Cybersecurity Preparedness CHECKLIST

LEGAL

- ☐ Does your team have experience with cybersecurity and cyber breaches?
- ☐ If not, do you have a partner/vendor that you can use during such events?
- ☐ Have you reviewed your vendors contracts to understand the scope of their cybersecurity impact?
- ☐ Have they minimized this exposure and risk as much as possible?
- ☐ Are the penalties for breaches in the contract explicit?
- ☐ Do they contain limits of liability and do they carry notification policies?
- ☐ Are those notification policies documented?
- ☐ Do you or your vendor's liabilities align with you or your vendor's insurance coverages?
- ☐ Have you reviewed all regulatory statutes, and understand what you/vendor must have in place?
- ☐ What cyber frameworks must you/vendor adhere to?
- ☐ What forensic capabilities must you/we have in the event of a breach.
- ☐ What do the regulations state for breach disclosure process?
- ☐ What fines are possible and are you/vendor covered for such limits?
- ☐ Do your internal polices match what is legal required and necessary?
- ☐ What is your vendor's process for engaging with you during a breach?
- ☐ What should your vendor do for internal communication to protect your privileged communication?

INSURANCE

- ☐ Is your insurance coverage in alignment with your potential legal and regulatory exposure?
- ☐ Do you have and understand all vendor contracts and your total liability?
- ☐ What do you need in place to receive coverage? Meaning, you often must follow cybersecurity best practices. If you are not, you may not get covered. Make sure you know the requirements and your technology team has a plan in place and can prove it.
- ☐ What is the notification and claim process? (who, when and how to notify, what data to keep during a breach event to provide as evidence, etc.)
- ☐ Does your tech team and appropriate partners and vendors know the process?

PR & MARKETING

- ☐ Do you know a company that can handle your PR and Marketing needs if a breach occurs?
- ☐ Do you have a communication plan during a breach with your PR vendor?
- ☐ What tools do you need in place to distribute messages if internal systems are down and you cannot get to them?
- ☐ What is the internal communication approval process?
- ☐ Is your process documented and stored both internally and with your agency?

INTERNAL COMMUNICATIONS

- ☐ Do you have an internal breach team established?
- ☐ Does your breach team have a communication plan, on call rotation and updated process?
- ☐ Do you have a simple, off network place to communicate all the critical info to your breach team, during a breach?
- ☐ Is there an emergency contact list documented and distributed to key personnel internally, vendors, partners, board members etc.
- ☐ What systems will you use, especially if outages occur and standard means of communication are unavailable?
- ☐ Has your board, legal team, insurance team and regulators approved the communication plan?
- ☐ Do all of parties know what they need, and when and how it will be captured and reported?
- ☐ Have you established, documented, and communicated who has authority during a breach?

FORENSICS

- ☐ Do you work with a cyber forensics firm or have a partner that does?
- ☐ Have you looked at your contracts, insurance policy and regulations to know what you must be logging, morning and reporting?
- ☐ Are your tech systems in alignment with that?
- ☐ Do you know what documentation, reports, data etc. you need to capture and produce during a breach?
- ☐ Does your team have a policy with a checklist of what they need to capture and freeze during a breach event?
- ☐ Do you have an offsite backup and cloud location?

RECOVERY CHECKLIST

- ☐ What is your risk tolerance, how much time can you be down?
- ☐ What expectations do your clients and partners have for outages?
- ☐ Are you resilient enough to respond and recover in the amount of time that is satisfactory to your business? (This is a technical question and should be asked through multiple lenses and scenarios.)
- ☐ Does your team understand the different attach scenarios?
- ☐ Do you know how long it would take to regain access with your current technology and plan?
- ☐ Do you know what systems can be recovered and how much data could be lost?
- ☐ Who is running point on your recovery efforts and what authorities do they have to spend, take up systems, take down systems?
- ☐ Is this plan documented and communicated to all necessary parties?

TRAINING & TESTING SIMULATIONS

- ☐ Have all employees been briefed and trained?
- ☐ Do they understand their roles and points of contact?
- ☐ How often are you reviewing the full scope of your DR processes and updating it?
- ☐ Have you tested your processes, especially in the middle of the night?
- ☐ Have you tested your plan in the last 12-months?
- ☐ How often do your test these systems and processes?
- ☐ Do you offer your employees cybersecurity training?
- ☐ How often are you reviewing your employee cybersecurity training results?
- ☐ Do you have a BYOD policy for remote workers?