يمكن أن تؤدي سرقة بيانات الاعتماد إلى انقطاع كبير في الشركة. تسعى محاولة التصيد الاحتيالي التي تهدف إلى سرقة بيانات الاعتماد إلى حماية هوية المستخدم النهائي من خلال سرقة كلمة المرور. فمن المحتمل أن يكون اللص عبر الإنترنت قد تمكن من الوصول إلى بيانات الشركة السرية للغاية. مما يمنع الوصول إلى الأنظمة والبيانات حتى يتم دفع المكافأة. توقع انقطاعًا كبيرًا في العمل أثناء عمل موظفي تكنولوجيا المعلومات لديك على تحديد برامج الفدية، يتمكن المحتالون من الوصول إلى الملفات ويمكنهم التلاعب بها ومراقبة سلوك المستخدم. يمكن للمهاجمين السيبرانيين سرقة بيانات الشركة المهمة بشكل نشط من خلال الوصول إلى هذه الملفات والتنصت على الحركات الرقمية للموظفين. الهندسة الاجتماعية يمكن أن تؤدي إلى سرقة الأموال. يتم استخدام الموظفين في هجمات الهندسة الاجتماعية مثل التصيد الاحتيالي للوصول إلى البيانات والمعلومات والشبكات وحتى الأموال. قد يتمكن مجرمو الإنترنت من الوصول إلى معلومات الموردين ثم انتحال شخصية هؤلاء الموردين، وتغيير الفواتير بتفاصيل مصرفية "محدثة" على أمل أن تدفع المنظمات الفواتير إلى حسابات إجرامية.