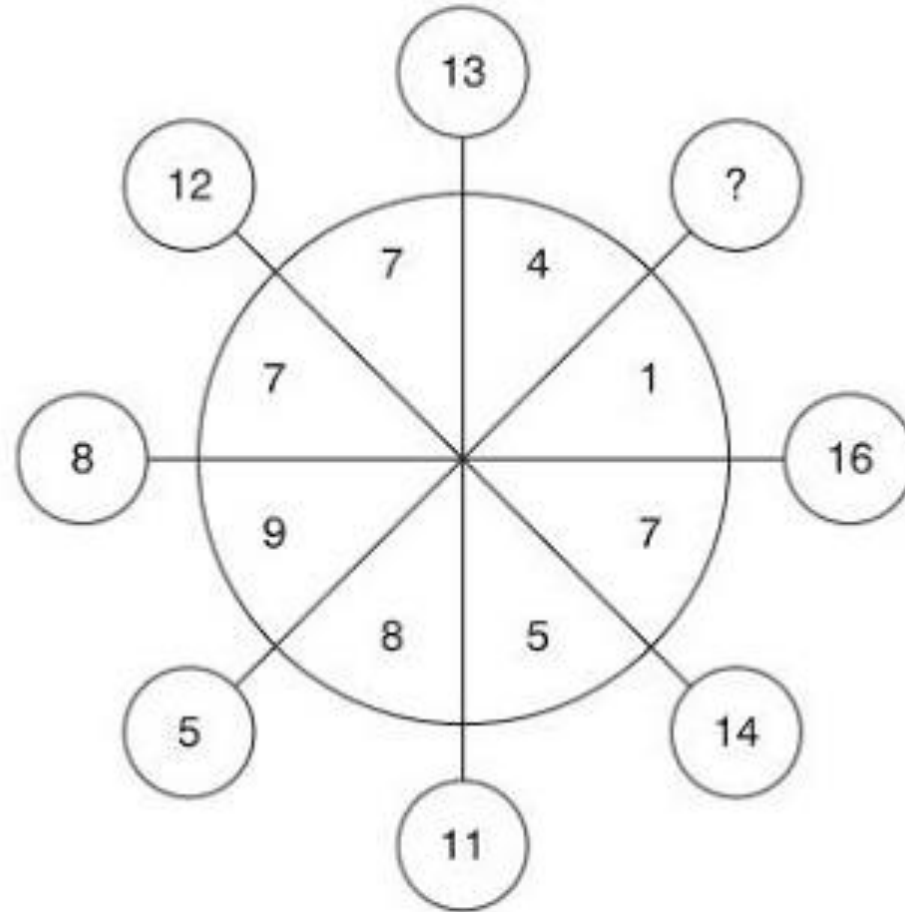




Pandemic: What Works and What Have We Learned?

Aaron Miller, CBCP, MBCI, PMP, CISA, CRISC
Business Continuity Analyst, RevSpring

A Math Puzzle





Agenda

Two Sections for our conversation:

- ▶ Covid-19 Considerations and Lessons Learned
- ▶ Current Considerations for a BC program

Lessons from Covid-19





What did your Pandemic Plan look like?

- ▶ Frequently an afterthought for plans
- ▶ High Impact / Low Probability Event
- ▶ Like a “Black Swan”: Events characterized by extreme rarity, severe impact, and the widespread insistence they were obvious in hindsight.
- ▶ Able to leverage pieces/parts of various BC/DR planning scenarios
- ▶ NBC Approach > Can cover Nuclear, Biological and Chemical scenarios

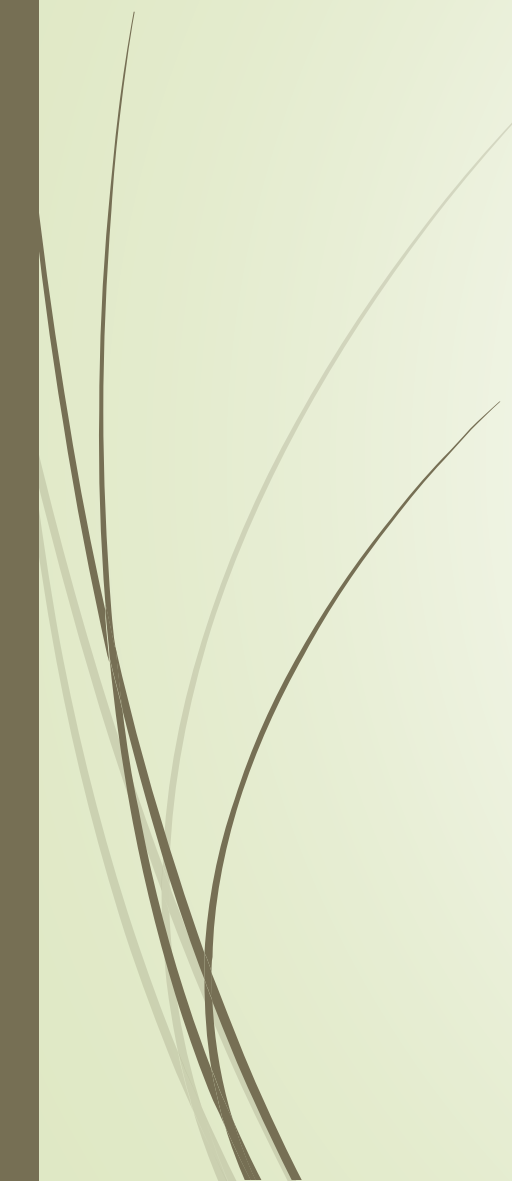


Remote Work / Process

- ▶ Did everyone have the equipment they needed?
- ▶ Could everyone access the files they needed?
 - ▶ Were those files available only inside a VPN connection?
 - ▶ Why or why not?
- ▶ What about printing?



Remote Work / Technology

- ▶ BYOD or not?
 - ▶ Home Wi-Fi
 - ▶ Security
 - ▶ Network speed
 - ▶ VPN
 - ▶ MFA
 - ▶ How are increased risks minimized or managed?
 - ▶ Is phishing and ransomware more likely or less?
- 



Lack of Laptops....

Problem: What if my organization has an insufficient number of laptops for its workforce?

Options:

- ▶ Employees use email and phone only
- ▶ Establish VPNs from personal computer to business network
- ▶ Remote access to workstation (LogMeIn, GoToMyPC)
- ▶ Can leverage thin clients

Source: Accume Partners



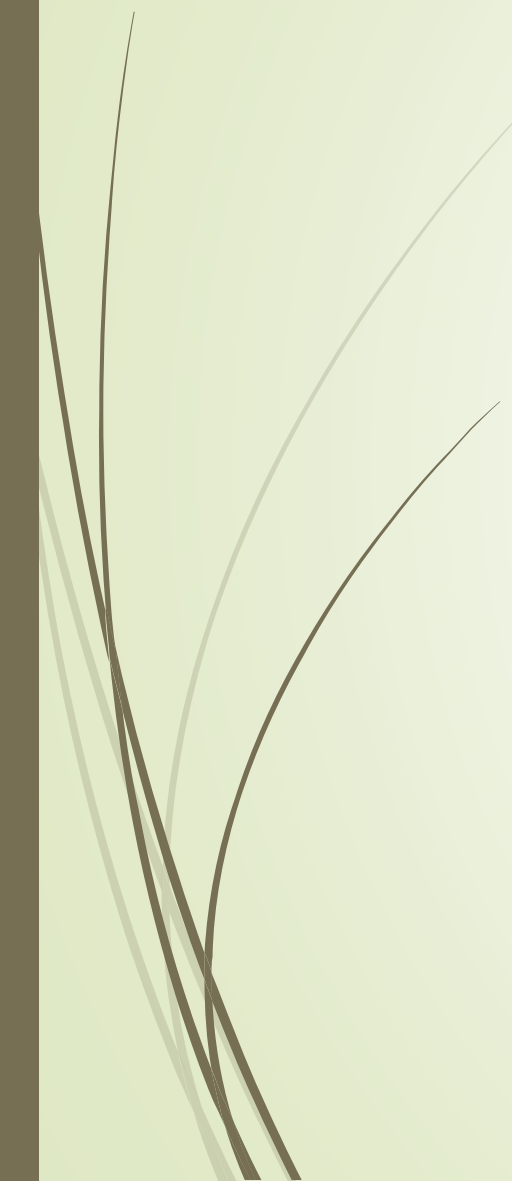
Laptop Technology Risks

- ▶ Businesses lose control of the location of their data
- ▶ Version control is limited and can become problematic
- ▶ Greater exposure to social engineering
- ▶ Insufficient access controls and limited use of Multi-factor authentication
- ▶ Higher risks to the business if personal computer is compromised
- ▶ May require firewall reconfiguration that could limit protections
- ▶ Thin clients can introduce risks if they have removeable storage

Source: Accume Partners



Response Plans

- ▶ Strength of Governmental Authorities to shut down usual business
 - ▶ What does resumption look like with social distancing?
 - ▶ What's the effect on business margins if capacities are diminished or limited?
 - ▶ What's the impact of limited/restricted travel?
- 



Supply Chain Management

- ▶ Set up a central emergency management center with clear decision-making rules. Include delegations at least two-deep
- ▶ Establish key priorities for which products should be built and which customers should be supplied first if capacity is significantly reduced
- ▶ Determine which of the company's suppliers make critical parts, track their inventories, and establish potential alternate sources
- ▶ In the near term, plan operations that will maximize cash flow rather than profits
- ▶ Maintain close communications with national and local authorities as well as with colleagues and partners on the ground

From Yossi Sheffi, The Resilient Enterprise, MIT



Supply Chain Example > Amazon

- ▶ Account for Chinese New Year in planning
- ▶ Covid-19 hit Amazon twice:
 - ▶ In 2020, plants did not re-open after New Year > Suppliers went offline, and vendors passed delays on to manufacturing clients
 - ▶ Many Amazon sellers (3rd party) source from China, and simply ran out of goods



Personal Protective Equipment (PPE)

- ▶ Do you require employees to wear masks/gloves?
- ▶ If so, do you provide them?

- ▶ Will you require customers to wear masks?
- ▶ What will you do if they refuse?

- ▶ How do you incorporate social distancing into your business operations?
- ▶ Do you have margins to support your business at 50-60% of capacity?



After-Action for Covid-19

- ▶ It is a real event, that has tested organization's resiliency and capability on both the continuity and recovery side
- ▶ Complete an after-action report and note what worked and what needs help. If you've already addressed some gaps, note that in the report
- ▶ Ensure that current BC/DR plans reflect all lessons learned and latest practices
- ▶ There will certainly be some unanswered questions. Document those and be courageous in seeking out answers
- ▶ Don't be caught unaware if a second wave occurs in the US in the fall or winter, which would align with flu season



Current Considerations



Supply Chain

- ▶ How long are items “on the water?”
- ▶ Are there risks in the international supply chain?
 - ▶ Geographic
 - ▶ Political
 - ▶ Logistical
- ▶ Just in Time management vs. Resiliency management
- ▶ Are there new regulatory considerations around vendors (App J)



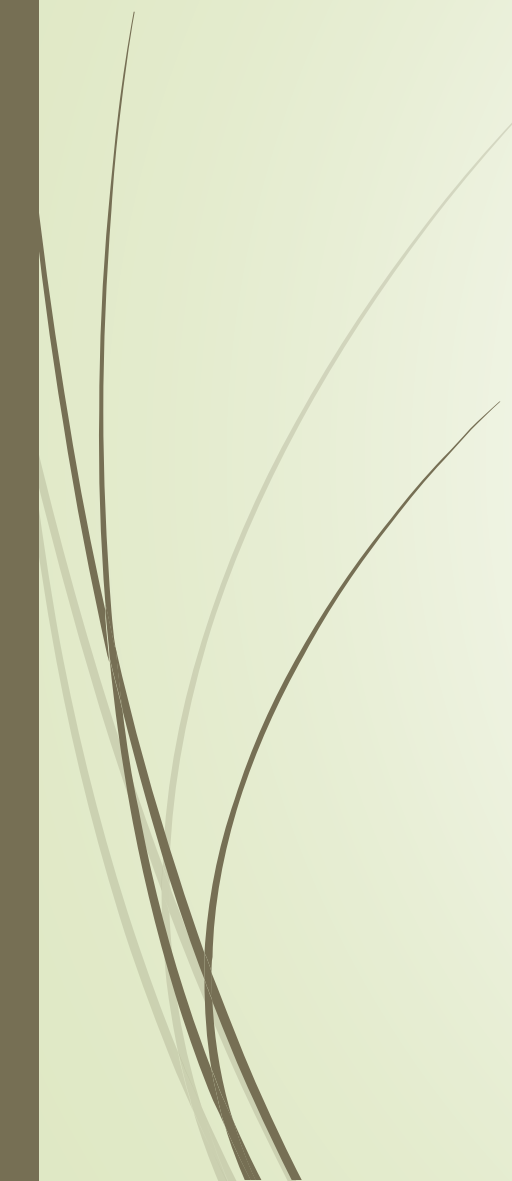
Vendor Management



- ▶ What are they delivering for you and your customers?
 - ▶ The risk remains yours and your company's image
 - ▶ SLA's are not guarantees
 - ▶ Track, test, verify
 - ▶ What if they won't say?
 - ▶ Who audits them and their work? You or them or a third party?
- ▶ If there's a hiccup, what's your responsibility? What's their responsibility?
- ▶ Who's going to care more about your business?



More Vendor Management

- ▶ Ensure contracts have “right to audit” clauses
 - ▶ Exercise DR/BC plans (BOTH) with the vendor to ensure capability
 - ▶ Do you have a contact beyond sales and/or customer service?
 - ▶ If data exchanges are involved, risks are higher
 - ▶ Are you or the vendor doing business internationally?
- 



Privacy Considerations

- ▶ General Data Protection Regulation
 - ▶ Affords protections to consumers in the EU
 - ▶ Imposed on US Companies doing business in EU
 - ▶ Forbids processing of data outside original purpose
 - ▶ Subjects have rights to request what's on file, and to be “forgotten”
- ▶ California Consumer Privacy Act
 - ▶ Right to know what's being collected
 - ▶ Is the data being sold or disclosed?
 - ▶ Discrimination based on data is now prohibited (definitions and limitations will evolve under law)
- ▶ Latest is NY Shield Act: Stop Hacks and Improve Electronic Data Security
Mar 2020



Identity Access Management

- ▶ Network access v. application/resource access
- ▶ Part of an integrated ERM program
- ▶ Who has rights to what?
- ▶ Based on what documentation, regulation or policy?
- ▶ Who reviews/enforces? How often?



Exercises

- ▶ Data Recovery Exercise
- ▶ Alternate Site Exercise
- ▶ Vendor Exercise
 - ▶ Their failure to your prod
 - ▶ Your failure to their prod



The Cloud(s)

- ▶ What's the security perimeter? How can you be sure?
- ▶ How do you optimize/secure
 - ▶ Vendor contracts
 - ▶ Vendor implementations
 - ▶ Vendor/in-house controls
- ▶ Cloud Access Security Brokers
 - ▶ On site or cloud-based
 - ▶ Monitor all activity and enforce security protocols



CyberSecurity



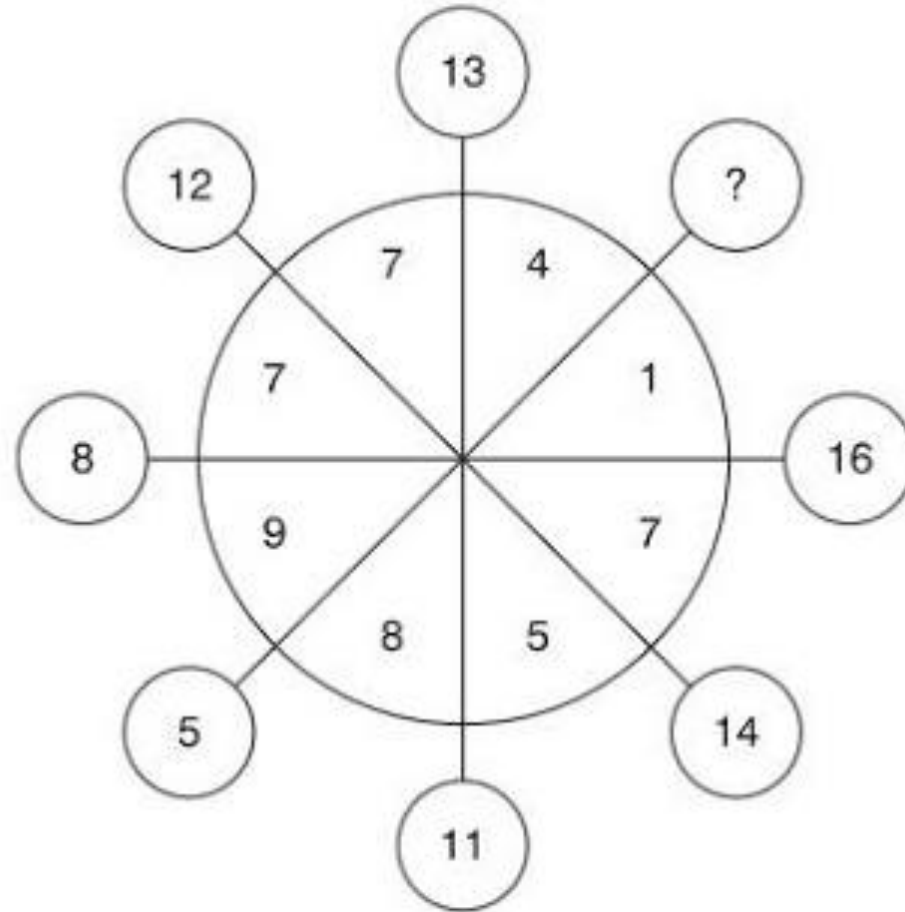
- ▶ Does your organization have a cybersecurity response plan for ransomware?
- ▶ How often are employees trained/tested on phishing exercises?
 - ▶ Best to send test and see
 - ▶ Train the ones that routinely make errors
- ▶ Working remotely heightens the need for employee awareness



BC/DR part of ERM Program

- Increasingly, BC/DR is moving from IT, Finance or Facilities into ERM
- Think of how BIA/Risk Assessment can help with ERM
- Not the whole picture
 - Include InfoSec
 - Include Internal Audit
 - Confidentiality, Integrity and Availability
 - SOX, HIPPA, NIST

Our Puzzle





Thank you very much!

Worry is not preparation

- Dr. Bryan Robinson

Aaron Miller

amiller@revspringinc.com