REMOTE ACCESS SECURITY
IN THE AGE OF CORONA

Tuesday, June 9, 2020 | 2:00PM-3:00PM

MAZARS

AGENDA

1. CURRENT OPERATING ENVIRONMENT FOR COVID-19
2. TELEWORKING OPERATING CONCERNS
3. EMERGING RISKS
4. MANAGING RISKS & OPERATING CONCERNS

CURRENT ENVIRONMENT

In the current business landscape companies are required to adapt new practices

- The number of employees working remotely has increased dramatically
  - Global Workplace Analytics estimates that work-at-home will save U.S. employers over $30 Billion a day in what would have otherwise been lost productivity during office closures due to COVID-19

- Companies are providing teleworkers required access to services through remote connections into their infrastructure
  - Services form on premise resources (Internal Network, systems and applications)
  - Cloud services
  - Public internet
  - Collaboration services

OPERATING CONCERNS

Changing operations is a financial impact

Operating Concerns

- Cost of laptops for remote access
  - Alternative approach is that many companies are allowing employees to connect in using their home computer

- Infrastructure to support increased remote workers
  - Increased teleworker connections to requires additional resources, incurs greater costs, and decreases performance
    - Teleworkers require access to company network first establish a trusted connection through VPN
    - Aggregating all teleworker traffic through a single location to enforce security policy at a central location
    - This security pattern also enables teleworkers to leverage the same connectivity to internal and cloud services / applications

EMERGING RISKS

- State sponsored attacks on new targets
  - The usual actors: China, Iran, Russia and North Korea
  - New targets: Restaurants and Delivery
  - Scenario: Mimic or hack into new targets - Gain access online accounts (Google/Yahoo…) – Gain access to Government and Healthcare worker work account

- Increased PHISHING attacks
  - PC Magazine - Phishing Attacks Increase 350 Percent Amid COVID-19 Quarantine
  - Zscaler - 20,000 unique incidents of phishing attacks

- Increased attacks on remote workers
  - CNET - 7,000 incidents in which victims were tricked into starting a download of malware, all of which referenced the health crisis.

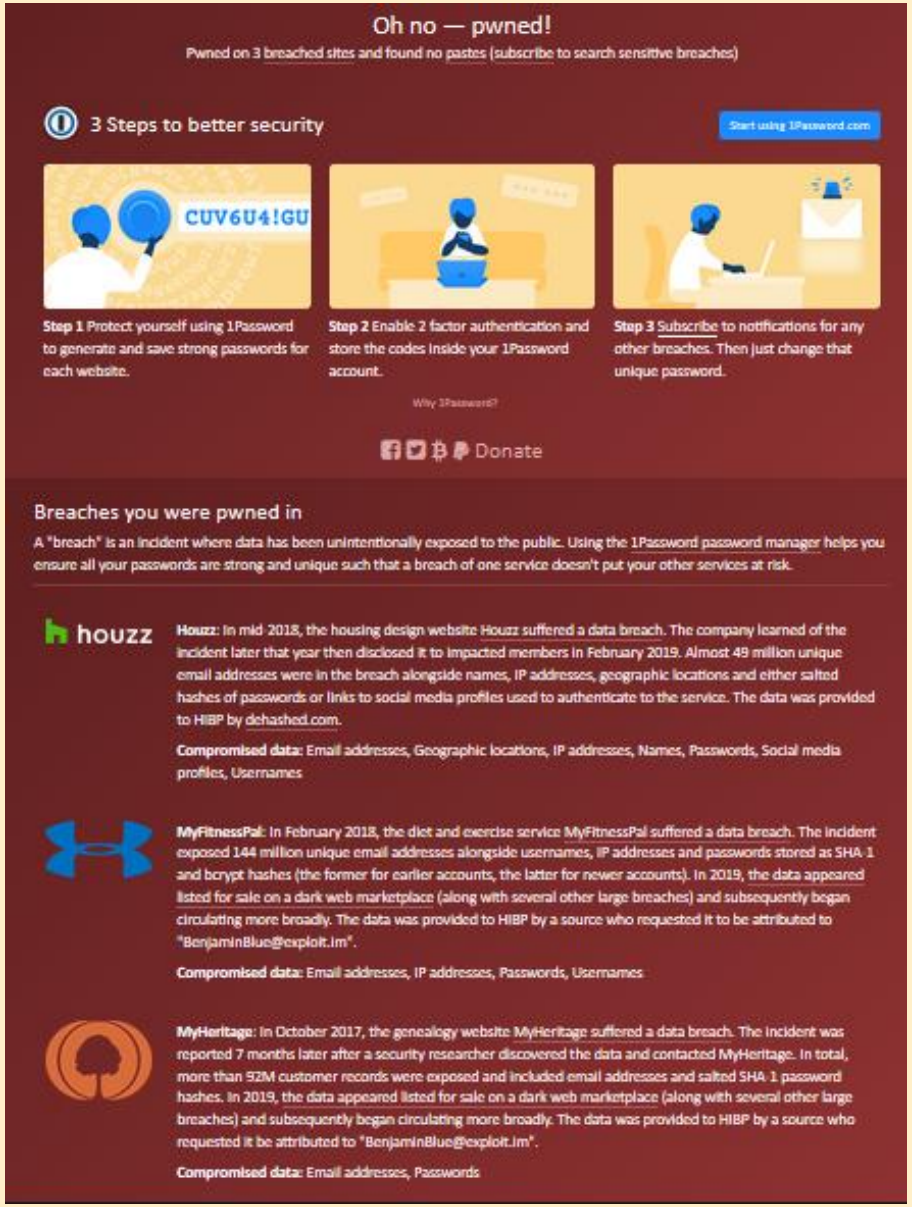
MANAGING RISKS & OPERATING CONCERNS

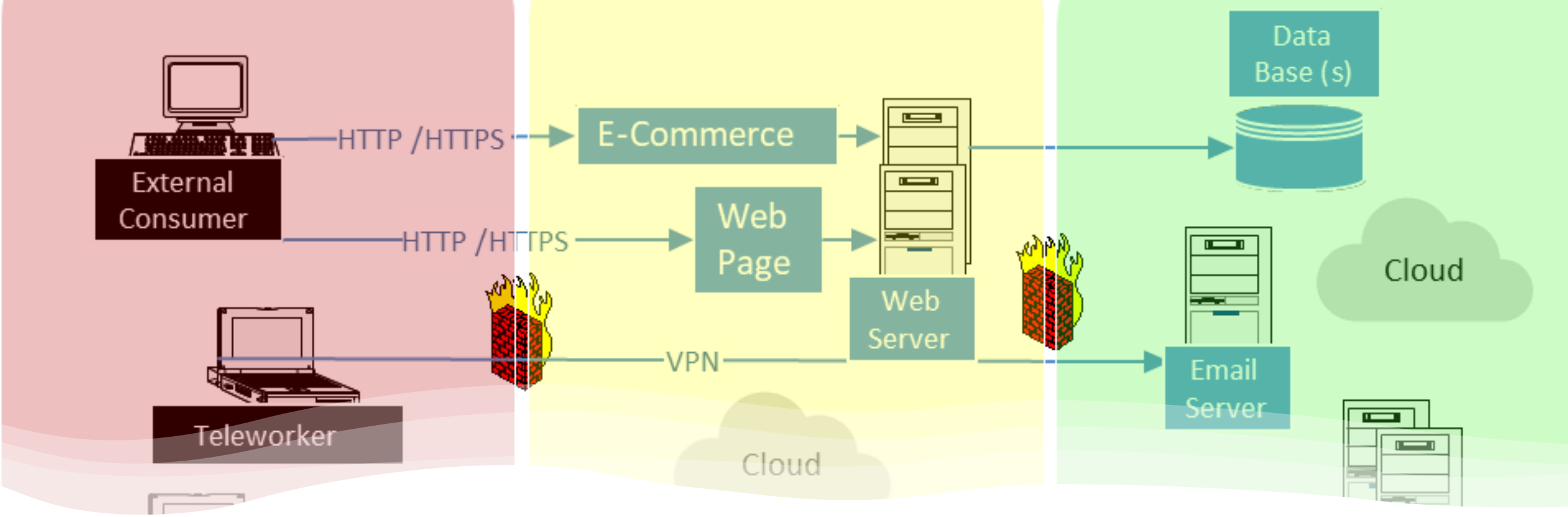
- **Laptops, home computer, PHISHING and attacks on remote workers**
  - Multifactor authentications (MFA) must be deployed for all users especially staff connecting via home computer
  - MFA for privileged accounts and staff with access to sensitive an private information
  - Standard security build and security tools that cannot be turned off

- **Infrastructure to support increased remote workers**
  - Segmentation of environment reduce overall impact and increase security
  - Teleworkers connect directly to the cloud for services where the same security policy can be enforces

- **State sponsored attacks on new targets**
  - Ensure passwords are complex and require regular changing of passwords
  - Reinforce to not use same passwords as personnel passwords and provide guidance for all employees to change password
  - Block all access outside the GEO location of workforce via web browser and conditional access rules in the cloud

Have employees check there work and personal accounts for confirmed data exfiltration at: https://haveibeenpwned.com/





*TELEWORKING **PRE-COVID-19, 3.6%** ESTIMATES RISE TO **25%-30% POST-COVID-19** * GLOBAL WORKPLACE ANALYTICS

- Zero Trust Architecture
  - Access based on user location, IP address and MFA, machine location and other data
  - Segmented networks based on purpose, sensitivity and criticality
  - Enforce common security policy on premise and in the cloud

PHILIP A. JONES
DIRECTOR - CYBERSECURITY

Telephone +1 813 760 5347
Philip.Jones@mazarsusa.com
My profile on LinkedIn

QUESTIONS AND ANSWERS

To ask questions, please use the **Q&A** box on the right-hand side of your screen