ANATOMY OF A CYBER SECURITY HACK

Big Boxes 4U is a major mass-market retailer with more than 1,500 locations in the United States. Its innovative designer partnerships, high-quality product mix, and great customer service have earned it a loyal customer following. But, like its high-profile industry counterparts, such as Target, Home Depot, Michael's and others, Big Boxes 4U has been breached by hackers and the personal data of millions of customers has been exposed. How did it happen?

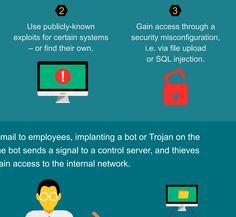
MAKING THEIR WAY IN

Customer information is typically captured at the point of sale.

In-store or online purchases:

The result is a central database that houses a collection of valuable customer information and gives you insight into how they shop, what they buy, and what products and services they prefer.

Customer data is like gold to mass-market retailers, and is the backbone of marketing and loyalty program efforts. Protecting that data is protecting the customer's trust.



UNDER ATTACK

Retailers are facing unprecedented cyber security threats.

Greater Threat: Expect a sharp increase in the number of retail data breaches until chip and pin technology is fully adopted.

Attack Internet-facing servers in three key ways:

1. Hack default or overly simplistic passwords.

2. Use publicly-known exploits for certain systems – or find their own.

3. Gain access through a security misconfiguration, i.e, via file upload or SQL injection.

Send a phishing email to employees, implanting a bot or Trojan on the internal network. The bot sends a signal to a control server, and thieves gain access to the internal network.

Access through third parties (i.e., suppliers) with access to the network.

Partner with a rogue employee to steal data electronically or work with thieves to implant a bot.

STEALING THE KEYS TO THE FORTRESS

Once inside the system, most hackers follow a familiar five-step path to get to the goods.

SECURITY BREACHES BY THE NUMBERS

Data breaches carry great cost and risks for businesses, sometimes with devastating effects.

$5.85 million

Average cost of a U.S. organization's data breach.

15%

Rate at which data costs increased from 2013 to 2014 and continue to rise.

$145

Average cost paid for each lost or stolen record containing sensitive information.

$686,000

Average cost per hour for a company experiencing downtime.

$148 million

Cost of Target's data breach, not including lower revenue forecasts.

REDUCING YOUR THREAT

Take action to reduce the threat and reduce the cost of breaches.

Factors that decrease the cost of a data breach:

- Having a strong security posture: **$14.14** per record
- Instituting an incident response plan: **$12.77** per record
- Having a Chief Information Security Officer: **$6.59** per record

Using disaster recovery as a service:

- Reduces your cost and losses by keeping your business running, even when it can't use the main network because of a breach.
- Provides increased security to detect and prevent threats when they emerge.
- Provides greater protection to your customers. Studies have found that customer loyalty decreases after a breach.

To better protect your company and customers' data, contact Sungard Availability Systems at

www.sungardas.com

Sources

- Experian, "2015 Data Breach Industry Forecast"
- Ponemon Institute, "Is Your Company Ready for a Big Data Breach?"
- The New York Times, "Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop"

SUNGARD® AVAILABILITY SERVICES™