Comerica Bank

FINANCIAL BRIEFS

July 2011

Protecting Your Small Business Against Internal Fraud

Technology has opened up doors for a new class of high-tech criminal. Business owners and consumers are bombarded with articles and news reports warning against the dangers of identity theft, computer hacking and other scams that were unheard of 25 years ago. While it's important to keep your computer and financial records safe from unknown tech-scam professionals, the criminal your business could fall prey to could be much more familiar.

"Unfortunately, many of the most common types of fraud cases are internal," says Terry Thornton, Senior Vice President and Fraud Services Director for Comerica Bank. "Employees have the easiest access and can sometimes harbor resentment or anger that pushes them to break the law."

Thornton offers the following information and advice to help you make sure that your company doesn't fall victim to internal fraud.

Be aware of internal fraud opportunities within the organization. Employee committed acts are the most common and most expensive type of fraud, accounting for more than half of all reported cases. According to the Association of Certified Fraud Examiners, $652 billion per year is lost to internal fraud. Small businesses are the most vulnerable, accounting for a whopping 80% of all internal fraud cases.

"The most common types of internal fraud include asset misappropriation, corruption and doctoring financial statements, as well as pilfering company cash or resources," says Thornton. "Common also are bribery and kickbacks, which involve vendors or others outside the business."

One thing that is helpful in alerting management to a possible internal theft is a company policy that requires employees to report suspicious activity of another employee. In order to be successful there must be a secure, anonymous method for the employees to report any such activity.

Take preventative measures. Many businesses fall victim to fraud because they trust their employees and think that it can't happen to them. One of the most effective measures a business owner can have in place to protect his or her business is a solid set of policies and procedures. Employees should be well-versed in these policies and know that violations will be not be tolerated.

Know who you hire and trust with your business. Small businesses should take measures to screen potential employees before they entrust them with the company's confidential information. Inform candidates they are subject to a background check for initial employment and a subsequent check if they move into a new function in a more sensitive area. Permission for credit checks should also be a condition of employment.

Additionally, separation of duties is an effective control a company can put in place to protect itself. For example, inventory warehouses can be full of loopholes that should be watched. It may be as simple as having a different person check out equipment than the one who checks it back in. Make sure that your employees know exactly what their responsibilities are and have been thoroughly trained.

Remain actively involved in your business. "It is best to be involved in your business and oversee all areas of the operations so if something doesn't look right, it can be addressed right away," says Thornton. For instance, keep control of your bank account. Too often, small businesses tend to give other people control of their accounts and do not monitor the account activity until it is too late. Also scrutinize checks for your signature and never signing a blank check. Avoid using a signature stamp, as that will limit the potential for someone to forge a company check. Finally, have an outsider review your books monthly, or at least quarterly, with no advanced warning to your employees.

Every business, no matter how small, can be vulnerable to fraud. Business owners should take a frequent and focused look at how their company operates and where its vulnerabilities are. Proactive steps now may pay off in the long run.

For more information, please contact Kristin Arena at 214.871.7723 or Kristin@allynmedia.com.

Source: Comerica Bank, Member FDIC. Equal Opportunity Lender.

RESUMEN FINANCIERO

Julio de 2011

Cómo proteger a sus pequeñas empresas del fraude interno

La tecnología le ha abierto las puertas a una nueva clase de delincuentes de alta tecnología. Los propietarios de empresas y los clientes son bombardeados con artículos y noticias que advierten sobre los peligros del robo de identidad, la piratería informática y otros tipos de estafas de las cuales no se tenía conocimiento alguno 25 años atrás. Si bien es importante mantener a salvo su computadora y sus registros financieros de profesionales en estafas tecnológicas desconocidos, es posible que el delincuente del cual su empresa podría ser víctima sea mucho más familiar.

“Desafortunadamente, muchos de los tipos de casos de fraude más comunes son internos”, indica Terry Thornton, vicepresidente sénior y director de Servicios contra el Fraude de Comerica Bank. “Los empleados son los que tienen más fácil acceso y a veces pueden tener sentimientos de enojo o resentimiento que los lleven a infringir la ley”.

Thornton pone a disposición los siguientes consejos e información para ayudarle a asegurarse de que su compañía no se convierta en una víctima del fraude interno.

Tenga conocimiento de las oportunidades de fraude interno dentro de la organización. Los delitos cometidos por los empleados son el tipo de fraude más común y más costoso, y representa más de la mitad de todos los casos denunciados. Según la Asociación de Examinadores Certificados de Fraude (Association of Certified Fraud Examiners), existe una pérdida de $652,000 millones por año debido a fraudes internos. Las pequeñas empresas son las más vulnerables, ya que representan el altísimo número de un 80% de todos los casos de fraude interno.

“El tipo más común de fraude interno incluye apropiación indebida de activos, corrupción y falsificación de estados financieros, como así también el robo de dinero o recursos de la compañía”, afirma Thornton. “También son comunes el soborno y la coima, que involucran a proveedores y terceros de fuera de la empresa”.

Lo que resulta útil a la hora de alertar a la administración sobre posibles robos internos es una política de la compañía que requiere que los empleados denuncien actividades sospechosas de otro empleado. Para que esto resulte exitoso, debe existir un método seguro y anónimo para que los empleados denuncien cualquier actividad de esa índole.

Tome medidas preventivas. Muchas empresas se convierten en víctimas de fraude porque confían en sus empleados y creen que el fraude es algo que no les sucederá. Una de las medidas más efectivas que un propietario de una empresa debe implementar para proteger su propia empresa es un conjunto sólido de políticas y procedimientos.

Los empleados deben conocer bien estas políticas y saber que no se tolerarán infracciones de ellas.

Conozca a quién contrata y en quién confía dentro de su empresa. Las pequeñas empresas deben tomar medidas para examinar a sus potenciales empleados antes de confiarles la información confidencial de la compañía. Infórmeles a los candidatos que se encuentran sujetos a una investigación de antecedentes para el empleo inicial y a una investigación posterior si son trasladados a nueva función en un área más confidencial. También debe ser un requisito de empleo el permiso para realizar investigaciones de crédito.

Además, la división de responsabilidades es un control efectivo que una compañía puede poner en práctica para protegerse. Por ejemplo, los almacenes de inventarios pueden estar llenos de vacíos legales que deben ser vigilados. Puede ser tan simple como tener una persona que revise los equipos y otra distinta que lo revise nuevamente. Asegúrese de que sus empleados sepan exactamente cuáles son las responsabilidades que tienen y para las cuales han sido cuidadosamente capacitados.

Manténgase involucrado activamente en su empresa. "Es mejor estar involucrado en su empresa y supervisar todas estas áreas, de modo que si algo no se ve bien, pueda solucionarse inmediatamente", sostiene Thornton. Por ejemplo, controle su cuenta bancaria. Con mucha frecuencia, las pequeñas empresas tienden a otorgarles el control de sus cuentas a otras personas y no vigilan la actividad de las cuentas hasta que ya es demasiado tarde. Además, examine detenidamente su firma en los cheques y nunca firme un cheque en blanco. Evite usar un sello con firma, ya que eso limitará la posibilidad de que alguien falsifique un cheque de la compañía. Por último, procure que una persona independiente revise sus libros de contabilidad mensualmente o por lo menos trimestralmente, sin advertencia anticipada a sus empleados.

Toda empresa, sin importar qué tan pequeña sea, puede ser vulnerable al fraude. Los propietarios de empresas deben prestarles atención de manera frecuente y enfocada al funcionamiento de su compañía y al lugar donde se encuentran sus vulnerabilidades. Tomar medidas preventivas puede dar sus frutos a largo plazo.

Para obtener más información, comuníquese con Kristin Arena llamando al 214.871.7723 o por correo electrónico a Kristin@allynmedia.com.

Fuente: Comerica Bank, miembro de la Corporación Federal de Seguros de Depósitos (FDIC). Prestamista con política de igualdad de oportunidades.