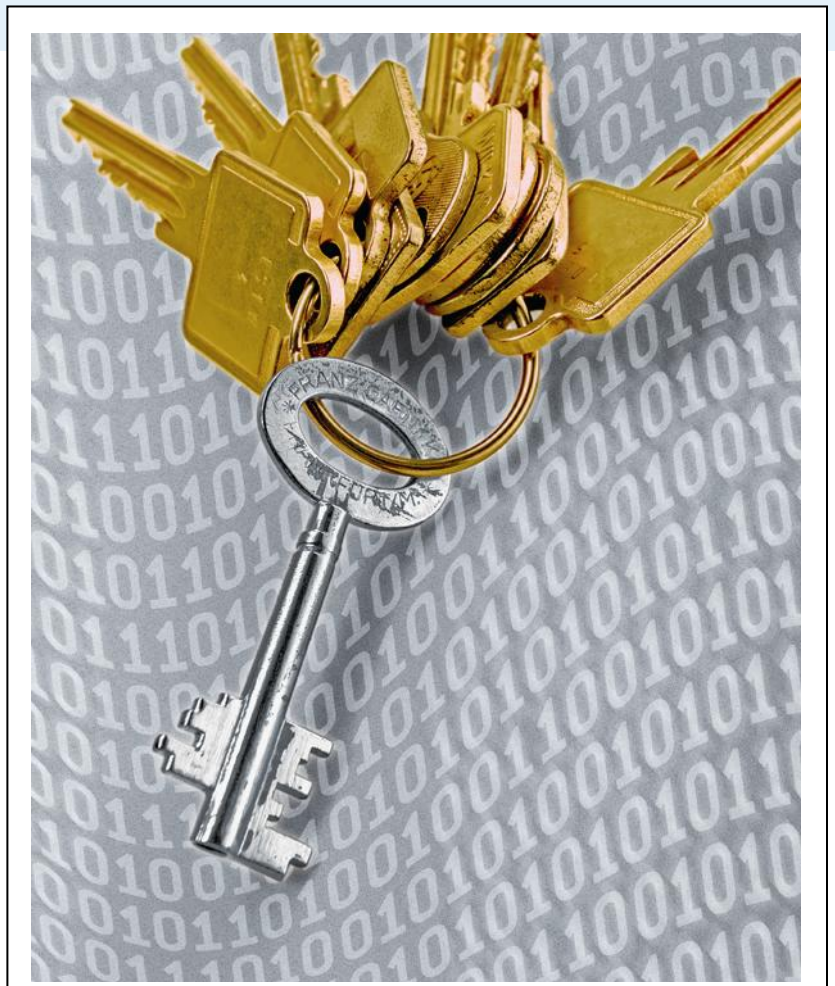




Learning from Data Breaches

Don't be the subject of tomorrow's headlines



Learning from Data Breaches

Don't be the subject of tomorrow's headlines

Several companies have recently learned that accidental or intentional data disclosure by employees can be both costly and embarrassing. To avoid being at the center of the next incident and becoming the next topic of news headlines, it makes sense to look at what these companies did wrong and learn from these experiences.

TJX, Fidelity Financial, Boeing, and the Georgia Department of Health Services have experienced some of the largest cases of information theft and disclosure of customer data. This whitepaper highlights some of the details of each of these cases and highlights what security professionals and IT management can do to avoid repeating their mistakes.

The Victims

» TJX

TJX, the parent company of TJ Maxx and other retail chains was attacked by criminal hackers over a period spanning several years. The target was customer credit card data stored on TJX's servers. All in all, customer data for 47 million individuals was compromised. The intruders and other criminals they sold these credit card numbers to used then for fraudulent purchases from many retailers that added up to millions of dollars. TJX just settled a number of claims resulting from this, and the actual costs to the company have surpassed \$100 million and are still growing. The indirect costs, including the loss of customer confidence in the company, are difficult to measure, but are probably even higher.

So, what went wrong? The details are still unclear, as TJX has been tight-lipped about what exactly happened, but some elements of the largest reported data breach in history are slowly emerging. It is clear that the hackers used several methods to get to the data and InformationWeek recently reported what some of them were. First, TJX apparently neglected to properly secure their wireless network, allowing hackers to get access to the corporate network and monitor data being transmitted between different computers and devices. TJX also placed computer kiosks on store floors to allow job applicants to fill out application online. These computers were directly connected to the corporate network and hackers simply plugged flash drives into the back of them to bring malicious software into TJX's network.

TJX could have easily prevented both of these attack methods by doing the following:

- Properly secure wireless networks. All wireless communications should be encrypted and authenticated. Among the available encryption mechanisms, WEP (Wired Equivalency Protocol), which TJX reportedly used, and WPA (Wireless Protected Access) are the most commonly used, but both of them can be easily broken by a determined hacker. WPA2 provides much better security and should be adopted as a standard.
- Prevent bridging of wireless networks. While there is no indication that this specifically played a role in the TJX case, wireless security should also ensure that client computers with wireless network connections don't allow anyone to connect to them while they are simultaneously connected to the wired corporate network. This prevents a hacker sitting in a car outside the office building from connecting to a client computer and using this connection to then get access to the entire corporate

network. Administrators can use DriveLock's network connection control to automatically disable wireless connections while a wired connection is active or to control which networks users are allowed to connect to.

- Use internal firewalls. When the hackers broke into the kiosk computers they had direct access to TJX's internal network. An internal firewall should have been used to separate kiosk computers from servers storing sensitive data and other parts of the internal network and to tightly filter the information flowing between them.
- Control the use of peripheral devices. There is no legitimate reason why anyone should connect a flash drive to a kiosk computer. TJX could have provided secure enclosures for these computers to prevent physical access to the USB ports. A software solution, such as DriveLock, that can both control and monitor access to all ports provides even better protection since it can distinguish between legitimate and malicious use of all external ports and alert administrators when someone attempts to perform any unauthorized access.
- Control the use of applications. Intruders at TJX were able to run unauthorized software on the kiosk computers. With DriveLock you can control who is allowed to run which programs on any computer in your organization.

» Certegy

Certegy, a subsidiary of Fidelity National Information Services, processes check approvals for a large number of retailers. As a result, it stores financial information about millions of customers. Earlier this year one of their database administrators was arrested for stealing the records of over 8.5 million customers and reselling them. Certegy reportedly only became aware of the incident after customers reported suspicious transactions. Today Certegy has to defend itself against a number of class-action suits and the loss of business due to customers losing their faith in them. The perpetrator copied the data he pilfered to a portable disk, apparently to avoid detection and not to leave any evidence of his action. There are several lessons to be learned from Certegy's experience:

- Don't trust insiders. The person who stole the data had worked for the company for several years and had been granted access to the data. As in this case, many cases of data theft are committed by trusted insiders. While we all want to trust the people we work with, it is a good practice to not let your guard down and to be on the lookout for suspicious activity.
- Monitor where your data is going. The data theft initially went undetected because nobody monitored which data was copied from a server to mobile storage devices. DriveLock can be used to control what data users can copy to and from mobile devices. Just as important, DriveLock can monitor data transfers and alert security personnel to unauthorized activity before it's too late.

» Boeing

A Boeing employee, who had been employed by the company for 18 years, allegedly stole 320,000 confidential documents. Boeing claims that he was prepared to share this data with its competitors and that the potential damage could have been \$5 billion. What makes this case unusual is the magnitude of the damage, but it is also an example for data theft by insiders. With effective device control Boeing could have prevented the data from being copied to a mobile storage device and been alerted to the employee's actions much earlier. DriveLock can provide granular control over what's copied to mobile devices and lets administrators create detailed reports that can alert them to unauthorized activity.

» Georgia Department of Health Services

A contractor for the Georgia Department of Health Services sent a disk containing sensitive data about almost 3 million individuals to the Centers for Disease Control, but the disk got lost in transit. Because of the risk of unauthorized data disclosure, the agency had to notify all affected individuals and provide them with information about the risk of identity theft they were exposed to. In addition to the measurable costs, both the state agency and the contractor suffered from a serious lack in public confidence. There are several lessons to be learned from this:

- Encrypt all data that leaves the organization. The data on the lost disk was unencrypted. A variety of encryption methods could have been used to encrypt the data before it was mailed. If the data had been encrypted, there would have been no risk of information disclosure and the agency would not have had to notify the individuals whose data was on the disk.
- Make encryption easy to use. Most encryption mechanisms available today can be very effective. However, employees often don't encrypt data when doing so is complicated. Even better, make encryption automatic. For example, DriveLock can automatically and transparently encrypt all data that's copied to mobile storage devices. This ensures that encryption always takes place; users don't need to perform any special steps or even think about encryption.
- Monitor data leaving the organization. When a disk containing personal data is lost you may have to notify everyone affected unless this data was encrypted. However, when it comes to taking action you need to be completely sure that the data was indeed encrypted. To assess the situation it's essential that you have auditing data that shows whether encryption took place. DriveLock's reporting can show you what data was copied to which device by whom—and whether it was encrypted or not.

Protect Yourself: Productive and Safe Use of Devices

Most of the threats from unapproved device usage can be eliminated by simply disabling the ports that these devices can be attached to. However, this is not a realistic solution for organizations that depend on selected external devices for approved business functions or need to move data between computers using mobile storage. To make this possible, it is necessary to have granular control over who can use which device on corporate computers. Windows does not give administrators this type of granular control, creating the need for specialized software solutions. DriveLock can help you secure your data in a number of ways.

» Comprehensive Device Support

To be effective, any device control solution has to be comprehensive. While USB devices are most common today, other connectivity methods, such as FireWire, pose similar challenges. And device control must be able to differentiate between different types of devices so administrators can, for example, allow the use of USB keyboards while preventing the use of music players. DriveLock can selectively allow or deny access to virtually any device that can be attached to a computer.



» Granular Control

Not everyone in an organization has the same requirements for legitimate device usage. For example, a mortgage company may determine prohibit call center employees from using mobile storage devices to prevent the theft of customer data, but help desk personnel may need to copy driver files from a flash drive to the help desk computers. A small company may perform a daily backup of local data to a portable hard drive every evening but does not want to allow the use of other portable storage. DriveLock can differentiate between devices by manufacturer, model, or even serial number, and it allows administrators to allow or deny device usage based on device, user, time of day, or a number of other factors.

» Data Protection

Many employees have a legitimate need to copy data to a mobile device. One employee may use a USB stick to give a file to a business partner. Another employee may use a portable hard drive to take files with her to work on them at home. DriveLock not only makes this possible, it also can ensure that the loss of a storage device does not result in data disclosure. It can automatically encrypt the data so that someone who finds a lost device cannot access the data. It can be configured to be completely transparent to the user and allows easy authenticated access to the data even on computers that are not managed by the organization.

» Monitoring

Being able to monitor how devices are used and what data is copied to and from devices is a crucial requirement for all but the smallest organization. More and more organizations face regulatory requirements that require them to notify customers and clients when personal data may have been compromised, even when this involves no confirmed misuse. Being able to show that the lost data is encrypted can eliminate the notification requirement with the associated cost and loss of reputation. DriveLock's monitoring is comprehensive, flexible, and include detailed information about device usage and the copying of files.

» Network Control

Employees who connect their computers to unauthorized networks, especially wireless networks outside the organizations pose a real and serious threat to your data. DriveLock lets you decide which networks users are allowed to connect to and what protection levels are enforced on each authorized network.

» Application Control

DriveLock lets you take complete control over who can run which program on any computer within your organization. You can use blacklists to block malicious software, or whitelists to restrict users to a tightly controlled set of programs. You can even combine both to meet the specific needs of your organization. Application control rules can even be specific to a network, for example allowing someone to run a communications program while away from the office, but not while connected to the corporate network,

CenterTools DriveLock™—The Leader in Device Control

DriveLock™ from CenterTools provides effective protection from mobile device threats, while addressing the requirements of organizations of any size. DriveLock™ is a lightweight software solution that helps you secure your computers. DriveLock™ offers dynamic, configurable access control for mobile drives (floppy disk drives, CD-ROM drives, USB memory sticks, etc.) and also controls the use of most other device types, such as Bluetooth, Palm, Windows Mobile, BlackBerry, virtual devices, Smartphones, media devices and many more. By configuring whitelist rules based on device type and hardware ID you can define exactly who can access which device at which time. Removable drives can be controlled according to vendor, product ID and even according to serial number, allowing you to define and enforce very granular access control policies. Additional features let you unlock specific authorized media and to define time limits and computers for whitelist rules. You can even unlock DriveLock's device control on a computer temporarily if required, and you can do this even when this computer is offline and not connected to a network. DriveLock's support for different device types and granular control make it easy to enforce virtually any corporate policies on device usage.

Installation of the client software (the DriveLock™ Agent) and policy deployment can be easily accomplished by using existing software deployment mechanisms or by using the Group Policy feature of Active Directory. Alternatively, you can distribute policies using configuration files for standalone computers or in environments without Active Directory (for example Novell).

DriveLock's auditing capabilities, coupled with its shadowing functionality give you the control and information you need to enforce policy compliance. By using the DriveLock™ Device Scanner you can detect any drive or

device used in your network, even if it is not longer connected to the computer. The DriveLock™ Agent doesn't need to be installed on the target computers to use the Device Scanner.

Automatic and transparent encryption of mobile data makes it easy for users to take data with them without administrators and management having to worry about unauthorized disclosure. DriveLock™ can enforce the use of encryption when data is copied to removable drives to secure sensitive information. The Security Reporting Center is DriveLock's central database and reporting console. The SRC consolidates all DriveLock™ events, information about whitelist rules, client configuration and Device Scanner results in a central SQL Server database. Administrators can then use this data to create dynamic reports for auditing and management reports. When you add network control and application control, it adds up to a comprehensive security solution that's easy to implement, easy to administer and easy to use.

To read more about DriveLock™ or to download a fully functional trial, visit www.drivelock.com. You can also contact CenterTools by calling (888) 627-7515 or by sending e-mail to info@centertools.com.

