The Remote Workforce: Managing IT and Cyber Security Risks
WEBCAST SERIES

HOST
Peter Stanton
Publisher/CEO
New England Business Media

MODERATOR
Allen Falcon
CEO, Cumulus Global

WEBCAST PANELISTS
Michelle Drolet
Founder & CEO, Towerwall

Patty Patria
Vice President for Information Technology and CIO, Worcester Polytechnic Institute
The Remote Workforce: Managing IT and Cyber Security Risks
Risks & Challenges

- Phishing / Ransomware / etc.
  - Personal Computers with Multiple Users
  - Older Hardware with Weak Malware Protections

- Applications
  - Business versus Consumer Versions
  - Access to in-house systems

- Access: Security / Performance / Easy of Use

- Phone Services
Put a Policy in Place

- Clear Expectations
- Company Responsibilities
- Employee Responsibilities
- Mutual Commitments

https://bit.ly/PersonalUsePolicy
### Platform + Access + Protection

#### Platform
- Devices Must Meet Requirements
- Resources
  - Bandwidth
  - Business Software
  - Files
  - Phones
- Accessorize
  - Headsets
  - External Monitors

#### Access
- Secure Network or VPN Connection
- Remote Desktop / VDI
- Desktop Integration
  - Drive File Stream
  - OneDrive Client
- Unified Communications
# Platform + Access + Protection

<table>
<thead>
<tr>
<th>Protection</th>
<th>Exit Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>NextGen EndPoint Protection</td>
<td>Rescind Access</td>
</tr>
<tr>
<td>Web / DNS Protection</td>
<td>Remove Software</td>
</tr>
<tr>
<td>Encrypt Disks / Files</td>
<td>Reclaim Licenses</td>
</tr>
<tr>
<td>Backup / Recovery</td>
<td>Recovery / Remove Data</td>
</tr>
<tr>
<td>PC Continuity</td>
<td>Know What You Will Leave Behind</td>
</tr>
</tbody>
</table>
The Remote Workforce: Managing IT and Cyber Security Risks
Moving to Remote Operations

• WPI moved from fully on-site work to fully remote work in 3 weeks by deploying new technology, helping faculty with remote teaching tools and providing remote software lab options for students.

• Taught 200+ faculty and staff how to use Zoom, Canvas, and Echo 360 to move classes and remote meetings fully on-line.

• In any given week, we have 9,500+ zoom meetings with 77,000+ participants, totaling 3.3 million minutes of meetings.
Moving to Remote Operations

• Students have viewed 434 pre-recorded lecture videos 58,000 times.

• Moved 6,000+ students to One Drive in a week to allow students to access files securely without VPN.

• Significantly increased the number of windows terminal servers and deployed new cloud based virtual desktops to support student remote course and lab work.
Moving to Remote Operations

• Deployed 70+ new soft phone clients to allow offices to answer main phones from their computers; offered all employees voicemail to email option for ease of use.

• Increased existing Virtual Private Network (VPN) capacity to allow all employees to work remotely; deployed new VPN to allow for secure student connections.
Cybersecurity Challenges with COVID-19

Phishing

• In April we saw a significant uptick of compromised accounts due to remote work and increase in COVID-19 related phishing.

• To mitigate, we required Multi-Factor Authentication (MFA) on all accounts flagged as High Risk.

• Looking to implement MFA on email for all employees, students, and alumni later this year which should reduce this in the future.
Cybersecurity Challenges with COVID-19

Zoombombings

• Although WPI did not experience any zoombombings, we have increased default zoom security and published educational articles for our faculty, staff and students around zoom security best practices.

Manage Zoom Settings For Better Security

https://hub.wpi.edu/spread/63/manage-zoom-settings-for-better-security
The Remote Workforce: Managing IT and Cyber Security Risks
10 Things I know about COVID-19 Scams

10) Pandemic Panic: Criminals thrive during a crisis, knowing people under stress and distraction are more prone to readily click a text or email link without thought to its legitimacy. As such, COVID-19-related phishing attacks grew 600% in Q1.

9) FTC Warnings: The Federal Trade Commission just reported $12 million in coronavirus scams calling it “tip of the iceberg” and warning of “low hanging fruit” brought on by at-home workers and “shadow IT operations” i.e., when employees run amuck with their own apps, systems and devices.

8) Robocallers purporting to offer “free COVID-19 test kits”, face masks, sanitizer and even fake cures, as a way to collect your personal and health insurance information, asking for payment over the phone.

7) Fake IDs: Text message scams impersonating the U.S. Department of Health and Human Services informs recipients that they must take a "mandatory online COVID-19 test".

6) Freed money: Scammers using Fed stimulus checks as a ruse to make people “verify” their personal information or bank account details in order to "release" the funds.
10 Things I know about COVID-19 Scams (con’t.)

5) Charity Exploit: Phone calls and texts impersonating the World Health Organization (WHO), or the Centers for Disease Control (CDC) falsely making donation requests or promising safety measures for protecting against coronavirus.

4) Leaky Indeed: Consumers receiving robocalls from HVAC duct cleaners that promise to "protect" your home, office, and family from the deadly coronavirus.

3) Job/Loan Scams: Beware of sudden COVID-19 themed work-from-home opportunities, alleged student loan forgiveness or repayment plans, SBA loans, online listing verification, debt consolidation offers.

2) Connectivity scare: Internet routers used from home are being targeted by DNS hijacking attacks that redirect users to fake COVID-19 resources; some Android users experience screen locking, forcing users to reset passwords.

1) Getting buy-in: Convince senior managers to take threats seriously: Conduct war games, asking the CEO to respond in real-time to worse-case scenarios proposed by cybersecurity experts.

Rule #1: The IRS, banks and government agencies will never ask for your personal or financial information via email, text, or phone. If this happens to you, beware, it’s probably fraud.
8 Best Practices to Secure Remote Workers in the New Normal

IT teams need to find compensating controls to manage the rapidly evolving and escalating cybersecurity situation. Here are some best practices that can help:

1) Take the time to sit down to ensure you’re prepared. Not taking time to do so can put you at risk of stressing systems that were never designed to scale. If you move quickly you can accidentally risk the security of your systems.

2) Look at business workflows; ensure your teams are covered for both remote and on-prem work. Take a good look at your infrastructure. Can your VPN support the additional load of more users? Do your existing collaboration tools pose bandwidth issues?

3) Acknowledge the norm has changed. Employee policies or rules of engagement must be put in place that define how workers conduct themselves when working from home.

4) Ensure your leadership is engaged and communicates regularly with employees.

5) Educate your teams to be vigilant about phishing attacks, especially those that carry a pandemic theme and ensure they follow cybersecurity hygiene.
8 Best Practices to Secure Remote Workers in the New Normal (con’t.)

6) There will be a sudden degradation of visibility into network activity as soon as endpoints leave corporate oversight. Here are solutions that can help regain some insight into your environment:
   • Enterprise VPN is a good solution to start with but there are bandwidth considerations and scaling issues.
   • Desktop virtualization (VDI) can be a potential solution for challenges around VPN scalability and performance.
   • Endpoint security or EDR (Endpoint detection and response) is a good vector of visibility back out into those devices that have gone home.
   • Single-sign-on, multi-factor authentication (MFA) can provide good visibility into what users are doing with their data.
   • CASB (Cloud Access Security Broker) solutions can help proxy all traffic through a central location and help monitor traffic.
7) Log collection must be a focus, always. Start from VPNs and SaaS applications like Office365. Once you have data in place you can ask different questions. Some log sources will carry more weight than others. Lead towards any critical infrastructure that you don’t have insight into or assets that have proprietary data. Invest in security tools that can provide visibility into tactics and techniques like phishing, denial of service, and ransomware.

8) Turn your attention to workers: what does their role look like day to day? That exercise can alone bubble visibility gaps. Another potential approach is to adopt a zero-trust cybersecurity model that allows access to applications that are relative to job roles. Such systems are more scalable than VPNs and can easily be integrated with SSO (single sign-on) platforms. The zero-trust approach also allows for creation of granular policies that can help define who can access what and from which device.

Remember that there is no one-size-fits-all strategy for securing a remote workforce. Adjustments will have to be made on the fly. Understand the shift to a new norm and regain control. Stay focused and vigilant.
Q & A