ICE
TRUSTED IT PARTNER

TELEWORK ESSENTIALS TOOLKIT
IT PROFESSIONALS

PART I:
THE TELEWORK ESSENTIALS TOOLKIT – FOR THE COVID ERA
WHAT IT PROFESSIONALS NEED TO KNOW.

Remote work practices are taking place everywhere in the country in response to COVID-19, and affecting businesses large and small, in all industries. To keep workers safe and healthy, many organizations have started planning for more permanent and strategic teleworking. Some technology companies are telling employees to work from home indefinitely. Given the uncertainty of the current pandemic that most say will last into 2021, CISA put together a telework guide that provides recommendations and additional resources on navigating the current environment. According to CISA, they are providing these recommendations to support organizations like yours in re-evaluating and strengthening your cybersecurity as your firm may need to transition your team (or part of your team) to long-term telework solutions.

In this **Part I** article, we will highlight the role of IT professionals. Stay tuned for Part II which will cover your executive leaders and teleworkers.

CISA is our nation's risk advisor and brings together partners in industry and the federal government to improve American cyber- and infrastructure security.

"As the nation's risk advisor, the Cybersecurity and Infrastructure Security Agency's (CISA) mission is to ensure the security and resiliency of our critical infrastructure. However, in today's digitizing world, as organizations are increasingly integrating cyber systems into their operations, they are also facing more diverse, sophisticated threats— cyber, physical, technological, or natural—that may have cross-sector impacts. The evolving risk landscape necessitates an evolved response."

FOR IT PROFESSIONALS: BE "SECURITY" AWARE, BE VIGILANT

Can you protect your growing enterprise from ransomware, security breaches, and other cyber threats to your systems and data — the lifeblood of your business? With more and more of your staff working from home, and accessing corporate resources, your IT professionals have to work even harder today to keep your organization safe and secure. Consider this statistic:

"The FBI has seen a [300%] spike in cybercrimes reported to its Internet Crime Complaint Center (IC3) since the beginning of the COVID-19 pandemic, as both domestic and international hackers look to take advantage of Americans' daily activities moving increasingly online."[1]

Businesses in all industries need to take these threats seriously. The Telework Essentials Toolkit provides six recommendations:

1 Ensure Patching and Vulnerability Management

As part of our Managed Services Agreement, ICE Consulting can help you:

- Patch all network hardware, servers, end points (Notebooks/Desktops), and applications on a set schedule to reduce threat vulnerabilities.
- Automatically update applications and operating systems (OS) on endpoints by Mobile Device Management (MDM). It should be noted that the need for MDM is even more critical today.
- Perform periodic security scanning of your infrastructure for vulnerabilities.

ICE has more than 30 years of experience working with hundreds of clients across the U.S. This is the expertise you need to stay safe.

2 Invest in Enterprise Cybersecurity Controls

Cybersecurity requires an investment. You must implement, maintain, and invest in best-of-breed enterprise cybersecurity to enable your employees to securely connect to your organization's network and assets. ICE Consulting uses industry best practices for secure remote access including zero-trust architectures that may be preferable in the modern IT environment of today. We can help you evaluate your current security architecture and ensure that it is working best for your business. In many cases, we recommend the use of VPN whether connecting to the cloud or an on-premise network.

We can audit your current environment and provide strategic recommendations that will enable you to focus on your core business.

3 Enforce Multi-factor Authentication

ICE recommends OKTA and other similar solutions for its "adaptive" multi-factor authentication (MFA) on untrusted connections before access can be granted. According to a 2020 Verizon Data Breach Investigations report, this is important because 80 percent of security breaches involve compromised passwords.[2]

The password policy and identity management system are extremely important. Talk to us about how we can help.

4 Maintain Corporate Approved Products

Be sure to maintain a list of corporate-approved products for collaboration, video conferencing or even social media, and provide users with guidance on using these tools securely. As an ICE client, we can help you maintain a list of approved applications. We use Mobile Device Management (MDM) to enforce applications and data access rules and policies on remote devices. An MDM strategy also helps ensure that applications are updated with the latest patches to address any performance and security vulnerabilities and bugs.

5 Perform Frequent Backups

Frequent backups are critical. You must verify backups regularly and store backups offline and offsite. Read our newsletter article on, "Backup is One Thing. Restore is Everything."

ICE Consulting highly recommends using endpoint backup solutions such as CrashPlan (enterprise-grade data loss protection) and enterprise backup solutions for servers to ensure all data and individual systems are backed up on a regular basis. Backups should be stored "encrypted" in protected cloud environments and tested and verified periodically.

6 Implement Domain-Based Message Authentication

Implementing a Domain-based Message Authentication, Reporting & Conformance (DMARC) validation system can help you address the increased risk of phishing schemes and prevent business email compromise in remote-working environments. ICE Consulting uses industry standards such as Proofpoint, Microsoft ATP, MimeCast (DMARC) email filtering and validation products to reduce your risk of lost data or sensitive email information.

ICE
TRUSTED IT PARTNER

CALL OR EMAIL US TODAY

888-423-4801

info@iceconsulting.com

www.iceconsulting.com

ICE
TRUSTED IT PARTNER

TELEWORK ESSENTIALS TOOLKIT
TELEWORKERS

PART II:

THE TELEWORK ESSENTIALS TOOLKIT – FOR THE COVID ERA

WHAT TELEWORKERS NEED TO KNOW

What will your organization look like in the future — post COVID? With new developments on vaccines, the future now looks brighter, but we must all do our part to stay safe and healthy over the next few months. Businesses and individuals are still struggling with the pandemic that will continue well into 2021, and some changes in the way we work may be permanent. As your business plans for more strategic teleworking, here are recommendations and actions for enhancing the security of home networks for teleworkers to consider. Keep in mind, our team at ICE Consulting can help you with all of these actions and are experts on all aspects of cybersecurity, IT infrastructure, and cloud solutions.

FOR TELEWORKERS: SECURE YOUR HOME NETWORK

Your remote workers need to be aware of security and vigilant of any threats. Here are four actions recommended by CISA in the Telework Essentials Toolkit — all have been recommended by ICE Consulting for years.

1 Configure and Harden Your Home Network

Make sure your employees have properly configured and hardened home networks.

- Change all default passwords and use complex passwords.
- Ensure your home wireless router is configured to use WPA2 or WPA3 wireless encryption standard at the minimum.
- Ensure the wireless network name (SSID) does not identify your physical location or router manufacturer/model.
- Use protective Domain Name System (DNS) service.

ICE will provide training and can assist users in the proper set-up of their home networking equipment and wireless environment based on your corporate policies.

2 Secure Practices and Organizational Policies

It's critically important that all remote users and on-premise corporate users follow organizational procedures for handling sensitive data such as personally identifiable information (PI), protected health information (PHI) as well as intellectual property (IP), and any other sensitive materials. We can provide training and manage organizational assets to ensure patching, encryption, acceptable use of assets, and adherence to infoSEC (Information Security) policies.

3 Use Caution with Email Attachments and Links

Use caution when opening email attachments and clicking links in emails. Increase your awareness of phishing tactics, current phishing campaigns and social engineering to effectively report suspicious engineering and report suspicious email and communications. We can help your team have more awareness of phishing tactics or current phishing schemes and how to use caution when opening email attachments and/or how to trust opening links. ICE can provide Phishing awareness training.

4 Communicating Suspicious Activities

Make sure you know the procedures for communicating suspicious activities to your organization's IT security team and promptly report all suspicious activity.

ICE SERVICIES

ICE OFFERS 3 CATEGORIES OF SERVICES

1. Strategic Services — that are actionable include comprehensive IT audit and assessment both Cloud and on-prem infrastructure, system and network design and security, disaster recovery and business continuity, and much more.

2. Upgrade and Migration Services — that are ready to scale for your future include system and network migration to the cloud infrastructure or on-prem, migration and implementation of secure and cost-effective applications and solutions that enhance productivity and help with office expansion and migration. We implement secure and high-performance wireless solutions.

3. Proactive Maintenance and Support — that reduces unplanned downtime, optimizes IT stability, and increases system and network security. These services include complete IT maintenance with 24/7 monitoring and live support by a qualified IT engineer. With more than 5,000 user reviews, we have a 97% net-client-satisfaction score.

ICE
TRUSTED IT PARTNER

CALL OR EMAIL US TODAY

888-423-4801

info@iceconsulting.com

www.iceconsulting.com

ICE
TRUSTED IT PARTNER

TELEWORK ESSENTIALS TOOLKIT
EXECUTIVE LEADERS

PART III:
THE TELEWORK ESSENTIALS TOOLKIT – FOR THE COVID ERA
WHAT EXECUTIVE LEADERS NEED TO KNOW

Even with good news on the vaccine front, the pandemic has forever changed business and will still impact business operations well into 2021. Here are recommendations and actions for executive leaders to consider. Keep in mind, that our team at ICE Consulting can help you with all of these actions and are experts on all aspects of cybersecurity, IT infrastructure, and cloud solutions.

FOR EXECUTIVE LEADERS: ENHANCE YOUR CYBERSECURITY STRATEGY, INVESTMENT, AND CULTURE

WHAT FOUR ACTIONS CAN YOUR EXECUTIVE LEADERS TAKE TODAY?

1 Review Organizational Policies and Procedures

We always recommend reviewing organizational policies and procedures on an ongoing basis, but that is even more important today. As your workforce shifts to more remote work, it's important that all your employees are aware of your security requirements. This is of strategic benefit to your organization. ICE Consulting can help with managing these policies and provide assistance in writing and/or revising and implementing the best corporate policies — all based on our 20+ years of expertise with best-practice procedures.

2 Establish Cybersecurity Training Requirements

Your team should have a good working knowledge of all the latest cybersecurity concepts and threats so your team can make the best decisions when assessing organizational systems and data remotely. We can help you develop training materials based on your corporate policies, provide input on the latest trends, and provide user security training and education.

3 Move Organizational Assets

Determine the cybersecurity risks associated with moving organizational assets beyond the traditional perimeter to activities not accessible by the organization's monitoring and response capabilities (e.g., printing at home, use of personal email accounts, use of personal devices, use of personal mobile devices). Develop, implement, and enforce enterprise-wide policies that address the threats and vulnerabilities presented by the new extended perimeter. These policies should include requirements for workers to securely configure and update corporate devices, personal devices, mobile devices, and home networks. ICE can assist you with developing such policies.

4 Develop a Cybersecure, Hybrid Culture

Most agree that the new way of working is not just temporary, but most organizations will need to refine strategies for this hybrid workforce culture. In the future, you may continue to have on-premise employees, remote employees, and those who prefer to do a combination of both. We recommend that you make sure that you address the basics of "cyber hygiene" — such as phishing, software updates, passwords/authentication, USB use, removable media, and more. ICE helps our clients develop the policies and can provide user security training on corporate assets.

ICE SERVICIES

ICE OFFERS 3 CATEGORIES OF SERVICES

1. Strategic Services — that are actionable include comprehensive IT audit and assessment both Cloud and on-prem infrastructure, system and network design and security, disaster recovery and business continuity, and much more.

2. Upgrade and Migration Services — that are ready to scale for your future include system and network migration to the cloud infrastructure or on-prem, migration and implementation of secure and cost-effective applications and solutions that enhance productivity and help with office expansion and migration. We implement secure and high-performance wireless solutions.

3. Proactive Maintenance and Support — that reduces unplanned downtime, optimizes IT stability, and increases system and network security. These services include complete IT maintenance with 24/7 monitoring and live support by a qualified IT engineer. With more than 5,000 user reviews, we have a 97% net-client-satisfaction score.

ICE
TRUSTED IT PARTNER

CALL OR EMAIL US TODAY

888-423-4801

info@iceconsulting.com

www.iceconsulting.com