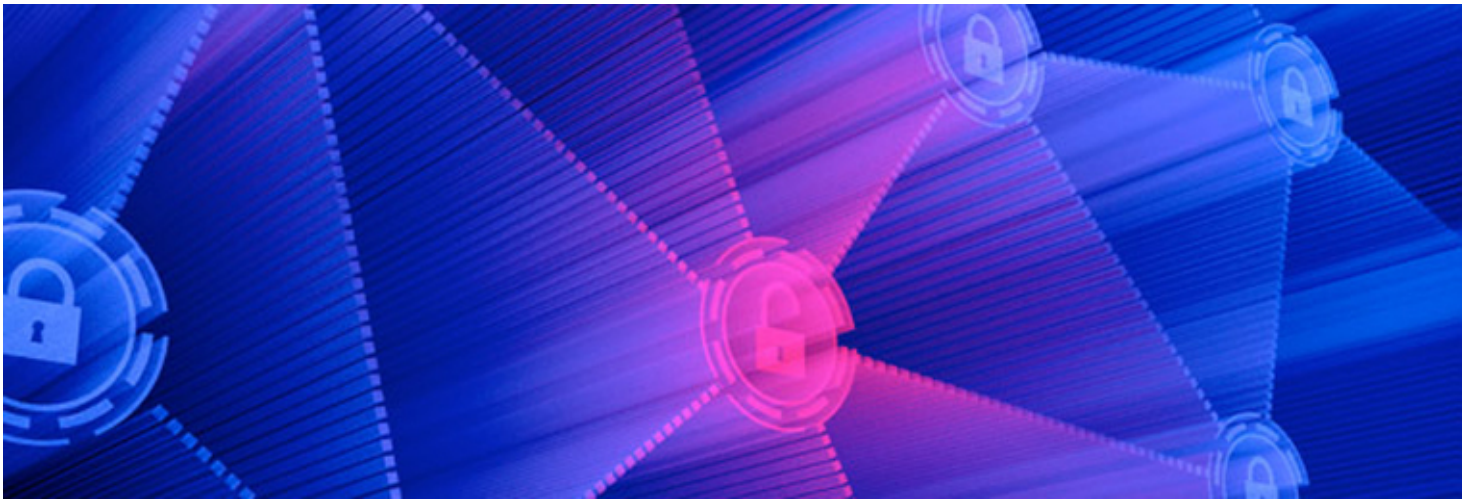

Plan now to use off-band communications during an incident response: key points

Cybersecurity Law Alert

27 OCT 2015
By:

Your company is in crisis mode in the throes of a security incident response (IR). But you are calmly executing your well-honed IR plan − a plan you developed and tested during mock exercises over the past year. You are confident in your team's ability to triage the incident and your technical security experts' ability to stop the attack. You know you will return your company to its fully operational state as soon as possible.

One of the first steps in your IR plan is to convene an IR team meeting. You have an IR team email distribution list at the ready, which saves valuable time. You send a calendar invite to your IR Team for 2:00 – 3:00 PM ET with the conference dial-in number, code, and – because you are prepared – a single-use password just for this call.

Your executive team, IT and Information Security leads and other IR team members convene in your board room and dial in to your conference line from other locations. As you get ready for the meeting, here are some questions to ponder.

Do you mind if the attackers dial in to the conference call too?

If attackers have infiltrated your network, they may have access to company email and other communications methods, including your IR Team crisis response meeting calendar invite and your single-use password.

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome. Copyright © 2022 DLA Piper. All rights reserved.

Do you mind if the attackers launch secondary attacks during the meeting?

If attackers know your best IT/IS staff are in a meeting, they may seize the opportunity to launch a second wave of attacks while your systems are not being monitored closely.

Do you mind if the attackers follow along with your IR Plan playbook?

If attackers have obtained a copy of your IR plan playbook, they will know where you are looking and – perhaps more importantly – where you aren't *looking.*

PREVENT ATTACKERS FROM TRACKING YOUR INCIDENT RESPONSE ACTIVITIES

Attackers may seek to read or listen to IR team and executive team communications to learn about your company's tailored tactical responses, your investigation and your efforts to stop their attack. Reduce the risk that this may happen. A robust IR plan should include communications techniques that operate outside regular company communication methods (so-called "off-band" communications methods). **But do not include off-band communication methods information in your IR plan,** in case attackers get hold of the plan. **Prepare an ancillary document for a very limited team;** do not widely publicize it in your organization or to an entire IR team.

HAVE OFF-BAND COMMUNICATIONS METHODS ON STANDBY

Companies should have off-band communication methods on standby for possible use during an actual or suspected security incident. **Again: do *not* list the off-band email addresses in your IR plan** in case attackers get hold of the plan. **Prepare an ancillary document for a small subset of people;** do not widely publicize it in your organization or to an entire IR team.

SELECT THE RIGHT OFF-BAND COMMUNICATION METHODS IN ADVANCE

Technical security experts who understand your company's regular communication methods should advise you in determining the right off-band communication methods for your company. The examples listed below serve as a guide, but may not necessarily be right for each company. Off-band communication method choices should be both safe and *usable*. An extremely secure communications method is *not* an effective option if it is difficult to activate.

NOT ALL YOUR OFF-BAND COMMUNICATION METHODS ARE NECESSARY IN EVERY INCIDENT

During an actual or suspected security incident, technical security experts should determine which off-band communication methods to use based on the characteristics of the specific security incident at hand. Not all off-band communication methods will be required every time.

CONTINUE USING YOUR REGULAR COMMUNICATION METHODS

Keep using regular communication methods, such as your conventional email and instant messages. This will help you avoid tipping off attackers to the fact that your executives or IR team are using off-band communication methods.

OFF-BAND COMMUNICATION METHODS ARE SUBJECT TO LITIGATION HOLD REQUIREMENTS

As in any situation where litigation is possible, counsel will advise company on litigation hold requirements (i.e., not to destroy potential evidence) according to established protocols. Off-band communications would be subject to the same litigation hold requirements as regular company communication methods.

TYPES OF OFF-BAND COMMUNICATIONS: EMAIL, INTERNET, COMPUTERS, PHONES AND MESSAGING

EMAIL

Attackers may have access to email from a number of vectors, including direct access to email accounts on a company email server, or by having control over computers or other devices on which employees access company email accounts.

- **IR team and executive team members should have non-company email accounts with multi-factor authentication activated.**
  - Many well-regarded free email service providers offer ***two-factor authentication*** at no cost.
  - ***Do not use regular personal email accounts*** - use accounts created solely for this limited purpose and

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome. Copyright © 2022 DLA Piper. All rights reserved.

discontinue use after a major security incident.
    - ***Do not circulate a list of off-band email accounts via company email***. Store copies in a location that attackers are less likely to access (e.g., a hard copy at home).

- **Be cautious** when writing emails.
    - Off-band email communication could still be compromised if attackers have control over computers; always use caution about what you write in emails – this is especially the case for IR team and executive team members. ***Before you click send***, assume the email will be read by an attacker.

- **Even this imperfect solution** significantly decreases company risk during an IR.

INTERNET

Attackers may intercept network traffic via wireless or wired networks.

- **IR team and executive team members (or the company as a whole) should access off-band email accounts other than from regular company wired or wireless Internet access.**
    - Consider MiFi hotspots, a DSL line or mobile phone hotspots that are ***not on regular company ISP service accounts***.
    - Consult with technical security experts about the safest method.
    - Do not use an insecure wireless network at a public location, such as a library or a coffee shop.
    - Assume executives' or IR team members' home networks may also be compromised.

COMPUTERS

Attackers may have compromised your laptops, desktops or other devices in addition to your systems and network. Even if an employee uses off-band email via an off-band Internet connection, if the employee's laptop is compromised an attacker could still potentially monitor the employee's communications on that compromised laptop.

- **IR team and executive team members as well as critical IT and IS staff should have separate hardware (laptops or tablets) that can be used during a security incident and then decommissioned.**
    - Many relatively **low-cost options** exist for purchasing barebones laptops or tablets that can be used to access off-band email via off-band Internet connections.
    - **Don't use this hardware for other purposes** to reduce the likelihood that it could be compromised by attackers.
    - **Store the hardware in a safe place** and bring it out only in the event of a security incident
    - Assume that personal laptops or tablets that were used to access company email, company networks or by the executive team for personal use **may have been compromised**.

PHONES

Attackers may have compromised a company's phone systems and mobile devices.

- **IR team and executive team members should have spare phones that can be used during a security incident**.
    - **Inexpensive non-smart phones** with prepaid service are one solution; also available are well-reputed phone-call apps with encrypted phone call options.
    - **Consult with technical security experts** about the best option for you based on your company's landline phone system and employees' mobile phone devices.

TEXT MESSAGING AND INSTANT MESSAGING

Attackers may have access to messages from a number of vectors, including direct access to a company messaging server, or by having control over mobile phones, computers or other devices on which employees send text messages or instant messages. Consult with technical security experts about these and other communications options.

Find out more about using off-band communication methods to protect your company during security incidents by contacting the author.

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome. Copyright © 2022 DLA Piper. All rights reserved.