Managing Risk in the Moving & Storage Industry

ISSUE 01

The Dispatch

MOVER'S CHOICE BRIEFINGS

Article Written By:
Matt Schiefferly

Matt Schiefferly, Principal, Paul Hanson Partners

Matt Schiefferly attended UC Davis where he studied Economics and Political Science. Matt has been a producer at Paul Hanson for 15+ years specializing in insurance placement and consulting for moving and storage companies. Matt has also been the director of Safety and Loss Control at Paul Hanson and has consulted with transportation companies and associations across the country on loss control, safety and risk management topics.

This article is informational only.

Data Breaches Put Moving & Storage Companies at Risk

Data breaches at retail and entertainment giants like Sony, Target and Home Depot grab the headlines due to their size and scope. But breaches affect companies in every industry and of all sizes. The moving and storage industry is no exception.

Any company with computer systems and customer data can be a victim. And small and midsize companies are among the most vulnerable orga-nizations. In fact, a 2012 data breach study by Verizon found 71 percent of data breaches happened in businesses with fewer than 100 employees.

As large companies invest heavily in sophisticated security strategies that make them harder to penetrate, cyber criminals are increasingly turning to small and midsize companies. These smaller companies don't always have adequate staffing to manage their websites and online business compared to larger organizations.

How Data Breaches Happen

Among the many types of data breaches are illegal activity on the Internet that results in the theft of bank accounts, intellectual property and trade secrets, confiscation and distribution of confidential information, disruption of everyday business and the spread of malicious computer viruses.

Any business is a potential victim that:

- Creates, collects, stores or processes client information, including payment information, client names, emails or other records.
- Has access to a business partner's website or personal information.
- Stores or has access to any other sensitive financial or proprietary information.

And today, cyber criminals have more access points than ever. Business is no longer conducted primarily over office-based computer systems. Companies and their employees use mobile devices, store data in the cloud and interact through social media platforms.

Moving and storage companies certainly are part of this trend, with movers increasingly using handheld devices to collect information for sales and creating an inventory of customer belongings. Our industry also increasingly sends data to the cloud as a more flexible and cost-efficient method of storage. As we do so, hackers can quite easily penetrate cloud-based storage by obtaining credentials from one type of malware or another.

Finally, consider that breaches are not always the result of a targeted cyber attack.

Data Breaches Put Moving & Storage Companies at Risk

Cyber crime can be the result of a stolen or lost laptop, lost smart phone, paper files left unattended or burglarized, or an email sent to the wrong person.

What's at Risk

When a data breach happens, the impact is usually significant for the victim:

- A company's reputation can be damaged both among customers who may have had their data compromised as well as among the public in general when it is reported in the media or as word spreads socially.
- Customers, business partners, employees and vendors may have their identities stolen in a cascading stream of victims.
- Business can be interrupted, affecting sales and market competitiveness.

Perhaps most acute is the financial burden a victim bears from customer lawsuits, forensic costs to investigate the attack and notification of victims, to name just a few of the potential costs.

A 2012 study by security company Symantec and the National Cyber Security

Alliance estimated cyber attacks cost small and medium

size businesses an average of more than $188,000, forcing many out of business. And according to the Ponemon Institute annual data breach report, data breach costs equate to roughly $200 per record.

Protecting Yourself

With so much at risk, prevention and protection are keys. Start with a comprehensive review of systems and safeguards, conducting either an internal review by a dedicated individual or team, or utilizing an independent specialist. Be sure every aspect of the computer system, data storage and mobile computing practices are analyzed to determine if there are any weaknesses that need to be addressed.

Following a risk assessment, also consider:

- Creating a written cyber security policy and incident response plan.
- Running frequent computer scans that search for vulnerabilities.
- Using a mobile security app for Android and Apple devices to better detect and prevent mobile cyber attacks.
- Using keystroke encryption software, which provides an additional layer of security against keyloggers and information piracy if there is malware (malicious software used to gain access to computer systems) embedded in computers.
- Training employees on best practices for cyber security and keeping them up to date on the latest information.

Cyber insurance or data breach insurance should also be considered an essential layer of security and investment. This coverage helps protect against the financial impact of a data breach, as well as for consulting services during and after an incident. In addition to the preventative measure mentioned above, policies typically cover:

- A computer forensic analysis to determine the cause and extent of the privacy breach.
- A crisis management review and advice from an approved independent crisis management or legal firm.
- Expenses associated with notifying affected parties to maintain goodwill or comply with any notification requirements imposed by law.
- Call center services for credit monitoring, identity theft education and assistance for affected individuals.
- Defense costs in any resulting lawsuits.
- Loss or theft of personal and/or business data.
- Regulatory fines and penalties.

With cyber attacks on the rise, all moving and storage companies should proactively take action and start addressing this increasing exposure. It is not only good business to better protect your customers, it is critical to at least engage the fundamentals to prevent an attack and protect your reputation and bottom line in the event a breach occurs.

MOVER'S CHOICE