***Scenario 1: Permit all office workers/employees to work from home -> Kaleb Alstott***

**Security Risks Involved in Working from Home**

**Risk Management Plan Part**

**Risk Identification**

* Accessing Sensitive Data Through Unsafe Wi-Fi Networks
* Using personal devices for work
* Ignoring Basic Physical Security Practices in Public Places
* Using Weak Passwords
* Email Scams
* Security Controls Are Weaker
* Cyberattacks on Remote-working Infrastructure (specifically DDoS attacks)

**Risk Assessment Plan Components**

|  |  |  |  |
| --- | --- | --- | --- |
| **Risks, Threats, and Vulnerabilities** | **Probability of Occurrence Annually** | **Risk Impact Level** | **Risk Importance Rank**  **(1 Least Worry – 10 High Importance)** |
| **Sensitive Data Through Unsafe Wi-Fi Networks** | **65%** | **Critical** | **9** |
| **Using personal devices for work** | **20%** | **Low** | **2** |
| **Ignoring Basic Physical Security Practices** | **25%** | **High** | **7** |
| **Using Weak Passwords** | **30%** | **High** | **7** |
| **Email Scams** | **20%** | **Medium** | **6** |
| **Weak security Controls** | **20%** | **Medium** | **5** |
| **Cyberattacks** | **70%** | **Critical** | **10** |

**Control threats**

* Accessing Sensitive Data Through Unsafe Wi-Fi Networks
  + Control: Increase Wi-Fi security by Wi-Fi encryption, sophisticated passwords for Wi-Fi, encryption of data, Wi-Fi router firmware, VPN, firewalls, etc.
* Using personal devices for work
  + Control: Company provides correct work equipment such as a laptop
* Ignoring Basic Physical Security Practices in Public Places
  + Control: Enforce the use of VPN, antivirus software, securing home Wi-Fi, firewalls, better passwords, etc.
* Using Weak Passwords
  + Control: Make sure to use at least a 12-character password along with a mixture of at least one capital letter, number, symbol, and lowercase letter
* Email Scams
  + Antivirus security controls, training from company on how to spot phishing scams, anti-phishing software, firewalls, think before you click.
* Security Controls Are Weaker
  + Control: Provide multifactor authentication, password management, a strong endpoint detection and response, firewalls, etc.
* Cyberattacks on Remote-working Infrastructure (specifically DDoS attacks)
  + Increased router and fire wall protection, an intrusion detection system, DDoS mitigation appliances (third party), possible hybrid or cloud based services.

**Risk Mitigation Slide**

|  |  |  |
| --- | --- | --- |
| **Risk** | **Mitigation Type** | **Mitigation Plan** |
| **Accessing sensitive data through unsafe Wi-Fi networks** | Mitigate | 1. First we are going to implement Wi-Fi encryption along with a sophisticated password that follows our password security protocol  2. Second, we are going to implement a VPN with firewall protection along with Wi-Fi router firmware  3. Lastly, we are going to make sure our data is encrypted when sending it to at home workers especially with sensitive data. |
| **Using personal devices for work** | Mitigate | 1. Company will provide a working laptop for at home employees that will have antivirus software on it as well as implemented company security protocols necessary. |
| **Ignoring Basic Physical Security Practices in Public Places** | Mitigate | 1. Enforce the use of physical security such as a VPN along with a firewall.  2. Security password protocol to enforce better passwords.  3. Implementing antivirus software  4. Securing home Wi-Fi with encryptions, passwords, router firmware  5. If basic physical securities are not being met, possible suspension/termination depending on frequency and exposure. |
| **Using Weak Passwords** | Mitigate | 1. Use at least a 12-character password along with a mixture of at least one capital letter, number, symbol, and lowercase letter.  2. Password management  3. Cannot reuse past passwords along with new passwords every 3 months that cannot be repeatable. |
| **Email Scams** | Mitigate | 1. Antivirus security controls along with anti-phishing software  2. Training from company on how to spot phishing scams, anti-phishing software,  3. Think before you click technique  4. Is it a trusted source or verified |
| **Weaker Security Controls** | Mitigate | 1. Provide multifactor authentication  2. Password security protocols along with password management  3. A strong endpoint detection and response  4. VPNs along with firewalls  5. Wi-Fi encryption to secure personal Wi-Fi |
| **Cyberattacks (DDoS mainly)** | Third Party | 1. Third party DDoS mitigation/security appliances  2. Preferably cloud-based services, if not hybrid at the least  3. Intrusion detection system |

**BIA slide**

|  |  |  |
| --- | --- | --- |
| **CBFs** | **MAO** | **Impact Level**  **(Low, Medium, High)** |
| **Desktop Computer** | 24 Hours | High |
| **Wi-Fi** | 24 Hours | High |
| **Firewalls** | 36 Hours | Medium |
| **VPN** | 36 Hours | Low |

|  |  |
| --- | --- |
| **Systems/Functions** | **Recovery Time Objective (RTO)** |
| **Internet Connection** | 6 hours |
| **Company Equipment such as desktop computers, phone, printer, etc.** | 5 Hours |
| **Password Protection/Protocols** | 24 Hours |
| **File Sharing Abilities** | 12 Hours |
| **Network Connectivity** | 7-8 Hours |
| **Antivirus Software** | 8 Hours |

**BCP Slide**

**Cover the 3 phases of**

**Plan Training, Testing, and Exercising**

Lastly, in this phase of the operation we have ultimately recovered from disaster and this phase would typically take place before a disaster would occur. To start off, all BCP need to be tested to find possible flaws or loops in the system. In this step we would set up exercises to test out our possible plan. A possible exercise that we could implement is possibly having employers work from home for a day to test our systems and how we would possibly hold up if a snowstorm were to happen. We have three main goals in this step which are

* Training—Teaching people details about the BCP
* Testing—Verifying that the BCP will work as planned
* Exercises—Demonstrating how the BCP will work

We have covered how we will test and what type of exercises we would do to be prepared for our BCP but lastly, we need to touch on the training for the BCP. Our training would look like how you would connect from an at home work station, when to stay home vs. come into work, how to connect to the companies VPN, and overall preparation for what to come.

**References**

[**https://heimdalsecurity.com/blog/cybersecurity-issues-with-remote-work/**](https://heimdalsecurity.com/blog/cybersecurity-issues-with-remote-work/)

[**https://mint.intuit.com/blog/early-career/pros-and-cons-of-working-from-home/**](https://mint.intuit.com/blog/early-career/pros-and-cons-of-working-from-home/)

[**https://usa.kaspersky.com/resource-center/threats/remote-working-how-to-stay-safe**](https://usa.kaspersky.com/resource-center/threats/remote-working-how-to-stay-safe)

[**https://www.digicert.com/blog/8-steps-stronger-wifi-security**](https://www.digicert.com/blog/8-steps-stronger-wifi-security)

[**https://www.phishing.org/10-ways-to-avoid-phishing-scams**](https://www.phishing.org/10-ways-to-avoid-phishing-scams)

[**https://cloudsecurityalliance.org/blog/2021/06/04/7-simple-but-effective-tactics-to-protect-your-website-against-ddos-attacks-in-2021/**](https://cloudsecurityalliance.org/blog/2021/06/04/7-simple-but-effective-tactics-to-protect-your-website-against-ddos-attacks-in-2021/)