WOODARD™

COVID-19 Roundtable

Tech Triage: Stopping the COVID-19 Technology Bleed

WOODARD™

- Education
- Coaching
- Community
- Resources

Joe Woodard

- Published author McGraw Hill, *Accounting Today*, *CPA Practice Advisor, AccountingWEB, The Journal of Accountancy and Insightful Accountant.*
- Career Trainer to over 125,000 accounting professionals
- 2012, 2014 – 2019 – Top 100 Most Influential People by *Accounting Today*

elliott davis

Brian Kirk
Director of Cybersecurity

Tom Uva
Director of Management Consulting Systems

WOODARD™

Topics for Discussion:

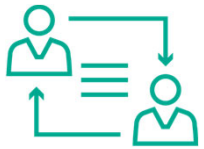
- Connectivity concerns for clients with on-premise and cloud-based technology solutions
- Increased privacy and security concerns or clients who have recently enabled their employees to work remotely from home
- Strategies for your own practice to facilitate efficient and safe client communications

Disclaimer

This material was used by Elliott Davis during an oral presentation; it is not a complete record of the discussion. This presentation is for informational purposes and does not contain or convey specific advice. It should not be used or relied upon in regard to any particular situation or circumstances without first consulting the appropriate advisor. No part of the presentation may be circulated, quoted, or reproduced for distribution without prior written approval from Elliott Davis.

Who is Elliott Davis?

Elliott Davis is a leading business solutions firm offering a full spectrum of services in the areas of tax, assurance, and specialized consulting services to diverse businesses and individuals. The firm, which has been providing innovative solutions since its founding in 1920, leverages a network of nearly 800 forward-thinking professionals in major domestic markets and alliance resources across the globe.



Consulting

Tax

Audit & Assurance

Cybersecurity Advisory Services

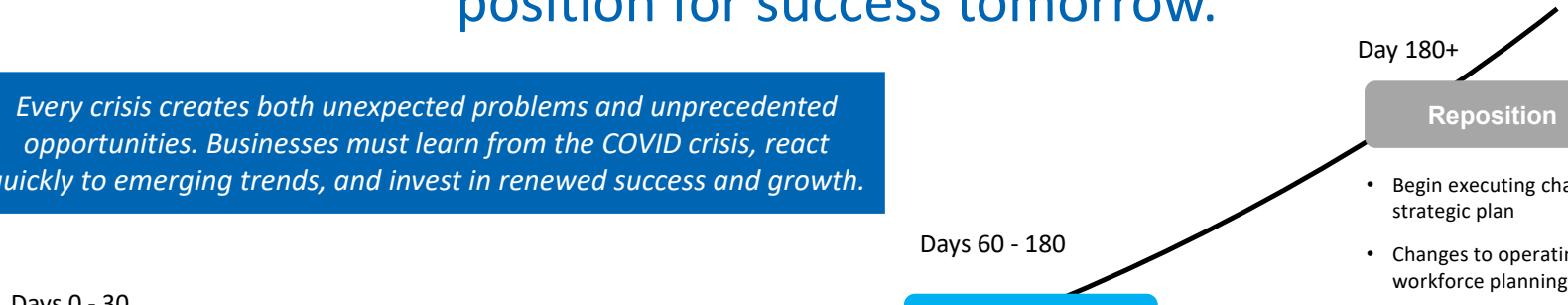
Securing Where You Want To Be

Elliott Davis Cybersecurity Advisory consultants work with customers to reduce their overall risk and impact of a cyber-attack by performing risk assessments, penetration tests, and architectural reviews. Consultants also evaluate the effectiveness of policies and procedures and can assist in the development and testing of incident response plans.

Pathway to Recovery & Success: The Big Picture Context

Business Leaders are faced with managing today's response but must also position for success tomorrow.

Every crisis creates both unexpected problems and unprecedented opportunities. Businesses must learn from the COVID crisis, react quickly to emerging trends, and invest in renewed success and growth.



Days 0 - 30

Respond

- Establish a safe and healthy employee work environment
- Ruthlessly gather, analyze, and respond to market intelligence
- Transition to remote work & monitor impact of absenteeism on operations
- Establish clear internal and external communication channels
- Establish "War Room" to enable timely, informed decisions and info sharing
- Secure technology platforms

Days 30 – 60

Stabilize

- Develop/refine cash projections & stress test financial models
- Stabilize cash flow via aggressive expense reduction actions
- Assess all options to secure additional capital as needed
- Begin to rebalance short-term supply and demand
- Step up communications with employees, vendors, and customers through "demoralization" phase

Days 60 - 180

Recover

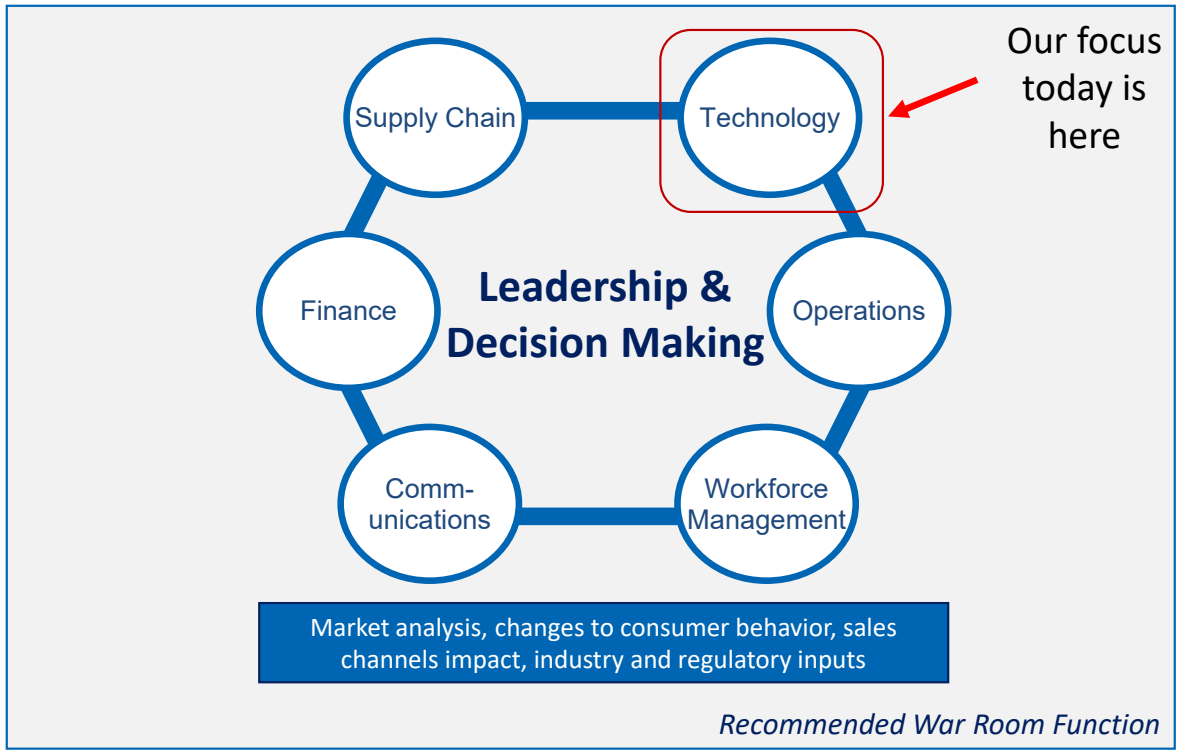
- Secure the workplace for safe return to work and resumption of activities
- Revisit/re-draft policies such as sick leave, travel, and remote work
- Begin implementing long-term supply chain risk-mitigation actions
- Identify which changes to consumer behaviors are likely to continue
- Updating marketing material to address new environment and consumer needs
- New performance indicators

Day 180+

Reposition

- Begin executing changes to five-year strategic plan
- Changes to operating model (e.g. new workforce planning, governance)
- Revisit and reprioritize capital expenditure plans
- Implement long-term supply chain risk mitigation actions

Successfully navigating the continuum requires managing multiple domains and their interdependencies.



Primary Leadership Objectives

Workforce safety, maintaining engagement

Managing cash flow and expense discipline

Effective coordination across stakeholders

Enablement of remote work, data security

Impact of latest regulatory news

Continuity of supply, maintaining production capabilities

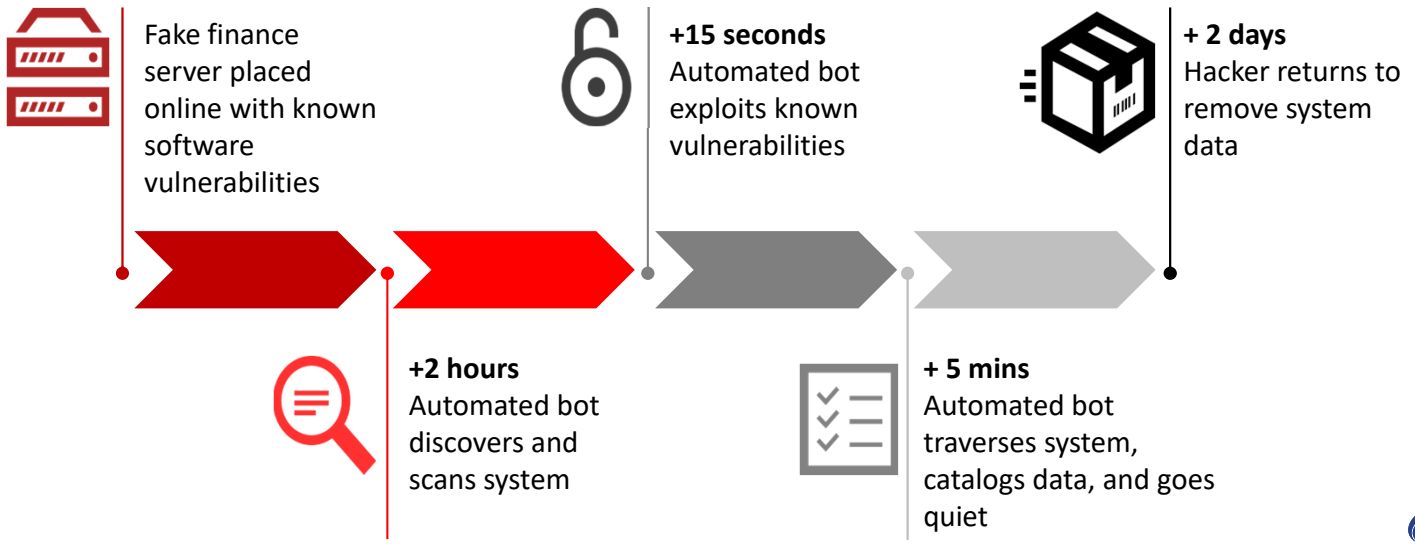
Recognizing shifts in top line performance and opportunities to replace

New Risks and an Increased Attack Surface

How Some Targets are Acquired by Criminals

Attacks are initially driven through automated ‘bots’ which either automate spam messages or scan the internet for vulnerabilities and carry out large portions of cyber attacks without any human interaction.

Live Security Test Performed



Impact on SMB

50% of small to medium-sized businesses (SMB) have been the victim of a cyber attack and over **60%** of those attacked go out of business.

– National Cybersecurity Institute

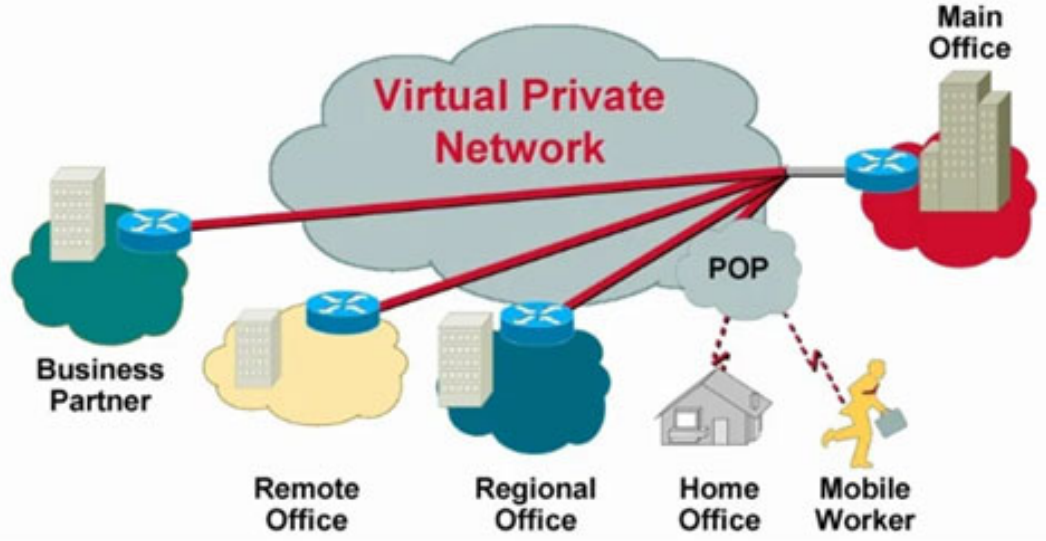
66% of senior decision-makers at SMBs still believe they're unlikely to be targeted by online criminals. Similarly, **6 in 10** have no digital defense plan in place, underscoring the need for heightened industry awareness and education across the board.

- Keeper Security's 2019 SMB Cyberthreat Study

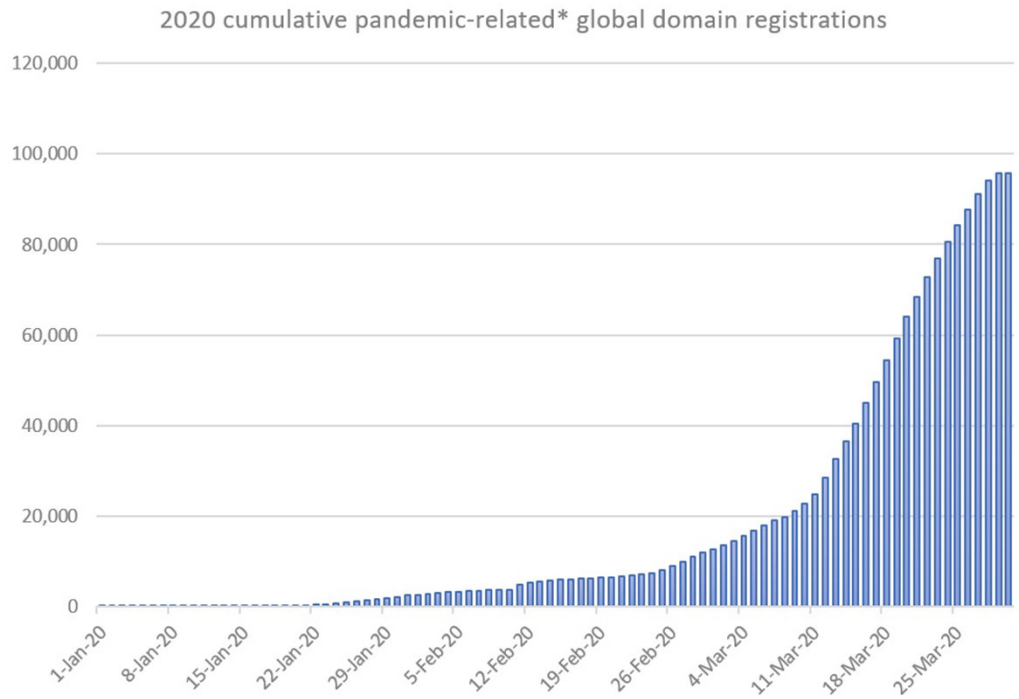
Virtual Private Networks (VPN)

Considerations when standing up a VPN

- Split tunneling
- VPN licenses
- VPN infrastructure
- VPN solutions
- Patching remote systems
- Users blurring the line between company and home networks
- User Awareness Training focused on the home network



COVID-19 Domain Registrations



Inside the word "emergency" is "emerge"; from an emergency new things come forth. The old certainties are crumbling fast, but danger and possibility are sisters.

—Rebecca Solnit, *Hope in the Dark*

Recommendations

- Review changes to remote access that have been made over the last two months
- Require multi-factor authentication for all remote access and cloud services (including O365). If you rolled out VPN without it, its time to circle back and add it now
- Make sure your cyber insurance policy is up to date if you have one. Consider coverage if you do not.
- Consider having a third party scan your environment for new vulnerabilities that have been introduced.

Information Technology Enablers & Considerations

Thought Triggers As You Work With Customers

Do	Don't
• Prepare to invoke remote workforce capabilities; chat, video, collaboration, voice, etc. Anticipate an increased need to support end-point devices & access. • Complete and inventory of IT equipment for associates to use at home & prepare for its cleaning and distribution. • Consider the exploration of work schedule flexibility options to levelize bandwidth, system and resource demand. • Inventory key IT operations and prioritize their execution to maximize resource availability. • Consider short-term contract arrangements to plug key tactical holes. E.g. remote work solutions. • Understand dynamic network availability options & monitoring with your communication carriers. E.g. have the ability to scale up bandwidth capacity on short notice, if needed.	• Simply focus on providing assets for home use scenarios. Determine what infrastructure support is needed to support a shift to an at-home workforce. E.g. VPN access, adequate network bandwidth, etc. • Forget about assets and providers who are not in your immediate vicinity or "low-risk" locations. Determine what services can be shifted away from "at risk" geographies should the need arise. • Fail to maintain good relationships with your third-party providers. Understand service level parameters in existing contracts - do this with your account team when possible. You may need them in a pinch. • De-prioritize Disaster Recovery & Backup operations. Ensure procedures are updated and working as designed.

Strategies for Your Own Practice to Facilitate Efficient and Safe Communications

FBI Public Service Announcement – March 20, 2020

FBI SEES RISE IN FRAUD SCHEMES RELATED TO THE CORONAVIRUS (COVID-19) PANDEMIC

ALERT NUMBER: I-032020-PSA

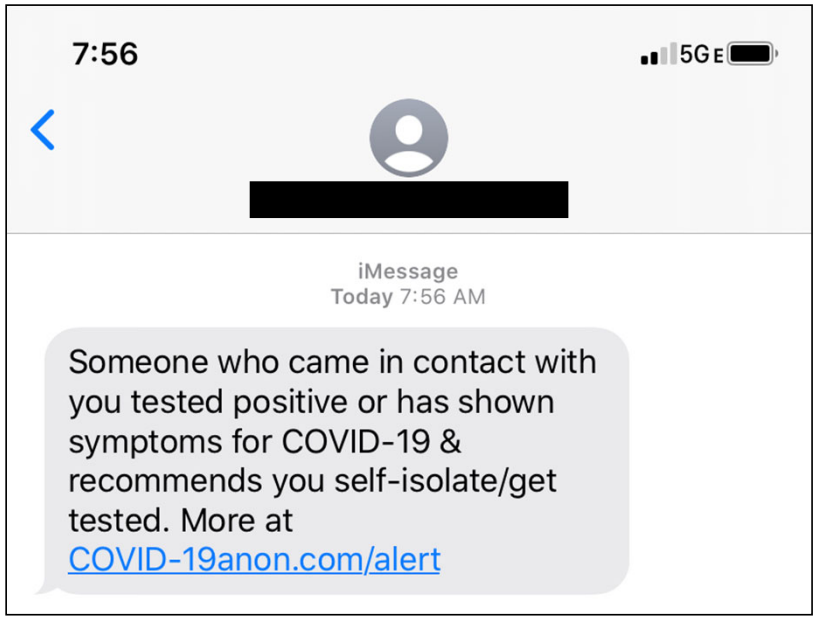
Warns against:

- Fake CDC Emails
- Phishing Emails (charitable contributions, general financial relief, airline carrier refunds, fake cures/vaccines, fake testing kits)
- Counterfeit Treatments or Equipment

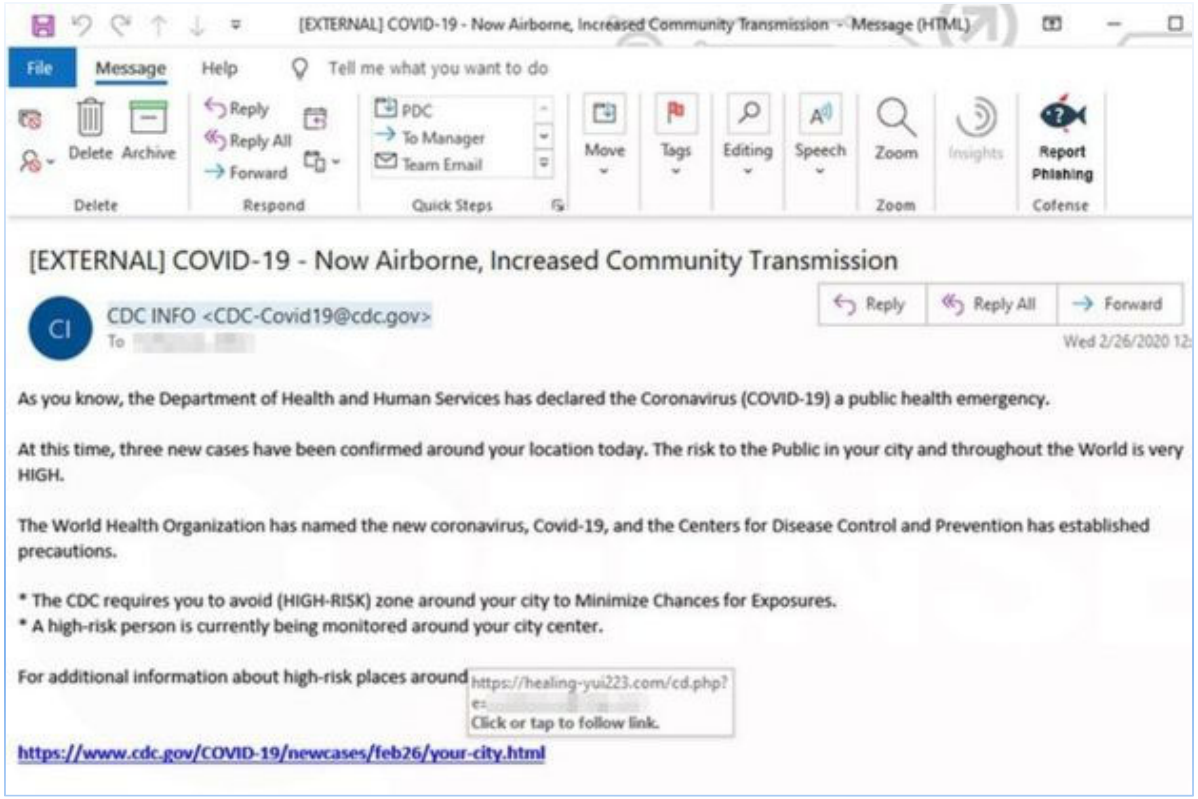
(We can expect a rash of phishing attacks related to the new stimulus bill that is in motion)

https://www.ic3.gov/media/2020/200320.aspx

Sample Text Message



Sample Phishing Email



Define Company Standards for Collaboration (Example)

Zoom Best Practices:

Using the password features for Guests

- https://support.zoom.us/hc/en-us/articles/360033559832-Meeting-and-Webinar-Passwords-

Using the "Waiting Room"

- https://support.zoom.us/hc/en-us/articles/115000332726-Waiting-Room

Monitor for phones numbers that connect to meetings

Keeping the Zoom up-to-date, lots of recent 0-days

- https://securityboulevard.com/2020/04/zoom-zero-days-for-sale-critical-rce-at-500000/
- https://threatpost.com/alleged-zoom-zero-days-for-windows-macos-for-sale-report/154846/

Avoid using public (untrusted wireless networks) - Zoom has had recent 0-days from local subnets

- https://www.zdnet.com/article/fbi-warns-against-using-free-wifi-networks-while-traveling/

Avoid using the recording feature - be careful where you store that offline recording.

- https://support.zoom.us/hc/en-us/articles/205347605-Managing-cloud-recordings

Zoom (as-of-3/31/2020) does not support end-to-end Encryption - consider a secure platform if that is needed

- https://theintercept.com/2020/03/31/zoom-meeting-encryption/
- https://signal.org/

Recommendations

- Make sure your users understand the acceptable use of company equipment and networks while working from home (an acceptable use policy is best)
- Make sure your users know how to identify official company communications (a signature alone is not sufficient)
- Verify that corporate security products work on equipment being used from home
- Clearly define which tools are to be used for remote collaboration (Webex, Teams, Zoom, GoToMeeting, etc). Once you define your product make sure to send instructions on proper use (meeting passwords, waiting rooms, etc)

Additional Resources: elliottdavis.com/covid19

- **Webinar**: https://www.elliottdavis.com/covid-19-webinar-business-continuity-uncertain-times/
- **Summary resource:** https://www.elliottdavis.com/maximize-incident-response-effectiveness-guidance-mid-market-companies/

This summary article has seven links:

- https://www.elliottdavis.com/maximize-incident-response-effectiveness-internal-external-communications/
- https://www.elliottdavis.com/maximize-incident-response-effectiveness-financial-readiness/
- https://www.elliottdavis.com/maximize-incident-response-effectiveness-human-capital-workforce-management/
- https://www.elliottdavis.com/maximize-incident-response-effectiveness-internal-operations/
- https://www.elliottdavis.com/maximize-incident-response-effectiveness-supply-chain-considerations/
- https://www.elliottdavis.com/maximize-incident-response-effectiveness-information-technology-enablers-considerations/
- https://www.elliottdavis.com/maximize-incident-response-effectiveness-data-analytics/

Questions?

We're here to help.

Brian Kirk
Director of Cybersecurity
864.242.2606
Brian.Kirk@elliottdavis.com

VISIT

elliottdavis.com/covid19

elliottdavis.com/cyber

EMAIL

cyber@elliottdavis.com

Tom Uva
Director of Management Consulting Systems
864.250.3933
Tom.Uva@elliottdavis.com

Questions

WOODARD™

COVID-19 Roundtable

Tech Triage: Stopping the COVID-19 Technology Bleed