CYBER RESILIENCE - STRONG CYBER FUNDAMENTALS

SAME

2020-05-13

A Passion to Protect

THE "MAGIC BULLET!"

- I've reviewed and worked with most of the national and international specifications on the classified side and on the unclassified side and I've built some of the most demanding high-performance, high-security systems in our country
- What it all boils down to is starting with fundamental security basics, understanding performance needs and working from there
- People focus on compliance and if they miss dotting an "i" or crossing a "t" they fail compliance audits
- They also fail to secure their systems – we believe in building security into IT resulting in a new reality – "Secured-IT"
- No matter which specification you're trying to comply to, the magic bullet is to focus on five points, build a strong security foundation, and go from there – you can afford to do this!!!

SSO's Five-Point Security Framework©

Five Elements

- Hardware
- Software
- Data
- Credentials
- Staff

Five Aspects

- Inventory
- Governance
- Security
- Budget
- Iterate

FIVE-POINT SECURITY FRAMEWORK © MATRIX

	Inventory	Policy	Budget	Security	Iterate
HW	HW-INV	HW-PLCY	HW-$$	HW-Lock	HW-CHK
SW	SW-INV	SW-PLCY	SW-$$	SW-Lock	SW-CHK
PW	PW-INV	PW-PLCY	PW-$$	PW-Lock	PW-CHK
Data	Data-INV	Data-PLCY	Data-$$	Data-Lock	Data-CHK
Staff	Staff-INV	Staff-PLCY	Staff-$$	Staff-Lock	Staff-CHK

Understand / Establish the Matrix

START WITH FUNDAMENTAL QUESTIONS

- DO YOU KNOW WHAT IT YOU HAVE IN YOUR COMPANY WITH A TRUE INVENTORY?
- DO YOU HAVE A POLICY IN PLACE TO GOVERN WHAT YOU HAVE, HOW IT'S USED, MANDATORY REQUIREMENTS ON HOW TO PROTECT IT, ETC.?
- DO YOU HAVE A BUDGET, A TRUE BUDGET, TO ADDRESS YOUR SECURED-IT NEEDS FOR THIS CATEGORY?
- NOW THAT YOU HAVE A GOOD INVENTORY OF WHAT YOU HAVE, A POLICY ON HOW TO PROTECT IT, AND A BUDGET IN PLACE, HAVE YOU USED THAT BUDGET TO IMPLEMENT THE NECESSARY SECURITY TO PROTECT IT?
- THINGS CHANGE – ALMOST ALL SECURITY SPECIFICATIONS REQUIRE YOU TO ITERATE (PERIODICALLY CHECK) TO MAKE SURE EVERYTHING IS STILL OK AND TAKE APPROPRIATE MEASURES TO RESOLVE ISSUES WHEN THEY ARE DISCOVERED

HARDWARE INVENTORY

- START WITH THE BASICS – DO YOU KNOW WHAT HARDWARE YOU HAVE THAT IS USED TO PERFORM BUSINESS FUNCTIONS? – ALL OF IT?
- IF YOU DON'T KNOW WHAT YOU HAVE, YOU CAN'T PROTECT IT
- WE START WITH SOME OF THE SIMPLE CONCEPTS:
  - DO YOU HAVE A PASSIVE HW INVENTORY?
    (EXCEL SHEET WITH REQUISITE INFO)
  - DO YOU HAVE AN ACTIVE HW INVENTORY?
    (COLLECTS AND STORES INFORMATION ON THE FLY)
  - DO YOU HAVE A PROACTIVE HW INVENTORY?
    (DETECTS NEW DEVICES AS THEY ATTACH TO YOUR NETWORK, COMPARES TO YOUR INVENTORY AND ADDS IF AUTHORIZED, FLAGS IF NOT AUTHORIZED)
- WHAT INFO DO YOU COLLECT?
  - COMPUTER NAME, MAC ADDRESS, MAKE AND MODEL, CATEGORY (LAPTOP, DESKTOP, SERVER, CORP PHONE, BYOD PHONE, NETWORK SWITCH, FIREWALL, ETC.)

Software Inventory

- Now that you know what Hardware you have do you know what Software is running on the Hardware?
- If you don't know what Software is authorized to run on it, how will you know if Unauthorized software is running on it?
  - How will you know if unlicensed software is running on it?
  - How will you know if Malware is running on it?
- This is a primary fundamental of cyber security to develop Secured-IT in your company
  - Do you have a passive SW inventory?
  - Do you have an active SW inventory?
  - Do you have a proactive SW inventory?
- How will you pass CMMC if you don't have these fundamentals?

Password Inventory

- We use the term "Password" but we're actually talking about user credentials
- Passwords are some of the biggest challenges in our companies, yet most companies don't have an inventory of passwords,
- If you don't have a Password Inventory, how can you confirm that your policies are being followed?
- The strategy for most companies is to "hope for the best!" – Hope is Not a Good Strategy
  - They can't revoke privileges if they don't know what they are or who has them
  - They can't confirm that people are using regular user accounts when they should, and admin accounts when they need to
- There are now readily available tools to help companies inventory and manage passwords (credentials)

Data Inventory

- "It's all about the data!"
- All Cyber Security is about protecting the data, but we find that very few companies actually have a data inventory
- If you don't know how important or critical the data is, how do you know how strongly you must protect it?
- You can't protect everything to the strongest level - $$$
- A good data inventory leads to developing a strong data classification system
- A strong data classification system leads to implementing the correct security measures
- This leads us to mapping the correct authorized access, using the correct credentials, for the right staff members to be given the correct level of access for the time period required

Staff Inventory

- It might seem simple if we ask if you have developed and maintain an accurate and relevant Staff inventory for your Secured-IT
- If you don't have an accurate and current Staff Inventory, how can you make sure the right people have the right things they need, and the right access to those things when they need it?
- This staff inventory will be mapped to the other elements and aspects in the Five-Point Security framework
  - User names will be mapped to devices
  - People's names will be mapped to training
  - People's names and User names will be mapped to credentials
- In Secured-IT, the Staff inventory is used passively, actively, and proactively in order to assign and remove time-based access privileges, and even in some cases, software licensing

PUTTING IT ALL TOGETHER

ASSESS, PLAN, REMEDIATE, ITERATE

FIVE-POINT SECURITY FRAMEWORK © MATRIX

	Inventory	Policy	Budget	Security	Iterate
HW					
SW					
PW					
Data					
Staff					

"Assess"
Evaluate your Baseline Secured-IT

Plan Remediation

- Develop a roadmap of what you want to remediate over multiple iterations
- Use the results of the baseline five-point security framework matrix to develop the first iteration of your Secured-IT Remediation Plan
- Target what you want to improve during the first iteration
  - In the SSO Five-Point Security Framework ©, prioritize remediation from the top left to the bottom right for the best risk mitigation
- Ensure you have the policies, or draft policies in place to help guide remediation
- Ensure you have sufficient budget in place for each iteration of your remediation plan – ensure you have management buy-in

"Plan"
Develop a Remediation Plan

Implement Remediation

- Using the Remediation Plan, carefully plan and implement your remediation to implement true Secured-IT
- Implement in small iterations to minimize the impact on your company's operations
- For each security control, Install, Configure, and Test & Verify to make sure each control is ready for use in your company
- Document as you go and don't assume that anything has been properly completed without verification
- you can use this documentation to help you pass reviews and audits – they want to see evidence of compliance
- update the Five-Point Security Framework © matrix as you progress

"Remediate"
Implement you Remediation Plan

ASSESS AND ITERATE

	Inventory	Policy	Budget	Security	Iterate
HW					
SW					
PW					
Data					
Staff					

"Iterate"
Assess your Improved Secured-IT –
Plan the next Iteration

PREPARING FOR CMMC

SECURE YOUR COMPANY – DEVELOP COMPLIANCE

PREPARE FOR CMMC

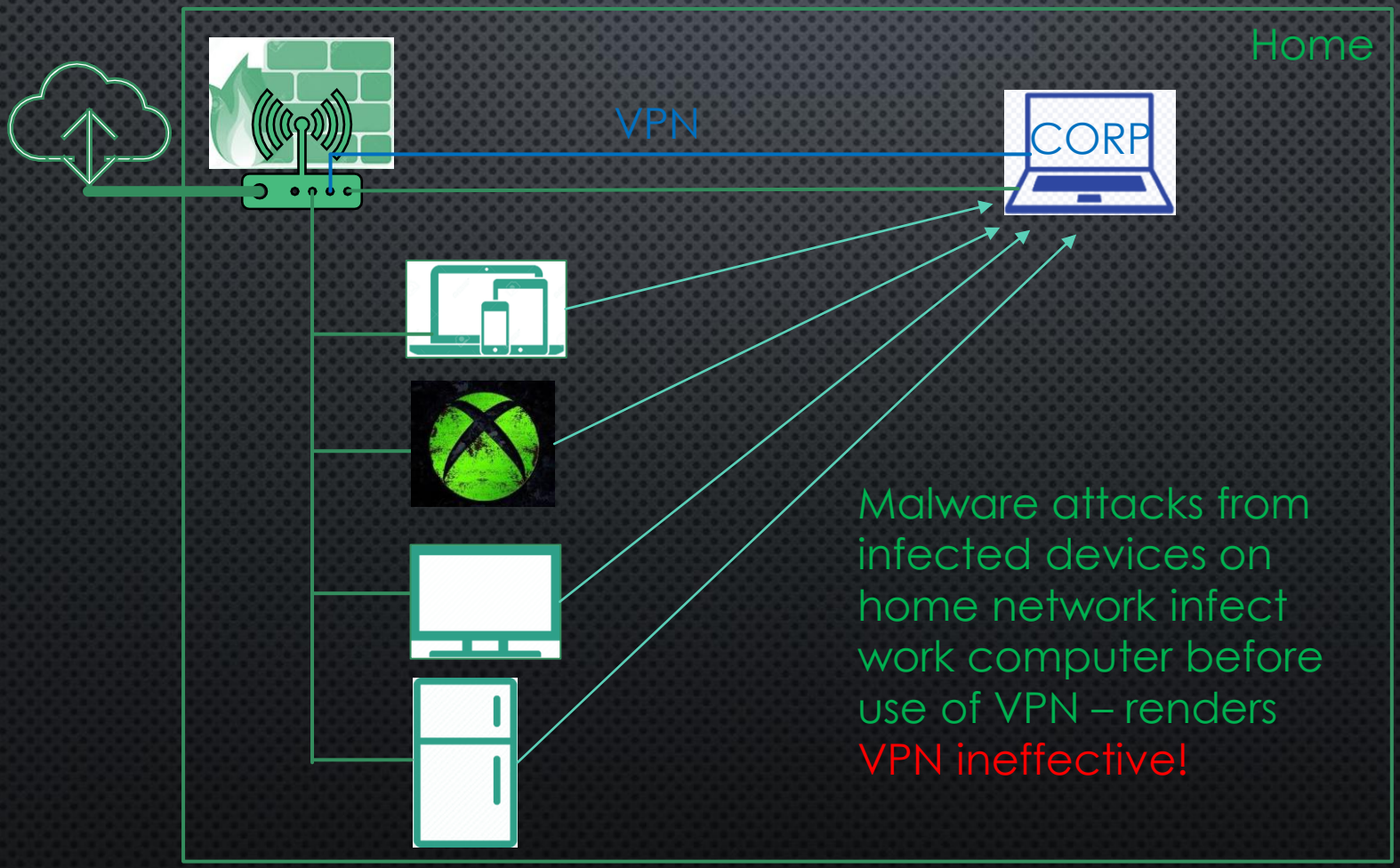
- CMMC COMPLIANCE IS COMING, EVEN THOUGH THINGS ARE STILL IN TURMOIL
- CMMC WAS ORIGINALLY BASED IN MEETING THE SECURITY CONTROLS DEFINED IN NIST SP-800-171
- EXO-STAR WAS USED BY LARGE DEFENSE CONTRACTORS FOR A SIMPLIFIED ASSESSMENT OF THE CYBER SECURITY READINESS OF THEIR SUB-CONTRACTORS AS ALIGNED WITH THE SECURITY CONTROLS IN NIST 171
- THE ORIGINAL EXO-STAR EVALUATION FORMS USE THE CYBER SECURITY CONTROLS FROM CIS-20 CSCS (CENTER FOR INTERNET SECURITY – 20 CRITICAL SECURITY CONTROLS) WHICH ARE MUCH EASIER TO FOLLOW
- WE USE THE SSO FIVE-POINT SECURITY FRAMEWORK © TO HELP COMPANIES COMPLY WITH THE CIS-20 CSCS AND ESTABLISH A STRONG SECURED-IT FOUNDATION TO PREPARE THEM FOR COMPLIANCE WITH OTHER SPECS

Prepare and Comply Remote

- How can you prepare for CMMC compliance with remote workers?
- How do you protect your corporate devices from infection?
- How do you protect sensitive corporate, client, and partner data?
- These are questions you should be asking now – before it's time for a CMMC audit
- Many people say "VPN" is the simple answer
- The next couple of slides illustrate some of the issues with that approach that render your VPN useless, as well as a solution that will help make your VPN effective and keep you compliant!

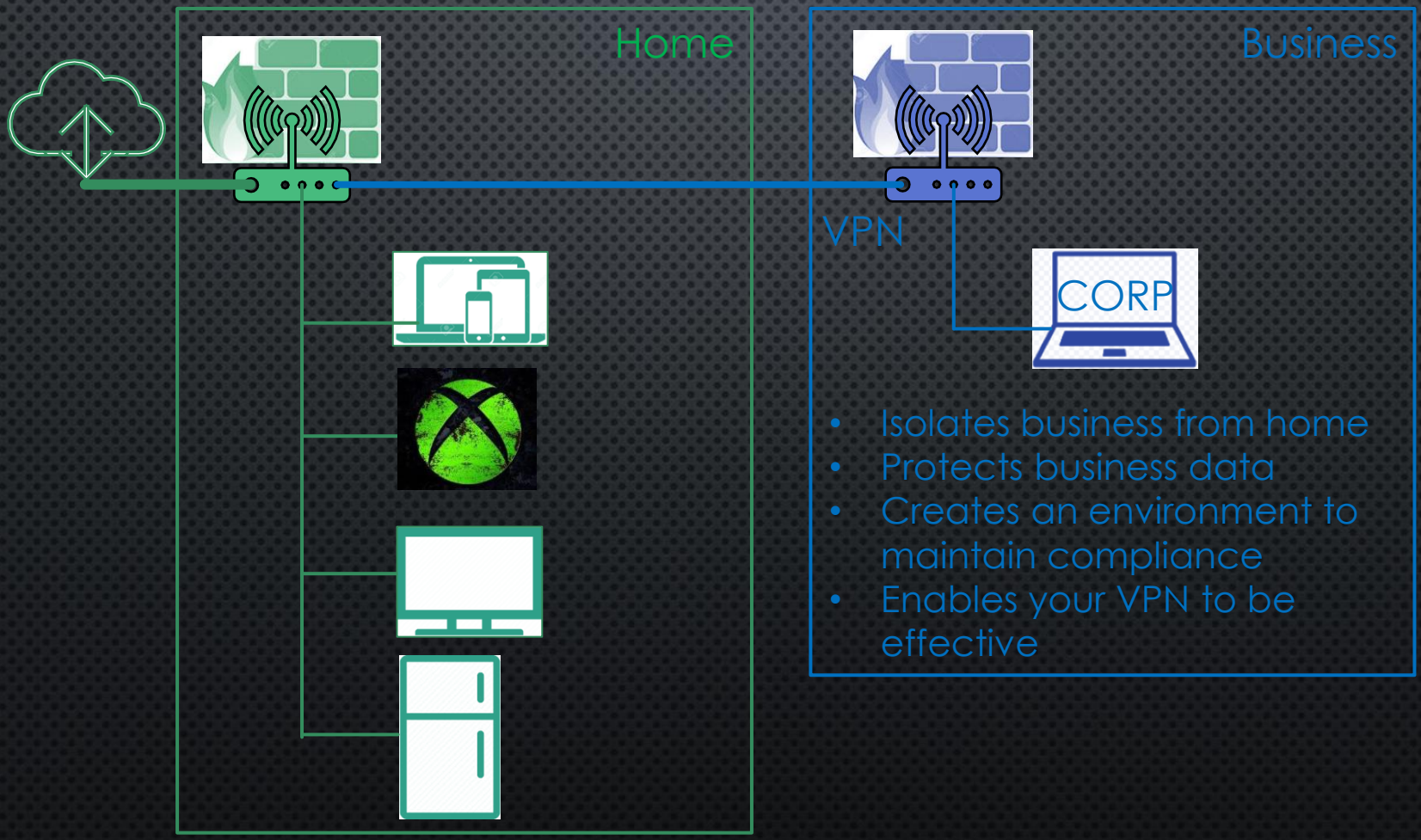
NON-SECURED HOME OFFICE

- INSTALL COMPANY WAP / FIREWALL FOR SECURE BUSINESS NETWORK



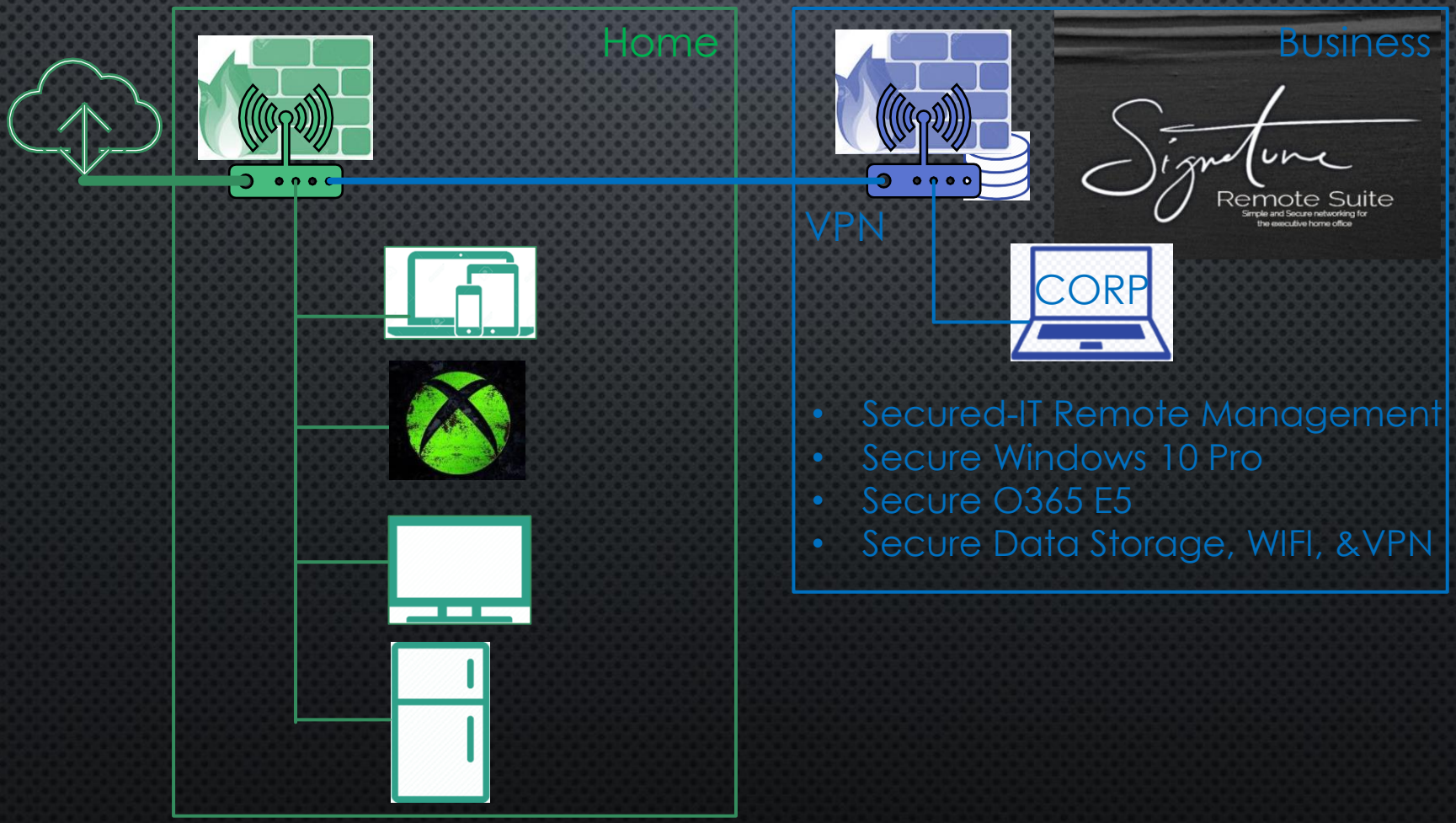
STEPS TO SECURE HOME OFFICE

- INSTALL COMPANY WAP / FIREWALL FOR SECURE BUSINESS NETWORK



SSO SECURES YOUR EXECUTIVE HOME OFFICE

- SSO SIGNATURE REMOTE SUITE FOR YOUR EXECUTIVE HOME OFFICE



THREE CHOICES

- We always let people know there are three choices to follow:
  - Do it yourself
  - Ask for Help
  - Hire the experts
- If you need some help, just give us a call
- If you want to hire the experts, we offer our services to you
- SSO has been remote since the day we opened and focuses on Small offices and home offices (SOHO):
  - SSO Signature Remote Suite is specifically designed for company leaders and their Executive Home Office
  - SSO SOHOWOW! package is designed for SOHO (Small Office / Home Office) from 1 to 100 staff members

QUESTIONS?

BACKUP SLIDES

USEFUL INFORMATION FOR REMOTE WORKERS

Remote Work Topics

- The unprepared and rapid migration of workers to uncontrolled, unmonitored, and unsecured environments puts most companies at significant risk
  - Cybercrime has increased significantly in attacks on this unprepared remote workforce
  - Unsecured Home computers are being used to perform business functions
  - Unsecured Home networks are being used to connect those computers
  - Company computers are being used on unsecured home networks
  - Often times home networks are shared with neighbors or easily accessed by non-family members
  - The physical security of home computers or corporate computers in homes might be poor
  - Companies are relying on their IT department (trained in IT but not trained in security) to secure remote workers rather than using a Security Company partner (trained in security)
  - Great time for Employee Training!!!

USING HOME COMPUTERS FOR WORK

- As a result of the rapid migration of workers to remote workplaces, many companies were not prepared to provide these remote workers with corporate devices
- As a result, they are using home computers
- Home computers are uncontrolled, often not properly patched, most often the operating system controls are not properly configured and very often, they are already compromised
- Most home computer users set up their computers with an admin account and then continue using those computers with that admin account –
  - This means if they are hacked, the cybercriminal has access to all of the admin functions and can perform many harmful functions or gain additional access in the home network

Home Computers for Work (Cont'd)

- Most often users have private information on their home computers and also use their computers in ways they would prefer to remain private – in some cases other family members do the same
- With this in mind, most companies' IT staff cannot install remote monitoring and maintenance software on those computers and their Security staff cannot install security software or configure security settings –
  - this leaves the computers potentially unstable and unsecured
- Even when remote workers access their work data repository in the cloud, or through a SaaS tool, using legitimate credentials, or even using a VPN (Virtual Private Network), if their home computer has already been compromised, their credentials could be captured by cybercriminals and used for additional access to business data and business functions

USING HOME NETWORKS FOR WORK

- In many cases, home networks have minimal security and other family members or friends have ready access
- Many home networks are even readily accessible by non-authorized persons
- Home networks often use home-based equipment, verses commercial level equipment, and the security and stability is marginal
- In most cases the homeowner controls the credentials and configuration of the home network devices, rather than the company's security department, so the security might be poor as a result

Using Company Computers on Home Networks

- Some companies have provided remote workers with corporate computers to use at home
- This lets the company manage and protect those computers remotely if they are allowed access to the home network by the remote worker
- This addresses the risk of using an unsecured computer to perform business work
- It does not address the risk of using a computer on an unsecured home network to perform business work
- Even if you use a VPN to access your corporate workspace, you are not necessarily secure if you are on an unsecured home network – your computer might already be compromised
- The answer is to set up a separate network for performing business and isolate your company computer from the remaining users on the home network
- A VPN is a good solution if you're using a separate network dedicated to performing work

Some Key Points

- Don't use your work email for personal shopping – that coupon from Nordtroms might look real but actually contain malware or send you to a hacker's site
  - We have responded to multiple CIRTs (Computer Incident Response teams) from executives doing personal shopping
- Set up a regular user account on your computer (work or personal) for doing business work from home, even if you have another Admin account on the computer –
  - If you get hacked, the criminal won't have access to your admin functions
- Set up a work network at home separated by a firewall, or set up in a Wireless Access Point capable of multiple secured / separate networks
- If you have to use a home computer, set up a separate account, as a regular user, for business purposes – do not use an admin account for day to day business
- Remember, your IT department is not your Security department – team with a security company to address these security challenges

Monitoring New Remote Workers

- Many companies who have not used remote workers in the past have not developed an inherent culture to successfully task and manage a remote work force
- Many employees are not good at managing their remote work
- With this in mind, many companies are leveraging remote worker monitoring software (generally on corporate owned devices) to capture relevant statistics on employee behaviors during work hours
  - URLs they visit – even screenshots
  - Time on keyboard – even key logging
- What impact does this have on company culture and how much does the software but also the settings and analysis cost?
- What policies and privacy issues need to be addressed? Costs?

The New "Mobile" Workforce

- Companies are seeing both the positives and negatives of having more of their population working remotely, but most haven't considered what many "new" remote workers have realized
- When you work remotely, there are very few actual dependencies on your company and it is much easier to change companies
- Companies on the other hand experience extensive costs in hiring and on-boarding new staff and off-boarding staff that leaves
- This places companies at another significant financial risk
- Companies need to compensate staff members for IT costs at home – internet, phone, PC, etc.
- Help your staff be productive, active and healthy – develop your company "Remote" culture
- What changes should companies make to address this new challenge?