Safely Working Remote

MTI | March 2020

Our Goals Today

- Discuss the immediate technology and security challenges remote workers present.
- Talk about cybersecurity frameworks along with a holistic approach to security.
- Look at what needs to be done ASAP to prepare for the transition securely.
- Discuss advanced security policies and proactive defense measures.
- Show why every company needs contingency planning, not just disaster recovery!
- Quickly review the critical technology you should be running right now!

The Major Issues with Remote Workforces in a National Emergency

- Infrastructure throughout the country is starting to be taxed heavily which could cause connectivity issues.
- Collaborative platforms like Zoom, conferences bridges, etc. are being overrun at the moment.
- You cannot control the internet bandwidth of your employee's home connections.
- Your office's internet connection and bandwidth may be fine when everyone is in the office but switching everyone to remote could overwhelm your office internet connection.
- Hackers are ramping up the targeting of home workers due to lack of security.
- Your office infrastructure may be older or out of date and now more exposed to the internet.
- If IT is home as well then no one may be monitoring the infrastructure for attack.
- There are legal gray areas when installing company issued software into a home computer.
- Poor security choices are made by panicked or stressed IT personnel such as opening up Microsoft Remote Desktop, etc.

Understanding Cybersecurity Concepts and Frameworks

- The C.I.A. is your best friend! Here's why:
  - Confidentiality – preserving authorized restrictions on access and disclosure, which includes means for protecting personal privacy and confidential data.
  - Integrity – guarding against improper data modification or destruction and ensuring data accuracy and authenticity.
  - Availability – ensuring timely and reliable access to the confidential data.
- THE GOAL HERE IS TO FOCUS ON AND PROTECT THE DATA!
- We execute the C.I.A. through the Safeguards Method.
- The Safeguards, or Controls, are designed to look at an organization holistically from three primary aspects:
  - Technical – the technology, and its policies and procedures for its use, that is in place to defend confidential data as well as to control access to it.
  - Physical – the physical measures, as well as the policies and procedures, used to protect confidential data from the unauthorized physical access and also protection from natural and environment hazards.
  - Administrative – the maintenance, policies and procedures with regard to the security measures that protect confidential data.

Knocking Out 95% of It – Cybersecurity Framework

- Understanding the concept of data security via C.I.A. and the practical knowledge of how to safeguard it we can now build a framework!
- The most universally used Cybersecurity Framework is NIST.
- NIST, while US based, is accepted worldwide by corporations and other governments as a model for Cyberdefense.
- Other major frameworks like PCI DSS, ISO, DFARS and CIS are at least partially, or fully, based on NIST's fundamentals.

Advanced Security Policies & Proactive Defense

Firewalls

- An Enterprise level firewall has the following critical features:
  - Unified Threat Management (UTM)
  - Zero Day Updating with Sandboxing for known threats
  - Coverage for mobile devices (VPN)
  - Application Whitelisting
  - SSL Traffic Decryption
  - Microsoft Login integration
- DO NOT CHEAP OUT ON THIS!!

Next Generation Antivirus

- An Enterprise level antivirus solution has the following critical features:
  - Utilizes Machine or Deep Learning Artificial Intelligence for threat detection.
  - Has centralized management that is monitored continuously for threats.
  - Can act as a self-remediation tool in case of outbreak.
  - Will cut off the infected computer from remote access or the network in case of infection.

Spam Filters

- An Enterprise level antivirus solution has the following critical features:
  - Cloud based spam filtering is superior to in-house or software on the computer.
  - Zero Day outbreak defense like the next generation firewall.
  - Filters not just attachments but also links and URLs.
  - Has a Continuity of Service feature to ensure uptime.

Identity Management

- Digital Identity is a lot broader than you may realize! Categories for this include:
  - User or person's identity within the network
  - An organization (inside or outside) the network
  - An application (inside or outside) the network
  - A device within the network
  - Basically anything with a "set of attributes related to an entity"
  - Your company's default Microsoft login is only one good tool in the arsenal.
- These solutions offer Single Sign-On (SSO) capabilities with threat detection (critical!)
- Identities need to be verified by multi-factor authentication, no exceptions!

Your Existing Network

Contingency Planning (Not Just Disaster Recovery!)

- Disaster Recovery is absolutely needed, but part of a greater contingency plan as its usually focused on the technical solution.
- The goal of a Contingency Plan is:
  - Establish a Communication System for during and after the disaster.
  - Create Recovery and Response thresholds with priorities.
  - Define the Roles and Responsibilities of key employees.
  - Create a scenario format for the type of disaster (earthquake versus hacking, etc.).
  - Execute the Disaster Recovery Plan to restore operations.
  - Perform an Impact Analysis to quantify the disaster (ideally in hard dollars!).
  - Document the disaster, its recovery and improvements needed!

Advanced Security Policies

- Enforce good password policies!
- Enable 2FA/MFA wherever possible (desktop logins, websites, everything possible!).
- Limit access through logon hour restrictions.
- Limit access to critical computer functions like Control Panels, application install/remove features and more.
- Limit access to needless data removal methods like USB drives, Dropbox, etc.!

Proactive Defense Measures

- Use and enforce a monitored patch management system like a Remote Managed Monitoring (RMM).
- Live monitoring critical infrastructure with a Security Information & Events Management (SIEM) system.
- Review configurations and products for existing defenses like firewalls and antivirus.
- Schedule and perform periodic penetration testing to ensure your defenses remain hardened (usually quarterly for this unless you're massive!).
- Monitor the Dark Web as a "canary in the coalmine" for data exposure.

Improvement Planning

- Improvement planning is not only for recovering from a disaster!
- Your company should have a quarterly and annual improvement plan that is no more than two years in total.
- Perform a Cybersecurity assessment based on a Cybersecurity Framework like NIST.
- Set a proper and accurate budget.
- Understand how your cybersecurity improvements help your company achieve its vision (beyond critical)!!

Quick Tech Review: Foundational Technology

- The Critical Components for Remote Cyberdefense
  1. Next Generation Firewalls
  2. Next Generation Antivirus
  3. Enterprise Level switches and wireless access points
  4. 24/7 SIEM/SOC Monitoring for all of the above

5. Encryption systems (at rest and in transit)
6. Advanced Identity Management for SSO & MFA
7. Awareness and Training Programs

- What this doesn't cover is everything beyond the technical solution such as asset management, policies, processes, etc.

The Immediate Steps You Need to Take for a Remote Workforce

- IT should calculate the bandwidth needs of a remote workforce as they connect to the office to gain access to databases etc. and the execute on bandwidth and infrastructure changes to increase capacity as needed.
- ALL infrastructure needs to be updated to current and reviewed for security vulnerability.
- ALL software needs to be updated and checked as well.
- The right remote access strategy needs to be determined for your business (Migrate to cloud, VPN to the office, remote access software like LogMeIn, etc.).
- Reconfiguration of the office network to limit remote users from gaining full access to the internal network (if possible).

About Nick Espinosa

An expert in cybersecurity and network infrastructure, Nick Espinosa has consulted with clients ranging from the small business owners up to Fortune 100 level companies. Since the age of 9 he's been on a first name basis with technology, building computers and programming in multiple languages. Nick founded Windy City Networks, Inc at 19 and joined forces in 2013 with BSSi2. In 2015 Security Fanatics, a Cybersecurity/Cyberwarfare outfit dedicated to designing custom Cyberdefense strategies for medium to enterprise corporations, was launched.

Regular columnist, member of the Forbes Technology Council, on the Board of Advisors for both Roosevelt University's Center for Cyber and Information Security as well as Bits N' Bytes Cybersecurity Education, award winning co-author of a bestselling book, TEDx Speaker and host of The Deep Dive nationally syndicated radio show, Nick is known as an industry thought leader and sought after for his advice on the future of technology and how it will impact every day businesses and consumers. Nick is an accomplished speaker and regularly speaks to audiences about Cybersecurity, technology and business management.

Keep Up with the latest in Cybersecurity at:

https://twitter.com/NickAEsp
f https://www.facebook.com/NickAEsp
in https://www.linkedin.com/in/nickespinosa

The Deep Dive Radio Show episodes: https://soundcloud.com/infosecgurus
Forbes Tech Council articles: https://www.forbes.com/sites/forbestechcouncil/people/nickespinosa1/
Smerconish.com articles: https://www.smerconish.com/news?author=5c735e4ce79c704c50cb9dbf