

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

don't believe in the integrity of a company and/or the reliability of its products will rarely, if ever, become buyers. And when you lose your customers' trust, you ...

Jun. 06, 2016



Trust is the foundation for most relationships—with husbands and wives, with parents and children, with employers and employees and with businesses and their customers. Trust is required for success, and the loss of trust dooms most relationships.

Trust is a major factor when a prospect is making a buying decision. Prospects who

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

misled its customers. The company's reputation was damaged, and trust was lost.

- T-Mobile hired Experian to handle customer credit reporting—and one of its servers was hacked. The data of 15 million individuals was stolen—leading to a crisis of confidence.

According to the Ponemon Institute, the average cost of a data breach is at least \$3.5 million per company. Costs include class action lawsuits, fines, deployment of new IT measures and the training of employees. But these costs pale in comparison to the loss of trust. It can lead to both short-term and long-term damage. In fact, some companies never recover from the loss of trust.

Hence, it is clear that a company's most valuable asset is its reputation. How can it best be protected?

IT Security and Subcontractors

Let's take a look at the Experian example mentioned earlier. T-Mobile used Experian, a subcontractor, to do the credit reporting for consumers who signed up for the company's mobile services. More than 15 million applicants had their personal information stolen by hackers from a server maintained by Experian.

No one knows exactly how the hack occurred. We do know that the stolen data included Social Security numbers, driver's license numbers and dates of birth, and this kind of information is gold to an identity thief. Unfortunately, the data may not have been encrypted on Experian's server.

These data crooks can open new credit lines, file bogus tax returns and in many other ways steal identities for profit. A breach that "only" compromises credit card information can be remedied by cancelling the card, whereas personal information is, well, personal!

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

laptop. The more information we store in the cloud, the more we need to secure the endpoints. Especially since user names and passwords are stored in the browser, a hacked laptop could mean giving away the keys to the kingdom, and it often goes unnoticed...until real damage is done.

Preventive 'Medicine'

Think of a company which has experienced a data breach as an injured patient. The doctor can prescribe "medicine" like credit monitoring or apply a "band aid" like paying fines to affected clients and customers. However, as with the protection of an individual's health, it is a lot easier and cheaper to be proactive and prevent a breach from occurring at all.

Encryption to the Rescue

CPAs and accounting firms, given the sensitive nature of the data to which they have access, are obligated to leverage third-party protection to the highest possible standard: full disk encryption. But there is a problem, especially in small- to mid-sized organizations. When it comes to the installation of full disk encryption, deployment and management are typically the responsibility of an IT department.

But small firms don't have IT departments, and the CPAs themselves are busy with day-to-day responsibilities and don't have the resources or the skills to handle this themselves. The ideal solution for these firms is to rely on a provider of endpoint security as-a-service to handle encryption deployment and management.

Trust me.

Ebba Blitz is CEO of [Alertsec](#), a cloud-based information security service that provides an easy and convenient way to protect information on an organization's laptops. No server, IT

knowledge or training is needed, as everything is included in the Alertsec subscription.

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.

© 2024 Firmworks, LLC. All rights reserved