

Telework: Risks, Challenges, Perils, and Successes

William Favre Slater, III, M.S., MBA, PMP, CISSP, SSCP, CISA, CDCP

IT Project Manager and Adjunct Professor, IIT School of Applied Technology

Agenda

- Introduction
- How do you “Telework”
- Telework Risks
- Telework Challenges
- Telework Perils
- Telework Successes
- What Can You Do in Your Organization
- Security and Teleworking
- Conclusion
- References
- Questions



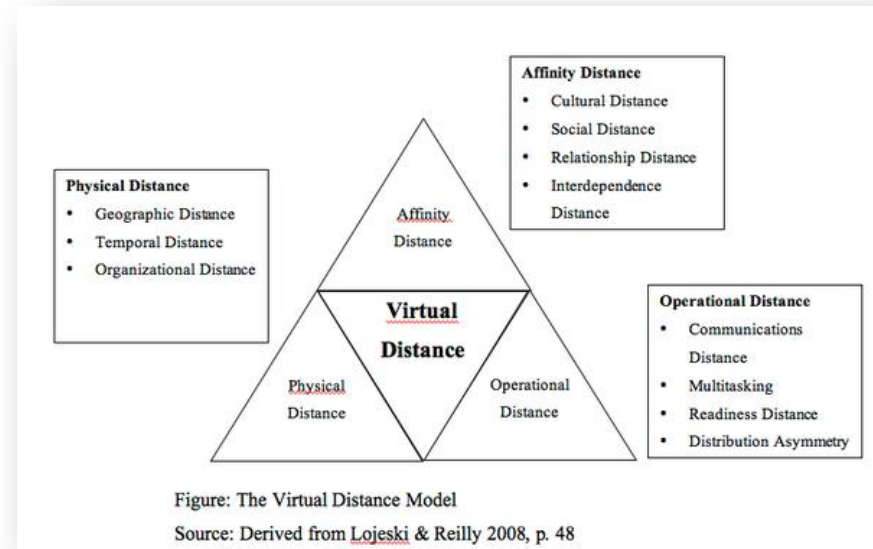
Introduction

- Telework has been growing in popularity during the past 20 years due to the steady growth of the Internet and secure enabling technologies.
- In 2010, the Federal Telework Act was signed into law providing 10s of thousands of Federal workers the option to perform Telework regularly.
- Telework is often misunderstood, and has its own unique risks, challenges, and perils.
- Not properly planning how and when your staff will perform telework, can represent unacceptable risk and provide a formidable barrier to your Team's success.
- This presentation will provide a good look at what teleworking is, and how to deal with the risks, challenges, and perils of telework.

How Do You “Telework”

Understand Virtual Distance

- “**Virtual Distance** is a psychological distance created between people by an over-reliance on electronic communications.”
- As **Virtual Distance** rises, these observed effects have been noted:
 - 50% decline in project success (on-time, on-budget delivery)
 - 90% drop in innovation effectiveness
 - 80% plummet in work satisfaction
 - 83% fall off in trust
 - 65% decrease in role and goal clarity
 - 50% decline in leader effectiveness



(Lojeski and Reilly, 2008)

Defining the Environment

- Remote workers, often working across multiple time zones
- Secure Internet connections, usually from the employees' homes
- E-Mail
- Teleconference meetings, via phone
- Phone calls (either land line or cell phone)
- Live Meeting (for presentations)
- Live Communicator (for online chats)
- Interaction with Management, Team members, and the Customer
- Work usually performed on company-supplied laptops after onboarding
- Occasional business trips, lasting from 2 to 5 days



Culture

To have a Successful Teleworking Organization, create a Culture that is:

- Supportive
- Electronically Connected & responsive
- Collaborative
- Informal to Semi-formal
- Mutual respect
- Responsive and Customer-focused
- Semi-autonomous & Self-managed



Teleworking Advantages

- Increased Productivity
- Minimal infrastructure and office support
- Cost savings
- Ecological benefits
- Easy to recruit & engage workers with disabilities
- Work - life balance
- Individual control
- Good for Employee Morale
- Extended reach for talent pool



Other Critical Requirements for Successful Teleworking



Source: <http://www.telework.gov>

Telework Risks

10 Telework Risks

Missing Employees, Unproductive Behaviors, Lack of Personal Accountability

Risk of unauthorized physical access to corporate information stored on a remote PC

An “always on connection” can be a likely target for attackers and malware.

Bridging networks from remote Home Networks to Corporate Networks creates the opportunity for cyberattacks (i.e. Zombies, botnets and other serious malware, APTs, etc.)

Teleworker behavior associated with downloading of unauthorized programs.

Lack of Telework Training

Lack of Telework Policies

Lack of Telework Agreement

Lack of Telework Schedule

Lack of Telework Work Plan

Telework Challenges

Telework Challenges & Solutions for Management & Teams

Category	Challenge	Solution
Management and Teams	Meeting Customer Expectations	Always show the Customer that we are Customer-focused and listening to his or her expectations.
Management and Teams	Managing and collaboration across Time Zones	Ask for flexibility and adaptability.
Management and Teams	Getting Access to Government Furnished Equipment and Customer Resources	Alerted the Customer about the issue(s).
Management and Teams	Meeting Schedule Challenges	Hire professionals that rise to meet the challenge.
Management	Keeping Team Members Productive, Engaged, and Motivated in spite of the Challenges	Hire professionals that rise to meet the challenges.
Management and Teams	Attending meetings and still getting work done and avoiding burnout	Hire professionals that rise to meet the challenge.
Management and Teams	Technical Support	Ensure that people are available and that they have back-ups.
Management and Teams	Meeting Customer Management Expectations, Delivery and Report Schedules	Hire professionals that rise to meet the challenge.
Management and Teams	Meeting Management Expectations and Reports Schedules	Hire professionals that rise to meet the challenge.

To Telework or Not to Telework

10 Reasons You May Not be Cut-out to Be a Teleworker

1. You fall prey to external distractions
2. You're a sitting duck for internal distractions
3. You can't put together the necessary equipment, services, or infrastructure to do your job
4. You can't sustain enough (or any) proactive contact with the office
5. You don't function well without a lot of structure
6. You have a manager who can't or won't manage remotely
7. You can't establish boundaries with friends, family, or neighbors
8. You can't bring yourself to quit for the day
9. You can't work independently
10. You hate missing out on collaborative opportunities



Source: <http://http://www.techrepublic.com/blog/10-things/10-signs-that-you-arent-cut-out-to-be-a-telecommuter/>

Telework Perils

Telework Perils

Top Telework Perils

Data Breach

Network Security Breach

Unauthorized Physical Access to Corporate Information on a Remote PC

An **“always on connection”** is a tempting Target for Attackers and Malware

Unwillingness or inability to abide by Telework Policies and Procedures creates vulnerability for the organization and introduces excessive risk.



Lessons Learned the Hard Way

Event	Lesson	Comments
The MIA Java Developer	Randomly check up on Team members	As a response, the organization put management processes into place to ensure that people are engaged and productive. It also raised the bar on screening and procurement and staff acquisition.
Who let the dogs out?	Remember that your home environment becomes part of your teleconference meetings.	The organization published and distributed Phone Etiquette guidelines.
Don't forget that Mute Button!	Remember to use the mute button during teleconference meetings.	The organization published and distributed Phone Etiquette guidelines.
You can't be a Baby Sitter AND a Business Analyst...	You cannot baby-sit your kids while you are working from home.	The Customer usually forbids this and so do most companies.

Telework Successes

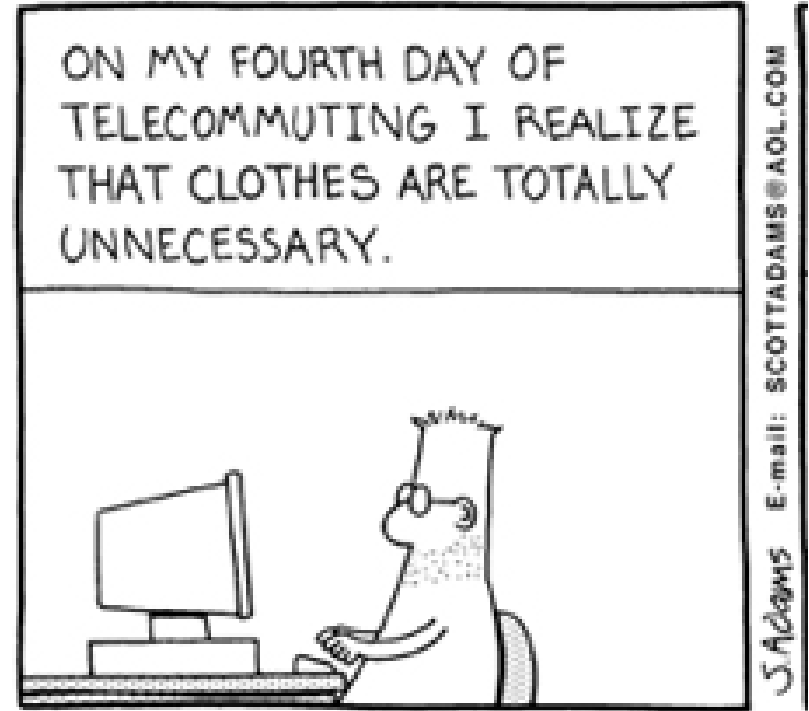
Some Success Stories

- **2010**: CACI won several U.S. Government contract Task Orders, built a 48-person Team that was 100% teleworking, and the Customer was extremely pleased with the performance and deliverables
- **2011**: CACI's Customer starts renewing Task Orders
- **2014 - 2015**: Managed a 7-person Team at on a U.S. Government contract where two Team members telework 100% and four others telework one day per week.



What Can You Do in Your Organization?

- Learn about and prepare for teleworking
- Get certified and have your Team members get certified to Telework
- Administratively lay the groundwork for Success
- Be sure to cover People, Processes, and Technology



Laying the Groundwork for Success

- Create & Maintain a shared vision for success
- Pursue business opportunities in which your organization can support the customer, be successful, and win follow-on opportunities
- Strong, capable technical recruiting
- Strategic partnering for staff augmentation
- Strong leaders with successful track records
- Reliable, talented, dedicated employees with successful track records
- Create work plans and schedules that are aligned with the Customer's requirements and demands
- Have flexibility with the Customer's requirements and demands
- Execute on your strategic and tactical plans
- Report the results
- Share the feedback and kudos, bad and good
- Make adjustments and improvements when necessary



Pearls of Wisdom for Teleworking

- Being open and flexible – telework is a dynamic work option.
- Focus on the *results* of work performed not *where* it is performed.
- Know, express, and agree on what constitutes successful job performance.
- **What makes a good teleworker is a good employee.**
- Be sensitive to the impact telework has on non-teleworkers.
- Communicate in a timely, candid, and constructive manner with employees.



Source: The Telework Collaborative

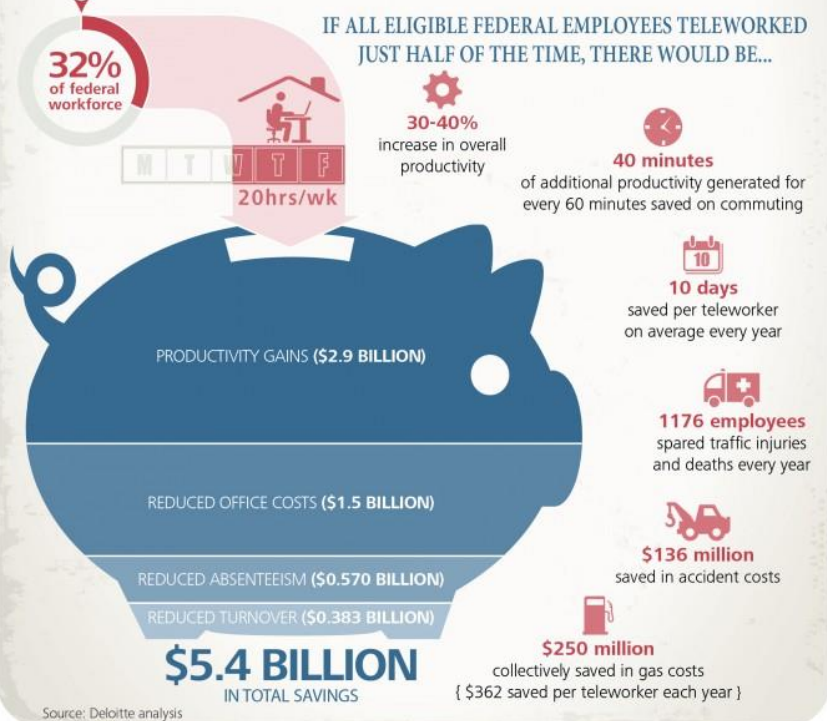
TELEWORK SAVINGS = \$5,400,000,000

According to the 2012 Federal Telework Report, only **7%** of US federal government employees telework.



YET APPROXIMATELY **32%** OF THE FEDERAL WORKFORCE IS **ELIGIBLE TO TELEWORK**.

IF ALL ELIGIBLE FEDERAL EMPLOYEES TELEWORKED JUST HALF OF THE TIME, THERE WOULD BE...



Other Benefits: Cost Savings

(Billions with a "B")

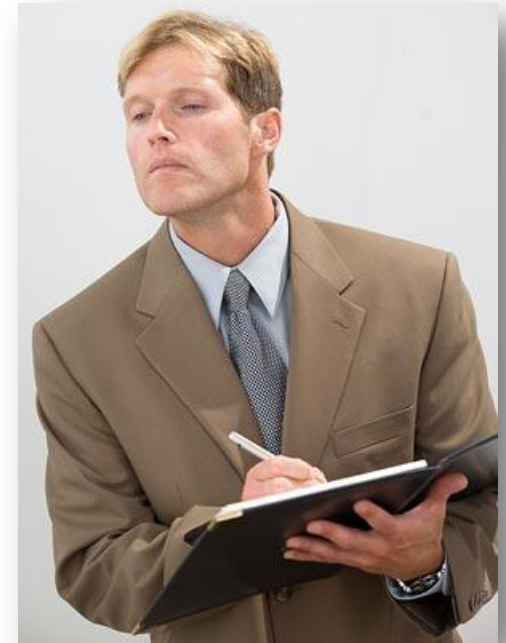


**Report on
2012 Savings
in Federal
Government**

Security & Teleworking

Security Risk Management

- Identify and classify critical cyber assets
- Identify and analyze the electronic security perimeter(s) (ESPs)
- Select security controls
- Perform a vulnerability assessment
- Assess risks to system information and assets
- Monitor and assess the effectiveness of controls



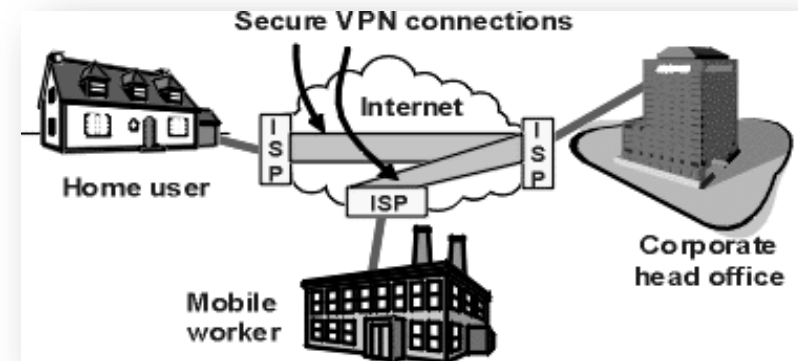
Source:

<https://www.smartgrid.gov/sites/default/files/doc/files/CyberSecurityGuideforanElectricCooperativeV11-2%5B1%5D.pdf>

Protecting the Electronic Security Perimeter (ESP)

The access points to each perimeter are:

- Firewalls
- Routers
- Modems
- Virtual private network (VPN) endpoints
- Proxy servers
- Web servers



NOTE: Perform a cyber vulnerability assessment of the access points to each ESP at least once a year.

Source:

<https://www.smartgrid.gov/sites/default/files/doc/files/CyberSecurityGuideforanElectricCooperativeV11-2%5B1%5D.pdf>

Training, Training, Training

- Adequately vet candidates for hire
- Establish an Information Security Awareness Program
- Train employees who have access to protected assets
- Enforce “least privilege” access to cyber assets and periodically review access privileges
- Get your teleworkers trained and certified to telework

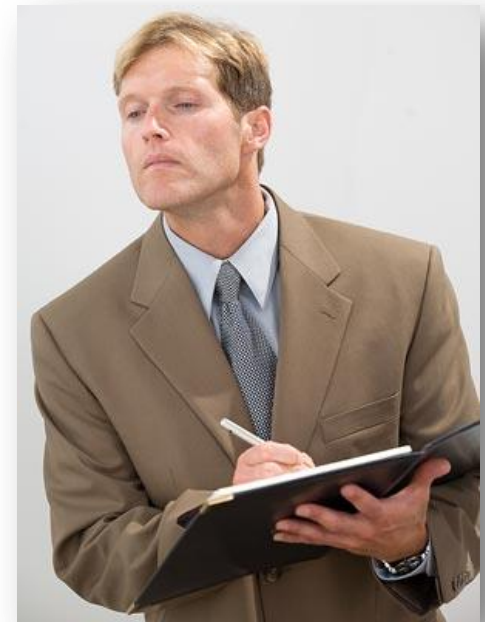


Source:

<https://www.smartgrid.gov/sites/default/files/doc/files/CyberSecurityGuideforanElectricCooperativeV11-2%5B1%5D.pdf>

Security Awareness and Training Program Should Include:

- The policies, access controls, and procedures developed for critical cyber assets.
- The proper use of critical cyber assets.
- The proper handling of critical cyber asset information.
- Action plans and procedures to recover or reestablish critical cyber assets, and the required access to these assets, following a cybersecurity incident.
- **Certification in Teleworking**



Source:

<https://www.smartgrid.gov/sites/default/files/doc/files/CyberSecurityGuideforanElectricCooperativeV11-2%5B1%5D.pdf>

NIST SP 800-114

NIST

**National Institute of
Standards and Technology**

U.S. Department of Commerce

Special Publication 800-114

User's Guide to Securing External Devices for Telework and Remote Access

**Recommendations of the National Institute
of Standards and Technology**

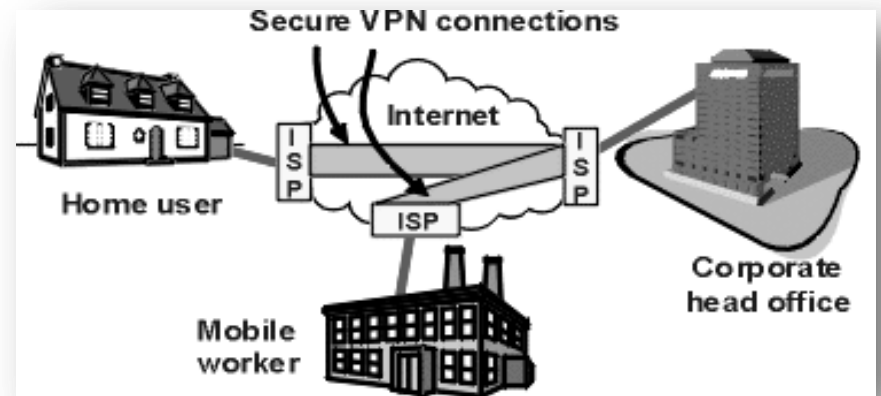
Source:

<http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf>



NIST SP 800-114 Concepts

- **Securing Your Home Network**
 - Wired Networks
 - Wireless Networks
 - External Networks
- **Securing Your PC**
 - Updates
 - User accounts
 - Networking Configuration
 - Attack Prevention
 - Primary Application configuration



Source:

<http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf>

NIST SP 800-46

NIST

**National Institute of
Standards and Technology**

U.S. Department of Commerce

**Special Publication 800-46
Revision 1**

Guide to Enterprise Telework and Remote Access Security

**Recommendations of the National Institute
of Standards and Technology**

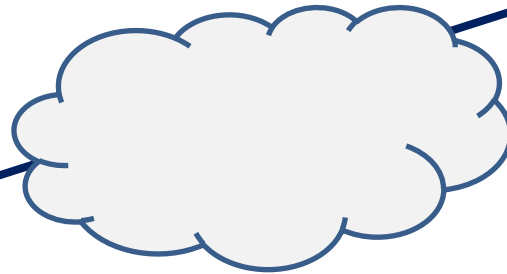
Source:

<http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf>



Secure Telecommuting Concepts

- Secure Connections
- Secure Data in Transit
- Secure Data at Rest



Source:

<http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf>



Tunneling (VPN) Architecture

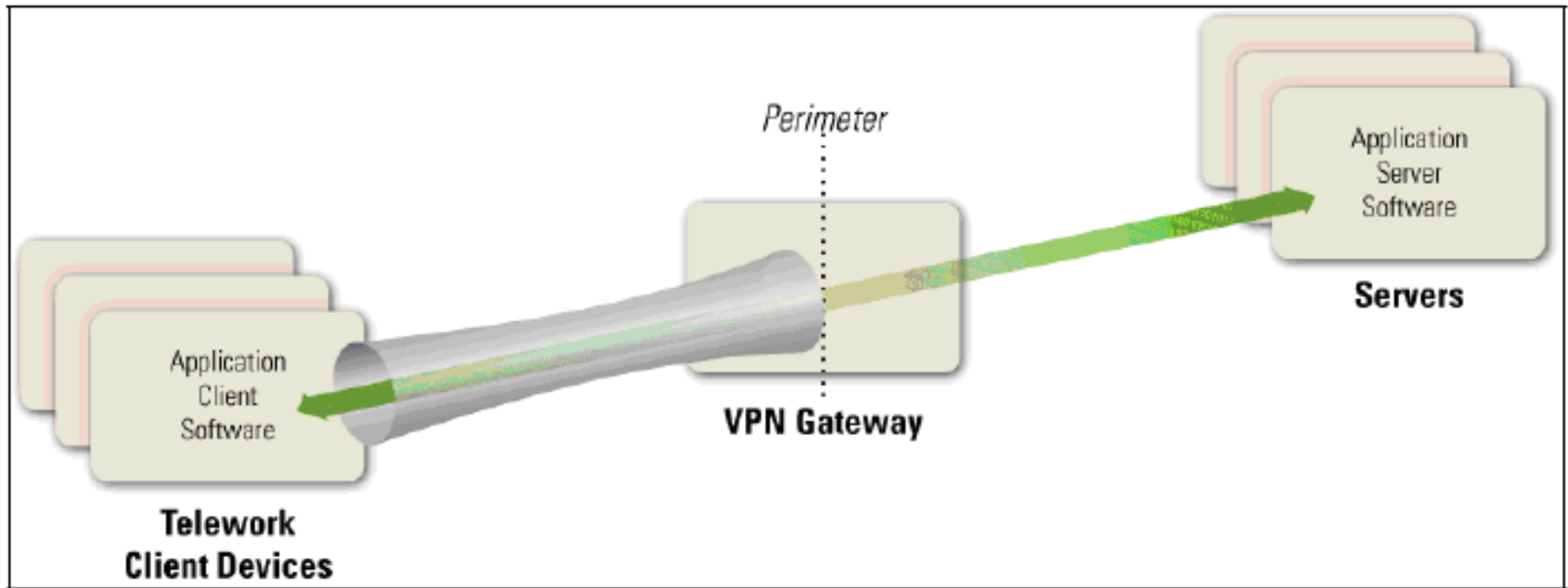


Figure 2-1. Tunneling Architecture

Source:

<http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf>

Portal Architecture

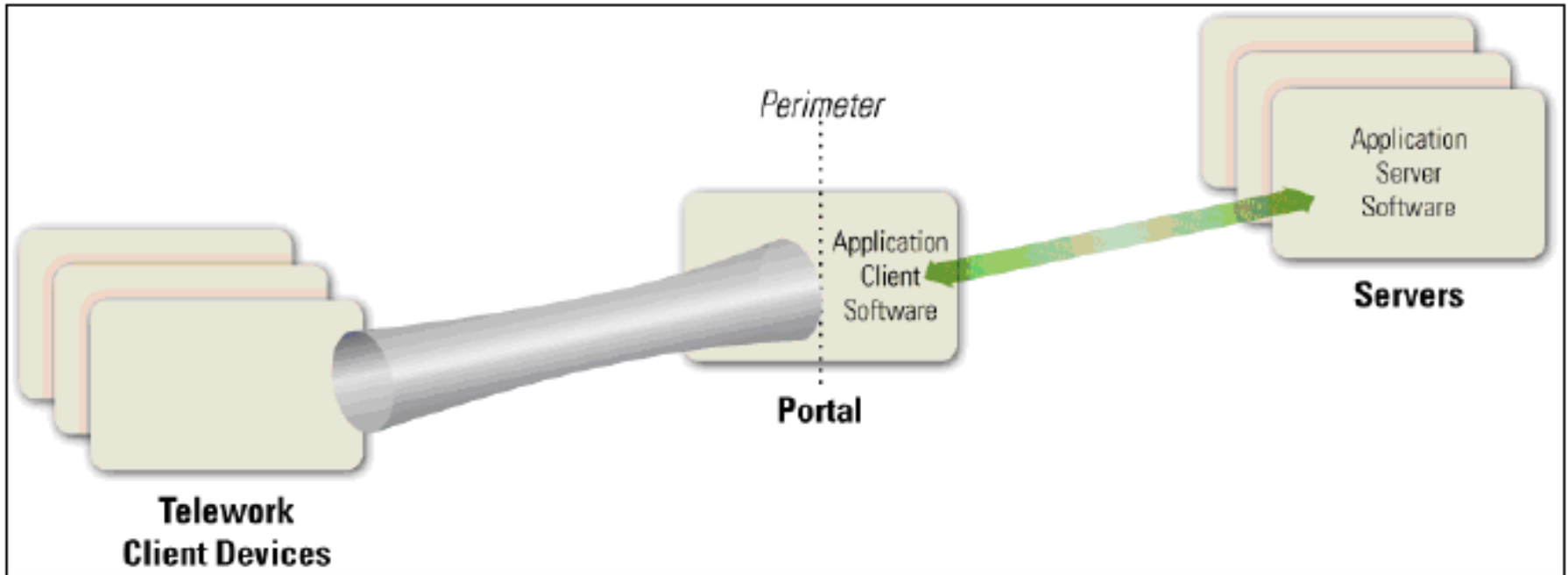


Figure 2-2. Portal Architecture

Source:

<http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf>

Remote Desktop Access Architecture

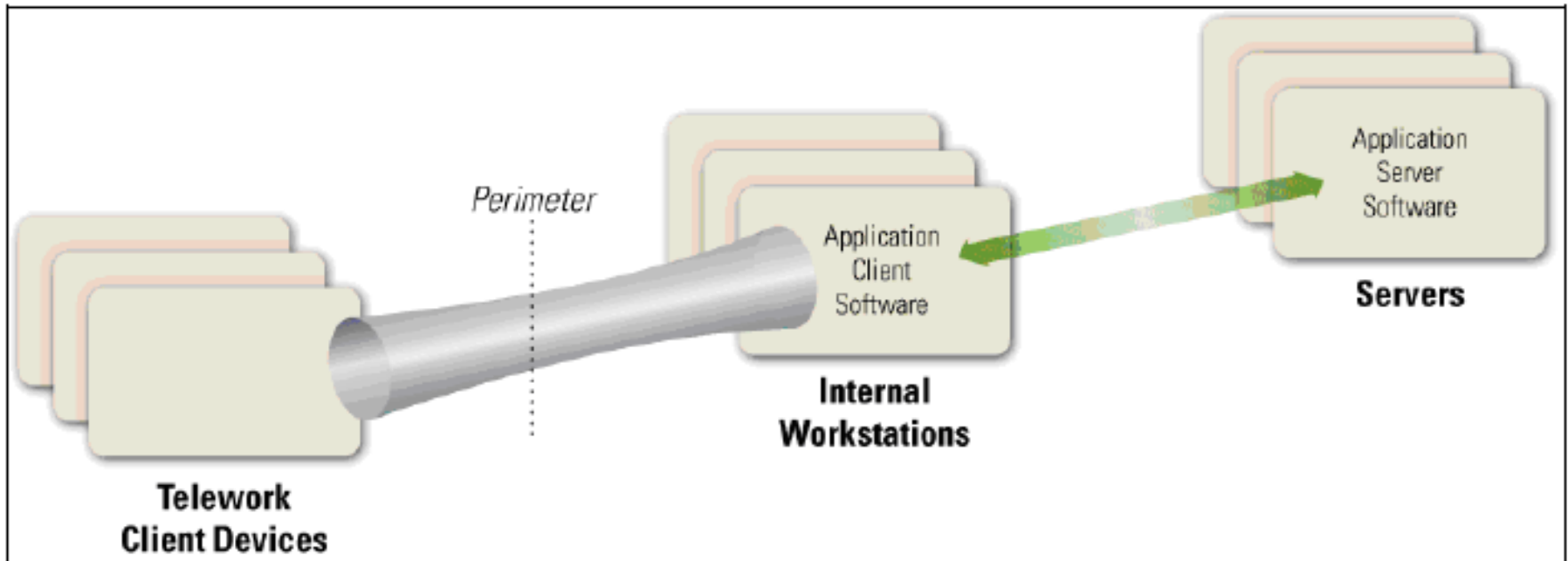


Figure 2-3. Remote Desktop Access Architecture

Source:

<http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf>

Direct Application Access Architecture

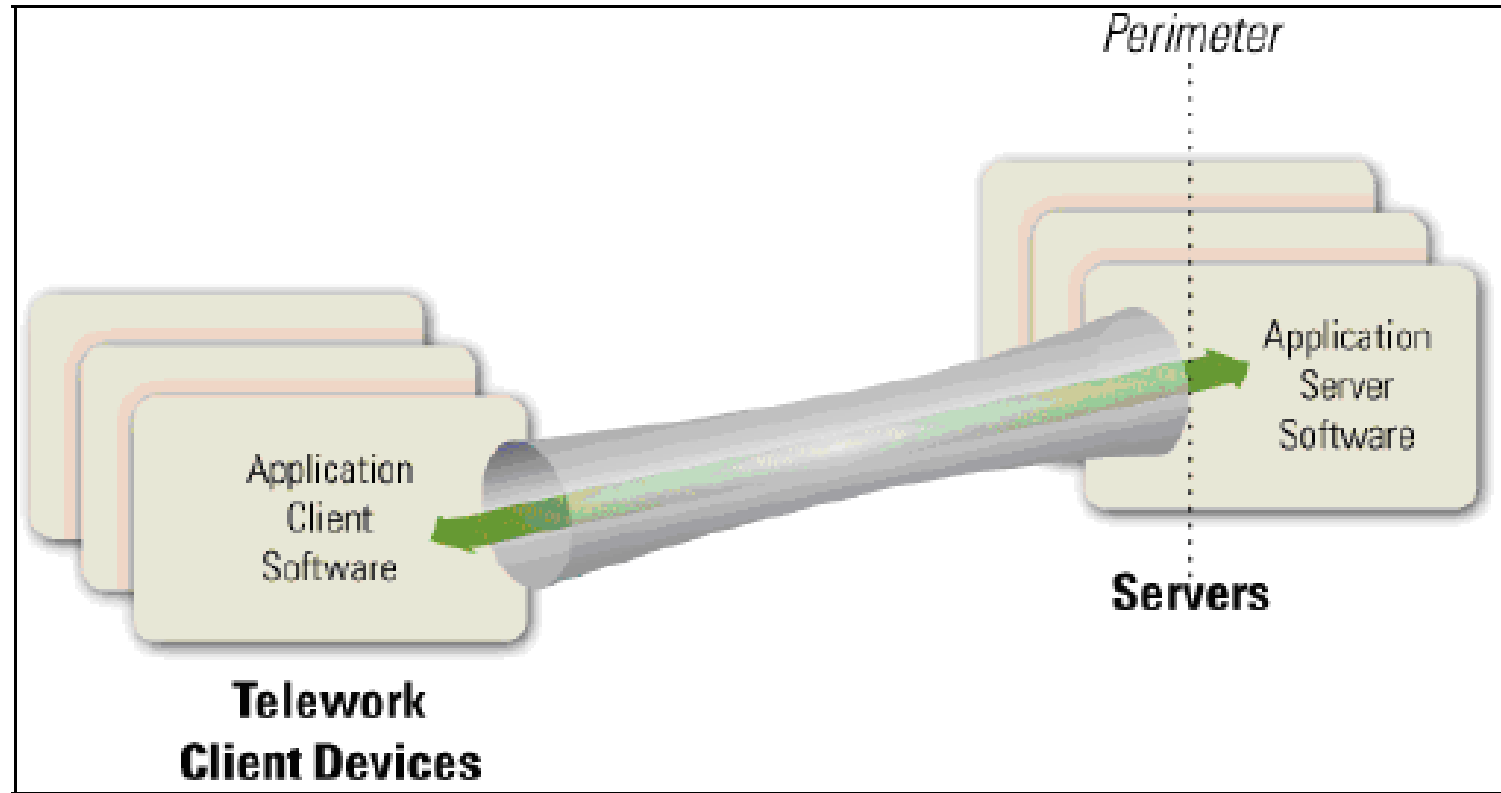


Figure 2-4. Direct Application Access Architecture

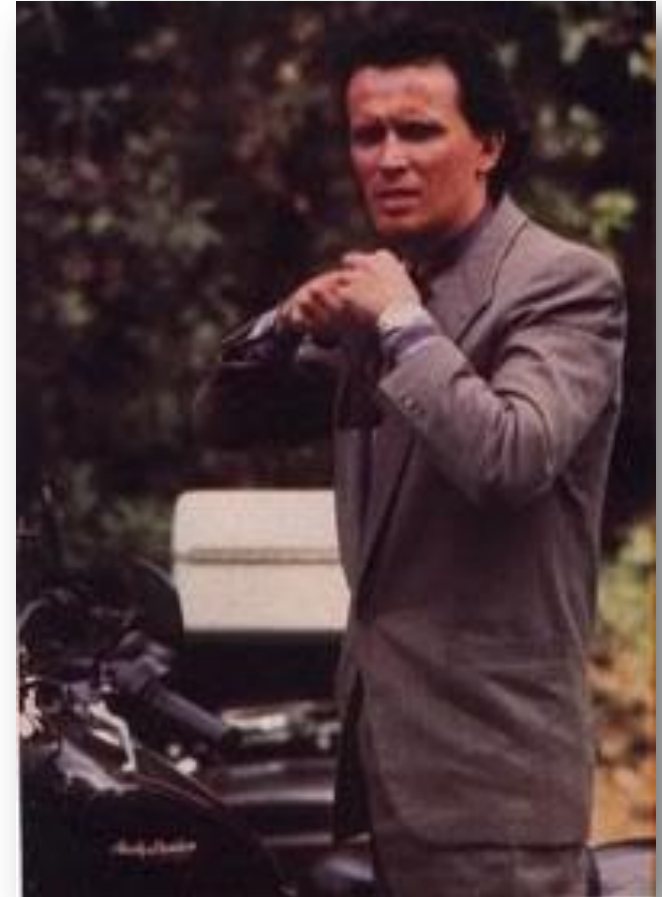
Source:

<http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf>

Famous Quotes

Famous Quote 1

- “No matter where you go, there you are...”
 - Buckaroo Banzai



Famous Quote 2

- “90% of Life is just showing up...”
 - Woody Allen



Of the remaining ten per cent, five per cent is getting started, one per cent is following the directions, and three per cent is finishing. The remaining one per cent of life is a mystery. -Jay Detweiler

Conclusions

Conclusions

- Teleworking works!
- Makes teleworkers happy
- Saves time and money
- Can be managed well, if you understand the risks, challenges, security needs, administrative requirements, AND you have the right People, Processes, and Technologies in place
- If the Customer does teleworking and understands it, and is happy with the results, then it makes good business sense
- Reduce your organizational and business risks: Get your teleworkers trained, create policies, get signed agreements, and have telework work plans
- Consider the security risks and understand and utilize best practices in teleworking security



Questions?



Source: <http://www.ivc.ca/images/Boss%20telework.jpg>



Supplemental Slides

References

- Amigoni, M. and Gurvis, S. (2009). Managing the Telecommuting Employee: Set Goals, Monitor Progress, and Maximize Profit and Productivity. Avon, MA: Adams Media.
- Brewer, D. and Nash, M. (2010). Insights into the ISO/IEC 27001 Annex A. Retrieved from the web at Retrieved from the web at <https://buildsecurityin.us-cert.gov/swa/downloads/McCumber.pdf> on August 1, 2012.
- Chickowski, E. (2008). Telework Tips: 4 Strategies for Leading Remote Workers. An article published at the Baseline.com website on June 25, 2008. Retrieved from <http://www.baselinemag.com/c/a/IT-Management/Telework-Tips-4-Strategies-for-Leading-Remote-Workers/> on June 25, 2012.
- Congress. (2010). Telework Enhancement Act of 2010. Retrieved from <http://www.gpo.gov/fdsys/pkg/BILLS-111hr1722enr/pdf/BILLS-111hr1722enr.pdf> on June 25, 2012.
- Dinnocenzo, D. (2006). How to Lead from a Distance: Building Bridges in the Virtual Workplace. Flower Mound, TX: The WALK THE TALK Company.
- Fischer, K. (2000). The Distance Manager: A Hands On Guide to Managing Off-Site Employees and Virtual Teams. New York, NY: McGraw-Hill.
- Froggatt, C. C. (2001). Work Naked: Eight Essential Principles for Peak Performance in the Virtual Workplace. New York, NY. Jossey-Bass Business & Management.

References

- Gilbert, J. (2008). 10 signs that you aren't cut out to be a telecommuter. An article published on January 8, 2008 at TechRepublic.com. Retrieved from <http://www.techrepublic.com/blog/10things/10-signs-that-you-arent-cut-out-to-be-a-telecommuter/290?tag=content;siu-container> on June 25, 2012.
- ISO. (2013) "Information technology – Security techniques – Information security management systems – Requirements", ISO/IEC 27001:2013.
- Lojeski, K. S., and Reilly, R. R. (2008). Uniting the Virtual Workforce: Transforming Leadership and Innovation in the Globally Integrated Enterprise. Redmond, WA: Microsoft Corporation.
- Nilles, J. M. (1998). Managing Telework: Strategies for Managing the Virtual Workforce. New York, NY: John Wiley & Sons.
- OPM and GSA. (2011). Teleworking fundamentals for Managers. Retrieved from http://www.telework.gov/tools_and_resources/training/managers/index.aspx on June 25, 2012.
- OPM and GSA. Annual Report of Teleworking – 2012. Retrieved from http://www.telework.gov/Reports_and_Studies/Annual_Reports/2012teleworkreport.pdf on July 12, 2012.
- Policy Shield. (2011). Information Security Policies Written to Mitigate Risk Under the ISO 27001 Security Compliance Framework. Retrieved from <http://www.informationshield.com> on March 15, 2011.
- SANS. (2001). Mitigating Teleworking Risks. Retrieved from http://www.sans.org/reading_room/whitepapers/telecommunting/mitigating-teleworking-risks_314 on June 25, 2012.

References

- Scarfone, K. and Souppaya, M. (2007). NIST SP 800-114 User's Guide to Securing External Devices for Telework and Remote Access. NIST: Washington, DC. Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf> on June 25, 2012.
- Scarfone, K., et al. (2009). NIST SP 800-46, rev 1 - Guide to Enterprise Telework and Remote Access Security. NIST: Washington, DC. Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf> on June 25, 2012.
- Telework Collaborative. (2012). Managing Telework. An article published at the Retrieved from the web at the Telework Arizona website. Retrieved from <http://www.teleworkarizona.com/mainfiles/supervisor/smanagingtelework.htm> on June 25, 2012.
- Tuutti, C. (2012). Why federal managers resist telework. An article published at the Federal Computer Week website (www.fcw.com). Retrieved from http://fcw.com/articles/2012/07/11/reasons-federal-managers-resist-telework.aspx?s=fcwdaily_120712 on July 12, 2012.

More Important Resources from the Web

Resource Sites

Site Name	URL
Home Computer Security	http://www.us-cert.gov/reading_room/HomeComputerSecurity/
Information for New and Home Users	http://www.cert.org/homeusers/
Interagency Telework Site	http://www.telework.gov/
NIST Security Configuration Checklists Program for IT Products	http://checklists.nist.gov/
Security at Home	http://www.microsoft.com/protect/default.msp#
Stay Safe Online	http://www.staysafeonline.info/

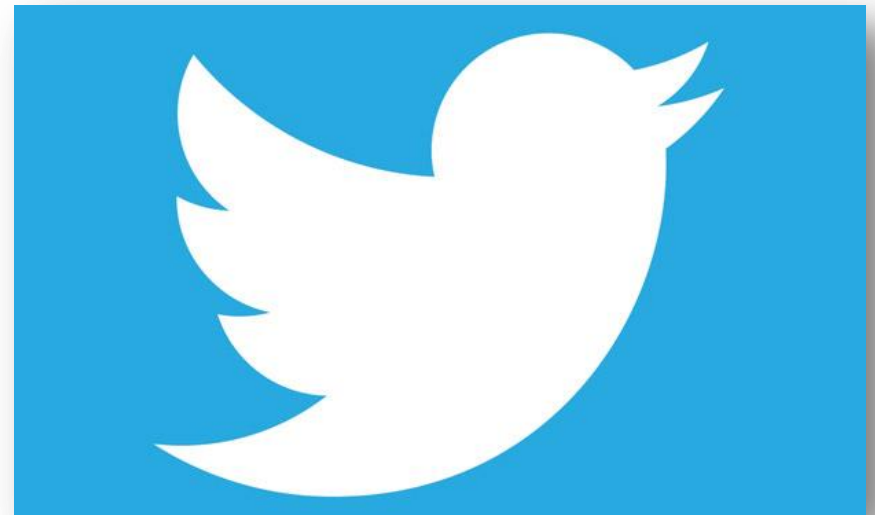
Documents

Document Title	URL
NIST SP 800-48 Revision 1, <i>Wireless Network Security for IEEE 802.11a/b/g and Bluetooth</i>	http://csrc.nist.gov/publications/PubsSPs.html
<i>Safe at Any Speed</i>	http://www.staysafeonline.org/basics/resources/FTCsafeatanysspeed.pdf
<i>Seven Simple Computer Security Tips for Small Businesses and Home Computer Users</i>	http://www.infragard.net/library/seven_tips.htm

More Important Resources from the Web

Some Teleworking Hashtags on Twitter

#Teleworking
#Telework
#Teleworkers
#Telecommuting
#Telecommute
#RemoteJobs
#Remotework
#RemotePositions
#WorkFromHome



Presenter Bio:

William Favre Slater, III

- Mr. Slater is a Senior IT Project Manager, Program Manager, senior IT consultant, and author who lives in Chicago and works in the Chicago area. He has worked in Information Technology since 1977, and his cybersecurity experience has spanned more than 30 years.
- Specialties Include: Cloud Computing, IT Security, Information Security, Cybersecurity, Disaster Recovery, Business Continuity, Crisis Management, Business Resiliency, Business Analysis, System Analysis, IT Infrastructure Management, Technical Architecture, Data Center Operations, Data Center Development, Cyberforensics, Cyberwarfare, Social Engineering, Risk Management, Incident Management, Problem Management, IT Change Management, Application System Development, Database Administration, Data Architecture, Technical Service Development, Service Management and Service Transition, Technical Leadership, and Technical Training
- Since the 1990s, he has worked on several significant projects related to Data centers and Cybersecurity. These included ISO 27001-based Information Security Management System implementations, security reviews, auditing, managing a Cloud Mega Data Center for Microsoft, and working as a subject matter expert on projects with Data Center vendors and other local businesses. He has also done security assessments related to Business Continuity, Disaster Recovery and Crisis Management Readiness at a major Health Care Insurance organization.
- Mr. Slater is an internationally published author on Cybersecurity topics related to Cyberwarfare, Social Engineering and various other topics.
- Mr. Slater has taught for seven years as an Adjunct Professor at the Illinois Institute of Technology and developed and delivered courses on these topics: the Illinois Institute of Technology in the areas of Data Center Operations, Data Center Architecture, Information Technology hardware and software, Java and Object-Oriented Software Development, Cybersecurity Management, and IT in Public Administration.
- Mr. Slater has earned an M.S. in Cybersecurity (2013, Bellevue University, Bellevue, NE), as well as an M.S. in Computer Information Systems (2004, University of Phoenix, Phoenix, AZ), and an MBA (2010, University of Phoenix, Phoenix, AZ). He has also earned 79 professional certifications, including a PMP, CISSP, CISA, SSCP, ISO 27002, and a CDCP.
- Mr. Slater is on a personal Mission to help make the world a better, safer and more productive place, especially when it means helping his students and colleagues become smarter about cybersecurity, Data Centers, the Internet, and other exciting areas of Information Technology.



William Favre Slater, III
Project Manager / Program Manager
slater@billslater.com
williamslater@gmail.com
Career Page: <http://billslater.com/career>
LinkedIn:
<http://www.linkedin.com/in/billslater>
Twitter: <http://twitter.com/billslater>

Certified Teleworker

2/20/2012

telework.gov

Telework Fundamentals - Manager Training

Certificate of Completion

awarded to:

William F. Slater, III