Katy Area EDC

HR Networking Group

In Person and Virtual Meeting

August 26, 2021, 8:00 A.M.

Fisher & Phillips

Collin Warren
Partner

Collin Warren, a partner in the firm's Houston and Dallas offices, has more than 20 years of experience representing clients in state and federal courts, as well as before the Occupational Safety and Health Administration (OSHA) Review Commission (OSHRC), Mine Safety and Health Administration (MSHA) Review Commission (MSHRC), Equal Employment Opportunity Commission (EEOC), and other state and federal regulatory agencies.

Collin was most recently the Chief Compliance Officer and General Counsel at APM, an affiliate of the General Electric Company, where he oversaw various functions including compliance, EHS, human resources, communications, facilities management, internal investigations, safety audits, employee relations, organized craft labor relationships, and various contested matters, investigations, and litigation involving the company.

He has first and second chair trial and arbitration experience and has handled numerous investigations, incidents, grievances, and litigation arising out of fatalities, significant injuries, property damage, employee complaints, and labor issues. He also has experience addressing workers' compensation and nonsubscriber issues.

Additionally, Collin assists clients with proactive EHS compliance.
He is a certified mediator.

Workplace Privacy in a Post-Pandemic Era

Katy Economic Development Council

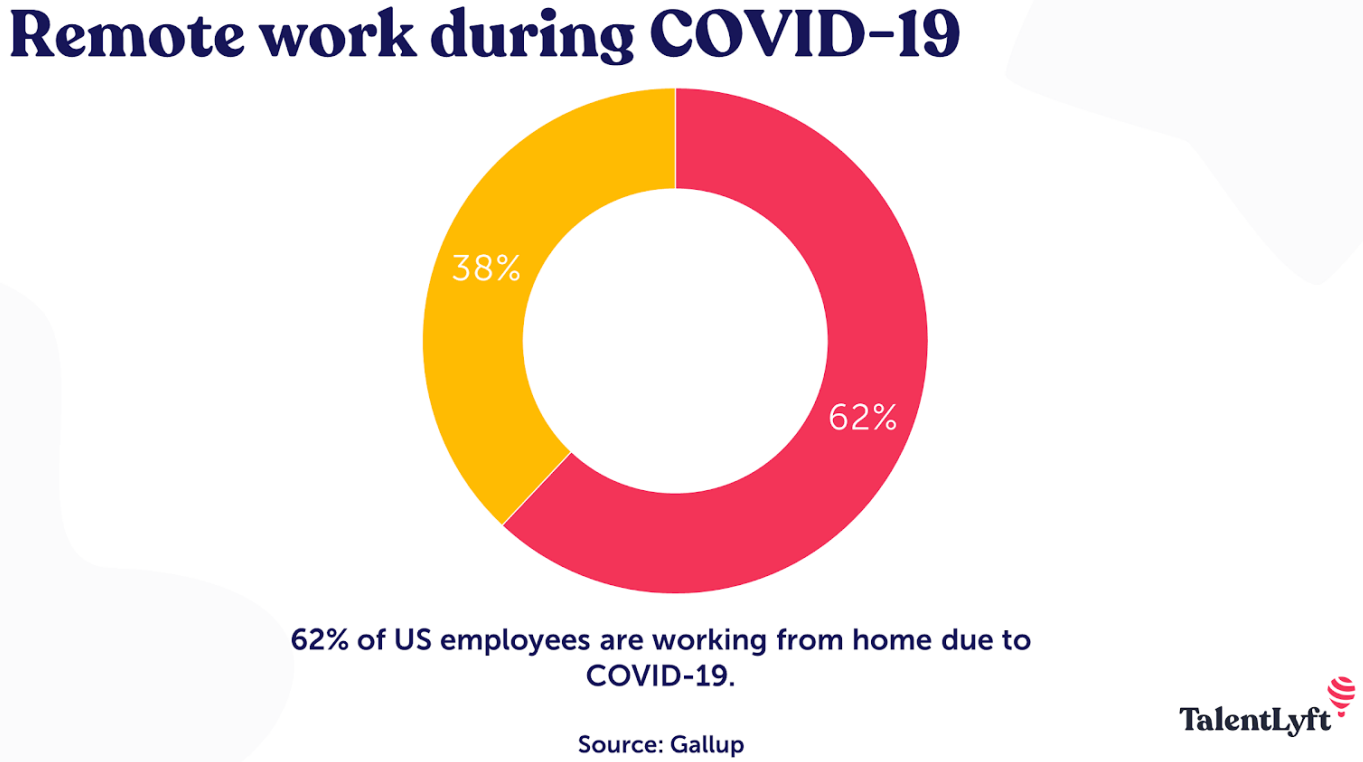
A. Kevin Troutman
Partner, Fisher Phillips
ktroutman@fisherphillips.com
(713) 5602

Collin Warren
Partner, Fisher Phillips
cwarren@fisherphillips.com
(713) 292-5633

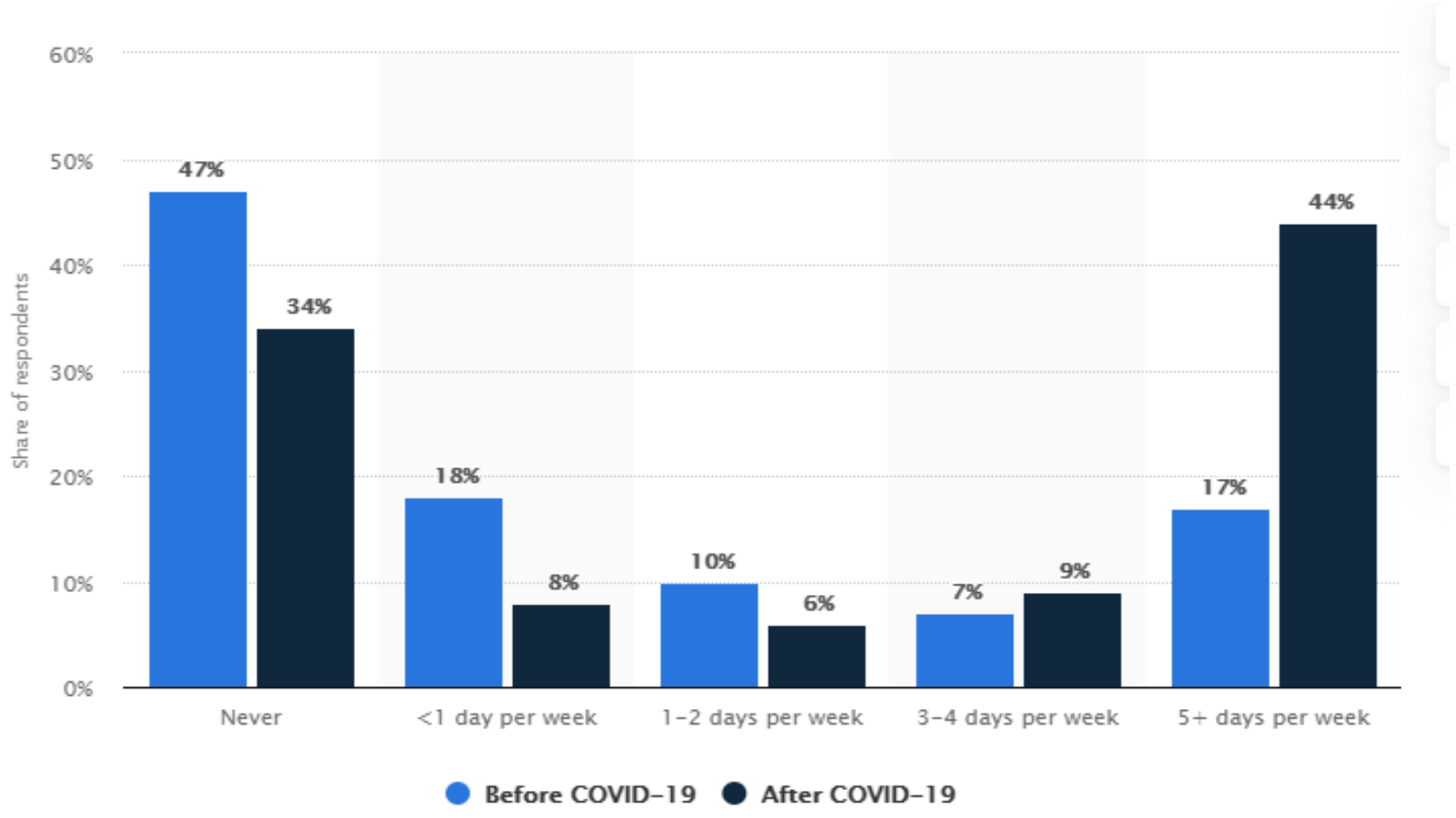
Overview

- Cybersecurity Risks of Remote Work
- Strategies for Avoiding and Mitigating Data Breaches
- Protection of Trade Secrets and Other Sensitive Information
- Employee Monitoring
- Statutory/Regulatory Compliance (*Biometric Privacy, Federal, State and International Regulations*)

Remote Work During the Pandemic



Change in Remote Work Trends During COVID-19 Pandemic



Post-Pandemic Remote Work Expectations

Chart 1: While less than one quarter of respondents reported more than 10 percent of employees worked primarily from home before COVID-19, this share is projected to significantly increase after COVID-19

Percentage of US full-time employees working primarily from home (at least 3 days a week) before COVID-19 and expectation 12 months post-pandemic

Source: The Conference Board report 'From Immediate Responses to Planning for the Reimagined Workplace: Human Capital Responses to the COVID-19 Pandemic'

www.conferenceboard.org

Post-Pandemic Remote Work Expectations

- **Remote work has been an overwhelming success** for both employees and employers. The shift in positive attitudes toward remote work is evident: 83% of employers now say the shift to remote work has been successful for their company, compared to 73% in PWC's June 2020 survey.
- **The office is here to stay, but its role is set to change.** Less than one in five executives say they want to return to the office as it was pre-pandemic. The rest are grappling with how widely to extend remote work options, with just 13% of executives prepared to let go of the office for good. Meanwhile, 87% of employees say the office is important for collaborating with team members and building relationships — their top-rated needs for the office.

From a January 2021 PWC survey

Post-Pandemic Remote Work Expectations

- **Employees want to return to the office more slowly than employers expect.** By July 2021, 75% of executives anticipate that at least half of office employees will be working in the office. In comparison, 61% of employees expect to spend half their time in the office by July.
- **There's no consensus on the optimal balance of work days at home vs. in the office.** Over half of employees (55%) would prefer to be remote at least three days a week once pandemic concerns recede — little changed from the 59% who said the same in June. For their part, while most executives expect options for remote work, they are also worried about the effects: 68% say a typical employee should be in the office at least three days a week to maintain a distinct company culture.

The Cybersecurity Risks of Remote Work

- Fraudulent websites
- Phishing/social engineering
- Hacking
- Ransomware attacks (sharp increases during pandemic)
- Careless transmission, disposal, or storage of confidential, sensitive or proprietary information
- Unauthorized access to data and devices

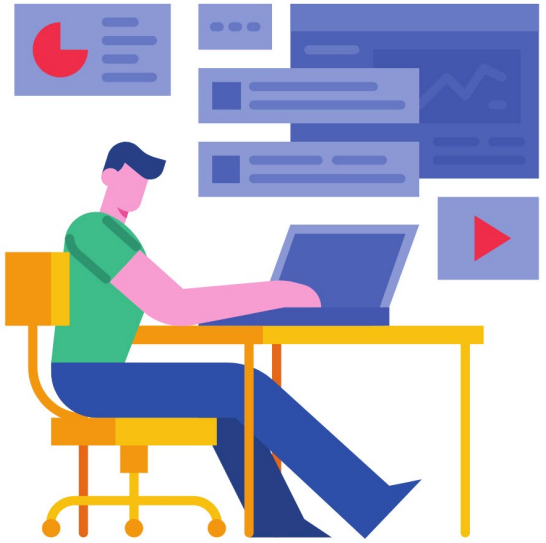
The Cybersecurity Risks of Remote Work: Ransomware Attacks

- 800% increase of ransomware attacks during pandemic
- Victims paid over $350 million in 2020
- Cost of ransomware attacks $20 billion in 2020
- Many fueled by nation state actors
- DOJ taskforce, OFAC
- Self Reporting

Sources: Chainalysis, PurpleSeC.

Strategies for Avoiding and Mitigating Data Breaches

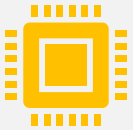
- Employee training
  - Most common threats arise out of employee errors
- Policies
- Internal audit
- Device compliance program
- Restricted access
- User identities continuously checked and verified
- Security patches up to date
- Consider employing a CISO, even if just part-time



Strategies for Avoiding and Mitigating Data Breaches

Data ethics considerations

Regular follow-up, monitoring and testing are crucial



Data protection is a constant effort. You are never “finished”.

Mitigation

Response Plan

Data Map

Contractual Obligations

Insurance Coverage

Notification Obligations

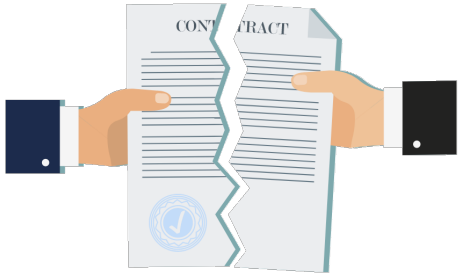
Protection of Trade Secrets and Proprietary Information

- Confidentiality agreements
- Train employees
- Reinforce policies/confidentiality obligations
- Limit access
- Implement password protections
- Restrict ability to save information on personal devices

Trade Secret Protection: Layoffs

Ensure return and no retention of confidential/sensitive information

- "Hard Measures"
  - ➢Written certification of full return and purge
  - ➢Systems analysis – does it show pattern of downloading or printing?
  - ➢Reminder letter from Legal or HR
- "Soft Measures"
  - ➢HR or Manager interview employees, if still possible
  - ➢Include data collection/retrieval questions in any exit interviews



Trade Secret Protection: Furloughs

Assess if covenant was running during furlough

- No clear law on this
- Language in most covenants runs time from termination of employment
- But will courts allow furlough to be a de facto lengthy garden leave period, without even having compensation (maybe just benefits)?
- Best practice – ensure agreements include covenants both *during* and *after* employment

Trade Secret Protection: Furloughs

- Determine whether furloughed employees should sign new restrictive covenants when they return as a condition of restarting
  - Like starting a new position in company?
  - Some states have the "material change" doctrine (e.g., MA)
    - A non-solicitation agreement or covenant not to compete may be deemed void if there are material changes in the employment relationship between an employee and the employer."
  - Or more akin to asking an existing employee to sign a new covenant ('mid-stream covenant' issues)?
    - ➢ Would additional consideration be required in states where mere continued employment is not sufficient?
    - ➢ Is recall from furlough such consideration?
    - ➢ Reaffirmation of old covenant?

Employee Monitoring in a Remote Work Environment

Reasons

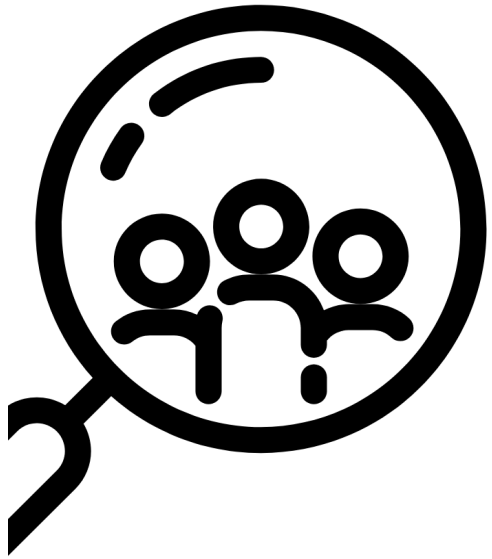
- Monitoring productivity/active working time
- Keeping track of hours for non-exempt employees
- Ensuring compliance with privacy/confidentiality obligations for sensitive data

Methods

- Keystroke monitoring
- Applications/software/website monitoring
- Photos taken remotely

Employee Monitoring in a Remote Work Environment

- State laws that must be considered
- National Labor Relations Act considerations
- What to do with all that employee data collected
- AI technology
- Vaccine tracking and pandemic-related information – add a new layer to employee privacy



Statutory Compliance – Getting More Complex

- Current and pending state legislation in the United States:
  - Biometric privacy (Illinois, Washington, Texas, California, New York, Arkansas)
  - Data breach laws: 50 states, 50 separate statutes
  - Consumer privacy (CA, FL, NY, VA, WA)
- Employee accessibility under the ADA
- Employer anti-harassment, discrimination, and retaliation policies must be adapted to remote work
- FTC likely to become more active under Biden administration

Statutory Compliance Getting More Complex

- International Privacy requirements moving ahead rapidly
  - In the European Union, GDPR enforcement will be stepped up, more emphasis on penalties in 2021
    - Regulatory enforcement of cookies a primary target
  - Canadian privacy
  - Privacy in the UK after Brexit

Final Thoughts – 7 Steps to Ensure Maximum Protection

1. Require all employees to connect to the company's network using a secure connection, such as a Virtual Private Network (VPN).
2. Antivirus software and advance password protection methods.
3. Issue a policy that outlines employee obligations relating to data security while working remotely.
4. Secure video conferencing applications.
5. Data encryption.
6. Email scanning software to help identify phishing e-mails.
7. Train managers and supervisors to focus on data protection and cybersecurity while working remotely.

Questions?

A. Kevin Troutman
Partner, Fisher Phillips
ktroutman@fisherphillips.com
(713) 5602

Collin Warren
Partner, Fisher Phillips
cwarren@fisherphillips.com
(713) 292-5633

Thank You!

A. Kevin Troutman
Partner, Fisher Phillips
ktroutman@fisherphillips.com
(713) 5602

Collin Warren
Partner, Fisher Phillips
cwarren@fisherphillips.com
(713) 292-5633