Business Risk Review

16 Jun 2021

Prepared For

AnyDesk

Prepared By

msp

EXECUTIVE SUMMARY

Background

This Business Risk Review summarizes the risk posture of AnyDesk, located at Alabama, United States, 555555. It is based on an evaluation of AnyDesk’s culture through the dissemination of the leadership’s position on security, and their expectations of its’ execution and performance. The Business Risk Review is a measure of the efficacy of its’ implementation, which is a determinant in AnyDesk’s CRIS (Cyber Risk Index ScoreTM) rating and will present itself as a Business Vulnerability Index (BVI) score.

CRIS is an accurate assessment of risk when all areas of AnyDesk’s business are made available and visible to our security team through the tools provided. The implementation of all the tools that measure business risk at the cultural, human, and technological layers provide the most accurate, effective, actionable measure of risk. Where tools were not otherwise available, that is denoted below and observed industry norms are used instead of actual outcomes.

The methodology that was used to perform some or all aspects of this business risk assessment was based on risk assessment concepts and processes described in relevant sections of NIST SP 800. An overview of the elements of the Business Risk Review assessment process is defined below:

ELEMENT	MEASURES
1	Risk Assessment (RA)
2	Policy Acknowledgement & Compliance (PAC)
3	End-User Training (EUT)
4	Phishing Defense & Resiliency (PDR)
5	Dark Web; Compromised & Exposed Credentials (CEC)

SUMMARY OF FINDINGS

A Business Vulnerability Index (BVI) Score weighs all elements of risk that bear on the cultural, human, and technological aspects of the organization. None of these can mitigate risk in isolation; when used concert with each other they raise the defensive posture of the organization such that the overall risk to AnyDesk is significantly lowered as the defensive fabric of the organization is interwoven together to mitigate risk. This defense-in-depth strategy achieves significantly lower levels of risk as the attack surface shrinks and threat vectors cannot penetrate the more secure organization. If just one of these elements are missing, overall risk rises precipitously due to the butterfly effect that an unprotected, interconnected element has on the organization.

Business Vulnerability Index (BVI) Score

ASSESSMENT	TRAINING
🟥	🟨
COMPLIANCE	RESILIENCE
🟥	🟩
BUSINESS VULNERABILITY INDEX	
692	

SCOPE

General Areas of Focus

1. Cultural Safeguards - An assessment of the policies and procedures that are in place to define how stakeholders interact with the AnyDesk, and what recourse both AnyDesk and its' stakeholders have. AnyDesk policies and procedures should exhibit a deference to Controlled Unclassified Information (CUI) such as, personally identifiable information, non-public information, trade secrets, financial information, copywrites and/or trademarks, inventions, business processes, etc. A comprehensive Risk Assessment uncovers both the existing state of the risk posture of AnyDesk, as well as the best opportunities to increase the company's resilience

    a. Policy and Procedure - A company's culture is conveyed through its policies and procedures and manifests itself through the adherence to them by the organizations team. The greater the compliance the more secure the organization.

2. **Technical Safeguards** - an assessment of the technology and related policies and procedures that are in place to protect CUI, and control access to it; together these are called controls. Proper controls help to shrink the attack surface and extend the protective layer over the organization. Controls should be appropriate as to effectiveness and the ability of the organization to implement and monitor.

    a. **Structural Protection** - How systems and people interact are defined by the structural controls put in place systemically. From Organizational Units to Security Groups, Access Controls to Password Policies, structure matters and can enforce a defined security posture that is predictable and scalable.

    b. **Malware Protection** – Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network. A wide variety of malware types exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, and scareware.

       Mimecast, a leader in email- based malware research refers to phishing protection as "security measures that companies can take to prevent phishing attacks on their employees… Attackers contact targets through email that is disguised to appear as if it is from a trusted source or a legitimate company. By convincing targets that there is a problem of some kind they must remedy quickly, attackers get users to click on a link that directs them to a fraudulent website where their sensitive information is captured and where malware may be downloaded to their computer."

       After training, malware protection like anti-virus or next-generation anti-ransomware, together anti-malware provides that second vital layer of protection for your computer or network. A robust anti-malware package is a core component of the technological defensive fabric of an organization.

       Well-designed anti-malware protection has several characteristics. It checks any newly downloaded program to ensure that it is malware-free. It periodically scans the computer to detect and defeat any malware that might have slipped through. It is regularly, and automatically updated to recognize the latest threats.

    c. **Perimeter Protection** – Perimeter appliances provide an initial line-of-defense that helps to both mask your presence on the internet as well as deny and defend against intrusions when that presence cannot or should not be masked.

    d. **Physical Security** – Ensuring that systems containing CUI are properly secured will lower the overall risk of a data breach. Systems include servers, desktops, laptops, portable media, etc. Wherever possible, these systems containing CUI should be placed in a secure location and/or properly secured, physically and technically. Access to the secure location should be restricted to workforce members that require access to perform their job function.

       Amongst the physical security measures, the security of portable media is of paramount importance – portable media constitutes a significant majority of all breaches involving malicious and/or careless actors with physical access.

       Portable media includes any device or media that can be easily transported including laptops, smartphones, USB drives, flash drives, portable backup devices and media, etc. It is critical that special attention be focused on protecting CUI on portable media. Wherever possible, limit or prevent the use of portable media. When preventing their use is not possible, the following guidance should be considered.

        i. **Minimize the amount of CUI** – if portable media must be used for transporting CUI then it is important to restrict the amount of CUI on portable media to the minimal needed to perform a function or task.

    ii. **Limit access** – it is important to limit who can copy CUI to portable media. It is also important to ensure that prior approval has been granted before CUI can be copied onto portable media.

    iii. **Track portable media** – ensure that a procedure is in place that tracks all portable media containing CUI that enters or leaves the organization.

    iv. **Encrypt core CUI repositories** – ensure that proper encryption is utilized to protect CUI sored in repositories. Ensure that all repositories are identified and tracked.

    v. **Encrypt portable media** – ensure that proper encryption is utilized to protect CUI on portable media. Ensure that portable media is not removed from an organization unless the CUI is encrypted

3. **Human Safeguards** – more than 99% of attacks and risk require human interaction to facilitate its' success. Therefore, the intersection of the AnyDesk and its' people pose the single biggest risk to the organization. Key elements of human safeguards are training and follow through.

   A robust training program with oversight and inspection will dramatically shrink the risk surface. the following guidance on training should be considered:

   a. **Workforce Training** – it is important to ensure that the workforce is properly trained to identify and therefore protect CUI. A properly trained workforce serves as a first, best line of defense against a breach and theft or destruction of CUI, and significantly lower the risk of a successful data breach. Proper training includes:

      i. **Formal Training** –each member of the workforce receives formal training on how to protect and secure CUI, and successful completion is monitored and audited.

      ii. **Regular Security Refreshers** – each member of the workforce who passed training should receive regular, routine "refreshers"; refreshers are micro trainings typically lasting 30-90 seconds and are designed to keep security and the contours of a breach top of mind. Such best practices are paramount for ensuring the protection of CUI. Security Refreshers may include best-practices for securing and protecting CUI, distribution of headlines that spotlight current threats, zero-day or critical software patches that need to be applied, policy updates that address new-found risks in the organizations' security posture, process changes that alter the flow of information, etc.

      iii. **Phishing Protection** – Social engineering constitute the biggest threat to an organization and Phishing is the single largest form of social engineering designed to attack any organization. Phishing is a form of cybercrime where attackers dupe targets into revealing sensitive data: bank account numbers, credit card information, login credentials, Social Security numbers and other personally identifiable information.

4. **Cyber Insurance** – some threats and risks to organizations cannot be mitigated to zero (i.e., Tornado destroying an office). Even organizations that implement strong security policies could run the risk of a data breach. Some data breaches occur due to employee misconduct (intentional or unintentional), computer viruses, phishing scams, etc. Breaches or loss of CUI can be costly due to remediation and recovery services including information technology, forensics, legal, credit monitoring, reporting requirements and possible regulatory fines. Cyber, Errors and Omissions, Property and Casualty and other business insurance can offset the expenses of CUI related risks that materialize.

   CGPartner - Demo works with dozens of insurance agencies, brokers, wholesalers, and companies. If you need or would like to speak with someone about this, please ask your client advocate and we'll be happy to make an introduction.

RISK ASSESSMENT

Background

Pursuant to a request by CGPartner - Demo monitors the ongoing use and effectiveness of security tools we have implemented to ensure the security posture of AnyDesk remains vigilant and effective. The goal of these efforts are to mitigate the risks facing AnyDesk by ensuring the tools we employ support that goal and enlist the organizations stakeholders to be core elements in the defensive fabric of AnyDesk.

Summary of Outcomes

Security Risk Score			
🟨 IDENTIFY		🟨 PROTECT	
🟨 I1	🟨 I2	🟩 P1	🟨 P2
🟨 I3	🟨 I4	🟨 P3	🟨 P4
🟩 I5	🟨 I6	🟩 P5	🟩 P6
🟨 DETECT		🟦 SCORE	
🟨 D1	🟨 D2	**D-**	
🟥 D3	🟥 D4		
🟩 D5	🟨 D6		

EMPLOYEE TRAINING

Background

A security training program was approved by and created for AnyDesk to raise awareness of the threat landscape and its' impact on AnyDesk. The purpose of the program is to increase the overall security posture of the organization by increasing the awareness level of its employees, thereby enlisting them in the defensive fabric of the company.

Awareness training programs are the cornerstone of a secure organization. Aside from being a component of responsible corporate governance and good stewardship of their stakeholders personally identifiable information, confidential information and private information, together Controlled Unclassified Information (CUI), a lack of awareness training is increasingly being used by insurance companies to deny claims and by enforcement agencies to assign liability and levy fines.

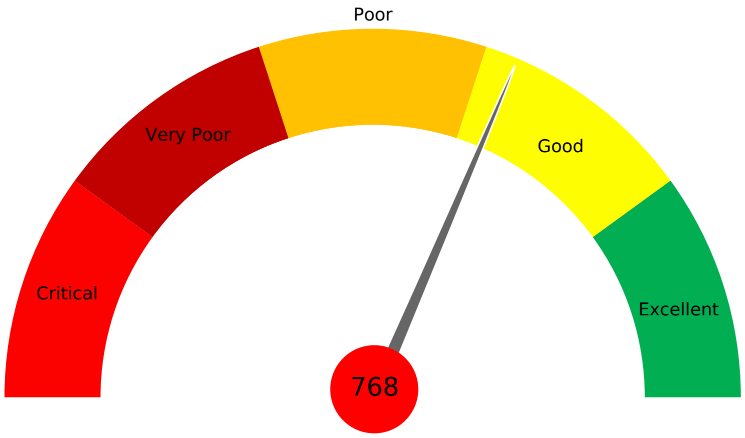
Nearly all studies shows that properly trained employees can recognize significantly more threats than their untrained counterparts. And when they do recognize a threat there is an 80+% drop in successful attacks such as ransomware, malware, and theft.

The risk-reward ratio of a robust training program is undeniable and demonstrates that an on-going training program is a proven vaccine against the threats that exist and will significantly reduce the risk to AnyDesk.

The methodology that was used to develop and employ this training program was based on risk mitigation training guidelines described in NIST SP 800-16 and referenced in the Cybersecurity Maturity Model for Compliance.

Employee Vulnerability Index (EVI)

Due to the significance of employee training on the total risk posture of AnyDesk, AnyDesk evaluated the employees' participation in the program at both a macro and micro level. The employee's participation rates, and test results inform their Employee Vulnerability Index (EVI); the measure of risk they pose to AnyDesk.



POLICY COMPLIANCE

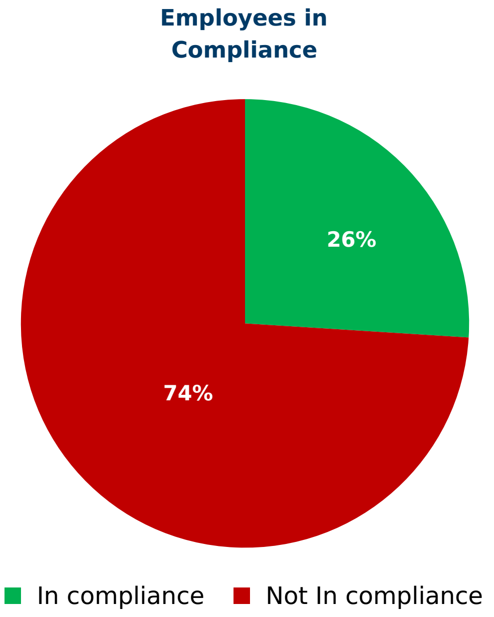
Background

Organizations disseminate their desired security posture through the policies it requires the employee to read, understand and follow. These policies define the behaviors that employees are expected to evince by outlining the company’s expectations and tolerances. Therefore, policies define an organizations culture and are the foundation of the employer-employee relationship.

Using AnyDesk’s robust, comprehensive policy management system, AnyDesk is able to monitor and follow up on each employee’s performance in reading and attesting to compliance with the policies set forth by AnyDesk.

Employee Compliance

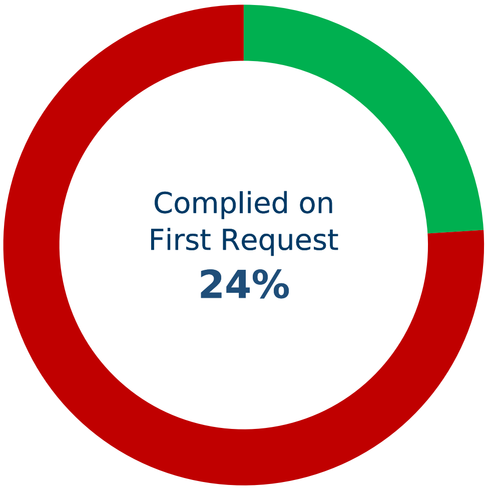
26% of AnyDesk's employees have attested to having read, understood and agreed to comply with the policies assigned to them by AnyDesk management. It took an average of **1.6** reminders to ensure compliance. There are **27** employees who have not even reviewed their policies.



Attesting to All Policies	10
Not Attesting to All Policies	1
Not Reviewed Any Policies	27
Total Reminders Sent	801

21

Average Number of Reminders Sent



PHISHING DEFENSE

Background

A simulated phishing attack both identifies employees who are “aware” and are vigilant, as well as helps the leadership to identify individuals who are not well versed with good security practices and in need of additional training or who may present a significant risk.

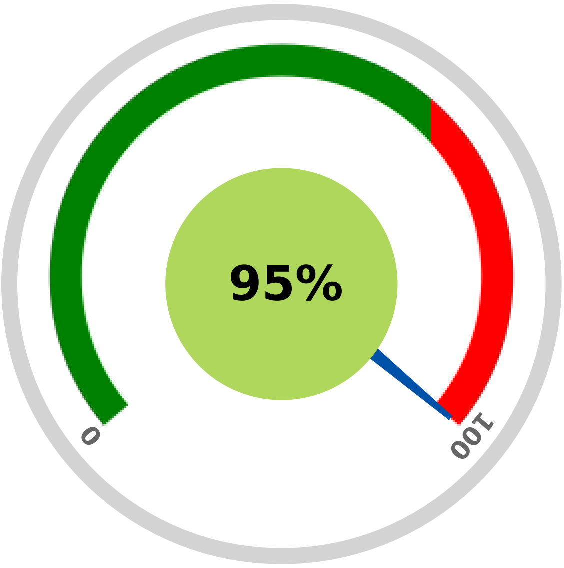
Using AnyDesk’s state-of-the-art simulated phishing, AnyDesk can measure the effectiveness of awareness training concerning social engineering attacks.

Summary of Phishing Simulations

66.67% of AnyDesk users fell victim to the simulated phishing campaigns AnyDesk launched between 04/02/2021 and 07/02/2021.

More than 91% of all successful cyber attacks are caused by the people we employ. The risk to AnyDesk can be substantially reduced by increasing employee resiliency to reduce AnyDesk’s Vulnerability Index

Vulnerability Index



DARK WEB COMPROMISED CREDENTIALS

Background

Dark Web Monitoring reduces the amount of time between the occurrence of a data breach and AnyDesk ’s ability to find out and make preventative moves to mitigate risk before the bad actors find and target AnyDesk.

Knowing about a compromise significantly shrinks the window of opportunity cyber criminals have to make copies of your data and sell it, and prevents the threat of AnyDesks confidential and private information from being exfiltrated (leaving your perimeter) without anyone knowing its gone until its too late.

Summary of Dark Web Exposures

33% of AnyDesk users fell victim to social engineering attacks by malicious attackers or otherwise used their business credentials (user names and/or passwords) on non-business related websites and forums. Some **75%** of the credentials exposed pose significant risk to AnyDesk

Of the compromises found, there were **4** verified breaches representing **0** total exposures and **0** of PII found.

Risk Rating