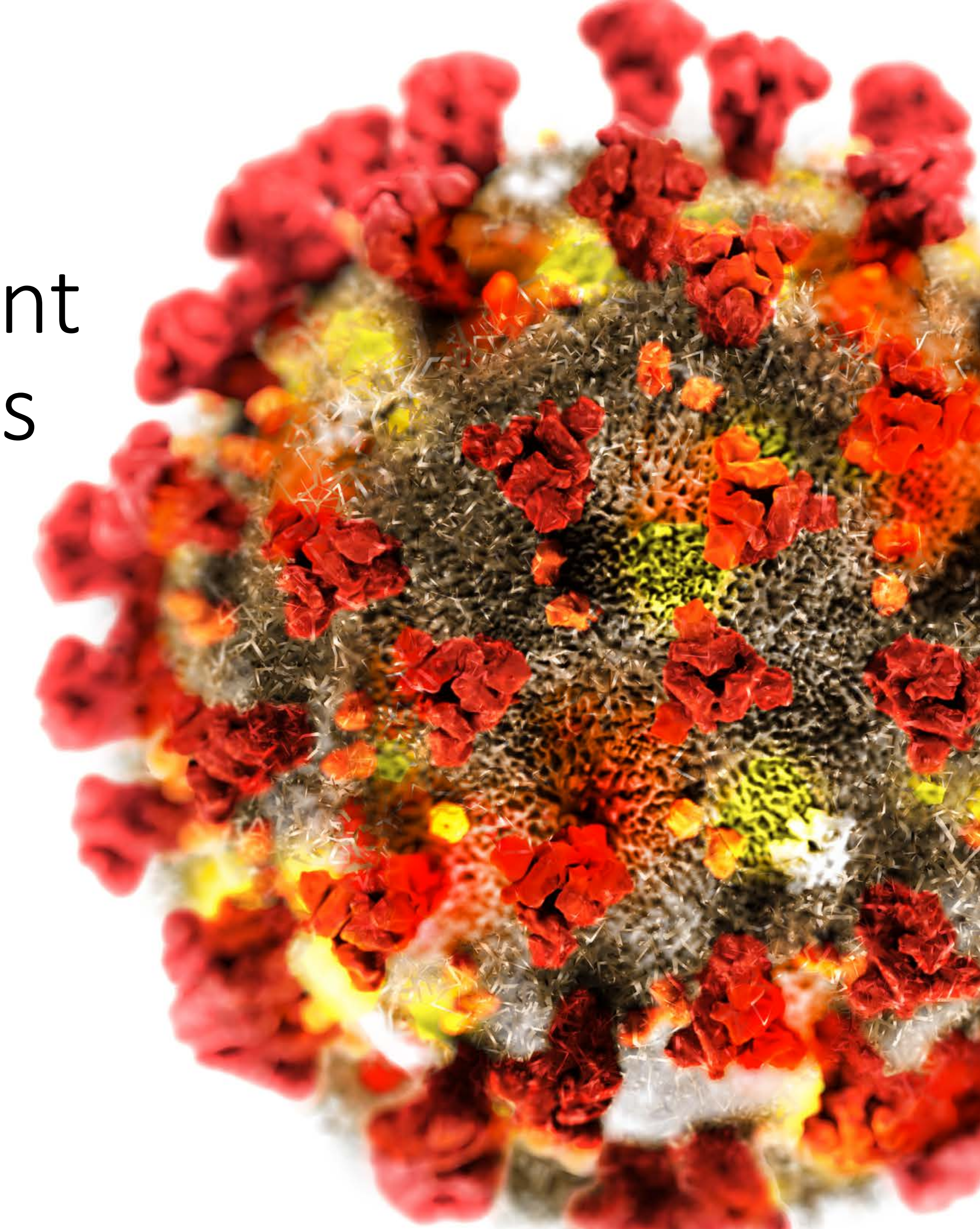
Increased COVID-19 Payment Scams & Cybersecurity Risks

April 16, 2020

pillsbury



pillsbury

Deb Thoren-Peden

Partner

Agenda

- High Level Warnings: Payment Scams & Cybersecurity Risks
- COVID-19 Impact on Operations and WFH Arrangements
- Remote Access Challenges, Risks and Key Controls
- Regulatory Expectations

Deborah Thoren-Peden
Partner
Corporate

pillsbury

Payment Scams/Cybersecurity Threat Trends

pillsbury

pillsbury

Brian Finch

Partner

Government and Regulatory High-Level Alerts

Brian Finch
Partner
Cybersecurity

- **Phishing Scams** -- The U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC) issued a joint alert citing an increase in phishing campaigns utilizing COVID-19 themes to lure in victims.
- **Ransomware Attacks** -- Interpol's Cybercrime Threat Response team has detected a significant increase in ransomware attacks against key organizations and infrastructure responding to the COVID-19 pandemic. Interpol has issued a Purple Notice to police in its 194 member countries alerting them to the heightened ransomware threat.
- **Investment Scams** -- The U.S. Securities and Exchange Commission (SEC) issued an investor alert, warning investors of internet and social media promotions that claim "the products or services of publicly-traded companies can prevent, detect, or cure coronavirus, and that the stock of these companies will dramatically increase in value as a result."

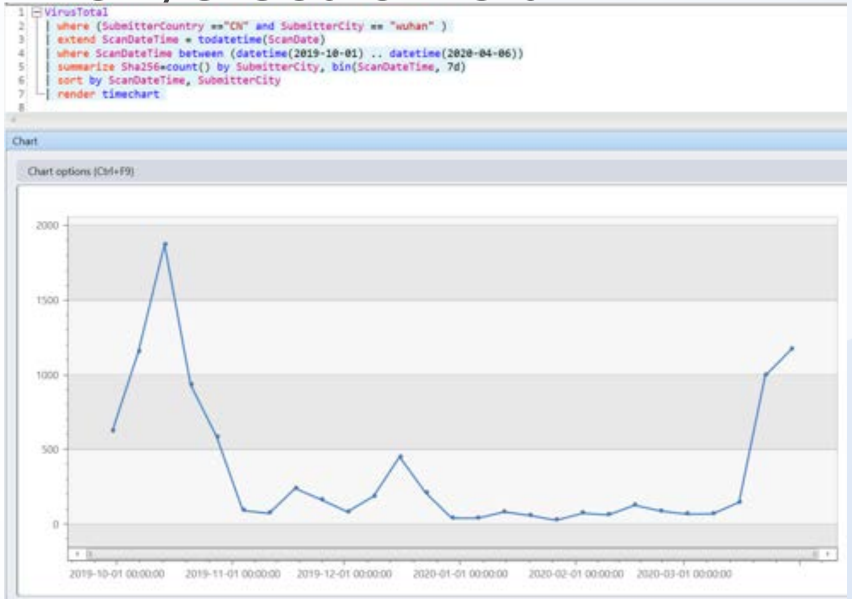
pillsbury

Ron Bushar

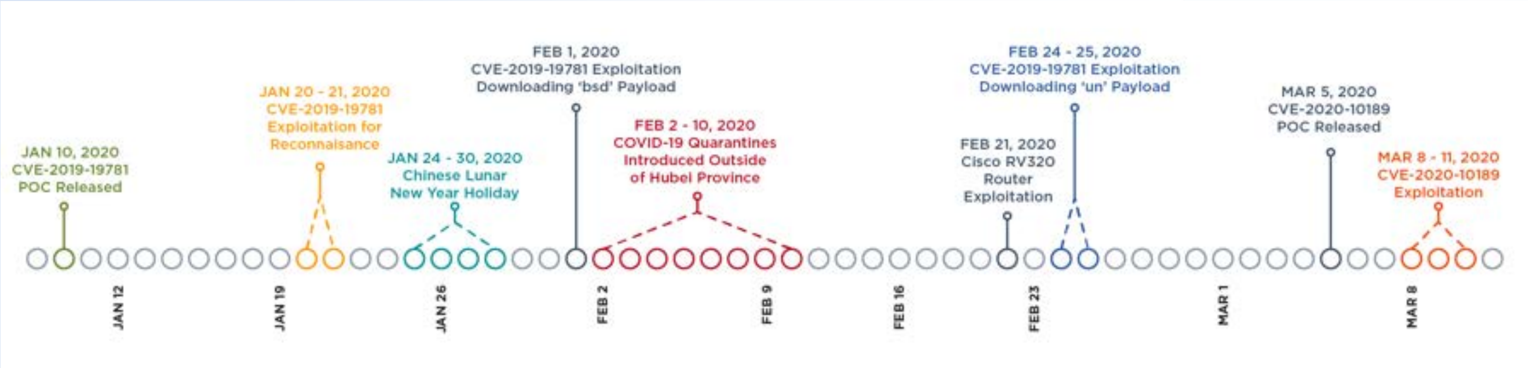
FireEye

Not All Threats are Socially Distancing

- Beginning in 2020, FireEye observed Chinese actor APT41 carry out one of the broadest campaigns by a Chinese cyber espionage actor we have observed in recent years
- Between January 20 and March 11, FireEye observed APT41 attempt to exploit vulnerabilities with Citrix NetScaler/ADC, Cisco routers, and Zoho ManageEngine Desktop Central for more than 75 FireEye customers
- Almost every industry / sector was targeted



```
VirusTotal
| where (SubmitterCountry =="CN" and SubmitterCity == "wuhan" )
| extend ScanDateTime = todatetime(ScanDate)
| where ScanDateTime between (datetime(2019-10-01) .. datetime(2020-04-06))
| summarize Sha256=count() by SubmitterCity, bin(ScanDateTime, 7d)
| sort by ScanDateTime, SubmitterCity
| render timechart
```



JAN 10, 2020
CVE-2019-19781
POC Released

JAN 20 - 21, 2020
CVE-2019-19781
Exploitation for
Reconnaisance

JAN 24 - 30, 2020
Chinese Lunar
New Year Holiday

FEB 1, 2020
CVE-2019-19781 Exploitation
Downloading 'bsd' Payload

FEB 2 - 10, 2020
COVID-19 Quarantines
Introduced Outside
of Hubei Province

FEB 21, 2020
Cisco RV320
Router
Exploitation

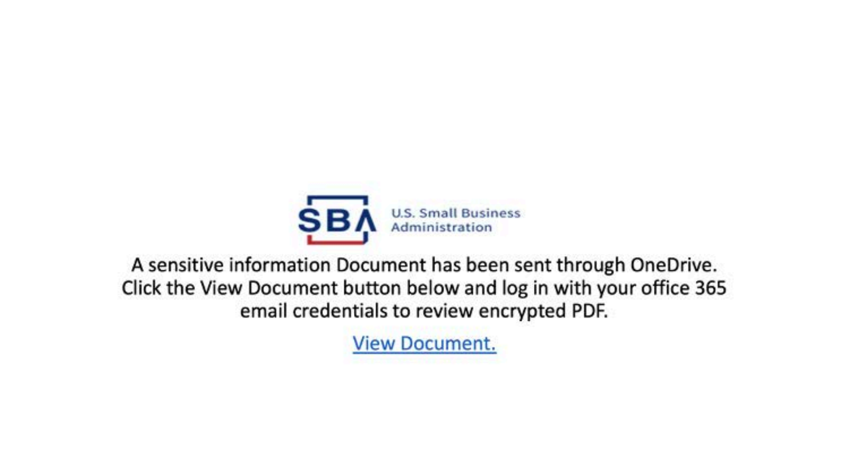
FEB 24 - 25, 2020
CVE-2019-19781 Exploitation
Downloading 'un' Payload

MAR 5, 2020
CVE-2020-10189
POC Released

MAR 8 - 11, 2020
CVE-2020-10189
Exploitation

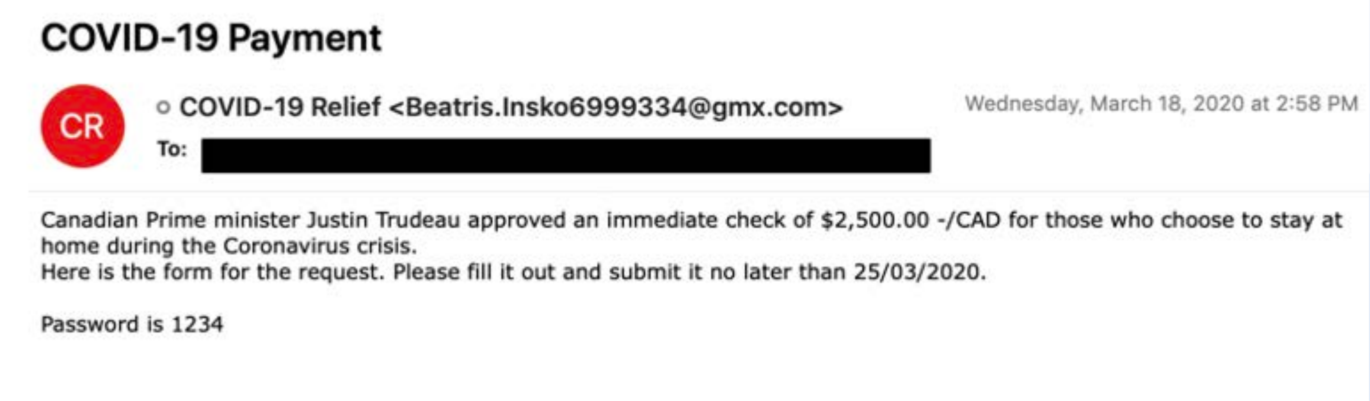
Continued High Profile Attacks

- HHS DDoS
- Zoom malware and widespread “bombing” of meetings
- Large increase in Covid and Stimulus based phishing campaigns
- Marriott – 5.2M additional records



A sensitive information Document has been sent through OneDrive.
Click the View Document button below and log in with your office 365
email credentials to review encrypted PDF.

View Document.



COVID-19 Payment

○ COVID-19 Relief <Beatris.Insko6999334@gmx.com>   Wednesday, March 18, 2020 at 2:58 PM

To: [redacted]

Canadian Prime minister Justin Trudeau approved an immediate check of $2,500.00 -/CAD for those who choose to stay at home during the Coronavirus crisis.
Here is the form for the request. Please fill it out and submit it no later than 25/03/2020.

Password is 1234

COVID-19 Impact on Operations

Jack O’Meara

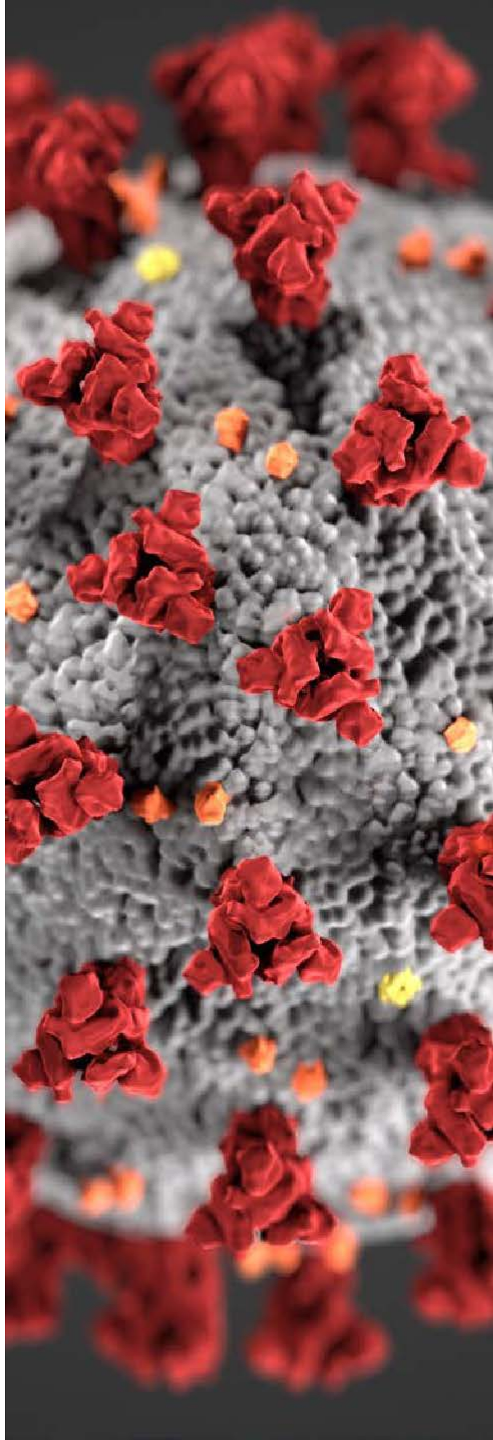
Guidehouse

COVID-19 Impact on Operations

Globally, organizations must adapt to maximize telecommuting, while enabling secure work environments for their workforces.

- Telecommuting reduces the risk of physically spreading germs but may increase the likelihood of cybersecurity threats for those accessing an organization's systems and applications away from the workplace location.
- As staff cope with a reduced workforce – either related to individuals falling ill or individuals carrying additional household responsibilities such as childcare – they may bypass standard security practice and do the minimum required to get the job done.
- In this time of uncertainty, adversaries have heightened efforts to exploit a reduced workforce and gain access to organizations' networks, systems, and data through a variety of schemes including but not limited to phishing and social engineering.

Now is the time for organizations to remind employees of your company's cybersecurity policies and protocols as well as how to respond to potentially malicious or suspicious activity.



Cybersecurity is a **Shared** Responsibility

Enhancing cybersecurity posture, especially when maximizing telecommuting, is must be shared between the organization and the employee.

Breaking Down the Cybersecurity Responsibility

Organizations

What **Organizations** Should Do

- Set up a virtual private network to secure connections to company systems
- Limit unnecessary applications and enforcing security patches
- Require multi-factor authentication to verify a person's identity before granting access
- Enforce password management
- Provide employees with tools to aid in the detection, identification, and remediation of cyber incidents

Breaking Down the Cybersecurity Responsibility

Employees

What **Employees** Should Do

- Use secure Wi-Fi
- Leverage company-approved devices to access company resources
- Encrypt and/or digitally sign sensitive emails or files
- Use only corporate tools and accounts to access an organization's proprietary data through approved secure channels
- Exercise caution with website links and social media

Remote Access Challenges & Risks

pillsbury

Ron Bushar

FireEye

Organizational Challenges

Transitioning Exclusive On-Site Workers

- VPN Enrollment
- Device management – Desktops -> Laptops
- Employees using personal systems for remote work

Remote Access Connectivity

- Managing remote access load
- Modification of security controls

Increased Consumption & Trust

- Covid related phishing campaigns
- Increased consumption of media
- Distractions abound

Response Readiness Reductions

- Reduced and remote security staff
- Increased alerts and noise
- Limited capability to deploy additional security technologies
- Collection of forensic images
- Cloud providers may be less responsive due to increased demand

Threats and Risks

- Visibility into actions
  - On the remote device
  - Through a service
- Exposed passwords / credentials
- Work done on unmanaged or BYOD assets
- Physical Risks
  - Physical theft
  - Work done in public places
- Personnel risks
  - Misuse of corporate resources
  - Lowered focus and awareness to defend against social engineering

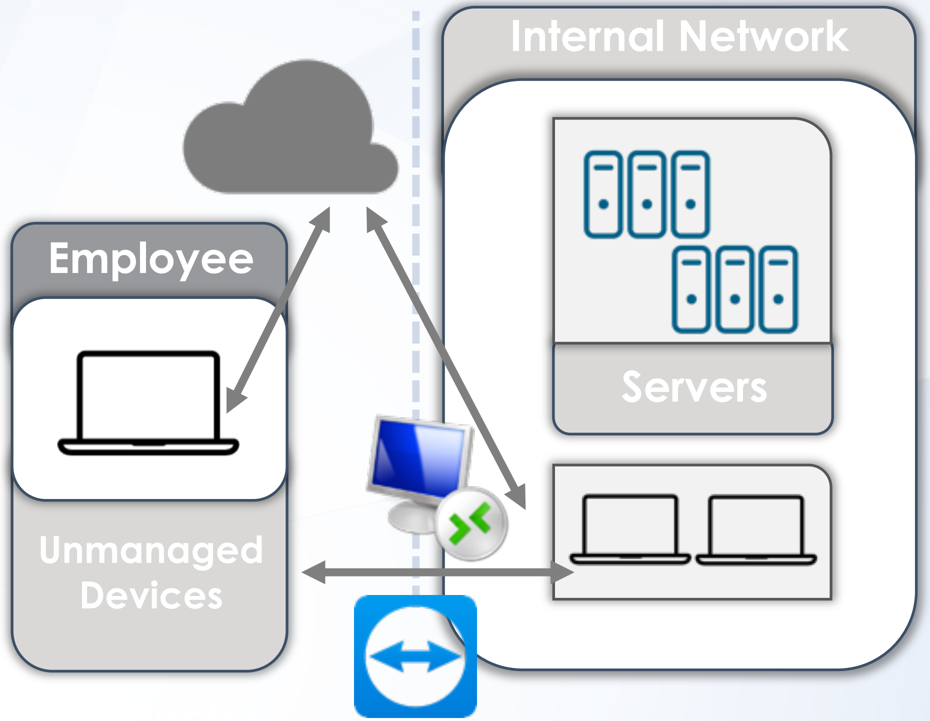
- Compromise of credentials
  - VDI compromise may expose all users on VDI server
- Lateral movement
  - VPN / VDI network segment may not have workstation network restrictions
- Compounding factors
  - Split-tunneling instead of full-tunneling
  - Use of unmanaged assets
  - Non-persistent VDI devices

Remote Access

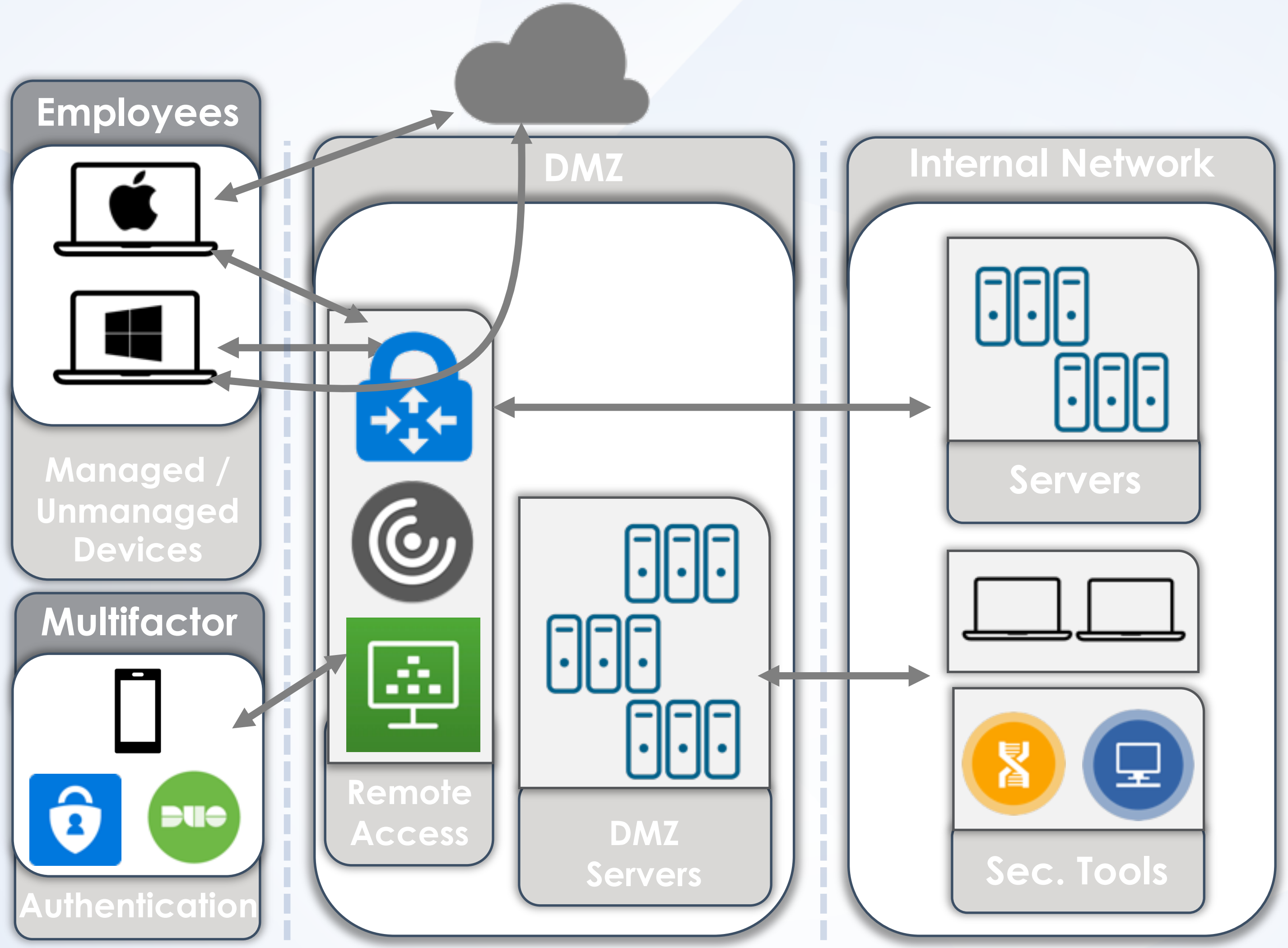
Architectural Approaches

Direct Access

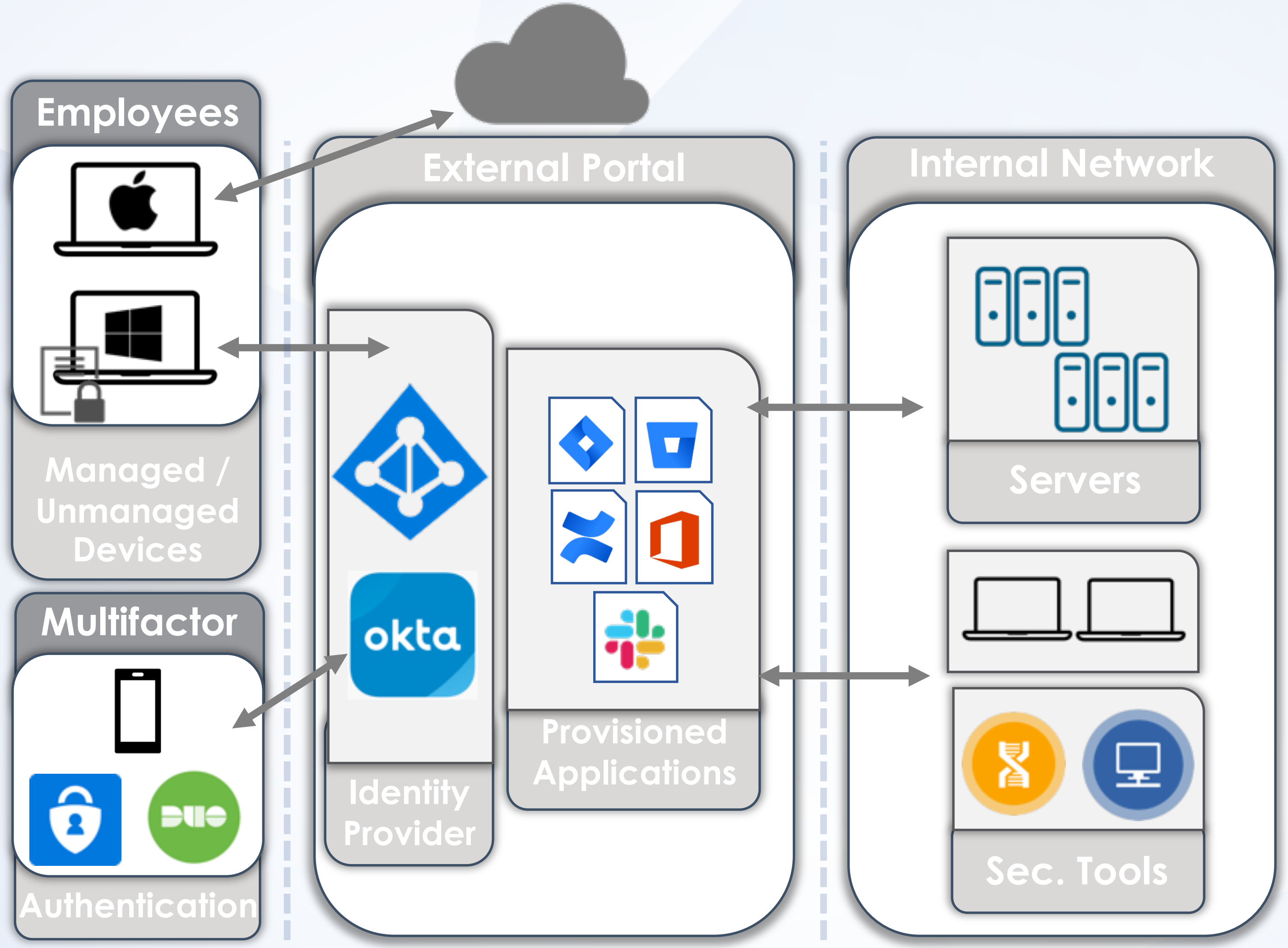
- Internal services exposed to internet
  - Remote Desktop
  - Internal wiki or intranet
- Rare but still happens
  - Can be faster to deploy
  - Requires less infrastructure planning
- Likely to see emerging during rapid remote workforce transitions



Enterprise Standard: VPN / VDI



Zero Trust


Employees
Managed / Unmanaged Devices
Multifactor
Authentication
External Portal
okta
Identity Provider
Provisioned Applications
Internal Network
Servers
Sec. Tools

Remote Access Key Controls

- **Multi-Factor Authentication (MFA)**
  - Effective when combined with educated users
  - SMS is weakest implementation
  - Log failed second factor
  - Remove or protect legacy protocols that do not support MFA
- **Device Trust**
  - Unique device certificates
  - Tie to user where possible
  - Can unmanaged devices connect to the VPN / VDI?
- **Endpoint Visibility**
  - EDR Platform
  - Local endpoint logs
  - Ensure visibility off network
  - Verification of updates pushed to remote systems
- **Privileged Accounts**
  - Should not be allowed to log in directly
  - Alerts if attempted remote usage is detected

Regulatory Expectations

pillsbury

pillsbury

Cassie Lentchner
Pillsbury

Brian Finch
Pillsbury

Regulatory Expectations

Brian Finch
Partner
Cybersecurity

- Senior Level Engagement
- Communication internal and external
- Implementation of required incident response and resiliency plans
- Training and Awareness
- Testing and Monitoring requirements in regulations continue – need to confirm that they new systems confirm with regulatory requirements in environment
  - Access Rights and Controls including MFA
  - Data Loss Prevention Programs
  - Mobile Security, Privacy and Encryption Requirements
  - Vendor Management Requirements
  - Document Retention Requirements

pillsbury

Examples of Regulatory Requirements

- Cybersecurity laws including the NY SHIELD Act, SEC Regulation SP, Gramm-Leach-Bliley Act, Privacy Rule, Safeguards Rule, NYS DFS Part 500 Cybersecurity Regulation
- Data privacy regulations – reporting requirement for breaches to regulators and impacted consumers, GDPR – includes requirements to maintain data security
- Supervisory Responsibilities and Expectations
- Reporting Requirements
- Payment requirements and procedures including BSA-AML and Anti-Fraud

Cassie Lentchner
Senior Counsel

Brian Finch
Partner

pillsbury

NYS DFS Guidance Regarding Cybersecurity Awareness During COVID-19 Pandemic

Cassie Lentchner
Senior Counsel

Brian Finch
Partner

- Reminder to report Cybersecurity Events to DFS within 72 hours at the latest.
- Remote Working
  - Secure Connections. Require Multi-Factor Authentication and secure VPN connections that will encrypt all data in transit. 23 NYCRR §§ 500.12 & 500.15.
  - Company-Issued Devices. New devices must be properly secured.
  - Bring Your Own Device (BYOD) Expansion. Expanded their BYOD policies must consider security risks and consider mitigating steps.
  - Remote Working Communications. Video and audio-conferencing applications should be limited, and employees must be given guidance on how to use them securely.
  - Data Loss Prevention. Regulated entities should remind employees not to send Nonpublic Information to personal email accounts and devices.
- Reminders and training regarding Increased Phishing and Fraud
- Third-Party Risk. Regulated entities should coordinate with critical vendors to determine how they are adequately addressing the new risks. 23 NYCRR § 500.11.

pillsbury

SEC Cybersecurity and Resiliency Observations
Office of Compliance Inspections and Examinations

Cassie Lentchner
Senior Counsel

- Senior Level Engagement
- Risk Assessment
- Policies and Procedures
- Testing and Monitoring
- Communication internal and external

- Access Rights and Controls
- Data Loss Prevention
- Mobile Security
- Incident Response and Resiliency
- Vendor Management
- Training and Awareness

Brian Finch
Partner

pillsbury

The SHIELD Act: *Cybersecurity Requirements*

Cassie Lentchner
Senior Counsel

- Designation and training of employees to coordinate cybersecurity compliance,
- Use of third-party service providers capable of maintaining appropriate cybersecurity practices, with safeguards required by contract,
- Risk assessment of the company's cybersecurity program, including both the network and software design and the information processing, transmission and storage,
- Processes and physical safeguards to detect, prevent and respond to attacks or system failures,
- Monitoring and testing of the effectiveness of the cybersecurity program,
- Processes to safely, securely and permanently dispose of data within a reasonable amount of time after it is no longer needed for business purposes, and
- Updates to the program periodically to address changes in the business or circumstances that would require the program to be changed.

Brian Finch
Partner

pillsbury

Increased COVID-19 Payment Scams & Cybersecurity Risks

If you have questions about how the 2019 Novel Coronavirus impacts you or your business, please contact us.

Brian Finch	*brian.finch@pillsburylaw.com*
Ron Bushar	*ron.bushar@mandiant.com*
Cassie Lentchner	*cassie.lentchner@pillsburylaw.com*
Jack O’Meara	*jomeara@guidehouse.com*
Deb Thoren-Peden	*deborah.thorenpeden@pillsburylaw.com*

pillsbury