BPM

Risk Mitigation and Practical Considerations

Maintaining Compliance, Security and Integrity in a Remote Environment

April 17, 2020
10:00 a.m. – 11:00 a.m. PT

Webinar

- Telework Best Practices Addressed
- Teleworking Threat Landscape
- COVID-19 Impact on Controls & Compliance

Note: Please submit all questions using the Q&A option at the bottom of the webinar platform for our panel to address.

Panel

Sarah Lynn, MBA

Security Advisory Partner

SALynn@bpmcpa.com

David Trepp, M.S.

Security Assessment Partner

DTrepp@bpmcpa.com

Ashwani Verma

Risk Assurance and Advisory Partner

AVerma@bpmcpa.com

Telework Best Practices Addressed

Client's Addressable Controls for Employees

Think about or review the items (controls) that are sometimes overlooked like:

- How your business should address security and privacy when you are in the home workspace? (Not just the laptop, VPN and access control)
- What are you printing or has your machine been properly configured NOT to print at home? (How to manage)
- What is on your desk at home? (How to audit)
- How do you leave your laptop when you take a break?

  (Locked/unlocked)
- WHO is allowed in your space where you work?

How to Acknowledge a WFH (Work from Home) Practice

Extra needed advice on points you may care about like:

- Writing WFH Practices and Policies
- Training on WFH Practices
- Acknowledging WFH Practices Employees (and contractors)
- Enforcing WFH Practices
- Auditing WFH Practices (some regulations require it)

Couple of Client Stories during this Time

- A Company who did not know if they could WFH and keep up their Compliance projects

- A Company who was hiring security professionals to staff up, suddenly had to slow down

- A Company working on Security architecture realizing it even more important than before, doubled down

- A Company planning their “continuous monitoring” leaned in for support

Teleworking Threat Landscape

A Telework Force Increases Attack Surface

- Mobile and remote devices
- VPN systems
- Remote email systems
- Cloud services/applications
- New social engineering attack vectors
  - “Hi, I’m calling on behalf of IT to help you secure your new remote access; I’ll just need you to divulge credentials or visit a malicious website while we talk”
  - “Click here to download the latest coronavirus map information for your neighborhood”

A Telework Force Increases Attack Surface (cont.)

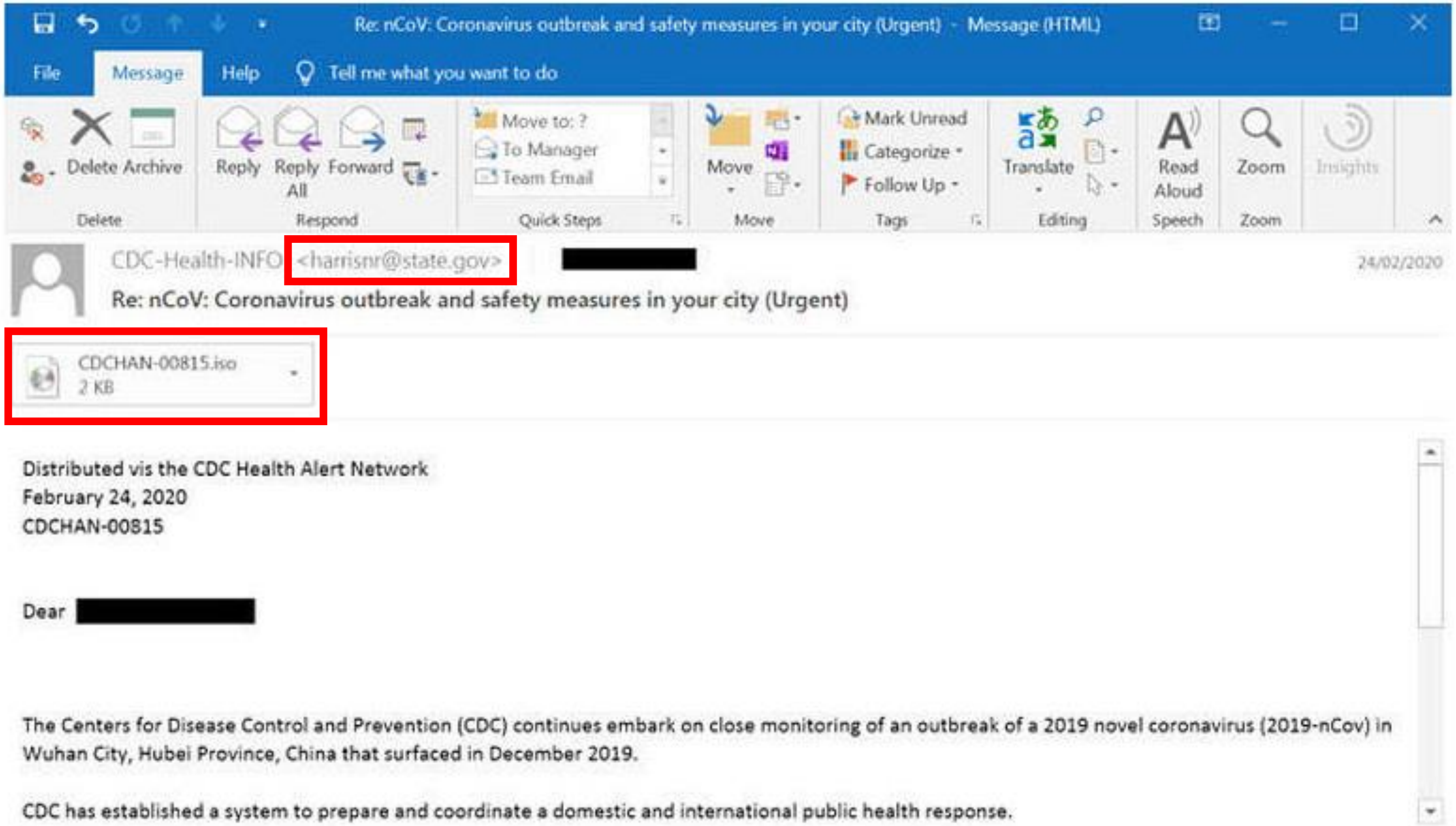
- Home routers/modems often have weak default passwords and lack adequate patches and updates

- Home networks (wired or wireless) often have weak encryption and/or passwords

- Home pc’s are often compromised (at least adware)

- Home workspaces often have IoT devices on the network
  - Thermostat
  - Garage door opener
  - Home alarm system
  - SmartTV
  - Etc.

Phishing 2.0: Exploiting Current Events



CDC-Health-INFO <harrisnr@state.gov> [redacted]

24/02/2020

Re: nCoV: Coronavirus outbreak and safety measures in your city (Urgent)

CDCHAN-00815.iso
2 KB

Distributed vis the CDC Health Alert Network
February 24, 2020
CDCHAN-00815

Dear [redacted]

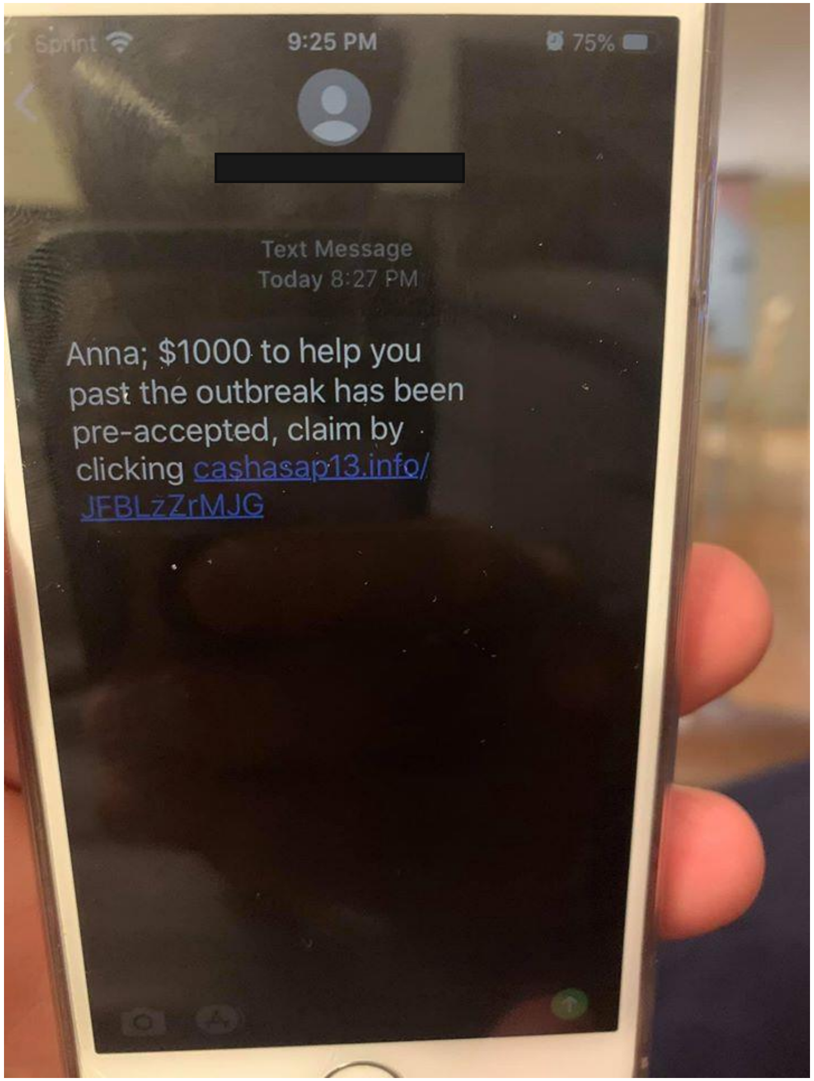
The Centers for Disease Control and Prevention (CDC) continues embark on close monitoring of an outbreak of a 2019 novel coronavirus (2019-nCov) in Wuhan City, Hubei Province, China that surfaced in December 2019.

CDC has established a system to prepare and coordinate a domestic and international public health response.

Phishing email related to coronavirus.

Image: Cybereason

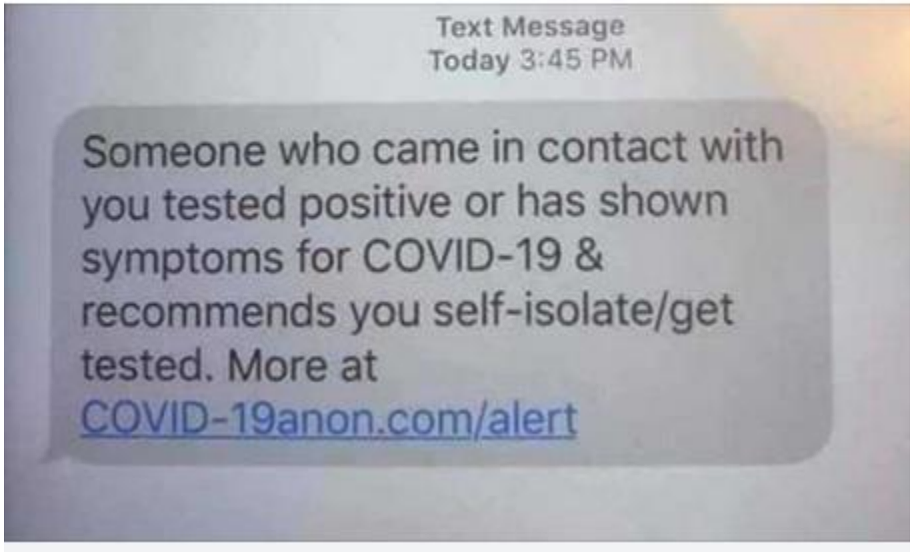
Phishing 2.0: Exploiting Current Events



[redacted]

Text Message
Today 8:27 PM

Anna; $1000 to help you past the outbreak has been pre-accepted, claim by clicking cashasap13.info/JFBLzZrMJG

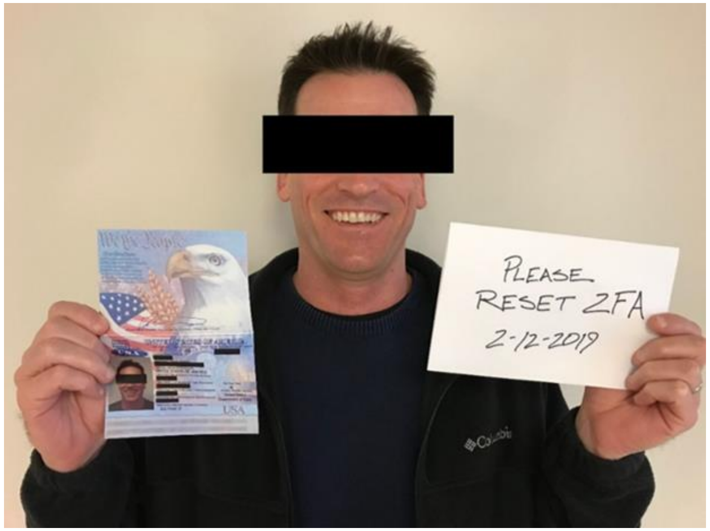


Text Message
Today 3:45 PM

Someone who came in contact with you tested positive or has shown symptoms for COVID-19 & recommends you self-isolate/get tested. More at COVID-19anon.com/alert

Defeating Multi-Factor Authentication (MFA or 2FA)

- Intercepting cookies/session IDs
  - Necrobrowser
  - Modlishka
- Help desk attacks
  - Convince them to switch the phone #
- Backdoor access that doesn't require MFA
  - Exchange Web Services (EWS)
  - Exchange modern encryption


[redacted]
[redacted]

- Ask the user for their one-time code
  - "We're from the bank's security department, and there's been some suspicious activity with your account; but before we go any further, we need you to verify it's you. Please read me the code you were just sent."
    - The code was sent by your legitimate financial institution, who sent it to you because the fraudster just entered your (stolen) username and password. Now the fraudster is calling you to request the MFA one-time code.
- SIM card swaps
  - If your phone suddenly tells you it has "No Service" or provides you an "access code" you weren't anticipating, contact your cell provider right away and ask them if there's been any activity on your account, e.g. a SIM swap

User Telework Security Considerations

- Understand and follow your company’s telework policies & procedures
- Use privacy screens on web cams when not in use
- Make sure your phone/TV/etc. is not activated when discussing sensitive information
  - “Texas” & “Lexus” sound a lot like “Alexa”
  - “Leery” & “Serious” sound a lot like “Siri”
- Practice safe application storefront protocols
- Inspect all links before clicking
  - https://www.**chase**.com vs. https://www.chase**.bank**.com
  - https://www.chase.**com** vs. https://www.chase.**net**
- Click “Reply” on an email to see if it’s really going back to the expected sender

User Telework Security Considerations (cont.)

- Use strong, *i.e.* long, passwords, *e.g.* passphrases
    - Avoid easy to guess slogans, lyrics, *etc*.
- Make sure your home Wi-Fi is configured securely
    - No WEP or WPA1 (WPA 2 or 3 is better)
- Consider segregating sensitive from non-sensitive networks
    - Sensitive Network: “Secure” computing only
        - Secure computer that is used only for activities involving PII
        - Security cameras, alarm systems
    - Non-sensitive Network:
        - “Unsecure” computers that visit Facebook, Instagram, etc.
        - Other IoT devices, *e.g.* smartTVs, alarm systems, etc.
- Apply the concept of “Least Functionality” to all devices
    - Whenever possible, disable
        - Location services
        - Bluetooth
        - Wi-Fi
            - Consider a personal hot spot

Organizational Telework Security Considerations

- Consider a Mobile Device Management (MDM) solution
  - Microsoft Office 365/Intune MDM, ManageEngine, Airwatch, Citrix XenMobile
- At the network level, ensure the VPN device/appliance has good logging controls
  - adequate log storage for 90 days
  - Make sure someone is paying attention
- Ensure multi-factor authentication for all remote access, VPN, webmail, cloud based apps, *e.g.* MS Office 365
  - If possible, disable EWS, Outlook native client backdoors
- Patch it all
  - Email platform, VPN device, routers/firewalls, mail filtering software, etc.
  - ISP Modems/routers, O/S, AV, browsers, etc.
- Apply the concept of “Least Functionality” to all access controls
  - Which employees need full remote access (beyond email)
  - When remotely accessing, which shares/folders/etc. do users actually need to access?

BPM’s Telework/Remote Access Security Assessment

- Our Telework/Remote Access Security Assessment service is quick and inexpensive, while allowing organizations to get needed assurance that their remote access is not creating unnecessary and/or unidentified vulnerabilities

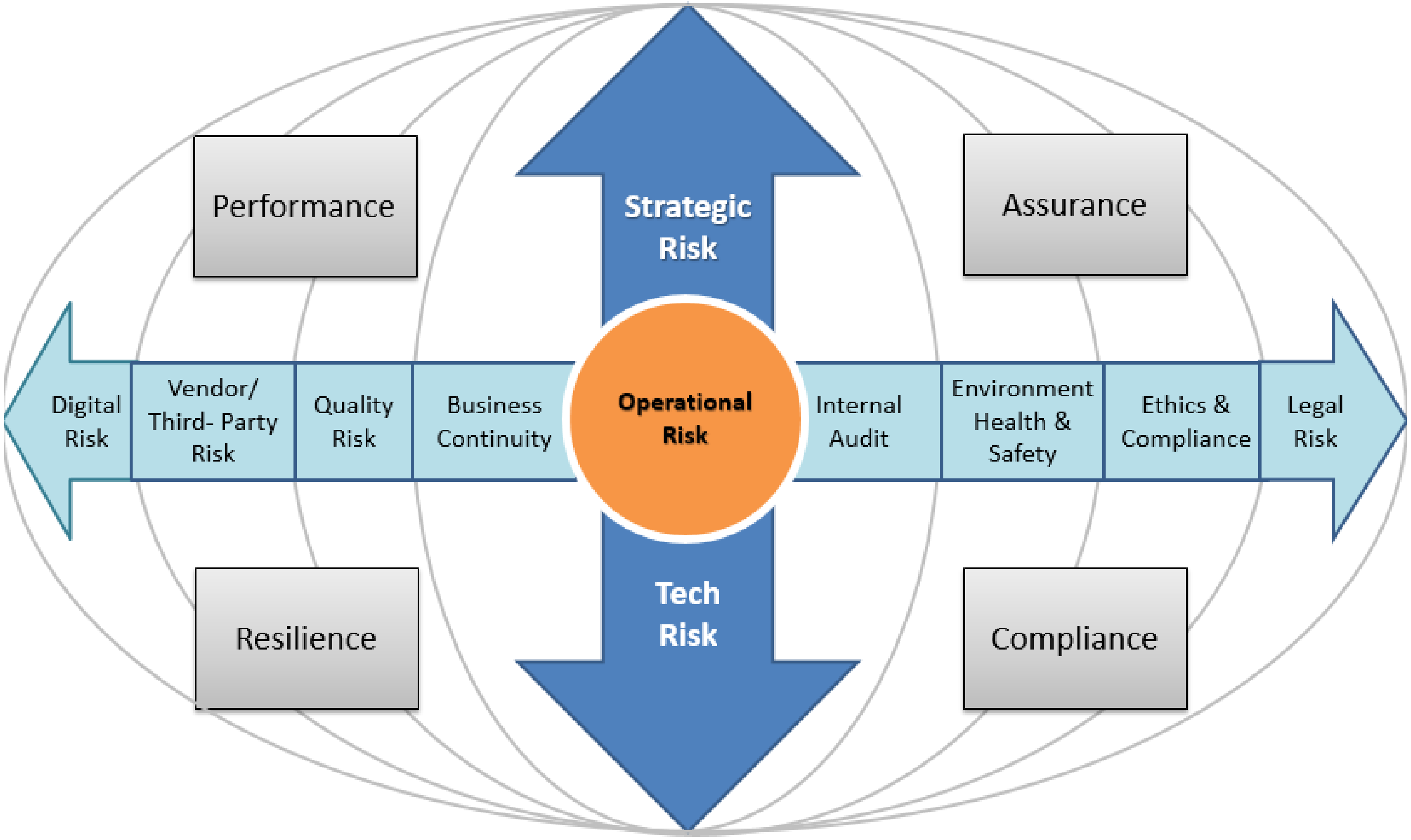
- Remote access assessment services include:
  - Remote Service Discovery
  - External Vulnerability Scan
  - Email Services, Malicious Attachments & Links, Spoofing vulnerabilities, etc.
  - Targeted Configuration Review of Key Remote Systems
  - Remote Work Policy Review

COVID-19 Impact on Controls & Compliance

COVID-19 & Enterprise Risks

- The coronavirus (COVID-19) has transformed from a growing medical crisis to also a macroeconomic one in a matter of weeks.
- During this pandemic, challenges & risks never before faced by the organizations are emerging.
- The potential impact of these unique risks; especially for the organizations operating in regulatory environments (i.e. SEC registrants, healthcare, banking, insurance, etc.) cannot be ignored and needs to effectively managed.

COVID-19 & Enterprise Risks


Performance

Assurance

Strategic Risk

Digital Risk

Vendor/ Third- Party Risk

Quality Risk

Business Continuity

Operational Risk

Internal Audit

Environment Health & Safety

Ethics & Compliance

Legal Risk

Tech Risk

Resilience

Compliance

Identifying & Assessing Internal Controls & Compliance Risks During COVID -19

- Impact on Organization’s internal controls
  - Lapse in internal controls due to remote work
  - Segregation of duties
  - Fraud factors
  - Management Override
  - Non-compliance with organization’s policies and procedures
  - Staff layoff: New control assignments may not be appropriate

- Audit & Compliance Documentation (Critical for SOX & Regulatory Audits)
  - Storing & collective audit/controls evidence
  - Insufficient management review of controls
  - Impact on audit testing (external, internal, SOX and compliance)

Identifying & Assessing Internal Controls & Compliance Risks During COVID -19 (cont.)

- Information Technology General Computer Controls (ITGCs)
  - Unauthorized and inappropriate access
  - System and audit logs
  - Non compliance of organization’s change management policy resulting into unauthorized system changes
  - Cyber security risks

- Regulatory Compliance
  - Continuous compliance with data privacy regulations (GDPR & CCPA)
  - On-going compliance with industry and company’s specific regulatory requirements

Identifying & Assessing Internal Controls & Compliance Risks During COVID -19 (cont.)

- Third Party Risk Management
  - Risks associated with third party vendors: critical for outsourced services
  - Business & Service continuity
  - Importance of SOC1/SOC2 Reports

- Financial Reporting & Disclosure Requirements
  - Companies with significant overseas operations may encounter delays in receiving financial data for consolidated financial statement
  - Potential new financial disclosure requirements (SEC filings)
  - Other financial reporting risks such as balance sheet risks and impairment analysis

COVID -19 & Risk Management – Suggested Approach

1. Update Company’s Risk Assessment
2. Stay in touch with your External Auditors/Regulators/Legal
3. SOX Compliance – Update your scoping and internal controls documentation, including any changes in in-scope systems
4. Internal Audit/Compliance – Reach out for guidance as their role is also changing during this crisis period
5. Integrated Approach
6. Benefits of system/automated controls – Make sure they are enabled
7. Enforce and monitor company’s compliance with policies and procedures and controls
8. Succession Planning – Important than ever

Q&A

Stay up-to-date with the BPM COVID-19 Resource Center at **bpmcpa.com/COVID-19**

Thank You!