Today's Agenda

- Introduction
- Top Cyber Security Issues
- Insurance Solutions
- Questions

What Businesses Need to Know

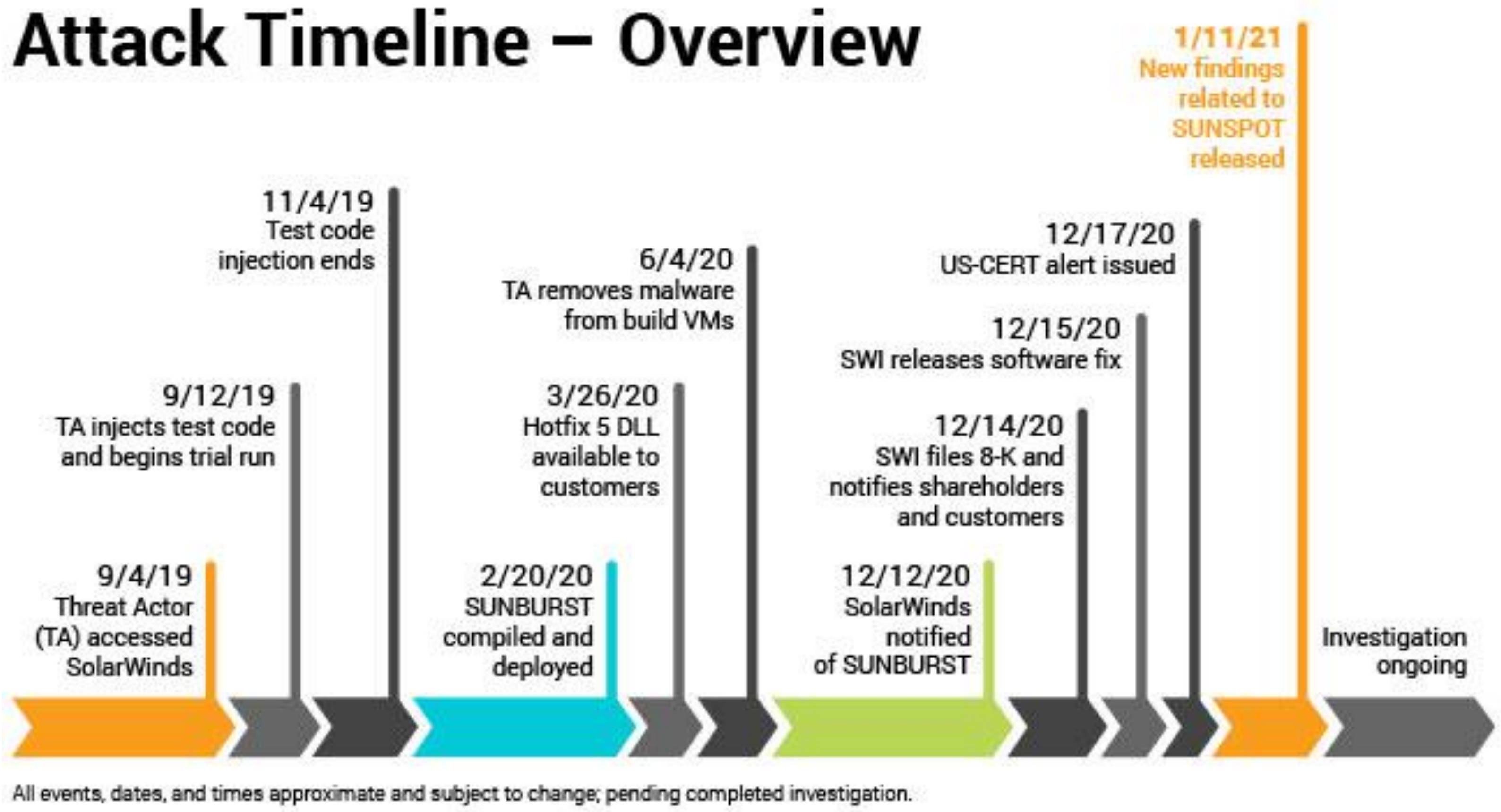
1. Criminals are patient and organized
2. Emails with banking information are often fake
3. Ransomware attacks are expensive
4. Data breach events are expensive
5. Certain controls have proven to be critical
6. Insurance is available, but market is challenged

1. Criminals are patient and organized

- Not teenagers in basements
- Cascade Medical Center
  - $1,040,000 bank transfers
  - 98 mules
  - Transfers all under $10,000
  - $500,000 recovered
  - litigation with bank?

1. Criminals are patient and organized

SolarWinds Breach



Attack Timeline – Overview

9/4/19 Threat Actor (TA) accessed SolarWinds

9/12/19 TA injects test code and begins trial run

11/4/19 Test code injection ends

2/20/20 SUNBURST compiled and deployed

3/26/20 Hotfix 5 DLL available to customers

6/4/20 TA removes malware from build VMs

12/12/20 SolarWinds notified of SUNBURST

12/14/20 SWI files 8-K and notifies shareholders and customers

12/15/20 SWI releases software fix

12/17/20 US-CERT alert issued

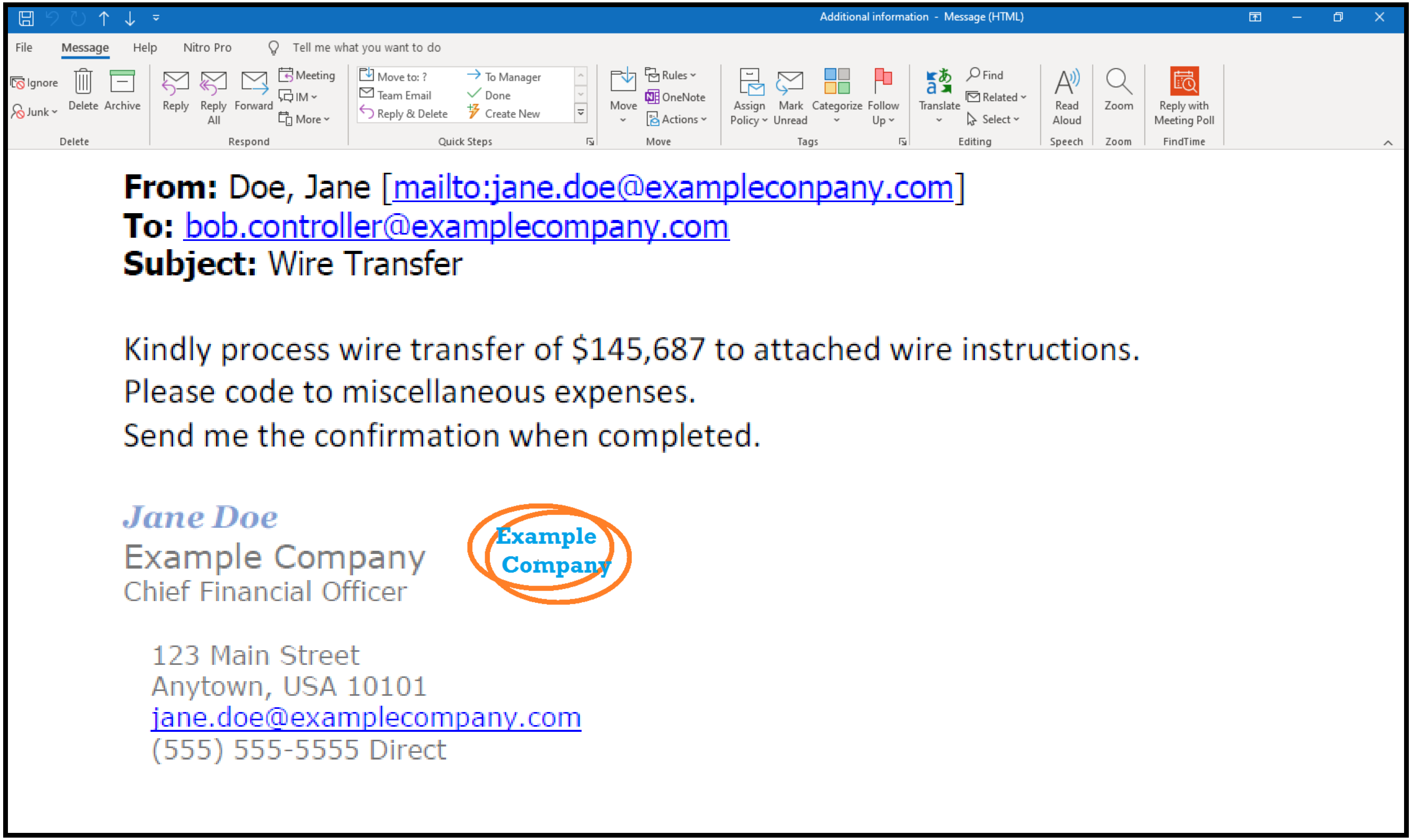
1/11/21 New findings related to SUNSPOT released

Investigation ongoing

All events, dates, and times approximate and subject to change; pending completed investigation.

Source of image: SolarWinds

2. Emails with payment information are often fake



From: Doe, Jane [mailto:jane.doe@exampleconpany.com]
To: bob.controller@examplecompany.com
Subject: Wire Transfer

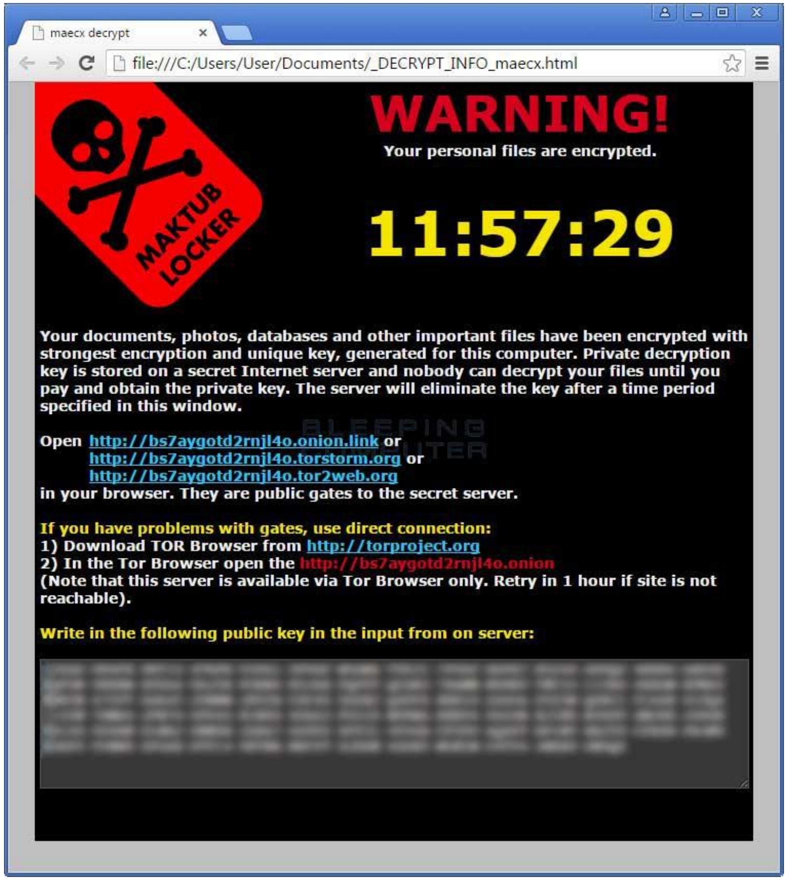
Kindly process wire transfer of $145,687 to attached wire instructions.
Please code to miscellaneous expenses.
Send me the confirmation when completed.

Jane Doe
Example Company
Chief Financial Officer

123 Main Street
Anytown, USA 10101
jane.doe@examplecompany.com
(555) 555-5555 Direct

3. Ransomware attacks are expensive

- Demands are larger
- Change in tactics:
  - Hackers “professionalized”
  - lay the “groundwork”
- “Double Extortion”
  - Release data to public
  - Encrypt files and operating systems
- More difficult to extract the malware from affected systems
- Average Ransom Paid in 2021 was $541k, up by 78%*
- Average Ransom Demand in 2021 was $2.2M, up by 144%*
- Average downtime is 21 days
- Industries targeted:
  - healthcare
  - government
  - professional services (increase)



WARNING!

Your personal files are encrypted.

11:57:29

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Open http://bs7aygotd2rnjl4o.onion.link or
http://bs7aygotd2rnjl4o.torstorm.org or
http://bs7aygotd2rnjl4o.tor2web.org
in your browser. They are public gates to the secret server.

If you have problems with gates, use direct connection:
1) Download TOR Browser from http://torproject.org
2) In the Tor Browser open the http://bs7aygotd2rnjl4o.onion
(Note that this server is available via Tor Browser only. Retry in 1 hour if site is not reachable).

Write in the following public key in the input from on server:

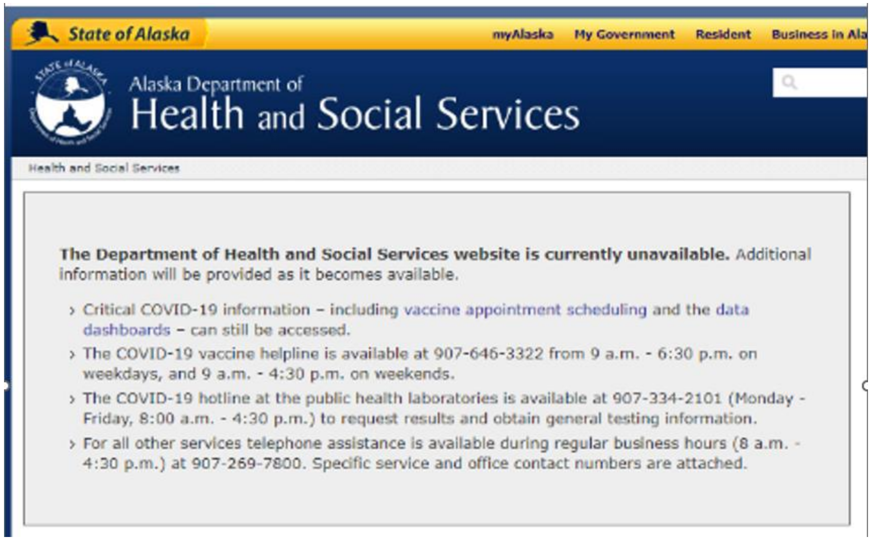
[redacted]

*cases worked by Palo Alto Networks

3. Ransomware attacks are expensive

Alaska Dept. of Health and Social Services

- May 2, 2021
- Notices to public Sept 27
- 500,000 records compromised:
  - Social Security numbers,
  - birthdates,
  - addresses,
  - phone numbers,
  - driver's license numbers and
  - health and financial information.
- $215,000 for credit monitoring
- $459,000 for computer forensic consulting from Mandiant



The Department of Health and Social Services website is currently unavailable. Additional information will be provided as it becomes available.

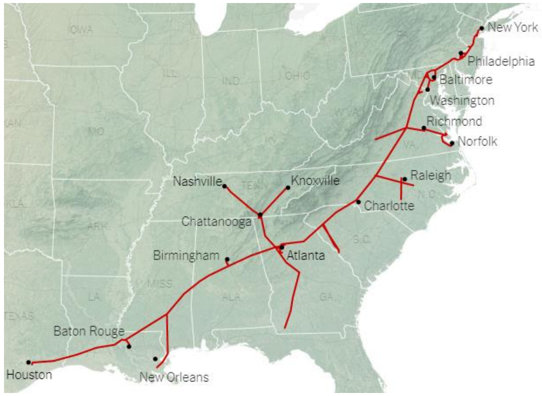
- Critical COVID-19 information – including vaccine appointment scheduling and the data dashboards – can still be accessed.
- The COVID-19 vaccine helpline is available at 907-646-3322 from 9 a.m. - 6:30 p.m. on weekdays, and 9 a.m. - 4:30 p.m. on weekends.
- The COVID-19 hotline at the public health laboratories is available at 907-334-2101 (Monday - Friday, 8:00 a.m. - 4:30 p.m.) to request results and obtain general testing information.
- For all other services telephone assistance is available during regular business hours (8 a.m. - 4:30 p.m.) at 907-269-7800. Specific service and office contact numbers are attached.

3. Ransomware attacks are expensive

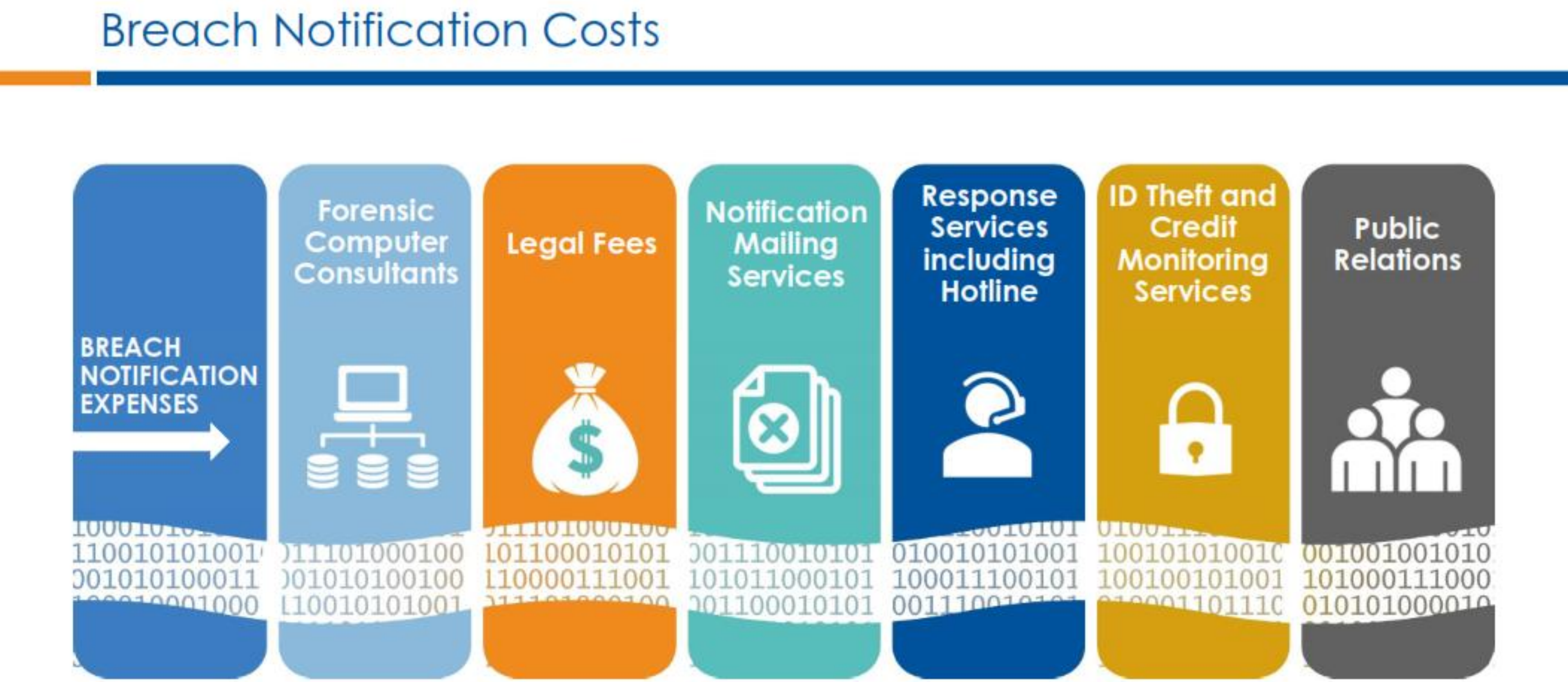
Colonial Pipeline

- May 6: attack launch
- May 7: payment of $5M in Bitcoin
- May 12: pipeline restarted

- Operational software for 5,500 miles of pipeline not affected
- DarkSide stole data, then locked up the billing and accounting systems
- They shut down the pipeline to be safe and be sure ransomware wouldn't spread
- US Government recovered $2.3M of ransom



4. Data breach events are expensive



Breach Notification Costs

BREACH NOTIFICATION EXPENSES

- Forensic Computer Consultants
- Legal Fees
- Notification Mailing Services
- Response Services including Hotline
- ID Theft and Credit Monitoring Services
- Public Relations

4. Data breach events are expensive

- It’s your data, even if you outsource the storage to the cloud
- If you have a breach, call in the experts (attorneys, forensics) early.
- Have a Breach Response Plan, and follow it carefully:
  - Maintain Attorney Client Privilege
  - Identify the source and extent of the breach
  - Address both the legal and ethical obligations
  - Be careful with communication and customer questions
  - Document everything
- Do a detailed post-mortem; Don’t try to go back to “normal” without evaluating what needs to be changed

5. Certain controls have proven to be critical

Access to Company Network

- Multi-Factor Authentication (MFA)
- Privileged Access Management (PAM)
- Bring Your Own Device (BYOD) controls
- Virtual Private Network (VPN)access
- IP Address Whitelisting controls

Endpoint Detection and Response (EDR)

- Utilized on entire network
- Vendor(s) used

Network Monitoring

- Internal or external or both?
- Logs and reports regularly monitored
- Penetration testing

System Backups

- Frequency
- Air gapped?
- Restrictive access
- Testing

Network Segmentation

- Critical systems
- End of Life (EoL) software

Patching

- Timing and frequency
- Timing for critical patches

5. Certain controls have proven to be critical

Other Issues

- Email identification and authentication tools
- Training and phishing campaigns
- Business Continuity Plan (BCP): recovery time estimated? Has BCP been tested?
- Size and budget of IT Department
- Ongoing and future security projects or changes to protocols
- Data destruction policies (in place and followed)
- Physical security at company location(s)
- Mergers & Acquisitions (if any): due diligence for IT of target companies
- Compliance with government regulations

6. Insurance is available, but market is challenged

Reactions of Cyber Insurers

- Raising rates
- Raising deductibles
- Introducing co-insurance
- Reducing offered limits
  - overall for companies buying $10M or more limits
  - line-item coverages (e.g., business interruption, ransomware)
- Much more vigorous underwriting
  - Demanding additional security (e.g., Multi-Factor Authentication)
  - Requiring specific software
  - Performing their own penetration tests
  - Questions about exposure to SolarWinds, Microsoft Exchange
- Exiting Cyber market altogether

Questions?

Charlie Morriss
Regional Director, EPS
USI Insurance Services

Charlie.Morriss@usi.com
206 992 1007