> Esta táctica es notablemente eficaz: Cuando un cliente involuntariamente espera las instrucciones, los ladrones usan esos datos de identificación para iniciar sesión como si fueran la víctima e iniciar transferencias no autorizadas desde esa cuenta.

La falta de imaginación es parte del ser humano. Después de experimentar una mala situación, una persona puede imaginar escenarios similares. El desafío radica en situaciones que una persona no ha experimentado antes.

2.2 ESTADO DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

La revolución de la microcomputadora –y con ello el surgimiento de las redes de área local, redes de área amplia e Internet- cumplió 35 años en 2010.[8] La interconexión de computadoras y redes ha traído grandes beneficios de productividad y abrió emocionantes nuevos campos de entretención e información. Acercó al mundo. Sin embargo, estas virtudes no están exentas de consecuencias imprevistas y, a veces, no deseadas.

El 01 de julio de 2003, entró en vigencia la California Senate Bill 1386, la primera ley de incumplimiento de divulgación de la nación. La ley exige que cualquier organización que realice negocios en California notifique a los residentes afectados si la organización tiene razones para creer que información personal no encriptada de los residentes de California ha sido adquirida por una persona no autorizada.[9] La mayoría de los estados ha seguido a California con sus propias leyes de incumplimiento de divulgación, y es probable una ley nacional.

En poco más de seis años desde que la ley de California entró en vigencia, la Privacy Rights Clearinghouse (2009) ha identificado más de 340 millones de registros de consumidores que han sido violados.

---

[8] Malcolm Gladwell data el inicio de la revolución de la microcomputadora en enero de 1975, cuando "la revista *Popular Electronics* lanzó un reportaje sobre una máquina extraordinaria llamada Altair 8800" Gladwell, 2008, p.63)

[9] Códigos Civiles de California 1798.29, 1798.82, y 1798.84.

Aquí hay sólo unas pocas de las muchas compañías que han reconocido que sufrieron violaciones de su información:

Choicepoint	T.J. Maxx	Ernst & Young	JP Morgan
Sam's Club	Citi Financial	Ralph Lauren	DSW
MCI	Kodak	Motorola	Deloitte
Bank of America	Time Warner	Ford Motor	Hanover

La cifra de 340 millones incluye sólo violaciones reportadas. No incluye las violaciones descubiertas, pero no reportadas, las violaciones no descubiertas u otras pérdidas de información –tales como robo en la banca en línea- que legalmente no es necesario que sea revelada.

Los 340 millones de registros de datos violados representan sólo la punta del iceberg. Ellos también demuestran cómo el cibercrimen ha cambiado en los últimos años. En el pasado, las grandes amenazas de los sistemas de información eran internas. Existían pocos piratas informáticos; de esos que lo hicieron, la mayoría era para su propio ego; y el máximo daño que causaban se limitaba al robo de los recursos informáticos y a la negación del servicio producto de ataques con virus.

Los piratas informáticos que usaban la piratería por placer o para hacer crecer su reputación, ahora están en eso por dinero (Herley & Florencio, 2009). Ellos son cada vez más sofisticados y aprenden a burlar las defensas. Una fuente informa que "los chicos malos están adaptando sus actuales estrategias de protección e inventando nuevas maneras para alcanzar los datos que ellos valoran" (Verizon Business RISK Team, 2009, p.47).

En julio de 2009, los cibercriminales se dirigieron a las cuentas de los titulares de YouTube con ataques de phishing[10] (Harwood, Junio 2009). El 17 de agosto de 2009, tres hombres fueron acusados de robar más de 130 millones de números de tarjetas de crédito. Ellos eran capaces de obtenerlas explorando las vulnerabilidades de los sitios Web corporativos (Trotta, 2009). También en agosto de 2009, el sitio de la red social Twitter fue deshabilitada por piratas informáticos que intentaron tomar represalias en contra de un solo usuario, pero

[10] N del T: estafas por suplantación de identidad

derribó todo el sitio (Acohido, 2009). Por cierto, tomó casi 100.000 bots[11] (software de aplicaciones que ejecutan tareas automatizadas) bajo el control de los piratas informáticos para derribar el sitio. Costó alrededor de US$ 5.000 arrendar esos bots. Además, continúan descubriéndose nuevas formas de acceder a las redes inalámbricas, en detrimento de las empresas (Mills, 2009).

En testimonio ante el Congreso, un experto en seguridad informática señaló lo siguiente acerca de los ataques de piratas informáticos (kellerman, 2009):

> los ciberataques se han convertido en un fenómeno totalmente generalizado, que se basa en parte en:
>
> - el aumento de la conectividad y disponibilidad de las redes atacables y de las vulnerabilidades de sistemas y aplicaciones
> - la capacidad de los cibercriminales para obtener importantes recompensas financieras a través de ataques exitosos
> - las federaciones mundiales entre las distintas clases de cibercriminales y desarrolladores de malware
> - el Estado-Nación, terrorista y políticamente dirigido a impulsar los esfuerzos del cibercrimen
> - la carencia de aplicación de una ley cohesiva alrededor del mundo

La extorsión cibernética ha empezado a levantar su fea cabeza y ahora es un problema para las empresas en Estados Unidos (Wagley, 2009). Los cibercriminales han descubierto que no necesitan cambiar su malware tan pronto, sino que pueden implementarlo en más sitios (Harwood, agosto 2009). Además, utilizan técnicas automatizadas que continuamente ponen en peligro sitios Web legítimos, aumentando la oportunidad de que los usuarios finalmente sean redirigidos a un sitio ilegítimo. Más aun, los criminales están cambiando el código de malware por lo que no es detectado por los sistemas antivirus tradicionales.

Tal vez, el desafío más serio es la reciente seguidilla de robos de banco en línea. Según el FBI (2009), los ladrones cibernéticos

---

[11] N del T: aféresis de robot, programa informático que imita el comportamiento humano.

pirateando la empresas se pequeño y mediano tamaño han robado alrededor de US$ 100 millones de cuentas bancarias estadounidenses. Algunos de estos ataques son lo suficientemente sofisticados para derrotar los sistemas de autenticación de dos factores.

El Computer Security Institute (CSI) Computer Crime and Security Survey (Richardson, 2008) descubrió que el fraude informático financiero promedio cuesta a la empresa víctima US$ 500.000 y un ataque bot promedio –un ataque a través de las computadoras cuya seguridad está en peligro, a veces cientos de miles- cuesta US$ 350.000. Esos ataques pueden tener serios impactos. Un caso afectó las operaciones de un hospital de Seattle (U.S. Attorney's Office, 2006). El informe del CSI también señala que el 27 por ciento de los ataques en 2008 fueron los ataques en los cuales una parche de malware fue escrito directamente para atacar una compañía específica.

La investigación de Verizon de 500 violaciones descubrió que durante el curso de estas violaciones, fueron robados 285 millones de registros (Verizon Business RISK Team, 2009). El estudio concluyó que el 74 por ciento de los registros fueron robados por fuentes externas. Kellerman (2009) corrobora la opinión de que los internos ya no son la causa de la mayoría de las pérdidas.

Además, el informe del CSI señala que los ataques de menor importancia siguen siendo un problema. Mischele Kwon, ex director del United States Computer Emergency Readiness Team (US-CERT) llama a esos ataques un "problema de higiene" (Kwon, 2009), es decir, un problema conocido que puede ser solucionado con due diligence. Sin embargo, es el ataque más sofisticado que está obteniendo la mayor parte de los registros robados (Verizon Business RISK Team, 2009).

El informe de Verizon señala que el profesionalismo del crimen informático está aumentando. La amenaza ya no viene de los "script kiddies"[12], sino de consorcios del crimen organizado, el cual tiene los fondos para realizar ataques más sofisticados. De hecho, Verizon concluyó que el 91 por ciento de los registros robados en 2008 fueron hechos por grupos del crimen organizado. CSI señala que los programas cortafuegos y antivirus son "fundamentalmente

[12] N. del T: anglicismo propio de la jerga de Internet que hace alusión a una persona falta de habilidades técnicas, sociabilidad o madurez.

imperfectos", y que el malware y otros ataques pueden eludir controles basados en la firma. Además, Verizon afirma que en la mayoría de las violaciones exitosas, alguien fue capaz de tomar ventaja de un error cometido por la víctima e instaló el malware para obtener ventaja de ello.

Las noticias no son tan malas. Aparentemente, hay un exceso de oferta en el mercado del inframundo para los números de tarjetas de crédito, por lo que ahora los números de identificación personal (PIN) son los objetos de interés (Verizon Business RISK Team, 2009, p.7):

> El valor potencial de participación en el cibercrimen no existiría sin un mercado para el robo de información. Como con cualquier sistema de mercado legítimo, el valor unitario de bienes y servicios fluctúa con la oferta y demanda...Los criminales han rediseñado sus procesos y desarrollado nuevas herramientas –como el memory-scraping malware[13]- para robar este valioso producto. Esto ha llevado a la exitosa ejecución de las complejas estrategias de ataque que antes se pensaba que sólo eran posibles teóricamente.

Más aun, el malware personalizado va en aumento. Verizon estima que el 8 por ciento de los 285 millones de registros violados fueron tomados con malware personalizado creado específicamente para el ataque.

Los criminales también están ocultando su trabajo, creando desafíos para quienes tienen que capturarlos o investigar las consecuencias de los crímenes. Los investigadores descubrieron "anti-forenses" –intentos de ocultar sus pistas- en más de un tercio de los casos en la investigación de Verizon.

También está aumentando el uso del ciberespacio por entidades gubernamentales. Por ejemplo, en el 2008, "el estado-nación de Georgia fue atacado por piratas informáticos, presumiblemente desde Rusia" (Wilson, agosto 2009). Wilson también escribe acerca de los ataques contra Estonia y del uso de la guerra cibernética en los enfrentamientos entre Israel y Hamas. En julio de 2009, sitios Web de Corea del Sur también fueron atacados presuntamente por Corea del Norte (Kim, 2009).

---

[13] N. del T: tipo de malware que ayuda a encontrar datos personales examinando la memoria RAM.

Rogueware, el software que pretende ser un software de seguridad, pero que realmente pone en peligro una computadora, también va en aumento. Se estima que los cibercriminales están haciendo US$ 34 millones al mes logrando que los usuarios descarguen este software malicioso (Correll, 2009).

Ahora, incluso los teléfonos no son seguros. El malware móvil es un centro de beneficios prometedor para los criminales (Dunham, 2009). Los usuarios de teléfonos podrían estar comprometidos antes de que incluso comiencen a realizar actividades bancarias en el teléfono.

Stewart Baker, ex secretario adjunto de seguridad nacional de Estados Unidos, ofrece este resumen (2009):

> En quince años, las redes descentralizadas se han trasladado de usos novedosos como el monitoreo de máquinas de café comunitarias a la gestión de activos financieros, telecomunicaciones, y la red eléctrica. Eso es bueno y malo, porque esta revolucionaria nueva tecnología representa riesgos reales. Confiamos mucho más de nuestros activos críticos a las redes TI de lo que alguna vez lo hicimos, y las vulnerabilidades de seguridad que pueden haber sido tolerables hace quince años pueden tener devastadoras consecuencias hoy en día.

Un informe de IBM concluye que "todo sitio Web debe ser visto como sospechoso y todo usuario es un riesgo" (IBM Global Technology Services, 2009).

El crimen y las situaciones descritas en esta sección afectan sistemas que los profesionales de seguridad usan en su trabajo cotidiano y que ellos están encargados de proteger. Los profesionales de la seguridad deben instruirse ellos mismos en las formas de la seguridad de la información –y también mantenerse al tanto de los cambios que se están produciendo.

2.3 ECONOMÍA DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Los incidentes de seguridad de la información cuestan dinero. Por ejemplo, un virus informático produce la pérdida en productividad del

personal de una organización además del tiempo y los gastos para que el personal de TI elimine el virus y restaure la disponibilidad. Por lo general, la pérdida de productividad es más costosa que el costo de la limpieza del ataque de virus. En un caso, eliminar el virus de la red de un bufete de abogados requirió tres días de trabajo por dos personas de TI y dos consultores, costando a la oficina aproximadamente US$2.400 en tiempo del personal y otros $10.000 en honorarios de los consultores. Mientras tanto, el bufete estimó que la productividad de sus 100 abogados se redujo en un 20 por ciento. El costo en pérdidas de facturación excedió los US$ 25.000, más del doble del costo de limpieza del ataque de virus.

El costo del robo de un secreto comercial por un ladrón cibernético es el valor del secreto comercial de la compañía. Las compañías deben preguntarse qué les costaría a ellos si un competidor tuviera la propiedad intelectual como sus listas de clientes, información de precios, estructura de costos, planes estratégicos o procesos patentados.

El costo del robo de los números de seguridad social de los clientes incluye el costo de notificar a los clientes además de los servicios de robo de identidad proporcionado para proteger a los clientes y los gastos legales, si se presentan demandas, más la pérdida de la buena disposición. El promedio de costo para cumplir con las leyes de violación de divulgación ahora excede los US$ 200 por registro (Claborn, 2009). Esto se traduce en los costos del incumplimiento de divulgación de más US$ 2 millones por un incumplimiento de una base de datos relativamente pequeña de 10.000 personas.

La implementación de la seguridad también tiene costos. Los cortafuegos y otras tecnologías ISS se llevan el capital lejos de otros usos. ¿Una compañía debería invertir en un nuevo sistema de gestión de ventas o aumentar su actual sistema de antivirus basado en la firma con un sistema moderno de prevención contra intrusos basado en el comportamiento?

El personal de seguridad de los sistemas de información (ISS) está a expensas del personal que puede contribuir más directamente al balance final. Un nuevo vendedor podría contribuir US$1 millón o más en nuevas ventas. ¿Qué contribuye un analista de seguridad de la información al balance final?

Cada hora que la gerencia pasa en reuniones de seguridad, o que el personal pasa en entrenamiento de conciencia de seguridad, es una hora que podría contribuir también al balance final.

En la gestión básica de riesgos, cuánto se debe gastar para prevenir un incidente de ISS es igual a la probabilidad del incidente multiplicado por su costo (Gordon & Loeb, 2006). En relación con la gestión de riesgos, es un deber legal de la empresa tomar medidas para asegurar sus activos de información. Este aspecto fue precisado más de 60 años atrás por el Juez Learned Hand en el caso *Estados Unidos v. Carroll Towing Co.* (1947), en el cual Hand escribió que una parte es negligente si el costo (B) de tomar medidas adecuadas para prevenir el daño es menor que la pérdida monetaria (L) multiplicado por la probabilidad (P) de su ocurrencia ($B < PL$).

Un incidente de ISS crece en número y el costo de la recuperación sube, las compañías deben estar preparadas para invertir más recursos en prevención. Usando los recursos corporativos eficientemente para proteger la información sensible y los sistemas, es uno de los objetivos clave de un programa de ISS (Braun & Stahl, 2005). Dicho programa consiste en todas las actividades y gastos que la organización necesita para proteger la información sensible. El programa puede ser formal, con un ejecutivo específico encargado de la responsabilidad de la gestión (recomendado), o informal, con las actividades y gastos efectuados según sea necesario. En cualquier caso, el objetivo del programa debe ser manejar prudentemente y en forma rentable el riesgo de que la información crítica pueda

- ser comprometida
- ser cambiada sin autorización, o
- no estar disponible

2.4 FACTORES CRÍTICOS DE ÉXITO

Tres dominios que co-evolucionan definen si el programa de ISS de una compañía cumple con el estándar de seguridad del debido cuidado:

- la legislación y regulación en cuanto a la obligación de quienes poseen la información para proteger la información privada de los demás en sus sistemas informáticos
- el derecho contractual y responsabilidad extracontractual sobre la seguridad de la información y los activos de información
- las prácticas de seguridad recomendadas por la comunidad profesional de ISS

En *An Emerging Information Security Minimum Standard of Due Care* (2005), Braun and Stahl analizan esos tres dominios e identifican siete factores críticos de éxito que un estándar de cuidado de la seguridad de la información debe cumplir:

- **Responsabilidad de la dirección ejecutiva**. Alguien de la alta gerencia tiene la responsabilidad de la gestión del programa de seguridad de la información de la empresa, la cual es gestionada de acuerdo con sus políticas de seguridad de la información.
- **Políticas de seguridad de la información**. La empresa ha documentado su enfoque de gestión para la seguridad de la información de manera que cumpla con sus responsabilidades y deberes para proteger la información.
- **Educación y entrenamiento de la conciencia del usuario**. Los usuarios reciben educación y entrenamiento en las políticas de seguridad de la información y de sus responsabilidades personales para proteger la información.
- **Seguridad de redes y computadoras**. El personal de TI está gestionando de forma segura la infraestructura de tecnología de una manera definida y documentada que adhiere a las prácticas efectivas de ISS.
- **Garantía de terceros de la seguridad de la información.** La compañía comparte información con terceros sólo cuando se tiene la seguridad de que esos terceros protegen la información al menos con el mismo estándar de cuidado con que la empresa lo hace.
- **Seguridad física y personal**. La empresa proporciona protección física adecuada a la información, investiga los

candidatos al empleo e incorpora la seguridad de la información en las responsabilidades del cargo.

- **Evaluación de riesgos periódica.** La empresa realiza una evaluación o revisión de su programa de ISS, preferiblemente a través de un tercero, abarcando la tecnología y la gestión, al menos una vez al año.

Un octavo factor –la clasificación y control de la información sensible- generalmente es parte del marco de recomendaciones de la política de seguridad de la información (como en ISO 27001 y 27002). Este factor llama a la empresa a comprender las leyes, regulaciones y contratos que le impone las obligaciones de seguridad de la información; identifica su propiedad intelectual que requiere protección; hace un inventario de la información sensible e implementa las medidas de seguridad apropiadas para protegerla; distingue la información como pública, para uso interno, o restringida; y asigna a los propietarios de la información la responsabilidad de definir quién necesita acceso a qué información. El personal que no pertenece al ISS obtiene una mayor comprensión del ISS cuando este octavo factor está incluido.

2.5 IMPLICACIONES PARA LA SEGURIDAD FÍSICA EN UN MUNDO CONVERGENTE

La convergencia de la seguridad física y de la información tiene numerosas definiciones. La Alliance for Enterprise Security Risk Management ofrece esta definición básica (Booz Allen Hamilton, 2005, p.3):

> la identificación de los riesgos de seguridad y las interdependencias entre las funciones empresariales y los procesos dentro de la empresa y el desarrollo de soluciones de procesos de negocios gestionados para abordar esos riesgos e interdependencias.

Aquí hay una definición más detallada (Tyson, 2007, p.4):

> La convergencia de la seguridad es la integración, de manera formal, colaborativa y estratégica, de los recursos acumulativos de seguridad

de la organización con el fin de brindar beneficios a toda la empresa a través de una mayor mitigación del riesgo, aumento de la eficacia y eficiencia operacional, y el ahorro de costos.

La convergencia permite que los dispositivos de seguridad física interactúen a través de una red para beneficio sustancial de la organización. Al mismo tiempo, crean un riesgo adicional para la organización debido a que los dispositivos de seguridad física ahora son accesibles desde cualquier parte en la red. En el antiguo paradigma, las cámaras de video, grabadoras de video, sistemas de detección de intrusiones y cuentas bancarias no eran accesibles a menos que una persona físicamente se acercara a ellos. Actualmente son potencialmente accesibles desde cualquier lugar del mundo.

Un buen resumen de estos asuntos proviene de un testimonio ante el congreso del director de Sandia National Latoratories' Information Operations Center (Varnado, 2005):

> Hoy en día, los sistemas heredados están siendo reemplazados gradualmente por los nuevos sistemas SCADA (supervisión del control y adquisición de datos) que usa Internet como la columna vertebral del control. Este cambio se está implementando para reducir costos y aumentar la eficiencia de la operación. Sin embargo, esta tendencia aumenta sustancialmente la posibilidad de disrupciones debido a (1) el número de personas que tienen acceso al sistema es significativamente mayor, (2) las disrupciones pueden ser causadas por piratas informáticas que no tienen formación en ingeniería de sistemas de control y, (3) el uso de Internet expone los sistemas SCADA a todas las vulnerabilidades inherentes a las redes informáticas conectadas entre sí que están siendo explotadas actualmente por piratas informáticos, el crimen organizado, organizaciones terroristas, y Estado-naciones. Los gusanos, virus, network flooding (inundación de la red), ataques imprevistos a través de routers (enrutadores) comprometidos, spyware (programas espía), ataques internos, extracción de datos por externos que obtienen privilegios internos (phishing), y ataques distribuidos de denegación de servicio son todos habituales. El combate eficaz a estos ataques requiere el aumento de la sensibilización, nuevas tecnologías y mejores respuestas y capacidad de recuperación.

Este paradigma es virtualmente idéntico a la actual situación en el campo de la seguridad física.

La Figura 2-1 muestra un sistema de video vigilancia, en el cual se necesitaría el acceso físico al sistema para comprometerlo. El acceso físico al sistema podría ser evitado con una barrera, un oficial de seguridad u otras medidas.

Figura 2-1
Diseño Video-a-Grabador

La Figura 2-2 muestra un diseño moderno de video vigilancia.

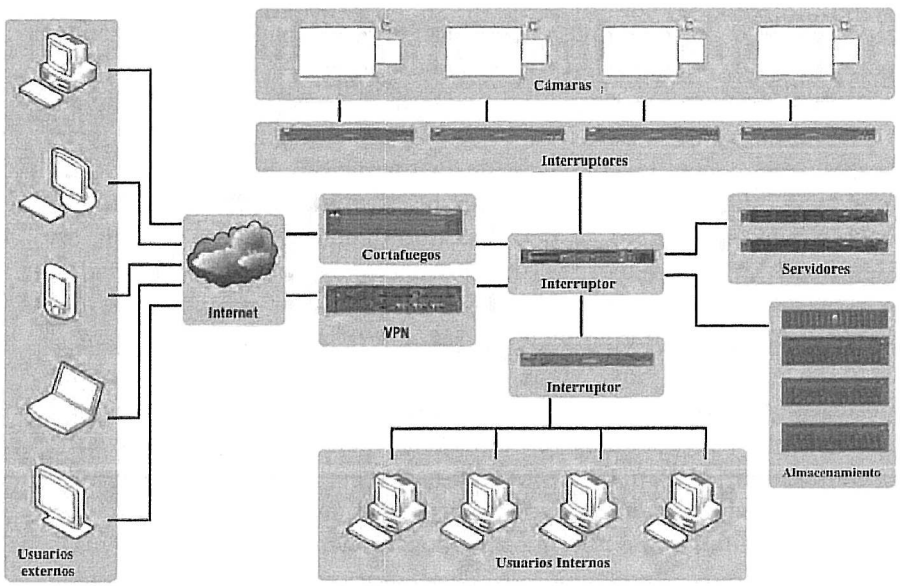

Figura 2-2
Infraestructura de Video

Múltiples computadoras en la red son capaces de acceder a un servidor que ahora almacena datos de video. Las cámaras en la red están poniendo esos datos de video en ese mismo servidor.

La seguridad física puede usar distintos modos de comunicación. En primer lugar, puede haber una conexión propia entre un dispositivo y otro. En segundo lugar, puede haber una conexión estándar de la industria entre dos dispositivos, tales como el protocolo Weigand entre un lector de tarjeta y un controlador. Y en tercer lugar, los dispositivos de la red generalmente conversan a través de TCP/IP (protocolo de control de transmisión/protocolo de Internet), el estándar mundial de Internet para la comunicación.

Los dispositivos pueden ser divididos en dos tipos de sistemas, integrados y basados en host (anfitrión). Los sistemas integrados (también conocidos como sistemas especiales) generalmente son programados por el fabricante y operan en sistemas operativos propios o no estándar. Estos pueden incluir cámaras de video, lector de tarjetas, controladores de acceso, paneles de control de detección de intrusión (alarma), convertidores de video análogo a digital, y así sucesivamente. Los sistemas basados en host operan en sistemas operativos más estándar, generalmente un sistema operativo Windows o Linux (Macintosh OS opera en una versión de UNIX, hermana del sistema operativo Linux). Los sistemas integrados son mucho más difíciles de cambiar que los sistemas operativos Windows, pero todos esos sistemas pueden ser comprometidos.

Dado que cualquier sistema que se comunica con algo más está potencialmente expuesto a un peligro, los profesionales de la seguridad física necesitan tomar decisiones informadas sobre qué sistemas pueden ir dónde. Por ejemplo, Underwriters Laboratories (UL) tiene reglas estrictas sobre cómo se deben implementar los sistemas de incendio, especialmente considerando los problemas de seguridad de la vida que surgen de esos sistemas. ¿Qué pasa si el servidor de un sistema de seguridad física de detección de intrusión fuera tomado e inutilizado por personas empeñadas en acceder al sitio?

La video vigilancia IP proporciona muchas ventajas sobre los anteriores sistemas, pero también es vulnerable. Los profesionales de la seguridad deberían hacerse estas preguntas:

- ¿Qué pasa si alguien tomó una cámara?

- ¿Qué pasa si alguien colocó una secuencia de video grabada anteriormente en lugar de la secuencia original?
- ¿El fabricante del equipo puso en práctica algún control para hacer esto difícil o imposible?
- ¿Qué pasa si los terroristas estuvieran viendo la secuencia de video?
- ¿Qué pasa si los ladrones apagaron el interruptor que trae el video en el sistema?
- ¿Qué pasa si alguien borró la evidencia de video?
- ¿Qué pasa si alguien apagó el video analítico por lo que no se enviaron las alarmas al oficial de seguridad?
- ¿Qué pasa si un ladrón cambió la función del video analítico de modo que repetidamente cause falsas alarmas?

Asimismo, el control de acceso electrónico proporciona muchos beneficios de seguridad, no obstante, también es vulnerable. Los sistemas de control de acceso generalmente contienen tres grandes componentes y hasta dos medios de transporte diferentes. El lector de tarjeta por lo general es la parte que ve el usuario, y presenta una tarjeta para, ya sea un mecanismo de contacto o un método sin contacto, a veces llamado tarjeta "prox" (proximidad). El lector de tarjetas se comunica a través de algún medio, ya sea por cable o inalámbrico, a un controlador que decide si la puerta se debe abrir o algo más debiera suceder (aunque esos dos sistemas pueden estar integrados). Finalmente, el controlador generalmente conversa con un servidor o una aplicación desde la cual obtiene instrucciones sobre qué hacer y qué información de la tarjeta almacenar localmente.

