SUTHERLAND

Cybersecurity Preparedness Checklist

What Every Company Should Be Doing Now

□ Prioritize cybersecurity within the company. Tone from the top matters. Cybersecurity should be periodically discussed with the board of directors and senior management. Determine whether you are going to participate in the voluntary NIST Cybersecurity Framework.

□ Identify your information security and incident response team, including legal, compliance and business leads for cybersecurity matters. Consider including outside counsel, forensic consultants and a public relations consultant with crisis management experience on the company team.

□ Review existing written information security policies and procedures with the team to ensure they reflect current regulatory requirements governing data security, privacy and contractual obligations. Assign and document roles and responsibilities for compliance. Determine if your policies align with the company's business goals and practices. Link to your business continuity plan.

- Ensure all applicable regulatory requirements have been built into company procedures. Confirm that the company has adequate compliance testing procedures in place and establish a schedule for testing.

□ Know what and where your information assets are. Ask each business unit where critical information is stored, how it is used and what critical processing takes place. Consider that some critical information may be stored or processed outside of the corporate data center(s), including on:

- Desktop and laptop computers (a surprising amount of critical data frequently resides in spreadsheets and similar electronic documents)
- Personal devices, such as smartphones and tablets (whether corporate- or employee-owned)
- Home personal computers for telecommuters or others working at home
- Vendors' systems
- The "cloud"
- Backup media at offsite storage facilities (frequently managed by vendors)
- Other portable media (thumb drives, DVDs, tapes, etc.)
- Non-traditional computing platforms such as phone and voicemail systems, physical security systems (e.g., door or gate access), operational systems (HVAC, SCADA, plant controls, etc.), and similar systems

□ Assess your security posture. Objectively assess your information security training, policies, procedures and implementation. Consider protecting your assessment under attorney-client privilege.

□ Develop a detailed incident response plan. Assume that a break-in will occur. Schedule simulations of breach incidents with the entire breach response team and use the results to continually improve your plan.

□ Ensure that you have a PR consultant with crisis management experience on board and ready to act in the event of a breach, assuming you have not already made such a consultant part of the breach response team.

□ Review your incident response plan with executive management and the board of directors to ensure that the board and management are adequately focused on cybersecurity and have established satisfactory internal controls and governance structures.

SUTHERLAND

Cybersecurity Preparedness Checklist

What Every Company Should Be Doing Now

□ Risk management principles apply to information security. Conduct periodic risk assessments to identify cybersecurity threats, vulnerabilities and business consequences. Consider whether you could operate if access to critical data is lost or denied. What are the potential operational, legal and regulatory consequences if an unauthorized party gains access and control over your data?

□ Establish cybersecurity information sharing processes across organizations within the company and with vendors. Consider joining an industry-focused cybersecurity information sharing initiative – information sharing and analysis centers have already been established in numerous industries.

□ Assess and document employees, contractors and consultants who have access to information assets, including remote access, and periodically review their compliance with procedures to confirm that continued access is appropriate; delete access rights for those for whom access is no longer appropriate. Document controls to prevent unauthorized access to your networks and devices. Update third-party vendor agreements to require representations and warranties regarding adequate cybersecurity controls (such requirements include network security, application security, data security, data destruction, security breach notification, vendor data use, and subcontractor data security requirements). Require periodic security certifications or conduct routine periodic compliance audits on these vendors.

□ Verify that third-party vendors have sufficient cybersecurity insurance coverage. Identify behaviors that may nullify the terms of their insurance.

□ Ensure that your cyberinsurance coverage is adequate. Review with key business unit leaders the coverage and exclusion terms of the company's insurance for cybersecurity incidents. Determine whether the terms are appropriate for the nature of the company's business and the likely risks you face.

□ Everyone has a role in cybersecurity. Conduct regular training of employees and vendors on your information security procedures and their responsibilities. Keep the content of your corporate security training program curent. Ensure that employees are trained in data protection measures and that procurement and marketing teams are required to vet their purchases through legal and compliance for cybersecurity risks.

Sutherland's Cybersecurity and Privacy Practice

We advise on the full spectrum of privacy and data security matters, including information security program development and assessment, data breach response planning and investigation, regulatory compliance, cyberinsurance, post-breach response and crisis management, regulatory enforcement, and litigation response. Our clients have access to the full resources of the firm to protect their interests and build their businesses. For more information, please visit www.Sutherland.com or visit our blog at www.SutherlandCybersecurity.com.