Remote Working: What We've Learned in the Past Year

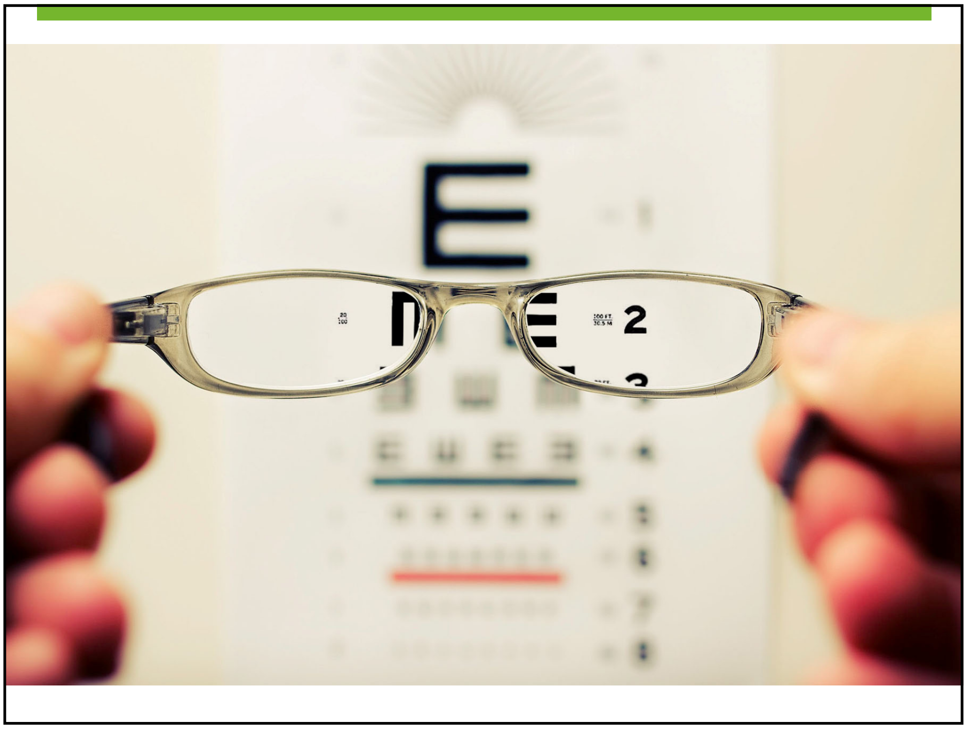
Allison Davis Ward, Partner
8.4.21

CAPINTECH

1

The content of this presentation, whether communicated in writing or verbally by partners, employees, or representatives of Capin Crouse LLP, is provided solely for educational purposes. This presentation is not intended to provide legal, accounting, investment, or fiduciary advice. Please contact your attorney, accountant, or other professional advisor to discuss the application of this material to your particular facts and circumstances.

2



3

Lesson 1: Expect the Unexpected

- Cannot predict the future
- Changes across all industries accelerating
- Must respond to threats and opportunities quickly
- No definitive timeline — evolution must continue!
- Need strategic foundation built on flexibility and adaptability

4

Lesson 2: Flexibility is the Key to Resiliency

- The rigid won't survive
- Strategically plan now with a focus on flexibility
- Allow yourself to be resilient in the future

5

Lesson 3: Technology Chokepoint

- Everything relies on support and input from IT
  - Infrastructure, system, and application support
  - Business continuity and disaster recovery
  - Supporting remote work environments
  - Implementing efficiencies
  - Managing vendor relationships
- Plan for efficiency, effectiveness, security

6

Lesson 4: Collaboration is Key

- Collaboration moves us forward
- Need efficient and effective ways to collaborate
- Many have not prioritized collaboration in planning
  - Ex: Zoom and “Zoombombing”
- Include all departments
- Internal and external needs

7

8

Trend Work: Hybrid Work Will Continue

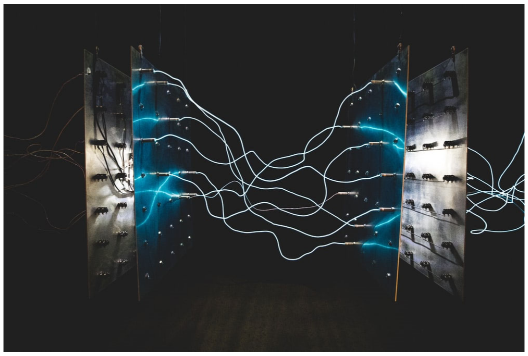
- Cutting ties to our physical location
  - Working from home
  - Investing in cloud technology
  - Expanding hiring pool
  - Reaching constituents and carrying out our mission in innovate ways

9

10

Collaboration Needs Connection

- Can’t have collaboration without connection
- Three major players
  - Amazon
  - Microsoft
  - Google



11

Focused on Cloud

- Numerous benefits by being cloud-focused
  - Availability
  - Accessibility
  - Centralization
  - Redundancy
  - Scalability

12

SmartVault

box

Dropbox

pCloud

OneDrive

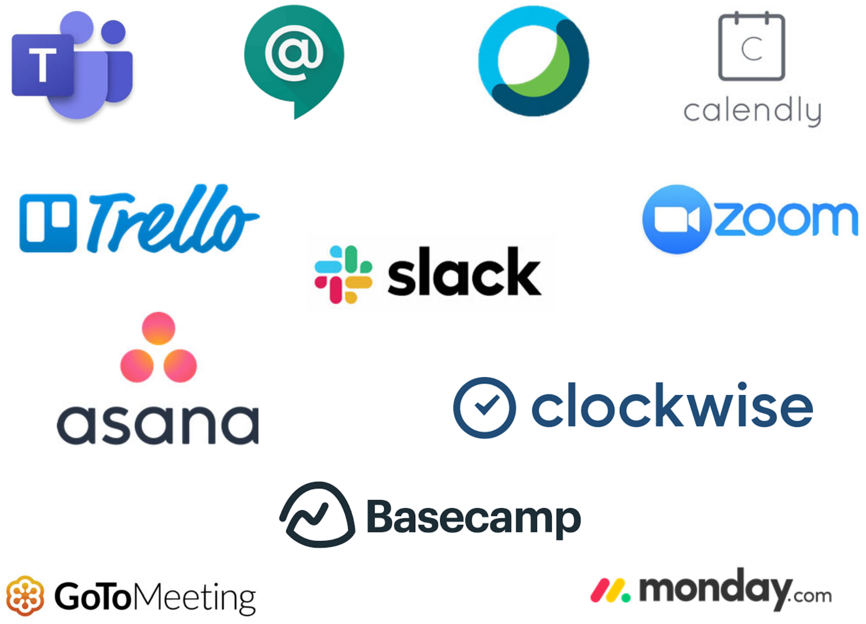
ShareFile®

13

Cloud Data Storage and Data Transfer

- Further cut ties with physical office
- Makes data accessible in a very easy way
- Can increase collaboration
  - Reduces duplication of files
  - Work at the same time

14



15

Collaboration Tools

- Help with efficiency and effectiveness
  - Managing teams
  - Audio and video conferencing solutions
  - Setting up meetings
- Can reduce number of emails (!!!)
- How effectively did we collaborate during the pandemic?

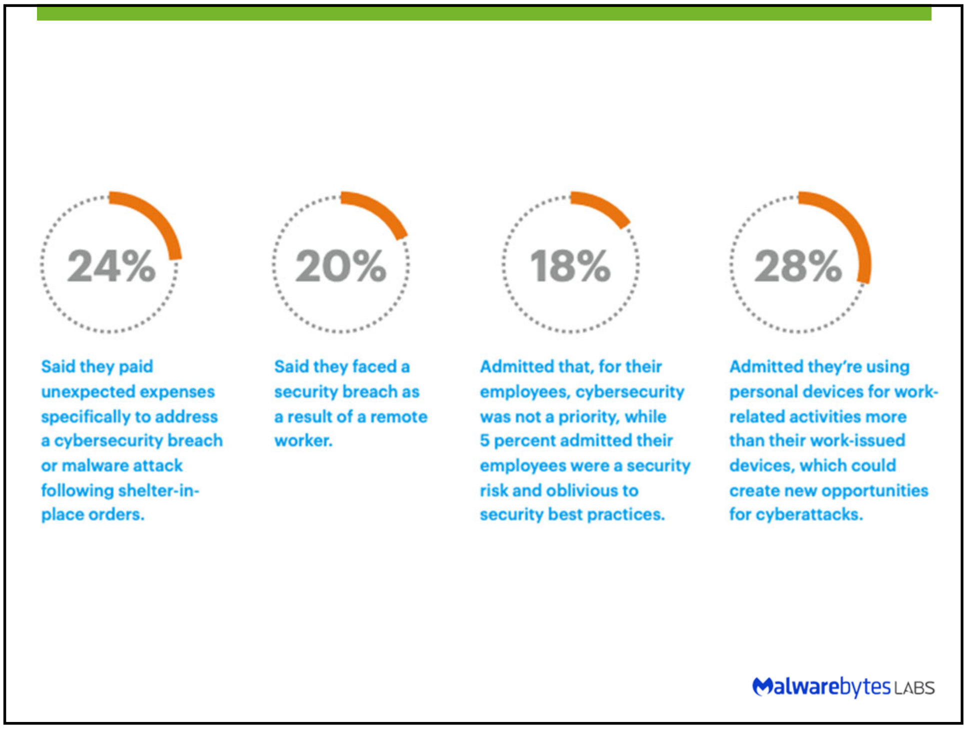
16

Make Your Tools Work for You

- Overwhelming number of choices
- Consider ease of use
- Consider integrations and compatibility
  - Internal and external usage
- Don’t create more problems
- Define acceptable usage

17

18



24% Said they paid unexpected expenses specifically to address a cybersecurity breach or malware attack following shelter-in-place orders.

20% Said they faced a security breach as a result of a remote worker.

18% Admitted that, for their employees, cybersecurity was not a priority, while 5 percent admitted their employees were a security risk and oblivious to security best practices.

28% Admitted they're using personal devices for work-related activities more than their work-issued devices, which could create new opportunities for cyberattacks.

Malwarebytes LABS

19

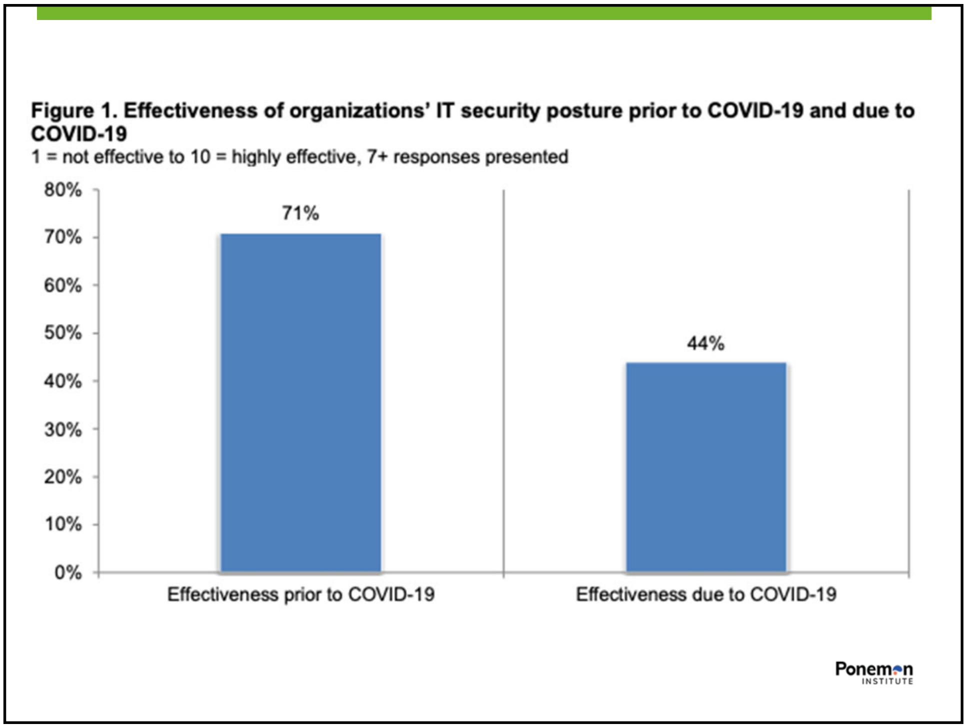


Figure 1. Effectiveness of organizations' IT security posture prior to COVID-19 and due to COVID-19

1 = not effective to 10 = highly effective, 7+ responses presented

Ponemon INSTITUTE

20

Blurred Lines & Blindspots Study

- Employees take more risks than they would in office
  - 27% knew they shouldn’t share devices but felt they had no choice
  - 69% of workers have used personal laptop, printer, or scanner for work activities
- Bad actors know remote workers are vulnerable
- Limitations in how we manage endpoints
  - Cannot rely solely on perimeter security

21

Strategically Planning for Security

- Third-party risk management
- Enhanced authentication
- Data management
- Endpoint management
- End-user awareness and support
- Adaptive security

22

Risks from Relying on Third Parties

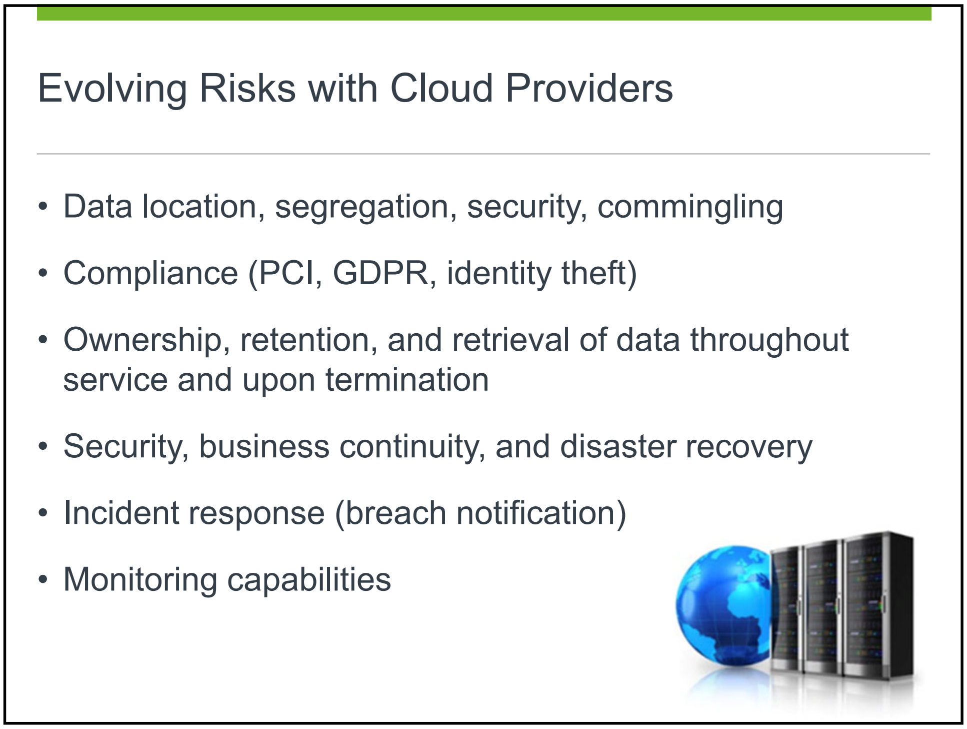
- Business, financial, and reputational risks
- Data loss via deletion, corruption, or alteration
- Comingling of data
- Unauthorized access
- Malware
- The list continues…

23

Third-Party Risk Management

- Retroactive due diligence
- Classification and inclusion in annual review
  - Cloud hosting and file transfer
  - Collaboration tools
  - Existing vendors with increased risk profile
- Controls for mitigating third-party risks should drive strategic plan

24



Evolving Risks with Cloud Providers

- Data location, segregation, security, commingling
- Compliance (PCI, GDPR, identity theft)
- Ownership, retention, and retrieval of data throughout service and upon termination
- Security, business continuity, and disaster recovery
- Incident response (breach notification)
- Monitoring capabilities

25

You Can’t Outsource the Oversight

26

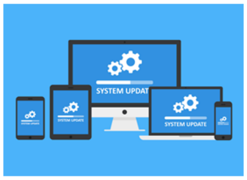
Enhanced Authentication and Data Management

- Single sign-on (SSO) solutions
  - Enhanced passwords and lockout settings
  - Multi-factor authentication and IP restrictions
  - User access management
  - Insight into devices being used
- Data management and data loss prevention (DLP)

27

Endpoint Management

- Enhanced inventorying and tracking
- Centralized management and monitoring
  - “Over the air” functionality
  - Enforcement of security policies
  - Limiting local administrative rights
  - Revisiting encryption management



28

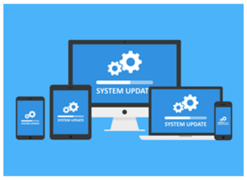
Endpoint Management – Mobile Devices

- Mobile device management (MDM)
  - Containerization
  - Restricting what can be accessed on device
  - Enforcing critical controls
  - Data loss prevention
- Limit impact to personal data

29

Endpoint Management – Home Office

- Update and secure across home network
- Secure router, streaming devices, voice assistants, appliances, smart home devices
- Separate home/guest wireless from business
- Consider risk of obsolete devices
- Reinforce employee awareness



30

End-User Awareness and Support

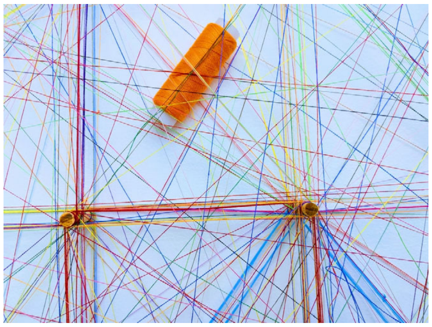
- Increase awareness around evolving threats
  - Phishing, ransomware, etc.
  - Home office security
  - Wireless networks
  - Devices used to access work data
  - Incident management and reporting
  - Shadow IT

Build Culture of Awareness

- Culture comes from the top – all should participate
- Find right method for your staff
- Tailor training for high-risk departments/staff
  - Roundtable testing
  - Discuss real-world examples
  - Walk through incident response plan

Biggest Challenges to Security in Hybrid Work

- Perimeter controls not comprehensive
  - Do not cover lateral movement if network penetrated
  - Do not cover all sources of data and endpoints (e.g., on-site, home office, vendor)
- Requires investment

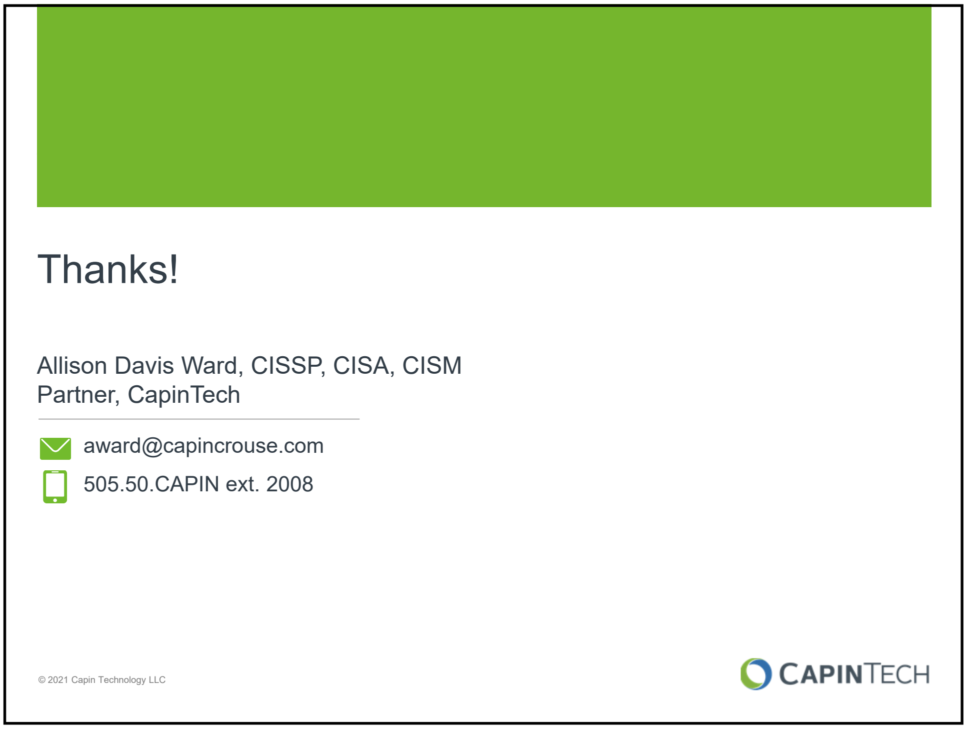


33

Shift Controls to Support Adaptive Security

- Controls need to be deep and wide
- Prevention + detection + response (add: prediction)
- Use behavioral learning and artificial intelligence for better monitoring and continuous learning/evolution
  - Ex: enhanced email filtering
  - Ex: ransomware controls

34



Thanks!

Allison Davis Ward, CISSP, CISA, CISM
Partner, CapinTech

✉ award@capincrouse.com
📱 505.50.CAPIN ext. 2008

CAPINTECH

35