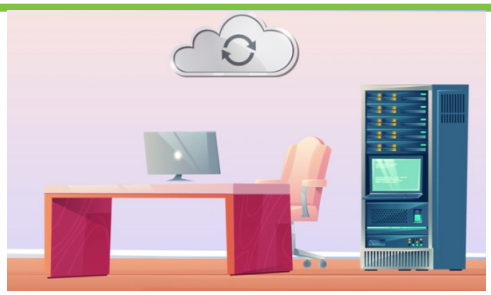
Click Thinking Spotlight

Data Loss Prevention

It's not surprising that the loss of data, especially sensitive information, can cause significant problems for a business. As such, preventing data loss in the workplace is critical—and everyone plays a role.

- A data classification policy sets ground rules that everyone can follow. It dictates what information can and can't be shared or may be accessed on a limited basis. The policy is the cornerstone of any data loss prevention strategy.
- Workplace data has migrated from file cabinets and desk drawers to digital hard drives, company servers and the cloud. While it often resides at a physical place of business, data also exists on the devices and in the homes of remote workers and third-party vendors.
- Where your company data lives directly impacts how you protect it from loss, whether by lock and key, digital barriers, security personnel or other means.
- Physical data can be stolen, misplaced, damaged or destroyed. Digital data is susceptible to these risks, too, as well as efforts by cybercriminals seeking access through hacks or phishing.
- While threats can come from anywhere, nearly half of all data breaches are internal, perpetrated by employees acting unwittingly or maliciously.
- While data can be compromised at any point it's highly vulnerable when in motion. For example, a file in an email can be stolen by hackers if it's sent through an unsecured network. And thumb drives containing sensitive data can go missing if the purse or brief case they're being transported in is stolen.
- Understanding when and how data is moving in and out of your organization is a key factor in protecting it.
- With a better sense of how your data is classified, where it lives, the types of threats it may be exposed to and when it's most vulnerable, you can assess your threat landscape—the extent to which your data is at risk.
- Observe how data moves through your company, noting where risks exist and when data losses occur. Determine what's working, what's not and where additional controls are needed, such as firewalls for the company network, e-mail protection or badge access to physical locations where data is stored.
- Once you've assessed and made adjustments, document your plan and share it. The goal is to foster a culture that appreciates the importance of protecting data.



For the Data Loss Prevention module, see your manager or information security contact.