Telework:
Risks, Challenges, Perils, and Successes

William F. Slater, III, M.S., MBA, PMP, CISSP, SSCP, CISA, CDCP
IT Project Manager and Adjunct Professor, IIT School of Applied Technology

-and-

Melanie Thompson, B.S.
Graduate student in Cyber Forensics and IT Security at IIT
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. In 2010, the Federal Telework Act was signed into law providing 10s of thousands of Federal workers the option to perform much of their work from home.

• However, telework is often misunderstood, and has its own unique risks, challenges, and perils.

• In fact, if a manager is not properly planning how and when his or her staff will perform telework, that in itself can provide a formidable barrier to success.

• This presentation will provide a good look at what teleworking is and how to deal with the risks, challenges, and perils of telework. It will also provide proven tips to make you and your organization a successful organization where telework is part of the culture, and an acceptable, productive way of working.
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 one or more time zones.
- Connected via secure Internet connections, usually from the employees’ homes
- E-Mail
- Teleconference meetings, via phone
- Phone calls
- Live Meeting
- Live Communicator
- Interaction with Management, Team members, and the Customer
- Work is initially performed on company-supplied laptops after onboarding
- Occasional business trips, lasting from 4 to 5 days
Teleworking Advantages

• Talent
• Productivity
• Diversity
• Minimal infrastructure
• Cost savings
• Ecological
• Work - life balance
• Individual control
• Good for Employee Morale
To have a Successful Teleworking Organization, create a Culture that is:

• Supportive
• Electronically Connected and responsive
• Collaborative
• Informal to Semi-formal
• Mutual respect
• Responsive and Customer-focused
• Semi-autonomous
• Self-managed
• Typical of IT Professionals who Telecommute
Other Critical Requirements for Successful Teleworking

- Telework Policy
- Telework Security Plan
- Telework Agreement
- Telework Schedule
- Telework Work Plan
- Telework Communications Plan

Source: http://www.telework.gov
Telework Risks
## 10 Telework Risks

<table>
<thead>
<tr>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing Employees, Unproductive Behaviors, Lack of Personal Accountability</td>
</tr>
<tr>
<td>Risk of unauthorized physical access to corporate information stored on a remote PC</td>
</tr>
<tr>
<td>An “always on connection” can be a likely target for attackers and malware.</td>
</tr>
<tr>
<td>Bridging networks from remote Home Networks to Corporate Networks creates the opportunity for Zombies, botnets and other serious malware.</td>
</tr>
<tr>
<td>Teleworker behavior associated with downloading of unauthorized programs.</td>
</tr>
<tr>
<td>Lack of Telework Training</td>
</tr>
<tr>
<td>Lack of Telework Policies</td>
</tr>
<tr>
<td>Lack of Telework Agreement</td>
</tr>
<tr>
<td>Lack of Telework Schedule</td>
</tr>
<tr>
<td>Lack of Telework Work Plan</td>
</tr>
</tbody>
</table>
Telework Challenges
<table>
<thead>
<tr>
<th>Category</th>
<th>Challenge</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management and Teams</td>
<td>Meeting Customer Expectations</td>
<td>Always show the Customer that we are Customer-focused and listening to his expectations.</td>
</tr>
<tr>
<td>Management</td>
<td>Managing across Time Zones</td>
<td>Ask for flexibility and adaptability.</td>
</tr>
<tr>
<td>Management and Teams</td>
<td>Collaboration Across Time Times</td>
<td>Ask for flexibility and adaptability.</td>
</tr>
<tr>
<td>Management and Teams</td>
<td>Getting Access to Government Furnished Equipment and Customer Resources</td>
<td>Alerted the Customer about the issue(s).</td>
</tr>
<tr>
<td>Management and Teams</td>
<td>Meeting Schedule Challenges</td>
<td>Hire professionals that rise to meet the challenge.</td>
</tr>
<tr>
<td>Management</td>
<td>Keeping Team Members Productive, Engaged, and Motivated in spite of the Challenges</td>
<td>Hire professionals that rise to meet the challenges.</td>
</tr>
<tr>
<td>Management and Teams</td>
<td>Attending meetings and still getting work done and avoiding burnout</td>
<td>Hire professionals that rise to meet the challenge.</td>
</tr>
<tr>
<td>Management and Teams</td>
<td>Technical Support</td>
<td>Ensure that people are available and that they have back-ups.</td>
</tr>
<tr>
<td>Management and Teams</td>
<td>Meeting Customer Management Expectations and Report Schedules</td>
<td>Hire professionals that rise to meet the challenge.</td>
</tr>
<tr>
<td>Management and Teams</td>
<td>Meeting Management Expectations and Reports Schedules</td>
<td>Hire professionals that rise to meet the challenge.</td>
</tr>
</tbody>
</table>
## 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

Telework Perils
# Telework Perils

<table>
<thead>
<tr>
<th>Top Telework Perils</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Breach</td>
</tr>
<tr>
<td>Network Security Breach</td>
</tr>
<tr>
<td>Unauthorized Physical Access to Corporate Information on a Remote PC</td>
</tr>
<tr>
<td>An “always on connection” Acting as a Target for Attackers and Malware</td>
</tr>
<tr>
<td>Unwillingness or inability to abide by Telework Policies and Procedures creates vulnerability for the organization and introduces excessive risk.</td>
</tr>
</tbody>
</table>
## Lessons Learned the Hard Way

<table>
<thead>
<tr>
<th>Event</th>
<th>Lesson</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>The MIA Java Developer</td>
<td>Randomly check up on Team members</td>
<td>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.</td>
</tr>
<tr>
<td>Who let the dogs out?</td>
<td>Remember that your home environment becomes part of your teleconference meetings.</td>
<td>The organization published and distributed Phone Etiquette guidelines.</td>
</tr>
<tr>
<td>Don’t forget that Mute Button!</td>
<td>Remember to use the mute button during teleconference meetings.</td>
<td>The organization published and distributed Phone Etiquette guidelines.</td>
</tr>
<tr>
<td>You can’t be a Baby Sitter AND a Business Analyst...</td>
<td>You cannot baby-sit your kids while you are working from home.</td>
<td>The Customer forbids this and so do most companies.</td>
</tr>
</tbody>
</table>
Telework Successes
Some Success Stories

• 2010: CACI wins several U.S. Government contract Task Orders, built a 48-person Team to telework 100%, and the Customer was very pleased with the deliverables

• 2011: The 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
- Lay the groundwork for success, covering People, Processes, and Technology
Laying the Groundwork 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
- Strong employees with successful track records
- Creation of work plans and schedules that are aligned with the Customer’s requirements and demands
- Flexibility with the Customer’s requirements and demands
- Executing on our plans
- Reporting the results
- Sharing the feedback and kudos, bad and good
- Make adjustments and improvements when necessary
- Shared vision for success
Pearls of Wisdom for Teleworking

Managing Telework

• Being open and flexible will allow you and your organization to get the most from telework – 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.**
• Look for telework opportunities to improve marginal employees’ performance.
• Be sensitive to the impact telework has on non-teleworkers
• Communicate in a timely, candid, and constructive manner with employees.

Source: The Telework Collaborative -
Other Benefits: Cost Savings

(Billions with a “B”)

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...

- 30-40% increase in overall productivity
- 40 minutes of additional productivity generated for every 60 minutes saved on commuting
- 10 days saved per teleworker on average every year
- 1176 employees spared traffic injuries and deaths every year
- $136 million saved in accident costs
- $250 million collectively saved in gas costs ($362 saved per teleworker each year)

$5.4 BILLION IN TOTAL SAVINGS

Source: Deloitte analysis

Graphic: Deloitte University Press | DiPPress.com
Security & Teleworking
Security Risk Management

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

Source:
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

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

Training, Training, Training

- Adequately vet candidates for hire
- Establish a 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

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 cyber security incident.

Source:
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:
Table of Contents

Executive Summary..........................ES-1

1. Introduction.........................................................1-1
   1.1 Authority......................................................1-1
   1.2 Purpose and Scope............................................1-1
   1.3 Audience......................................................1-1
   1.4 Document Structure..........................................1-1

2. Overview of Telework Technologies..................2-1
   2.1 Remote Access Methods.................................2-1
   2.2 Telework Devices.............................................2-2
   2.3 Telework Device Security Overview.....................2-3

3. Securing Information.................................3-1

4. Securing Home Networks and Using External Networks...4-1
   4.1 Wired Home Networks.......................................4-1
   4.2 Wireless Home Networks....................................4-2
   4.3 External Networks..........................................4-4

5. Securing Telework PCs..............................5-1
   5.1 Software Updates...........................................5-1
   5.2 User Accounts and Sessions...............................5-2
      5.2.1 Use Accounts with Limited Privileges...............5-2
      5.2.2 Protect Accounts with Passwords.....................5-2
      5.2.3 Protect User Sessions from Unauthorized Physical Access...5-3
   5.3 Networking Configuration...............................5-3
      5.3.1 Disable Unneeded Networking Features.............5-3
      5.3.2 Limit the Use of Remote Access Utilities........5-4
      5.3.3 Configure Wireless Networking......................5-4
   5.4 Attack Prevention...........................................5-4
      5.4.1 Install and Configure Antivirus and Antispyware Software...5-5
      5.4.2 Use Personal Firewalls................................5-6
      5.4.3 Enable and Configure Content Filtering Software........5-7
   5.5 Primary Application Configuration....................5-8
      5.5.1 Web Browsers...........................................5-8
      5.5.2 Email Clients...........................................5-10
      5.5.3 Instant Messaging Clients............................5-11
      5.5.4 Office Productivity Suites..........................5-11
   5.6 Remote Access Software Configuration...............5-11
   5.7 Security Maintenance and Monitoring................5-12

6. Securing Telework Consumer Devices................6-1

7. Considering the Security of Third-Party Devices.....7-1

Source:
NIST SP 800-46

Guide to Enterprise Telework and Remote Access Security

Recommendations of the National Institute of Standards and Technology

Source:
Secure Telecommuting Concepts

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

Tunneling (VPN) Architecture

Figure 2-1. Tunneling Architecture

Portal Architecture

Remote Desktop Access Architecture

Figure 2-3. Remote Desktop Access Architecture

Direct Application Access Architecture

Figure 2-4. Direct Application Access Architecture

Famous Quotes
Famous Quote

• “No matter where you go, there you are...”
  – Buckaroo Banzai
Famous Quote

• “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
• 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

References


References


More Important Resources from the Web

### Resource Sites

<table>
<thead>
<tr>
<th>Site Name</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information for New and Home Users</td>
<td><a href="http://www.cert.org/homeusers/">http://www.cert.org/homeusers/</a></td>
</tr>
<tr>
<td>Interagency Telework Site</td>
<td><a href="http://www.telework.gov/">http://www.telework.gov/</a></td>
</tr>
<tr>
<td>NIST Security Configuration Checklists Program for IT Products</td>
<td><a href="http://checklists.nist.gov/">http://checklists.nist.gov/</a></td>
</tr>
<tr>
<td>Security at Home</td>
<td><a href="http://www.microsoft.com/protect/default.mspx">http://www.microsoft.com/protect/default.mspx</a></td>
</tr>
<tr>
<td>Stay Safe Online</td>
<td><a href="http://www.staysafeonline.info/">http://www.staysafeonline.info/</a></td>
</tr>
</tbody>
</table>

### Documents

<table>
<thead>
<tr>
<th>Document Title</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST SP 800-48 Revision 1, Wireless Network Security for IEEE 802.11a/b/g and Bluetooth</td>
<td><a href="http://csrc.nist.gov/publications/PubsSPs.html">http://csrc.nist.gov/publications/PubsSPs.html</a></td>
</tr>
<tr>
<td>Safe at Any Speed</td>
<td><a href="http://www.staysafeonline.org/basics/resources/FTCsafetanyspeed.pdf">http://www.staysafeonline.org/basics/resources/FTCsafetanyspeed.pdf</a></td>
</tr>
</tbody>
</table>
Presenter Bio:
William F. Slater, III: An Introduction

- 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.


- He is presently working as a senior IT consultant Project Manager on a software migration project in a U.S. Government agency. 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 F. Slater, III

Current Positions –
Project Manager / Sr. IT Consultant at a Medium-sized Government Contracting Organization, President & CEO of Slater Technologies, Inc. , and Adjunct Professor at the Illinois Institute of Technology - Working on projects related to

- Software Development and Migration at a large U.S. Government Agency
- Security reviews and auditing
- ISO 27001 Project Implementations
- Subject Matter Expert for preparing Risk Management and Security Exams at Western Governor’s State University in UT
- Created an eBook with articles about Security, Risk Management, Cyberwarfare, Project Management and Data Center Operations
- Providing subject matter expert services to Data Center product vendors and other local businesses.
- Also developing and presenting technical training materials for undergraduate and graduate students at the Illinois Institute of Technology in the areas of Data Center Operations, Data Center Architecture, Cyber Security Management, and Information Technology hardware and software.
Certified Teleworker
Melanie Thompson works in the Chicago area as a Congressional Aide for the federal government. Melanie received a Bachelor's of Science degree in Business Administration from California State University, Stanislaus. She is presently pursuing a Master's degree in Cyber Forensics and Security from the Illinois Institute of Technology (IIT). Melanie serves as President of the High Technology Crime Investigation Association school charter at IIT. In her spare time she is a member of several local organizations including the Chicago Council on Global Affairs, the FBI Chicago Citizens' Academy Alumni Association, the Chicago Electronic Crimes Task Force and is a volunteer Wish Granter for the Make A Wish Foundation-Illinois Chapter. Melanie prides herself on continually striving for opportunities that will positively enhance the Chicago community and beyond.