PROTECTING TAXPAYER DATA

What Departments of Revenue Should Know Before Choosing a Business Partner

exela TECHNOLOGIES

THE AGE OF THE DATA BREACH

In 2013, Target announced a massive data breach in which personal information for millions of its customers, including full names, account numbers, and email addresses, was compromised. The Target breach was the first in a wave of data breaches through the end of 2014 in industries as diverse as retail, food service, banking, and healthcare. The world is now painfully aware that all businesses and organizations that collect and maintain information on its customers are vulnerable, no matter their size or annual revenue.

Over 400 million people have been exposed in data breaches since the 2013 Target breach. That is more people than the population of the United States. The financial implications of such information being used fraudulently are staggering. Individuals who have had their personal information compromised are at risk for identity theft that could drain their bank accounts and ruin their credit. When thieves use that information to scam governments, the cost increases again as it grows to include tax fraud. The Internal Revenue Service estimated that it paid $5.2 billion in fraudulent ID-theft-related refunds in the 2013 filing season, while blocking attempts at another $24.2 billion in such refunds, according to an August 2014 report by the U.S. Government Accountability Office.

As more transactions move into the electronic sphere, and more confidential information is moved into the digital space, more organizations will leave themselves vulnerable to attack.

©2018 Exela Technologies, Inc. | +1 844-XELATEC | exelatech.com | @exelatech

Many people think that malicious cyberattacks are behind most data breaches—sophisticated networks of computer hacker geniuses executing meticulously planned and intricate attacks on targeted systems. In truth, the majority of breaches originate because of weak security processes or negligent employees. The Ponemon Institute's 2013 publication says that while 37 percent of data security incidents involved a malicious or criminal attack, a combined 64 percent were attributed to human error or system glitches.

While organizations do have cause to fear malicious hackers, they have even more to fear from inadequate policies, inefficiently applied security measures, and inept employees.

The Cost of Inadequate Security

The costs associated with data breaches are astronomical and multi-leveled. According to the Ponemon Insitute's 2014 "Cost of a Data Breach" study, the average cost of a data breach is $5.9 million. Putting a cost on data breaches is complicated and involves analyzing several different areas of impact, both direct and indirect. Most obvious is the cost to identify and correct the gaps in security that allowed the data breach to occur in the first place. Once a breach has been identified, the organization has to invest in technologies and professional services to figure out where the breach happened, how to fix it in the short-term, and how to implement a long-term solution to keep it from happening again. Just repairing the broken system itself can carry astronomical costs in terms of time, tools, and expertise.

There are other expenses incurred by dealing with a data breach that may be outside of most organizations' normal scope. For example, notifying the public about the breach, coordinating and executing emergency response plans, and investing hours into investigation activities all require

additional work, either from internal employees or outside consultants. The human resources cost can therefore be quite significant. Organizations also have a responsibility to the people who entrusted them with sensitive information. Typically, impacted customers receive credit monitoring for a year, and some organizations offer an insurance policy to cover any future fraud associated with the stolen information. The more customers who were compromised, the greater these associated direct costs.

Litigious action is also a very real financial threat in the wake of a data breach. Individuals can sue organizations for not adequately protecting their data at the same time that operations are scrambling to recover from the breach itself.

This puts the organization in the uncomfortable position of being the victim of a cyberattack and the perpetrator of criminal negligence simultaneously—never a profitable stance. Settlement costs can be huge, as can the overhead to stage a courtroom defense.

Finally, organizations must address the public relations effect of the breach. In terms of damaged reputation, decreased sales, and loss of public trust, the fallout from failure to secure confidential information can last for years and financially cripple some institutions.

The Challenge for Departments of Revenue

Even more than most institutions, departments of revenue and their taxing authorities are at high risk of being targeted by hackers because of the highly sensitive material they handle. As a result, they have a much larger obligation to the individuals who are entrusting them with that personal information.

Unlike retailers, service providers, or other private sector entities, taxing authorities are not an optional presence in taxpayers' lives. Individuals are required to provide names, addresses, social security numbers, and other secure information to their departments of revenue, and they should be able to rest easy knowing that every measure has been taken to secure their financial wellbeing.

Departments of revenue have a responsibility to the taxpayer to implement strong security measures, including outsourcing processes to partners that have the knowledge, resources, and secure infrastructure to reduce chances of being hacked.

Ponemon and other analysts have identified several areas where organizations can invest in a data breach prevention plan that will reap the biggest benefits. These reports confirm that organizations should work to develop a strong incident response plan and ensure they are following the strictest regulatory recommendations available – but just as importantly, they should partner with outside consultants and vendors that can serve to fill critical gaps in their security processes to the highest standards. Security comes at a price and, in many cases, the strict protocols and advanced technology required to keep data breaches at bay may be too much for one department to handle.

©2018 Exela Technologies, Inc. | +1 844-XELATEC | exelatech.com | @exelatech

Security Personnel Clearances and Training

In addition to outlining the means by which data must be physically stored and destroyed, the IRS Publication 1075 guidelines offer instructions on how to qualify security personnel who have access to sensitive federal tax information (FTI). The publication dictates that any person who has contact with sensitive taxpayer data must complete a background investigation to ensure they are suitable for their positions and can be trusted. Any personnel with administrator access to the records may be subject to additional background checks. Access to the data can only be granted by operational supervisors or resource owners, and must be audited by internal security auditors. All personnel must receive user-specific training for their roles that includes how FTI security requirements are communicated.

After passing the background check and receiving security clearance, all personnel—both internal and outside vendors—must be appropriately trained. Departments of revenue and their business partners should start with the online training resources on Publication 1075 that the IRS provides on its website, and then develop internal training programs following the training outlined at the state level. Optimally, vendors will be allowed by participate in the same state-sponsored training program as employees of the department of revenue to ensure consistency and uniformity. However the training is administered, all internal and third-party personnel should be required to sign confidentiality agreements acknowledging they understand any legal consequences associated with violating FTI security requirements.

Choosing a Business Partner

Any organization that comes into contact with FTI is a possible target for data breaches, and it is the responsibility of the department of revenue and its chosen business partners to ensure there are proper controls in place to prevent, detect, and respond to data breaches. IRS Publication 1075 provides bottom-level requirements for securing FTI, but mature companies know they must exceed those requirements in order to remain trusted service providers and protect their clients' information.

Currently nearly 50% of Exela partners/customers require compliancy to IRS Publication 1075, but because our infrastructure and security processes are all NIST 800-53 compliant, every one of our clients receives security that goes beyond those mandates.

We believe that it's always better to own than to rent, so we own our infrastructure. Our NIST-compliant physical servers are centrally located and open to visits from our clients so they can see where their data is being secured. On the other end of the infrastructure spectrum, we constantly monitor our systems at the point of input. Unlike some service providers that use home keyer systems, all of our services are performed in a brick and mortar company-owned facility, so our customers can walk onto the production floor and watch their work being processed from one central location. In addition, our information is encrypted and NIST compliant.

Every single person who comes into contact with hard copies of FTI data at Exela has passed a comprehensive background check or received clearance from a department of revenue. And before any personnel gains access to sensitive information, they undergo extensive security training.

Departments of revenue are at an elevated risk for data breaches because of the highly sensitive nature of the information they handle. Due to the extremely high cost of innovating operations, equipment and processes to keep up with the demands of evolving technology, it may make the most fiscal sense for taxing authorities to outsource certain business functions to reputable, responsible partners.

Exela's solutions typically provide our Department of Revenue clients a savings of 30% as compared to an in-house model. In 2015, Exela processed over 20 million paper tax returns for Department of Revenue or tax collection agencies in New York City, New Jersey, Georgia, Alabama, Kentucky, South Carolina, Arkansas, and Arizona. By applying our proven, tested, and repeatable tax operations platform, we are able to process these tax returns in less than seven days at quality levels exceeding 99.5%.

It remains imperative that outside vendors must be held accountable to the same standards of security that internal employees must meet. We constantly push ourselves to meet and exceed the requirements outlined by the most stringent regulatory bodies in order to provide our clients the highest levels of excellence and security possible.

©2018 Exela Technologies, Inc. | +1 844-XELATEC | exelatech.com | @exelatech