.

Fair and Accurate Credit Transactions Act (FACTA)

- La regla “Identify Theft Red Flags” bajo FACTA requiere el desarrollo e implementación de un Programa de Prevención del Robo de Identidad (Programa) para combatir el robo de identidad en conneción a cuentas e información en posesión de la institución financiera.

- El Programa debe incluir políticas y procedimientos para detectar y prevenir el robo de identidad, y permitir a la institución financiera a:
  - Identificar prácticas y actividades que son “red flags” (banderas rojas) en cuanto a posible robo de identidad.
  - Detectar banderas rojas que han sido incorporadas al Programa.
  - Responder de manera apropriada a cualquier bandera roja detectada para prevenir el robo de identidad.
  - Revisar el Programa periódicamente para reflejar cambios en riesgos relacionados al robo de identidad.

Family Educational Rights and Privacy Act (FERPA)

- FERPA es una ley federal que aplica a escuelas superiores y que busca proteger la privacidad de los records educacionales de sus estudiantes.

- Estudiantes de escuela superior tienen el derecho bajo FERPA a:
  - Inspeccionar y revisar sus records educacionales mantenidos por la escuela.
  - Demandar que la escuela corrija records que estimen estén incompletos o inexactos.
  - Salvo bajo ciertas excepciones, dar permiso por escrito antes de que la escuela comparta o provea información sobre los records educacionales.

HM BR HOGAN MARREN BABBO & ROSE, LTD

Leyes Sobre Notificación de Brecha de Seguridad

- Todos los 50 Estados, DC, Guam, Islas Virgenes y Puerto Rico han adoptado legislación que requiere entidades públicas y/o privadas a notificar a individuos afectados por brechas de seguridad que envuelvan “personallly identifiable information” (PII).

- Estas leyes usualmente establecen quienes deben cumplir con las mismas; proveen definiciones de PII (e.g., nombres conjunto a SSNs, número de licencias de conducir, números de cuentas de banco, etc.); que constituye una brecha; los requisitos para la notificación (e.g., cuándo y cómo se debe efectuar, quién debe ser notifcado, etc.); y excepciones (e.g., para información encriptada).

- Las leyes de Puerto Rico relacionadas a este tema se encuentran en 10 Leyes de Puerto Rico §§ 4051 et seq.

HOGAN MARREN BABBO & ROSE, LTD

Directrices y Referencias del USDOE

- El USDOE provee mas directrices y otra información sobre este tema en relación al Program Participation Agreement (PPA), inclueyndo los requisitions de:
  - Mantener records correctos y completos sobre la eligibilidad de participar en el program.
  - Proveer acceso a dichos records a oficiales del USDOE.
  - Salvo bajo ciertas excepciones, obtener el permiso escrito del estudiante para divulgar su PII.
  - Establecer un program de seguridad completo y riguroso para proteger la información de padres y estudiantes.

- El Acuerdo de Inscripción del Student and Internet Gateway (SAIG) establece que escuelas superiores deben asegurarse que toda informacion relacionada a aplicaciones para Federal Student Aid (FSA) este protegida de acceso indebido de parte de personal no autorizado. También se requiere de las escuelas que, en el evento de alguna breacha de seguridad de PII, se notifique al FSA del mismo inmediatamente.

Directrices y Referencias del USDOE (cont.)

- El PPA y el SAIG requieren que escuelas superiores tengan en efecto protecciones establecidas por el GLBA.

- La falta de tener las mismas expone a la institución a ser determinada no capz de administrar fondos Título IV por el USDOE.

Directrices y Referencias del USDOE (cont.)

- El Handbook del FSA y los siguentes Dear Colleague Letters (DCL) añaden requisitos y recomendaciones para escuelas superior en cuanto a este tema:
  - DCL GEN 15-18: Habla sobre la proteccion de data usada en los programas del Título IV y alienta a las escuelas a evaluar los riesgos y posibles daños en caso de acceso indebido o no autorizado; determinar los niveles de seguridad para distintos activos de información; implemetar políticas y practicas para minimizar riesgos y daños; y constatemente evaluar y mejorar los controles sobre la seguridad.
  - DCL GEN 16-12: Le sigue al anterior DCL y provee información sobre los métodos a usarse por el USDOE para evaluar la capacidad de escuelas de mantener segura PII, incluyendo National Institute of Standards and Technology (NIST) Special Publication 800-171, el cual recomienda, entre otras cosas, limitar el acceso a solo personas autorizadas, proveer el entrenamiento apropriado, y crear records de auditoría para sistemas de informacíón.

Qué Constituye una Brecha de Seguidad?

- Como establece el GLBA, una brecha de seguridad de información es cualquier divulgación no autorizada, mal uso, alteración indebida o destrución de información bajo control o posesión de la institución.

- Es importante tener en mente que las leyes y reglas anteriores generalmente:
  - No exigen un mínimo tamaño o número de records a ser comprometidos.
  - No están limitados a información digital o recursos computerizados – aplica también a información en papel.
  - Cubre información guardada (storage), en tránsito o siendo procesada.

Qué Constituye una Brecha de Seguidad (cont.)?

- Cada escuela superior debe tener medidas administrativas, técnicas y físicas para (i) asegurar la seguridad y confidencialidad de información estudiantil, (ii) anticipar y lidiar con amenazas a la seguridad e integridad de records estudiantiles y (iii) proteger en contra del uso indebido.

Qué Constituye Reportar una Brecha?

- El Acuerdo de Inscripción del SAIG requiere que, como condición a la participación en los programs bajo el Título IV, se notifique al USDOE de cualquier brecha – real o sospechada.

- Escuelas que se enteran de una brecha, o se sospechan de una, deben notificar al USDOE el mismo día de dicha deteción.

HM BR HOGAN MARREN BABBO & ROSE, LTD

Qué Constituye Reportar una Brecha (cont.)?

- Escuelas deben reportar dichos eventos por email (cpssaig@ed.gov), llamando al 202-245-6550 o atravéz del FSA website, incluyendo la fecha, impacto y método de la brecha, su punto de contacto, y pasos propuestos a tomarse en respuesta.

- El USDOE tiene el poder de penalizar a escuelas que no cumplan con el requisito anterior de “self-report”, incluyendo sanciones monetarias de hasta $54,789 por violación (34 C.F.R. § 36.2).

Qué Deben Hacer Las Escuelas Superiores -- NIST?

- Seguir las directrices que se encuentran en el NIST 800-171 (“Gold Standard”).

- El NIST 800-171 provee información bién detallada relacionado a lo que constituye un programa de información de seguridad efectivo.

- Los requisitos bajo NIST son los siguientes:

    1) Identificación: El entendimiento de los riesgos cibernéticos hacia las operaciones de la institución y el establecimiento de una estructura interna que da prioridad a la identificación y solución de dichos riesgos.

    2) Protección: El manejo de información y records de manera consistente con la estrategias de la institución y la implementación de soluciones de seguridad técnica para asegurar la seguridad e integridad de información y sistemas.

Qué Deben Hacer Las Escuelas Superiores – NIST (cont.)?

3) Detección: El percibimiento de actividad anómala y el entendimiento del impacto potencial de dicha actividad, y el mantenimiento adequado de procesos y procedimientos de detección.

4) Respuesta: Las respuestas de la institución a tales actividades son coordinadas con todas las partes interesadas – tanto internas como externas – y son conducidas con el fin de prevenir el efecto de dichos incidentes.

5) Recuperación: La implementación de medidas para la pronta restauración de sistemas y otros bienes afectados por eventos cibernéticos.

HOGAN MARREN BABBO & ROSE, LTD

Qué Deben Hacer Las Escuelas Superiores – Auditoría?

- La alternativa al cumpliento con los requisitos de NIST es cumplir con aquellos reflejados en el estándar de auditoría del USDOE para el año fiscal 2018 – el cuál es mucho menos estricto que NIST.

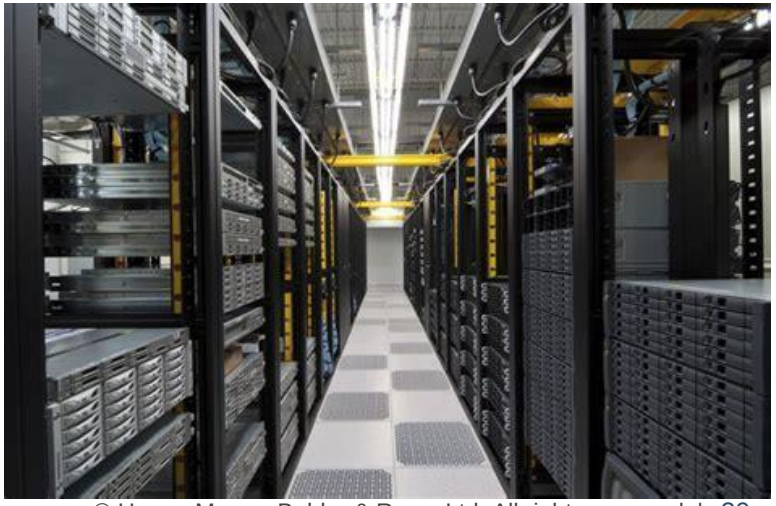
- Bajo dicho estandár, hay basicamente two requisitos principales:
  - Designar un “Information Security Officer” (Oficial de Seguridad de Información); y
  - Completar una evaluación de riesgos cibernéticos y establecer controles internos para minimizar los riesgos identificados.

HOGAN MARREN BABBO & ROSE, LTD

Qué Deben Hacer Las Escuelas Superiores – Auditoría (cont.)?

- La evaluación de riesgos cibernéticos debe enforcarse en información proveida por USDOE, especialmente aquella relacionada con la administración de los programas bajo Título IV.

- Como mínimo, debe cubrir información en:
  - Los sistemas de manejo de asistencia financiera;
  - Las redes donde se encuentran los archivos de SAIG;
  - Sistemas estudiantiles relacionados a registros y notas;
  - Sistemas de admisiones; y
  - Sistemas de cuentas estudiantiles.



HOGAN MARREN BABBO & ROSE, LTD

 |

Recomendaciones y Sugerencias

- Establecer un diálogo con líderes escolares sobre la importancia de la seguridad cibernética y los requisitos del USDOE en cuanto al mismo, y crear consiencia sobre los possibles riesgos atraves de la institución.
- Confirmar que la escuela haya designado un “Information Security Officer” (Oficial de Seguridad de Información).
- Asegurar que la escuela haya completado una evaluación de riesgos cibernéticos, e implementado controles para minimizar riesgos identificados – consistente con la políticas y prácticas de la institutción.
- Dar prioridad a las areas de mayor riesgo para las operaciones de la institución.

Recomendaciones y Sugerencias (cont.)

- Implementar una estructura formal de gobernanza sobre seguridad de información.
- Minimizar la cantidad de PII mantenida por la institución y limitar el aceso a la misma.
- Incluir cláusulas en contratos con proveedores para que los mismos cumplan con los requisitos, y revisar aquellos contratos que no tengan dichas cláusulas.
- Mantender sistemas y software actualizado, y preparar y poner en práctica un plan de respuetas a incidentes cibernéticos.

Preguntas?

Dennis Cariello
(Dennis.Cariello@HMBR.com)

Jay Rosselló
(JR@HMBR.com)

Hogan Marren Babbo & Rose

HOGAN MARREN BABBO & ROSE, LTD

