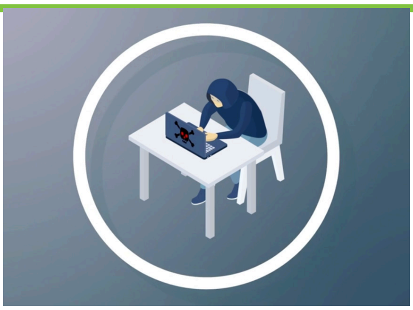
Click Thinking Spotlight

Data Breaches

Data breaches have cost companies billions in losses. With some insights and planning, however, you can prevent your business from adding to this total.

- Simply put, a data breach is the unauthorized access of private digital information. Not all breaches are the same, however.
- Cyberattacks, by far the most publicized data breaches, occur when cybercriminals gain access to a company's network—usually by phishing—to steal sensitive information or deploy ransomware.
- Laptops, smart phones and thumb drives carrying proprietary information can easily lead to a data breach if they end up in the hands of motivated criminals through loss or theft.
- People make mistakes. Employees can fall victim to social engineers who trick them into sharing sensitive information. Or a mis-configured server, application or website could accidentally expose customer data.
- The fact that employees can steal or expose data cannot be overlooked. This growing form of cyber espionage may be motivated by financial, nationalistic or personal reasons such as vengeance.
- How you respond to a data breach will determine its impact. Having a plan ready is critical and starts with a team that can address the breach from a variety of areas, including Information Technology, Risk Management, Communications, Human Resources, Legal Counsel and Senior Management.
- The team may include several employees or a handful who wear many hats, depending on the size of your business. Regardless, members should be experienced in their roles and with the company so they can outline steps to take if a breach occurs.
- IT might be responsible for determining the cause of the breach and the steps to take to prevent re-occurrence. Risk management would work with insurers to cover costs of the breach. Communications would develop messaging for external and internal audiences. Human Resources could roll out training to deter further incidents. Legal could assess if the company is liable or defend it from lawsuits. And Senior Management could provide reassurances to shareholders and board members that the breach has been addressed.
- The goal is to coordinate the team and the response so that data breaches are pre-empted in the future or swiftly mitigated. And to use the knowledge gained to further refine responses.



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

A digital newsletter for Barracuda PhishLine.