# Tabletop Exercises Package

Use these scenarios to help test the effectiveness your incident response communications plan. Be sure to consider all sides of the situation, evaluate what the characters do, don’t do, and what they could do to improve. After each section, stop and brainstorm ideas about the most effective way to communicate in these situations. Be sure to cover the developments sections with a piece of paper so no information is learned out of turn. Also, remember to consider both internal and external communications and the processes that need to be in place for them to run smoothly.

Note: both these scenarios are fictional. Any similarity to real life events is purely coincidental.

# Scenario 1 – Ransomware

**Background:** Elinor arrives at work on Monday morning at SaaS Co. International. Following her usual morning routine, she checks her email. She opens an email that seems to be from her company’s head office. The email explains that there has been a security breach and that the IT department needs to verify the login credentials for all employees. Elinor is a hardworking employee and takes her role as a management accountant very seriously, so she happily enters her information and sees to it that her colleagues also quickly comply with the email’s request.

In total, five other employees follow Elinor’s lead and respond to the email. Six hours later, Elinor and her co-workers are getting ready to go home for the weekend when something unusual happens. They each receive an official-looking notice that their computers must be restarted, but after rebooting, they each receive a message explaining that their data has been encrypted and that they will need to pay a ransom of 1 Bitcoin before the decryption key will be provided to them. They quickly realize that this is not a joke and that they are unable to access any of the files on their computers.

Elinor decides that it is best to report this incident to management. An hour later, IT arrives to take a look, at management’s request. By this time, however, several others have received the same notice and are now unable to use their computers.

Greg, the head of IT, notifies management that he suspects these computers have been infected with SamSam ransomware and explains he will need some time to investigate further the extent of the damage.

**- Stop -**

**Development 1:** On Monday morning, things have worsened. 60% of all the company’s computers are now infected with ransomware and the phones are no longer working. Also, clients are reporting online services are not working properly and that it is disrupting their business.

**- Stop -**

**Development 2:** It is now Wednesday and the situation is still uncontained. The incident is receiving increased media interest and local news stations have asked several employees for an interview. It is becoming clear that this is a major setback and management is urging IT to resolve the issue quickly and is considering paying the ransom, though local law enforcement has advised against this.

**- Stop -**

**Development 3:** Two weeks later the incident has been contained and remediation efforts are underway. However, some clients are still reporting that they have not yet regained full access to the online services they need to operate their businesses and are angry that the disruption of service is causing them to lose money. The clients also explain that their own customers are becoming very frustrated and are using social media to vent their displeasure, causing reputational damage.

**- Stop -**

**Development 4:** We-R-Here-4-U Inc., one of SaaS Co.’s clients, is now suing for lost profits. The public seems to have sided with We-R-Here-4-U, and the hashtag #payupSaaS has begun circulating on social media.

# Scenario 2 – Data Breach

**Background:** While doing some routine system checks for Super Mega Business Global on a Thursday morning, Hector, the head of IT, notices some unusual activity, and he is beginning to suspect that the company may have been attacked by cybercriminals. After investigating the issue for a few hours, he decides that the situation needs to be escalated, so he reports it to Frida, the company’s CISO. Frida tells him to keep investigating, and to let her know as soon as the incident is confirmed to be an attack. After several more hours of investigation, Hector realizes that the incident is serious. He is able to confirm that an attack took place and that data was stolen, but he is not yet sure how many accounts were affected. Hector reports these details to Frida and advises her that the Security Incident Response Communications Team (SIRCT) should meet and a statement should be drafted and released as soon as possible.

Frida, however, thinks Hector is acting too rashly and tells him to continue the investigation. Hector determines that approximately 1,000 accounts have been breached and some personal data was exposed, but he is not yet sure specifically what data was taken.

**- Stop -**

**Development 1:** As Hector continues his investigation, he learns that the breach resulted in the exposure of clients’ passwords, email addresses, and phone numbers. He reports these new details to the SIRCT via email.

**- Stop -**

**Development 2:** The breach turns out to be bigger than Hector initially thought. It now appears that over 1,700 accounts were affected, with at least 500 also having their payment card information stolen.

**- Stop -**

**Development 3:** Hector learns that there was an unknown security vulnerability that allowed the attackers to steal the data. He also discovers that a faulty encryption protocol was to blame for the exposure of payment card information. It turns out Hector received a warning about this encryption flaw several months ago. While he corrected the flaw for newly created accounts, he forgot to fix the problem for the existing accounts.

**- Stop -**

**Development 4:** The media has taken a keen interest in this story and several employees have been contacted for interviews.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For acceptable use of this template, refer to Info-Tech's [Terms of Use](http://www.infotech.com/terms). These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.