Megan Moore
Buff ID: 1014735

Contingency Plan Assignment

RISK MANAGEMENT PLAN # 1

Revision 0 Date: 10/30/2022

Software Asset Name: Social Media profiles – Facebook and Instagram

Risk Description and Consequences:

Threats: Account suspension, password breach, Identity theft, reputation harm. Threat for this software asset is ranked as confidentiality high due to large impact from personal information exposure which includes images, contacts, names, etc; integrity high due to potential reputational damage which could occur both personally and professionally; availability low as I do not share posts to my social media pages every day nor check them every day so daily access is not necessary.
Description: These synced social media profiles were the most important software asset from my personal risk assessment as I determined the reputation damage which could occur from account theft or loss could spread very quickly through my network of contacts and be difficult to combat.
Consequence: Theft of personal identity and reputational damage from posts made with bad intent. Difficulty in repairing relationships depending on situations created from such posts. Critical friend and family exposure of their identities, location, habits, etc.

Mitigation Strategies:

Currently, my mitigation strategies involve the following. To lessen the risk of the vulnerability of my login credentials being stolen by a phish attack or key logging software, I strictly avoid using public computers and open wifi networks found as common areas like coffee houses or cafes. These areas are very public with no control of who utilizes them so refraining from their use is my best method for mitigating the risk. Another step I have currently in place is my phone is notified immediately in the instance of a password change and I must confirm I requested that change. Many social media or other accounts now have 2FA (multifactor authentication) and I have this setup for my accounts as well. While it makes logging in to them more troublesome, I feel the lessened risk is worth the effort.

Contingency Actions and Trip Wires:

Social media is tricky to notice when things are hacked unless immediate bizarre posts begin occurring. The first trigger I have on my accounts is two factor authentication. If my phone is pinged to reset my password, I would immediately know the risk is happening real time and react accordingly to report the attempt to the platforms. If this is somehow bypassed, I would then fall to my backup social profile I have connected with my main accounts. This way I would notice if strange posts occurred or if spam messages requesting funds, etc began. Actions to take upon identification that the risk is happening include notifying immediate friends and family to broadcast a warning message on social media along with contacting both social media platforms to note the profiles have been stolen. In these cases, it is difficult to recover a stolen profile so the best the platform can possibly do is delete the account. If such a step did occur, my plan would be to create new social media profiles and then go through the process of readding all of my contacts. The data from the facebook profile would be lost and unrecoverable however, all posts from the Instagram profile are saved and downloaded to my phone once posted so I at least have those items which I can reload.

Resources needed:

Current mitigation plans do not involve any training. Social media profiles have limited methods for securing access if lost. Phone number and two factor authentication is enabled on both social media accounts. Another resource is my contact list which I also already have saved both on my computer, phone and hard copies.

Megan Moore
Buff ID: 1014735

Contingency Plan Assignment

Notifications:

90% of my contacts currently I am connected with on social media I have their emails, phone numbers, etc. The remainder are inconsequential. Should my social media accounts be lost or hacked/stolen, I would notify a few key individuals who share the same contacts and then they would be able to send out a blast notification on social media highlighting the issue and to avoid communicating with the stolen profiles.

Subject Matter Expert/Person Responsible for implementing plan:

The SME for handling the implementation of the plan would be myself. As these social media accounts are full of my own personal information and connected with the information for many other individuals, the responsibility to implement a backup would fall to myself. While others can be impacted such as friend and family contacts, there is not much they can do except know to reach me by phone to confirm any suspicious activity they may receive via a social media message or post.

Date Plan Must be Ready:

My contact list for notifications is already staged and ready to go. As social media accounts are hacked frequently, this is something myself and my family and close friends all have established already.

Approvals:

The individuals needed to approve of this plan are only myself, with a simply need to know to my spouse so they are aware of our action plan. Should the event occur, I can then reach out to my contacts via other methods (phone, text, social media) to inform them of what to watch for and report. This is already identified in the notifications section.

Megan Moore
Buff ID: 1014735

Contingency Plan Assignment

RISK MANAGEMENT PLAN # 2

Revision 0 Date: 10/30/2022

System Asset Name: Google Email Accounts

Risk Description and Consequences:

Threats: Account suspension, password breach, email account server inaccessible. Threat for this system is ranked as confidentiality high due to large impact to damage if access is exposed; integrity high due to potential reputational damage which could occur both personally and professionally; availability moderate as access can be suspended for a few days before becoming necessary.
Description: This system was the most important asset from my personal risk assessment as I determined it was the weakest as it was capable to exposing me to the greatest amount of risk.
Consequence: Theft of personal identity along with ability to reset passwords to all major financial related accounts and work accounts as my google email accounts are the main methods for how I manage all my personal information, financials, career growth, personal contacts, family affairs, bill payments, etc. My google email accounts are a critical system for my every day tasks as well as crucial responsibilities.

Mitigation Strategies:

Currently, my mitigation strategies involve the following. To lessen the risk of the vulnerability of my login credentials being stolen by a phish attack or key logging software, I strictly avoid using public computers and open wifi networks found as common areas like coffee houses or cafes. These areas are very public with no control of who utilizes them so refraining from their use is my best method for mitigating the risk. Another step I have currently in place is the installation of both tracking software for my devices as well as remote wipe capability. If I was to experience a theft or simply lose a device which can occur either by accident or through damage, I have ways to protect my login credentials for this system.

Contingency Actions and Trip Wires:

I had to truly do a great deal of consideration on what kinds of indicators or trip wires I might be able to establish in order to alert me when the risk is happening. As I check my google email accounts quite frequently throughout the day, if either my computer login or mobile login failed to allow me to access my accounts, this would be the most obvious trip wire that something has happened and I am now locked out. One contingency action I did setup for safety was if or when I change my login password, a notification is auto sent to my google synced accounts. This would be another tip off that my system has been jeopardized. Potentially, my accounts could be recovered at this stage as the notification would ask if I requested the change to my password. In the case of a theft or loss, I would say no I did not request this change and Google has protocols in place to assist when emails have been hacked. For my email accounts, the process I would follow to recover quickly would be to first notify my call tree along with immediately going down my punch list of critical sites which use my emails as the method of login. Also, if my accounts are being accessed from a stolen device, I would activate the location tracking software along with remote wipe capability.

Resources needed:

Training for how to use the tracking software and remote wiping capabilities is completed. Also completed is both my call tree list and the punch list of websites which would need to be accessed one at a time to change the login email account. That list is something I have maintained for a long time already and have hard copies of. Backup email to use as an alternate need to be established. Timeline to research a best option and configure this is about a week. Then once created, another 1-2 weeks to update all software and contacts to recognize the alternate account.

Megan Moore
Buff ID: 1014735

Contingency Plan Assignment

Notifications

Should my email credentials happen to be breached, I maintain an offline saved contact list for all personal and professional individuals, as well as hard copies of accounts should I need to access them. If a breach or theft occurred, I would then send out a massive text notifying my contacts of the incident and to be cautious if receiving anything from my accounts.

Subject Matter Expert/Person Responsible for implementing plan:

The SME for handling the implementation of the plan would be myself. As these email accounts are full of my own personal information and contact information for many other individuals, the responsibility to implement a backup would fall to myself. While others can be impacted such as friend and family contacts, there is not much they can do except know to reach me by phone to confirm any suspicious activity they may receive in email.

Date Plan Must be Ready:

Review of potential backup options for email systems should my accounts be stolen or go through a period of being unable to use is immediate, so before the end of the year or as soon as possible. In the next week, location tracking software should be installed along with remote wiping capabilities on all devices where these accounts are used. While this only protects my accounts should a physical theft of a phone or laptop with my credentials signed in occur, this is a very important step. The training necessary for these software programs to be configured correctly should take a few days by researching online forums and reviewing Youtube videos. Long term would be reviewing a best potential backup email account which can be added as backup to all important financial accounts. Training involved for this would be research of online options available and the staging for this backup plan could take a few weeks. Once the backup account is determined and established, then each individual financial account would need to be accessed and have the new backup account added as a method for account recovery.

Approvals

The individuals needed to approve of this plan are only myself, with a simply need to know to my spouse so they are aware of our action plan. Should the event occur, I can then reach out to my contacts via other methods (phone, text, social media) to inform them of what to watch for and report. This is already identified in the notifications section.