Data Theft Prevention Checklist

i-Sight®

With the average cost of a data breach at $3.8 million and rising every year, it's more important than ever for companies to have policies and procedures in place to protect their sensitive information. We've consulted with top information security experts to create this comprehensive checklist for preventing data theft in your organization.

Storage and Access

1. Shred the following:

- Mail with a name and address
- Luggage tags
- Trip itineraries and boarding passes
- Credit offers
- Price lists
- Vendor payment stubs and invoices
- Cancelled checks
- Receipts

2. Have your IT Department set up access roles to restrict access to your sensitive data to only those who require it.

3. Find out what you need to protect through an audit or assessment of your data.

4. Hold third parties and contractors your company engages to the same strict data privacy controls you implement in your own organization.

Technology

1. Protect all computers and devices with passwords and enable remote wipe capabilities.

2. Install or enable a firewall to keep outsiders from accessing your company network.

3. Protect your wireless network with a password and use encryption and security to hide your wireless network from outsiders.

4. Encrypt all sensitive information being transferred. Install encryption on all company laptops, mobile devices and removable media.

5. Use a proxy to access the internet in public places where wifi may be shared by other users.

6. Activate two-factor authentication.

7. Prohibit the transfer of personal information, such as social security numbers or medical information, via portable devices.

8. Purchase and use up-to-date anti-virus software and anti-spyware.

People

1. Require strong passwords at least eight characters long with uppercase and lowercase letters, numbers and special characters.

2. Enforce a “clean desk” policy prohibiting employees from keeping working papers and sensitive documents in view.

3. Train employees to recognize and report “phishing”, “smishing” and other forms of social engineering.

4. Set up a separate wireless “guest” network for personal devices to keep your company network safe.

5. Implement social media policies to prevent employees from oversharing on social media or falling for social media scams and frauds.

6. Be nice to your employees. A disgruntled employee can be the most dangerous vulnerability in your data protection program.