

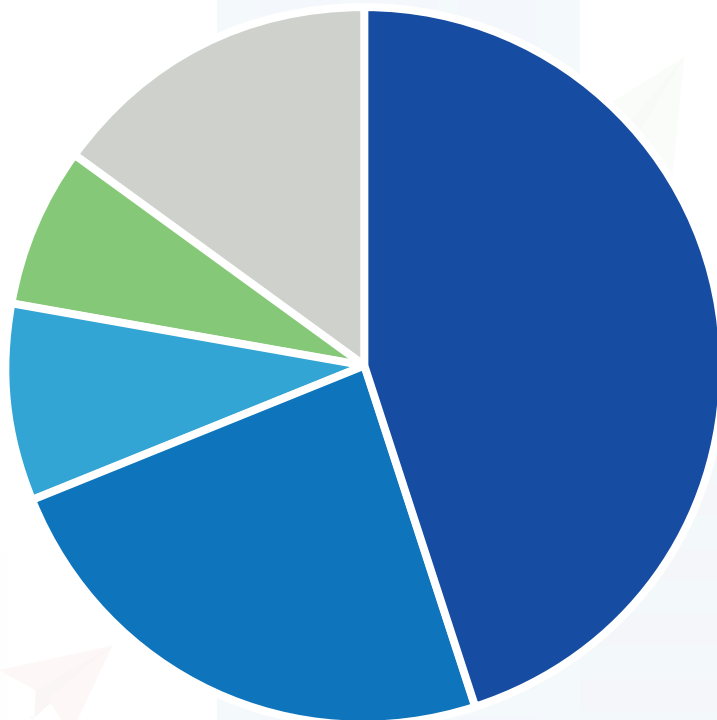


VULNERABILITIES CREATED THROUGH YOUR VENDORS



NUMBER OF BREACHES, BY INDUSTRY

SECURITY BREACHES, BY INDUSTRY



Now that the most recent Target breach has been linked to a third-party service provider, it's important to understand how vendor risk management and email security go hand in hand, and how Sendio can work to protect you from just such a breach.

Third party vendors risk is fairly well documented in the infosec industry. According to the 2013 Trustwave Global Security Report, 63% of data breaches are linked to a third-party component of IT system administration, and according to Verizon's 2013 Data Breach Investigation Report, 76% of network intrusions exploited weak or stolen passwords. The majority of these breaches occurred in the retail industry, but the food and beverage, hospitality and financial services industries were also likely targets.

- Retail 45%
- Food and Beverage 24%
- Hospitality 9%
- Financial Services 7%
- Other 15%

TARGET BREACH, VISUALIZED

So what path do intruders use to gain access to critical information?

In the case of the Target breach, it all began with a phishing email sent to the third-party HVAC service provider **Fazio Mechanical**. Then it moved along the following path:



STEP 1

Phishing email is sent out (Fazio Mechanical)



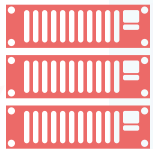
STEP 2

Malware is downloaded (Fazio Mechanical). There are a number of different types of malware but the goal is pretty much always the same: to gain access to a critical server.



STEP 3

Fazio Mechanical and Target connection (through a small level computer/connection)



STEP 4

Once a server is accessed, hackers need to move to the larger corporate network (at Target).



STEP 5

From there the thieves can access valuable information like that of point-of-sale (POS) machines (At Target)



STEP 6

Credit card swiped at POS (at Target)



STEP 7

Credit Card Data routed all the way back through and transmitted back to the bad guys.

SOURCE: Krebs On Security, Email Attack on Vendor Set Up Breach at Target. Feb. 14, 2014. <http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/>

MOST COMMON TACTICS FOR BREACHES

There is surprisingly little variation in system breaches, and the majority of them use one of the following eight tactics in order to gain access. These can be used on either the target company, (which, ironically, in this case was Target,) or a third-party vendor with access to a critical server.

Weak and Stolen Credentials, a.k.a. Passwords: According to the Verizon Data Breach Investigations Report, four out of five breaches occur because of weak or stolen passwords. Even if you think your security is up to snuff, your vendor might not be treating the passwords given them quite as securely.

BACK DOORS, APPLICATION VULNERABILITIES

Malware: Malware and phishing go hand in hand. We have published several times on the dangers of opening sleazy looking emails and following shady links. Brian Krebs even reported that the malware eventually found responsible for the Target breach was most likely downloaded through a phishing campaign.

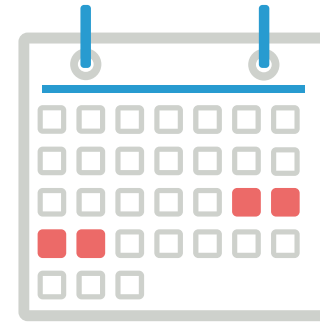
Social Engineering: Social engineering has been around for centuries, but it's become much easier in the digital age. Often social engineering campaigns begin with just an email and a name, and can get almost anywhere from there. Even those prepared for such a trick can sometimes be fooled, which is why its so important to know exactly who's allowed in your inbox.

- Too Many Permissions
- Insider Threats
- Physical Attacks
- Improper Configuration, User Error

RESULTING LOSS

Breaches don't come cheap, and some companies aren't big enough to absorb the damage from a major intrusion. Breach costs have grown steadily since 2006, and in 2010 data breaches cost companies an average of \$214 per compromised record, up 5% from last year. More importantly, breached companies often lose more in public trust, lawsuits that result from compromised customer information and other less obvious consequences.

In fact, after the breach, Target was forced to offer unplanned discounts and boost advertising in order to minimize losses during the holiday season, an act that took a major bite of their profits. Bringing back customers can be costly, and the 40 million customers that were compromised aren't likely to forgive anytime soon. Taking a look at the company's Buzz Score, a measurement of brand popularity, it's clear the effect that a large breach can have on a company: Target's score dropped 45 points between the Friday when the breach was announced and the following Monday. It's always important to remember that regardless of the costs of system patches and security manpower, it's a trifle compared to possible damage that a major breach can do.



CALCULATING LOSS

Perhaps a better way to illustrate the loss that a major data breach can effect, is to calculate the average customer lifetime value (CLV) for your industry and the cost to replace customers (CtR), and then work through to find the amount of people directly influenced by the breach. By plugging these numbers into the following equation:

You can get a basic idea of the effect that a breach can have on your business. But let's say that for some reason you don't know your CLV and CtR, you can still use the model to get an idea of how quickly costs add up. Imagine that each of your customers is worth about \$10 annually, and that each customer has a lifetime of around 10 years. We'll then suppose that there are 100 records compromised. By plugging in this information we see that:

$$\begin{array}{l} \text{Affected customers} \times \boxed{\text{CLV}} \\ + \\ \text{Affected customers} \times \boxed{\text{CtR}} \\ + \\ \left[\frac{\text{Influenced people}}{50} \right] \times \boxed{\text{CLV}} \end{array}$$

Cost of reputation loss from breach







Affected Customer Loss: $100 * (\$10 * 10) = \$10,000$

Influenced Customer Loss: $100 * (100) = 10,000 * 100 = \$1,000,000$

Total Reputation Cost: \$1,000,000

And this is, of course, before cost to replace these customers has ever been added to the equation. All too often companies see email security as pretty low on the list of business priorities, however when you consider the potential loss of customers multiplied by the actual value per customer, you'll see that what appears to be a minor breach (only 100 records after all), can have a serious effect on business for years to come.

TIPS TO PROTECT YOURSELF

-  **Hold Vendors Accountable:** Companies that wish to avoid the consequences of a data breach need to hold vendors and partners to the same standards that they hold themselves to. It's crucial that third party service providers comply with state and federal regulations, and that your organization maintains control of the data at all times.
-  **Consolidate Remote Access Tools:** Take measures to understand what remote access tools your vendors are using or which systems they're accessing. You can increase security by decreasing the number of vendors that have access beyond what's necessary.
-  **Enforce Multi-Factor Authentication:** Enforce the use of secure credential and force vendors to use multi-factor authentication to login. Not only will this reduce the chance of stolen vendor credentials, but also improve your compliance with regulations like PCI DSS.
-  **Make a Plan:** Determine the outcome of a possible vendor breach, the risk of harm to your customers and how to respond when one happens.
-  **Keep Current:** A critical step to keeping safe is staying on top of security software updates and patches. Although applying patches takes time and resources, an unpatched system is just waiting to be exploited by hackers.
-  **Put it in Writing:** Include some additional protections around data breaches in your vendor contracts. This can do a great deal to secure a vendor's active cooperation in investigating and remediating any incident.



For more information or to start your free 30 day trial visit sendio.com.

Follow us!



Get started with Sendio



Watch us on YouTube



Follow us on Twitter



Connect with us on LinkedIn



Like us on Facebook



Subscribe to our Blog