NATIONAL CENTER FOR THE MIDDLE MARKET

SELF-ASSESSMENT: HOW WELL DO YOU UNDERSTAND YOUR RISKS?

IN COLLABORATION WITH

THE OHIO STATE UNIVERSITY FISHER COLLEGE OF BUSINESS · SUNTRUST · GRANT THORNTON · CISCO

	PEOPLE	PROCESS	TECHNOLOGY
BEFORE *PROTECT & PREVENT*	**1.** Is there someone with specific responsibility and accountability for cybersecurity governance and charters? **2.** Is there a cybersecurity Center of Excellence (CoE)? Are its scope and charter clear and up-to-date? **3.** Do you have clear policies communicated to all employees? **4.** Is training in security provided for all employees? **5.** Have you assessed and deployed appropriate access controls and employee monitoring with properly identified business owners? **6.** Do you have support from HR, legal, and physical security staffs? **7.** Do you have a 3-5 year security strategy?	**1.** Do you conduct an independent, annual review of cybersecurity risk and strategy? **2.** Have you identified your "crown jewel" data and protected it with extra security? **3.** Are you fully aware of regulations that apply to your industry, vendors, and customers? **4.** Does your cybersecurity team regularly update top management and the board? **5.** Do you monitor industry best practices and regulations? **6.** Do you have real-time monitoring of all internal and customer-facing IT systems? **7.** Do you have a mature, tested Incident Response/Crisis Management process? **8.** Do you have all your assets inventoried and classified in accordance with their impact to privacy and business risks? **9.** Do you understand and comply with your organization's archiving and retention policy? **10.** Do you assess and monitor your 3rd party risks? **11.** Do you have a mature threats and vulnerability management program that includes penetration testing, vulnerability scanning, and threat hunting services?	**1.** Do you have automated defense against known threats? **2.** Are security updates automatically applied to all connected devices, from data center to desktop to pocket? **3.** Have you assessed your current technology against the "Before, During, After" attack continuum? **4.** Do you have mobile and wireless technology protection currently in place? **5.** Do you have protections in place against the risks associated with the Cloud? **6.** Have you deployed technology segmentation architecture? **7.** Do you have an encryption policy and is it followed? **8.** Have you identified and protected against loss of protected data? **9.** Have you evaluated what technology should be on premises/ off premises, and what should be insourced/outsourced? Are your decisions based primarily on cost?
DURING *DETECT & RESPOND*	**1.** Are duties and responsibilities clearly communicated? **2.** Do you have defined cybersecurity metrics and reporting to the Exec team / Board and properly identify impact to business? **3.** Do you have a clear escalation plan to include to outside agencies? **4.** Do you already know the legal authorities (FBI, Secret Service, etc.) with whom you should work if attacked?	**1.** Do you have an established process for communicating (a) to IT (b) from IT to leadership (c) to entire company? **2.** Do you have an established process to communicate risk and breaches to vendors/customers/ authorities? **3.** Do you have a regular process for threat assessments? **4.** Are third-party security assessments performed on a regular basis and are third parties required to sign a BAA? **5.** Is there an automated approach to inventory the environment and automatically update security tools? **6.** Have you performed scenarios (fire drills) to model attacks?	**1.** Do you have real-time sensing from world-class provider (scaled to risk)? **2.** Do you have a tested way to shut down systems and perform forensics? **3.** Have you already lined up the expertise you would need to call on for remediation, and lined up the budget, as well?
AFTER *RECOVER*	**1.** Have you performed regular disaster recovery testing? **2.** Have you identified the internal and external resources needed to clean up, do forensics, and plan remediation?	**1.** Is cybersecurity fully integrated with risk management and discussed at senior and board levels in that context? **2.** Have you investigated whether to purchase cyber risk insurance? **3.** Do you work with your legal team to understand risk and liability, and manage discoverability? **4.** Are remediation efforts prioritized according to level of business risk?	**1.** Do you have backup systems? **2.** Are there "air gaps" between backup systems and your ordinary system? **3.** Do you regularly test and update your backup systems? **4.** Do you have and have you deployed a disaster recovery plan?