IT & CYBERSECURITY

HEALTHCHECK

AAFCPAs
great minds | great hearts

AAFCPAs designed this comprehensive **IT & Cybersecurity HealthCheck** to assist clients in surfacing, understanding, and managing priority IT risks that may be mitigated to better secure your organization's Personally Identifiable Information (PII), client records, proprietary information, and/or other sensitive data.

Clients are encouraged to utilize this resource in discussions with your IT services group and as part of a more comprehensive Enterprise Risk Management Program. Please contact AAFCPAs' IT Security professionals or your AAFCPAs Partner to discuss how to implement resource-appropriate security measures to mitigate risks.

Evaluate Your Countermeasures/Prevention Techniques:

	Remote Workforce	Yes	No	Unsure
1	Did you have a set of standard, practicable measures to ensure IT security and system availability for a remote workforce?			
2	Have you provided additional security awareness training to your workforce about the additional cybersecurity dangers during this time?			
3	Have you performed an IT Risk Assessment that covers all aspects of remote access? If you performed an IT Risk Assessment pre-COVID, you should re-assess risks and identify if there are new risks and gaps to address.			
4	Have you ensured users have changed the default name of their home WiFi and confirmed network passwords are unique, strong, and changed per the corporate standards?			
5	Have you advised users to turn on their wireless router's maximum encryption setting (any router with encryption settings below WPA2 should be replaced with one that is more capable), and disable SSID broadcasting to the general public?			
6	Have you ensured the wireless router's firewall is turned on? Or have you installed a good firewall solution?			
7	Have you ensured user devices have up-to-date operating systems, security software, and firewalls? Tools can be used to verify the most up-to-date patches have been applied.			
8	Do you use a virtual private network (VPN) or remote desktop protocol (RDP) to access your network?			

9	Have you assessed and advised employees of risks associated with home Internet of Things (IoT) devices, such as smart TVs, speakers, sprinklers, thermostats, video doorbells, printers, and more? Are these devices on a secondary or guest network?		

Software & Hardware Configurations		Yes	No	Unsure
1	Have you established and documented your change management process, i.e. your process for monitoring additions, adjustments, and decommissions of any applications or infrastructure?			
2	Does everyone adhere to your change management processes?			
3	Have you adopted a standard for secure configurations, such as NIST, SANS, or CIS?			
4	Have you performed a configuration review to ensure your organization complies with existing, adopted standards?			
5	Have you adequately secured systems both inside and outside your firewall?			
6	Have you performed a firewall configuration review?			
7	Have you performed a Vulnerability Scan to inspect potential points of exploitation?			
8	Have you performed a Penetration Test to attempt to exploit any noted vulnerabilities?			
9	Do you perform Vulnerability Scans and Penetration Tests annually?			
10	Do you perform Vulnerability Scans and Penetration Tests as new systems are added or a configuration has changed?			

Web Applications		Yes	No	Unsure
1	Have you performed a Web Application Vulnerability Assessment to identify vulnerabilities such as HTML or SQL injections, cross-site scripting (XSS), and URL redirections?			
2	Do you regularly assess the most prominent vulnerabilities in web-based applications, e.g. OWASP analysis/scans?			

IT General Controls (ITGCs)		Yes	No	Unsure
1	Have you implemented a least permissive, and resource-appropriate approach related to programs and data access for employees based on best practices and mandated regulations?			
2	Have users been made aware of their responsibilities to maintain the security of these applications and sensitive data?			
3	Have you evaluated your processes related to change management and Software Development Life Cycle (SDLC) to improve the root cause of vulnerabilities?			
4	Are program changes authorized, tested, approved, and restricted to being performed by properly authorized and appropriate staff who are independent from those that developed the changes?			
5	Are all program development initiatives authorized, tested and approved?			
6	Do you have controls in place to ensure data migrated to a new application or system has maintained its integrity?			
7	Are batch jobs controlled, data available when needed, and is end user computing such as excel or report writing tools adequately governed?			
8	Have you implemented safeguards to prevent access to systems and data by unauthorized parties?			
9	Do you annually perform an ITGCs assessment?			
10	Were your ITGC assessments performed by professionals with a deep understanding of information technology operations, information security, and internal controls from a design, implementation and testing perspective?			

Social Engineering Attacks		Yes	No	Unsure
1	Do you have on-going training & awareness campaigns to ensure employees remain vigilant?			
2	Have you outlined your “suspicious email response protocol”?			

3	Do you have a zero-tolerance policy to bypassing internal controls?		
4	Are employees aware of your zero-tolerance policy?		
5	Do you monitor & test your internal controls?		
6	Have you tested your employees with simulated phishing and vishing expeditions?		

Internet of Things (IoT)		Yes	No	Unsure
1	Do you have an updated inventory of all IoT devices on your network?			
2	Do you review applicable IT policies & procedures, such as your written information security policy, when a new device is introduced on the network?			
3	Have you performed a vulnerability scan in order to identify, examine, and classify your IoT devices, connections, configurations, and monitor the types of data transmitted?			

Outsourcing Services		Yes	No	Unsure
1	Do you outsource services such as payroll processing, loan servicing, data center/co-location/IT managed services, Software as a Service (SaaS) or medical claims processing? If yes, have you evaluated their System and Organization Controls (SOC) Report to ensure they have adequate controls?			
2	Have you ensured any 3rd party cloud-based systems (e.g. CRM, financial systems) or managed-service providers used are following similar or better security practices?			
3	Have you developed and documented a vendor risk assessment program?			
4	Does everyone in your company adhere to your vendor risk assessment program?			

Infrastructure Resiliency		Yes	No	Unsure
1	Have you documented and tested your Business Continuity Plan?			

2	Have you re-assessed the effectiveness of your Business Continuity?		
3	Have you documented and tested your IT Disaster Recovery Plan?		
4	Do you have a sound backup and recovery strategy?		
5	Do you regularly perform a top down IT Risks and Controls Assessment to identify, prioritize, and remediate deficiencies?		

Physical Security		Yes	No	Unsure
1	Do you require visitors to sign in?			
2	Do you provide visitors with a temporary badge?			
3	Are visitors accompanied at all times?			
4	Are office entry doors always locked?			
5	If you have RFID badges, do you issue radio frequency shielding badges?			
6	Do you have a Clean Desk policy & locked workstations?			
7	Have you performed a physical security assessment?			

Talk Technology Security

Partner, Business Process & IT Consulting

James Jumes, MBA, M.Ed.

774.512.4062 | jjumes@aafcpa.com

Partner, Analytics, Automation & IT Security

Vassilis Kontoglis

774.512.4069 | vkontoglis@aafcpa.com

Certified Ethical Hacker

Mr. Anderson, MCSE, CCNP, CISSP, CEH

774.512.4066 | manderson@aafcpa.com