Coronavirus Crisis: Pandemic Response & Cybersecurity Considerations

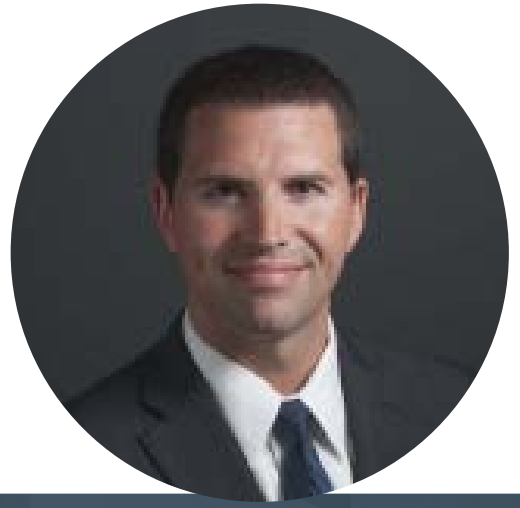
The Worst Case Scenario Happened

BKD CYBER

Presenters

Ron Hulshizer, CMA, CGEIT, CISA
Managing Director | BKDCyber
Oklahoma City, Oklahoma
rhulshizer@bkd.com

Cy Sturdivant, CISA®
Director | BKDCyber
Nashville, Tennessee
csturdivant@bkd.com



Agenda

- ❑ Discuss the impacts and lessons learned from COVID-19
- ❑ Assess strategies for how to respond to such events in the future
- ❑ Identify how existing cybersecurity threats are more dangerous now than ever before
- ❑ Useful Resources
- ❑ Questions

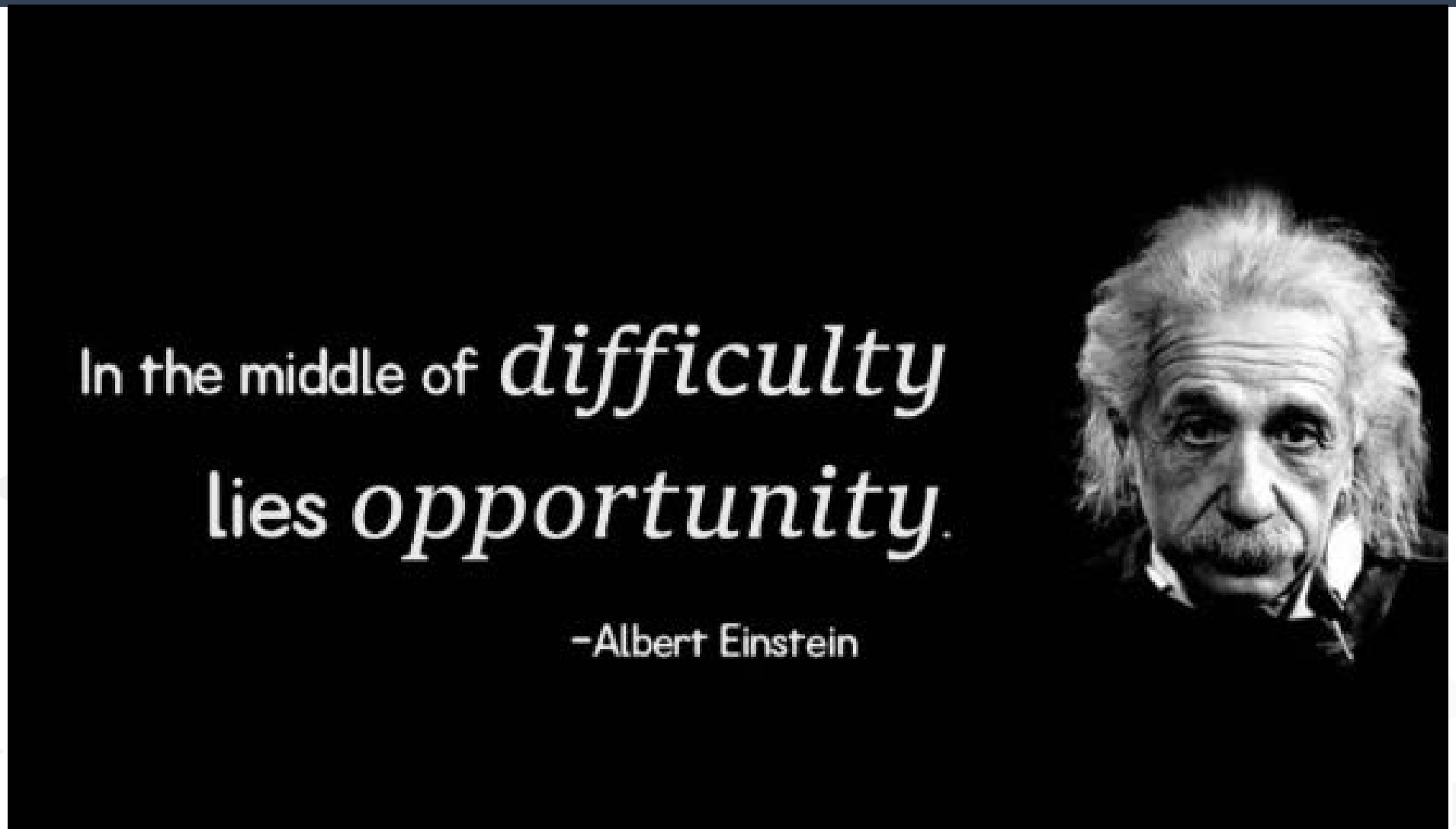
Impacts and Lessons Learned

We did not see this coming!

TOP IMPACTS

- Lag in converting to a remote workforce due to a lack of hardware. *i.e. laptops, monitors, phones, etc.*
- Difficulty configuring new devices (or repurposed devices) in such a short timeframe.
- VPN capacity and MFA licensing issues *i.e. bottlenecks and availability*
- Absenteeism/distractions due to extended remote period with family members
- Increased demand on IT/IS with wide range of hours (internal and MSP)
- Struggles with onboarding new personnel and/or furloughing employees
- Increased focus on customers due to demands, depending on your services

TOP LESSONS LEARNED



TOP LESSONS LEARNED

- The need to understand the full maturity needs for operating remotely. *i.e. hardware, deployment, hardening, communications, security, employees, etc.*
- Mobile devices and cloud technology are now a must have. *i.e. O365/Azure/Teams, AWS, Google, BYOD, etc.*
- The need to enable secure remote access software. *i.e. Citrix, Virtual Box, VMWare, etc.*
- The need for cloud based security platforms operating outside the network
- Enabling scalable VPN / MFA solutions with license retainer is a must
- Training needs of extended remote workforce for appropriate use of VPN, virtual software, soft phones, etc. *Note: More focus on cross training*
- Communication is paramount – from who, simplicity, timing, etc.
- Creating a culture of mobility and remote expectations

BKD

TOP LESSONS LEARNED CONT…

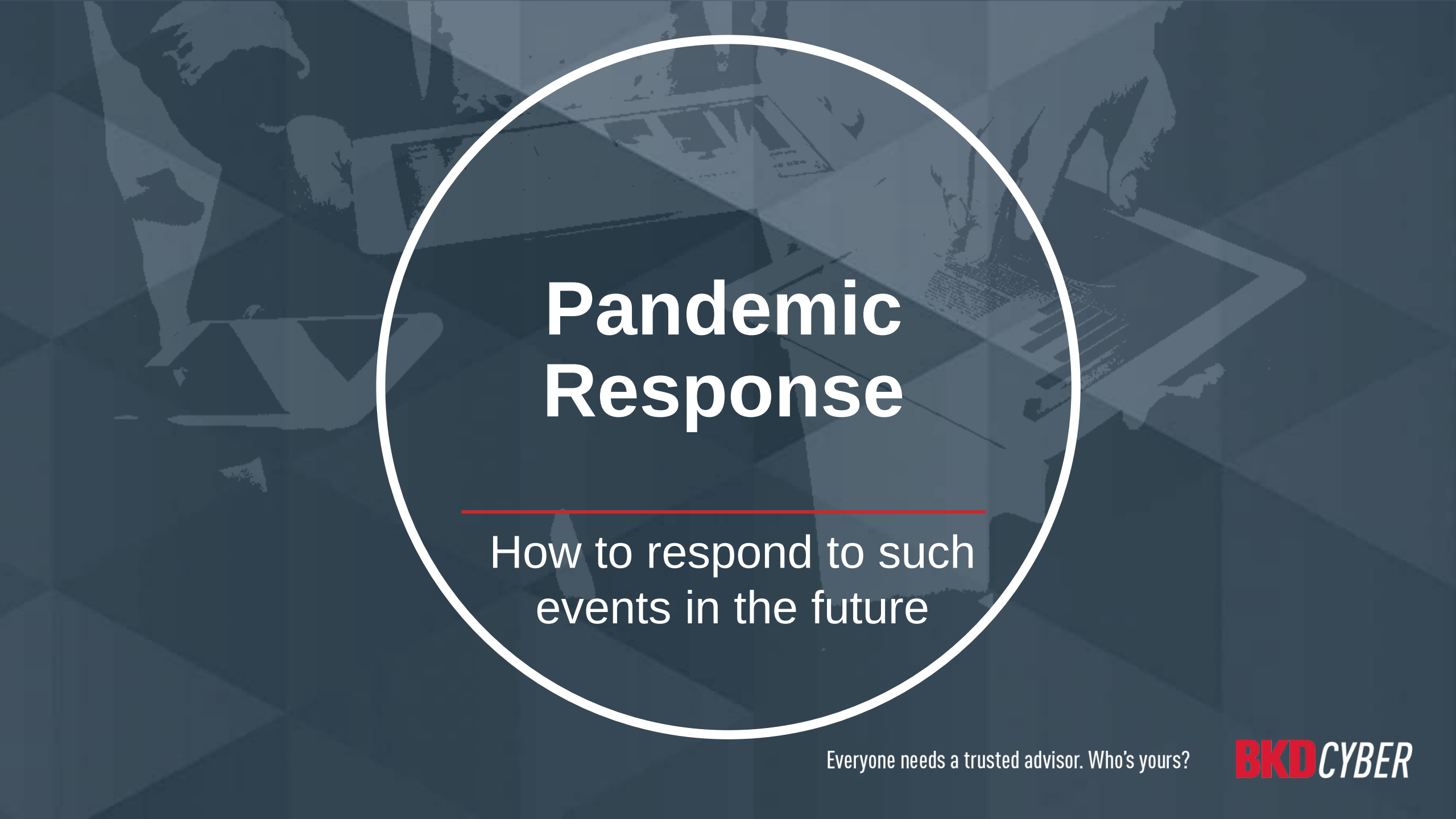
Our existing Pandemic Plan and Business Continuity Plan efforts were not designed to handle this event!

Also, we need a three month supply of…

toilet paper!

TOP ONGOING SUGGESTIONS

- Switch onsite visits to appointment-only. Review appointment reasons to see how you might transfer future visits to virtual, call center, or digital channels.
- Adjust location hours and staffing mix. For example, establish set teams with alternating staffing days to avoid cross-contamination. Additionally, adopt “golden hours" at the beginning of the day to serve vulnerable populations.
- Address how to handle physical contact with customers. Wear masks!
- You may want to consider options for idle real estate, such as dispersing call center employees to unused locations for social distancing.



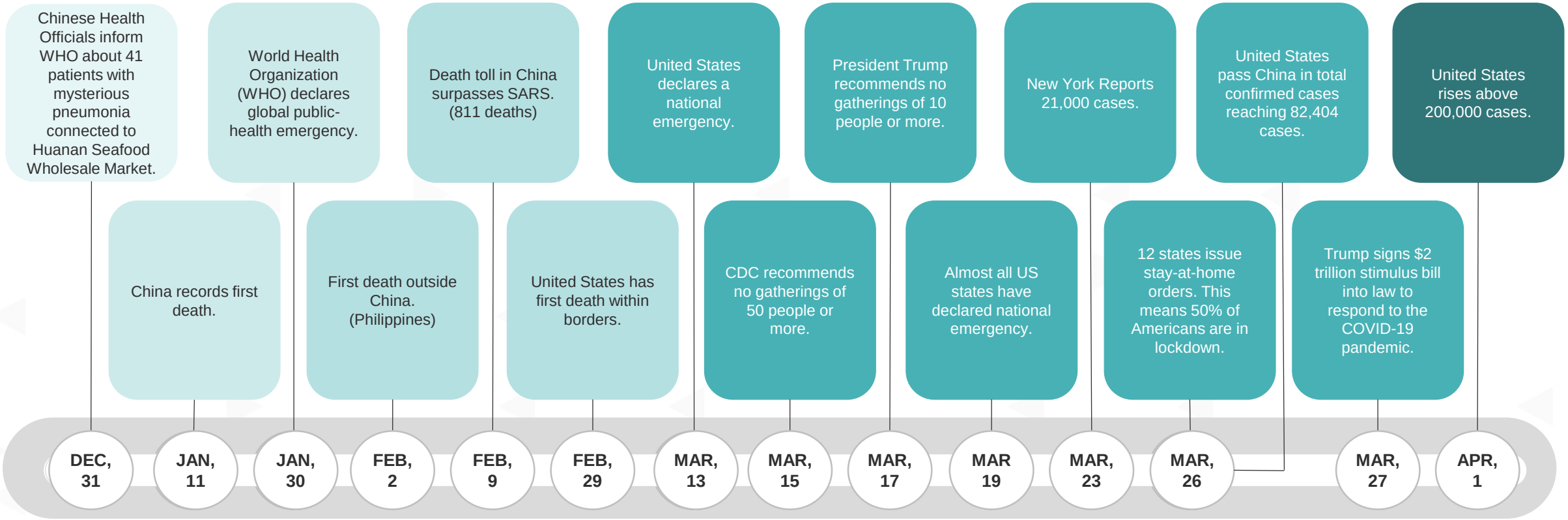
Pandemic Response

How to respond to such events in the future

Everyone needs a trusted advisor. Who's yours?

BKD CYBER

COVID-19 TIMELINE



TRADITIONAL BUSINESS CONTINUITY

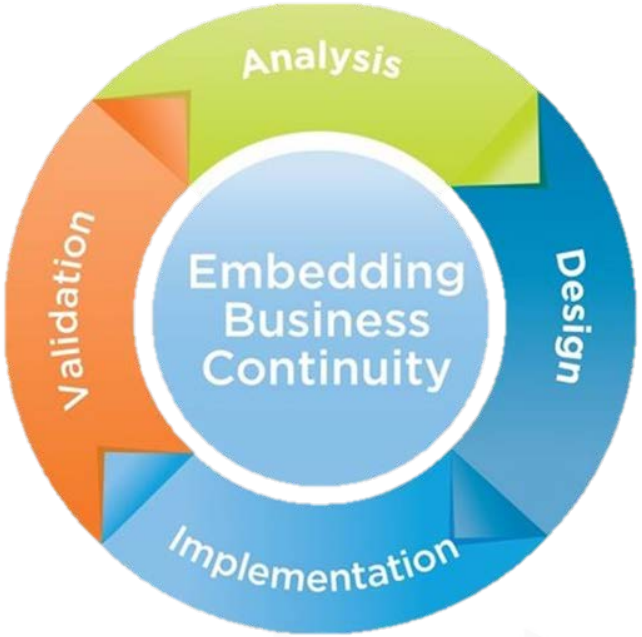
Considers an impact to one office or a geographic location:

- Natural Disasters
- Power outage
- Cyber attacks

This assumes another office takes on the work

Looks to resolve issues and maintain operations:

- Maintain operational efficiencies
- Back-up site and connections
- Pay the ransom
- Emergency relief



COVID-19 WAS A FIRST

Traditional

- Considers only a portion of facilities being impacted
- Operations would resume at other company locations
- Provide a means to restore data
- Could follow the playbook of a pre-written plan

COVID-19

- All locations and departments were impacted
- You had to adjust to remote conditions quickly
- Data was not directly impacted
- Most BC plans were not the right fit; consider elements from various plans

BKD

PANDEMIC PLAN MUST CONSIDER THE BIA

- ALL business processes must be assessed.
- “Mission Critical” functions within each business process must be identified
- Potential threats and impacts should be assessed per business process
- Supporting technology systems must be mapped to business processes and mission critical functions.
- Viable business process risk scenarios should be considered, by grouping (natural, technical, social, and human)
- Estimate dollar-loss for each viable business process risk scenarios to help determine financial impact

Cybersecurity Considerations

We fear what we do not understand

Everyone needs a trusted advisor. Who's yours?

BKD CYBER

Breach Detection and Expense

You can't afford to ignore cybersecurity – Especially now!

Average total cost of a data breach in FS **$3.92 million**

Average cost per lost or stolen record **$150**

Likelihood of a recurring breach within two years **29.6%**

Mean time to identify a breach **206 days**

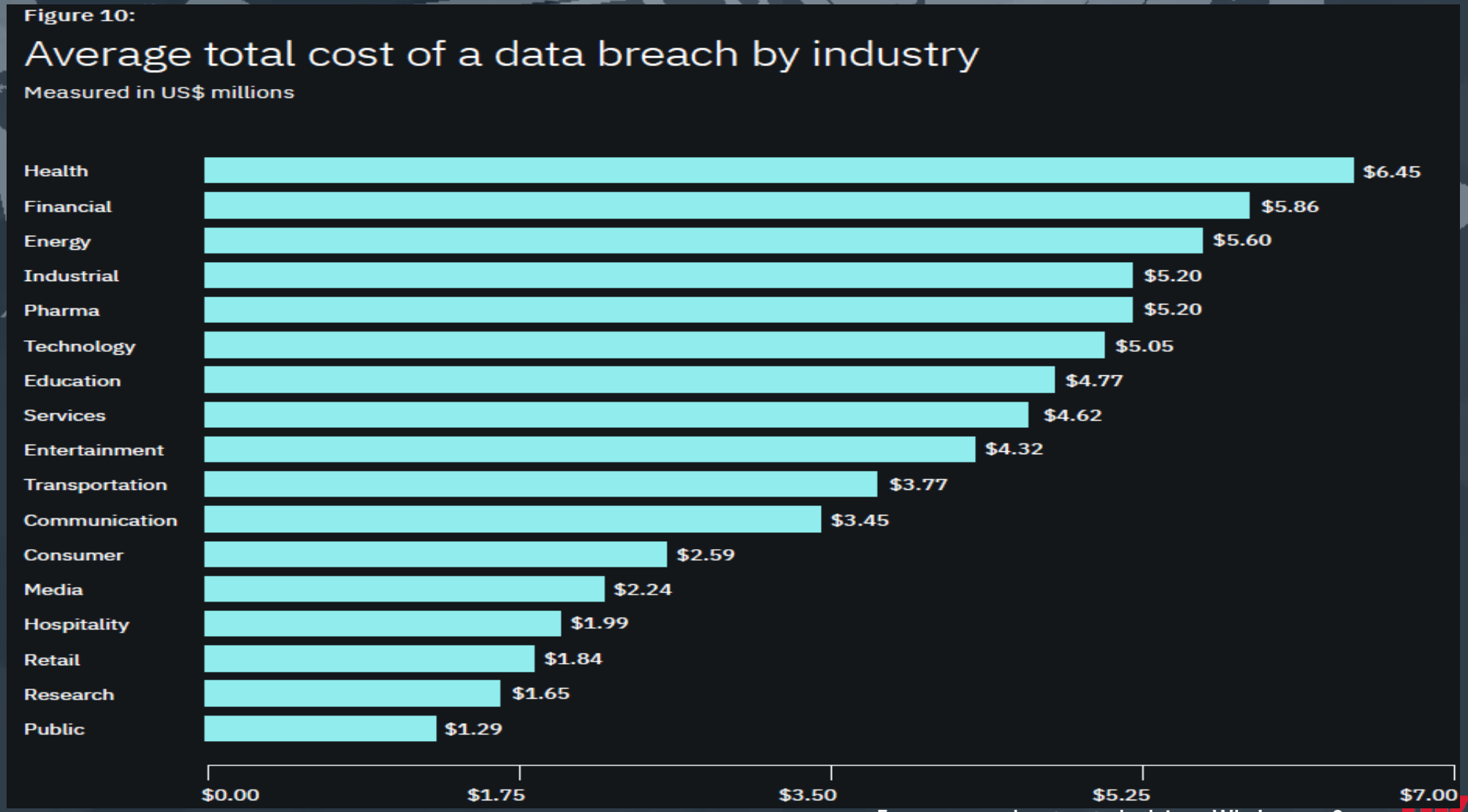
Mean time to contain **73 days**

Companies with an incident response team and extensive testing of their response plans could save over $1.2 million

Source: Ponemon Institute 2019 Cost of Data Breach Study

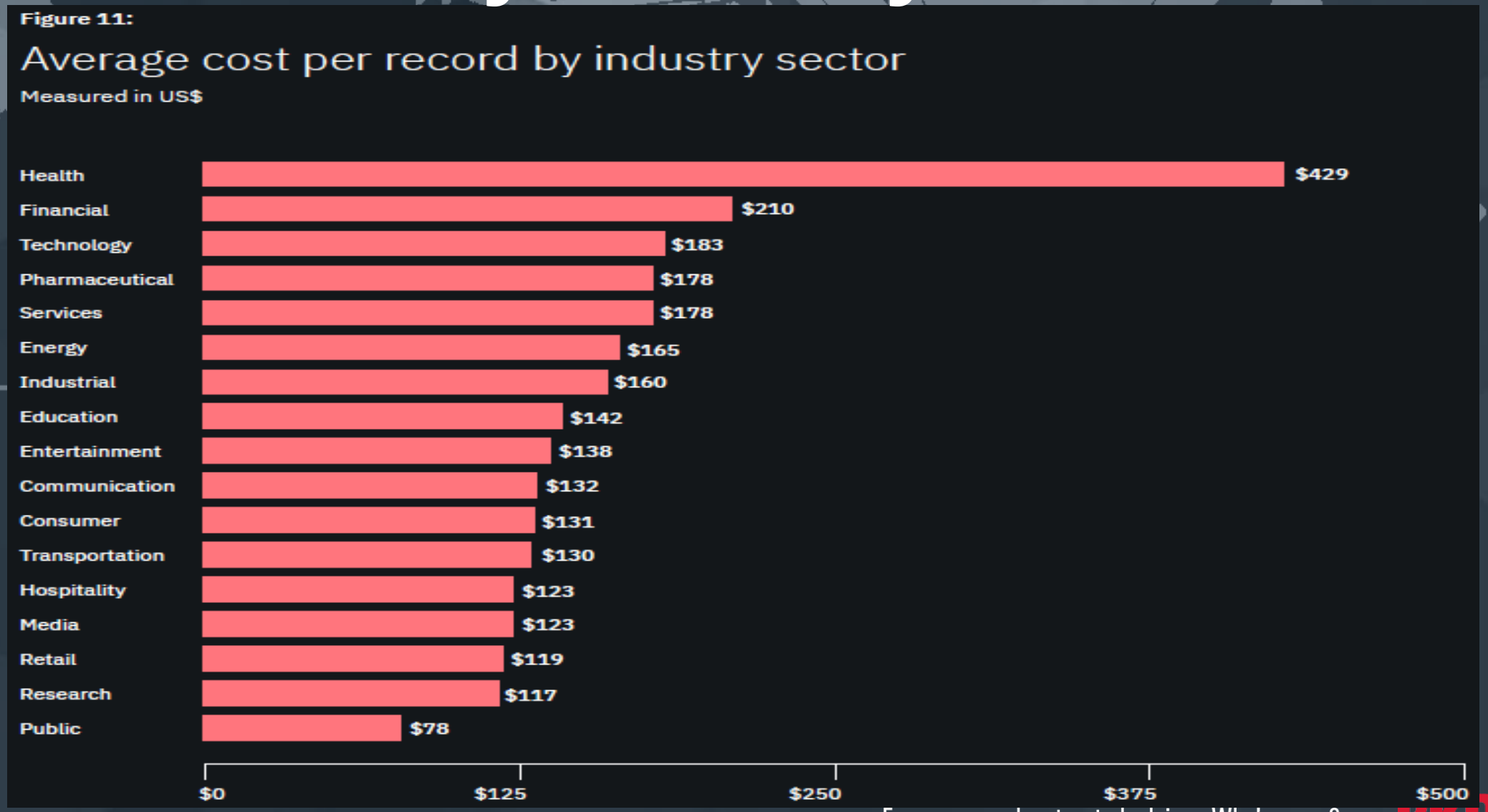
Breakdown by Industry

Figure 10:



Breakdown by Industry

Figure 11:

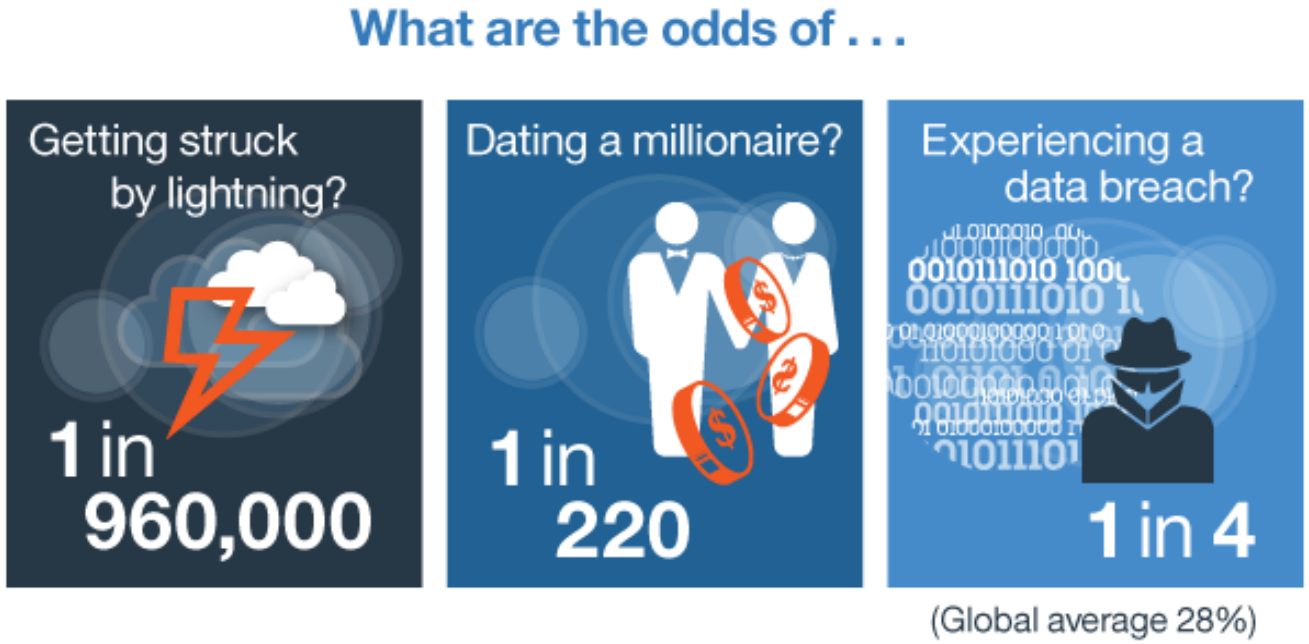


Don’t Equate Small With Safe

Despite significant cybersecurity exposures, 85% of managers and owners believe their organization is safe from hackers, viruses, malware or a data breach.

Symantec’s study found that 40 percent of attacks are against organizations with fewer than **500** employees.

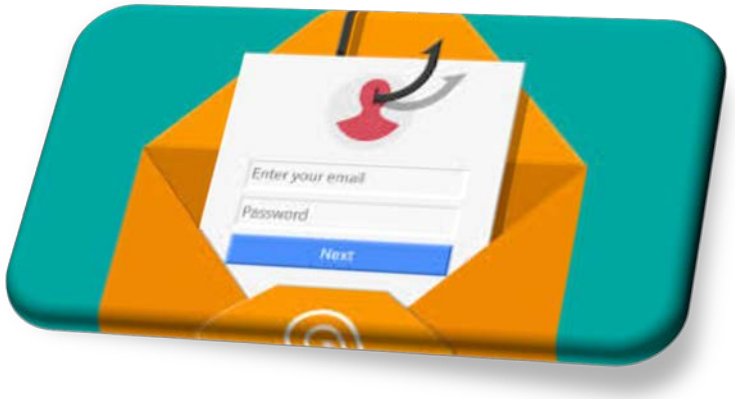
Over 60% of breaches take place at organizations with less than **1,000** people



IBM: Cost of a Data Breach

Cybersecurity Threats Are Now Magnified

- Social Engineering Attacks – Phishing
- Malware/Destructive Malware
- Cyber Extortion
  - Ransomware
- Business Email Compromise
- Corporate Account Takeovers



Root causes of cyber attacks: Inadequate training, ineffective patch management, weak privileged access controls & unmonitored detection systems

Global Domain Registrations Correlated with Pandemic Growth

1. Phishing
2. Malspam
3. Ransomware
4. Mask campaigns
5. Web Skimming
6. Spyware

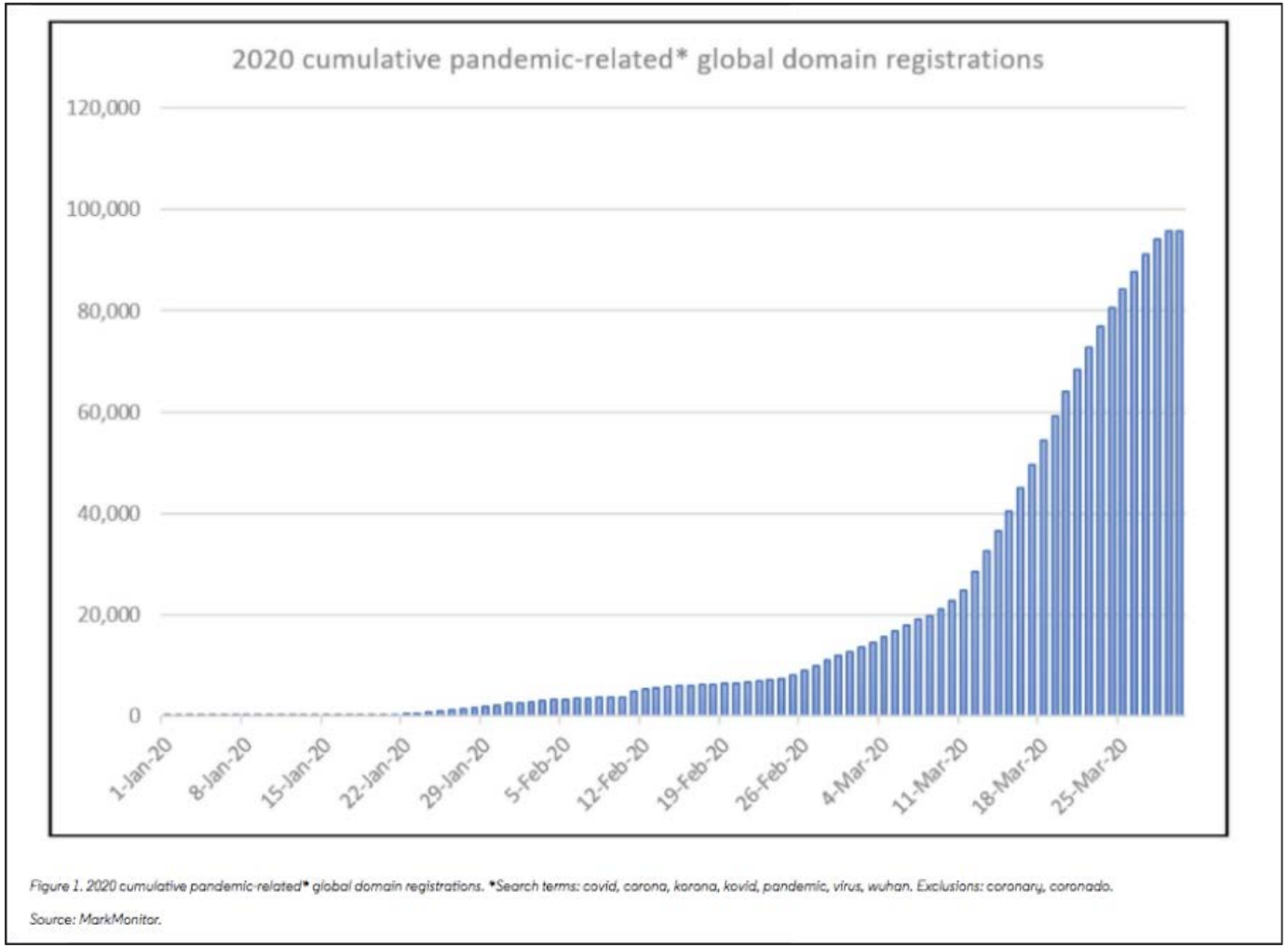
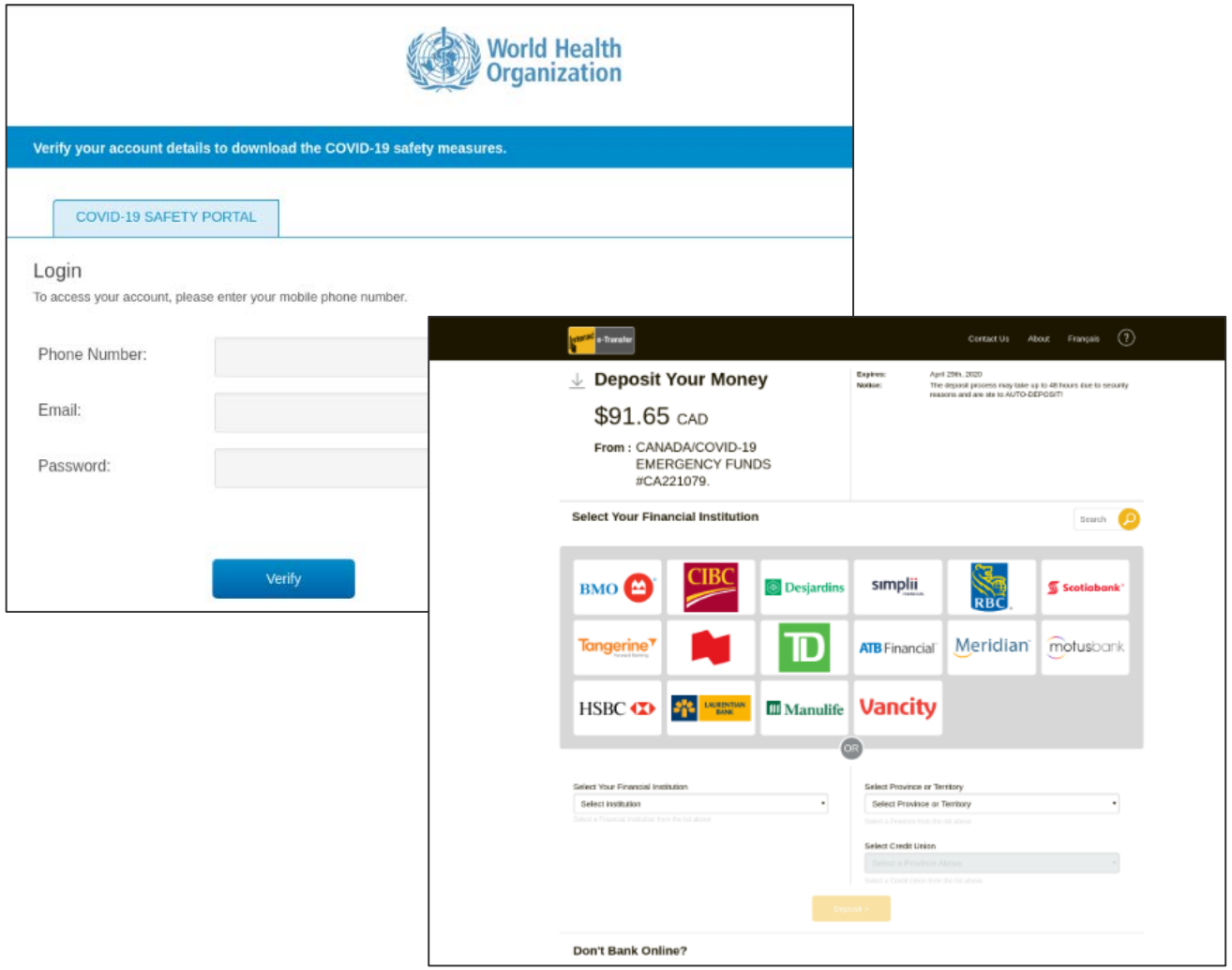


Figure 1. 2020 cumulative pandemic-related global domain registrations. *Search terms: covid, corona, karona, kovid, pandemic, virus, wuhan. Exclusions: coronary, coronado.*

Source: MarkMonitor.

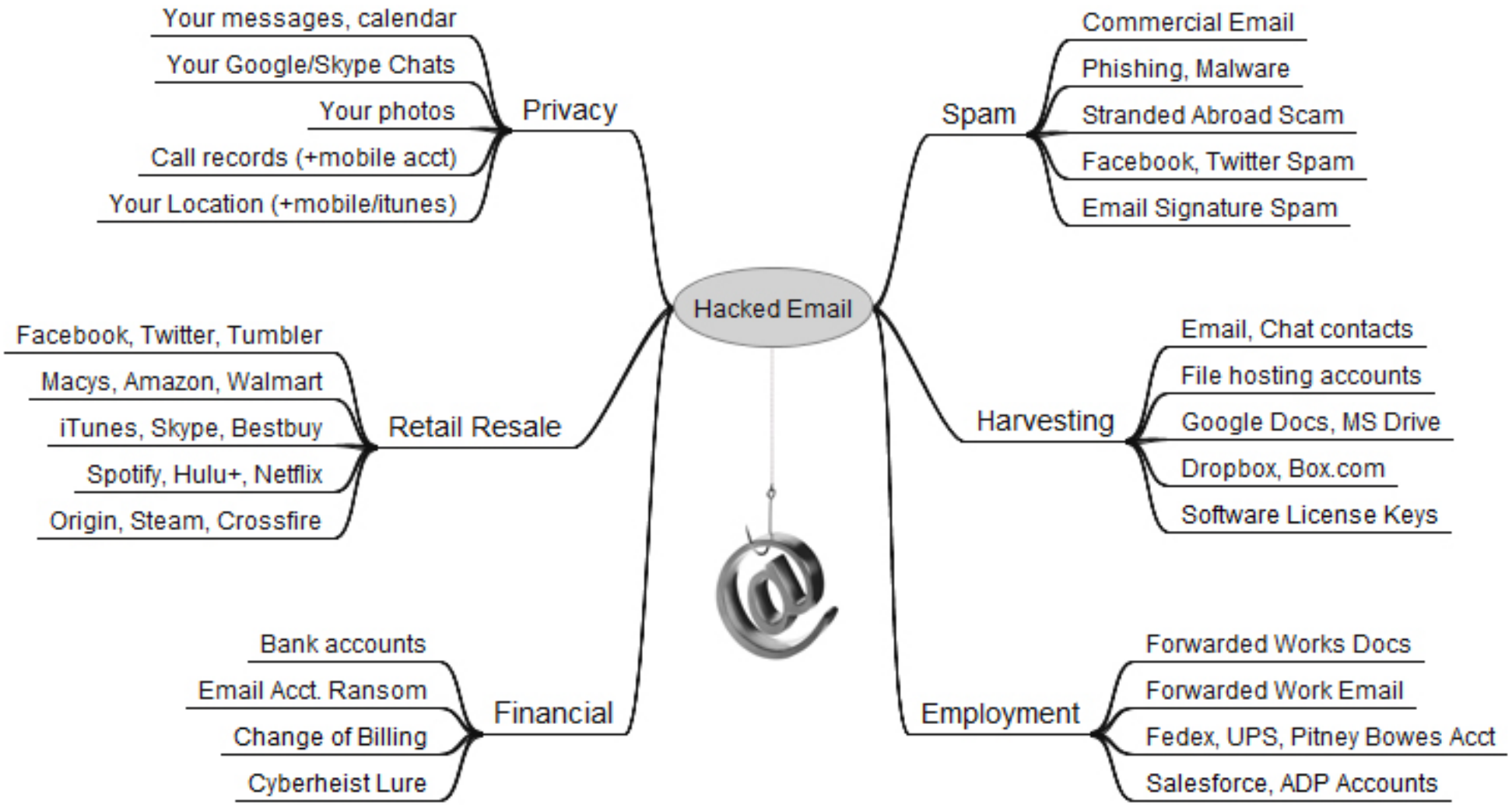
Fake Sites

- They will look very legitimate and clone beneficial organizations
- Goal is to install software or collect personal information
- In several cases, they will want donations and/or payment information



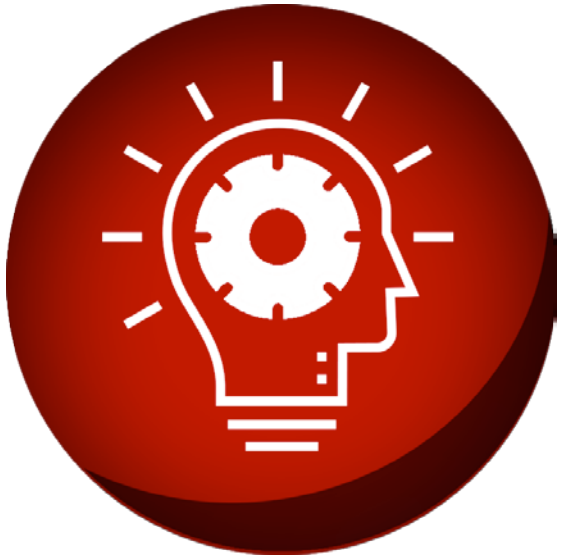
Source: Trendmicro https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

The Ultimate Gateway - Email



Single Biggest Risk - Users

Importance of Awareness Training

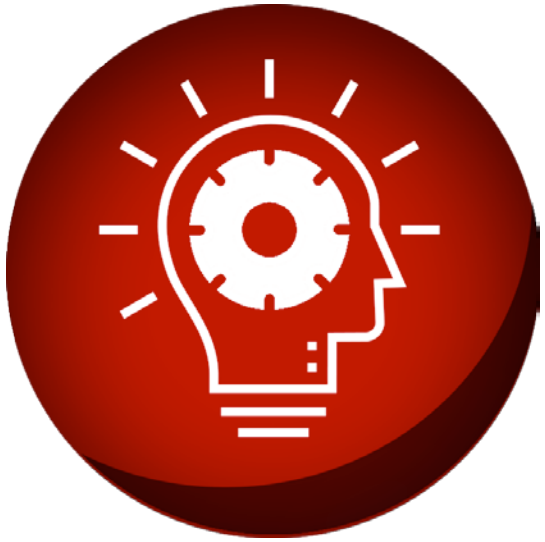


C-level executives are 12 times more likely to be the target of social engineering attacks.

85-90% of all breaches and incidents relate to human error. Most are the result of phishing campaigns!

Single Biggest Risk - Users

Importance of Awareness Training



Training and Awareness

- Cybersecurity is as much a mindset as it is technical.
- **Reduce access levels of staff to the minimum required to perform daily duties. Nothing more**.
- More frequent training now than ever before.
- “Simplify” methods to notify staff of emerging threats – **don’t bury those alerts**
- Strong information security policies and strong acceptable use policy are a must!

Key Considerations: Focus on Technical Controls

- Use **multi-factor** or **two-factor** for O365, VPN, Remote sessions and privileged access.
- Track, report, independently test & update security **patches** based on a risk priority schedule (Microsoft & non-Microsoft patches)
- Maintain accurate **asset inventories** for Hardware and Software, including **data classification**
- Enforce **application whitelisting** controls and **remove** unauthorized applications
- **Remove local administrator** rights to reduce malicious software installs
- **Tune existing security tools:** web content, email filtering, end point, etc.
- Deploy **Cloud based security** software and end-point protection (Sophos, Web Root, etc.)

Key Considerations – Technical Controls Cont.

- Implement strong cloud based **data loss prevention** controls
- Use **Security Information & Event Management (SIEM)** tools with **"defense in depth"** approach
- **Change** your passwords more frequently during this time
- Ensure **data encryption** is enforced to protect confidential data
- **Segment** internal Networks to isolate critical systems
- Be aware of **insider threat** – layoffs, disgruntled, etc. Think zero-trust!
- Consider installing **secure home Wi-Fi routers** for Key personnel
- Consider **posture checking** on corporate devices prior to joining VPN / network

What Cybercriminals See, if You Fail!

SUMMARY / FINAL THOUGHTS

- Communication and commitment from senior leadership is key!
- Keep providing “value add” updates to all employees
- Keep documentation of activities and events to update the plan during the post mortem
- Use company approved devices and services only, trust less not more!
- Be suspicious of emails that appear urgent
- Stay connected – virtual meetings or similar check-ins
- Focus on family and local businesses!

Resources:

- BKD COVID-19 Resource Center - https://www.bkd.com/covid-19-resource-center
- Overview Statistics - https://covid19.healthdata.org/united-states-of-america
- The Top Cyber Threat Intelligence Feeds – thecyberthreat.com/cyber-threat-intelligence-feeds

Key Note: Follow your Local and State information sites for up-to-date guidelines!

Questions?

Thank You!

bkd.com | @BKDLLP

BKD
CPAs & Advisors