CYBERSECURITY CONTROLS

Please note that in the future we may revise these or adopt additional data security controls which could apply to you as Panel counsel. The Hartford reserves the right to assess the firm's controls and security practices to ensure compliance with our requirements.

Information Security Executive

This is defined as a credentialed senior-level executive with the designated responsibility for establishing and maintaining the enterprise vision and strategy of a comprehensive cybersecurity program for the entire organization to ensure information assets, systems and technologies are adequately protected.

Cybersecurity Program

A cyber security program is a documented set of your organization's information security policies, procedures, guidelines, and standards. Cybersecurity Programs should be based on widely accepted industry best practices (i.e. ISO 27002, NIST 800-53 or Cobit). In addition, security programs typically adapt to changes in the regulatory environment and any other changes to the industry. Security program should provide a roadmap for effective security management practices and controls that include:

- Identifying all types of data including sensitive data. Whether its customer information, patient health records, personal financial information, or intellectual property, every company has sensitive data it stores, processes, and transmits to conduct business. Each data type may have specific control requirements to comply with regulatory and information security requirements.
- Documenting where all data is stored. In addition to locations like databases, information resides in spreadsheets or in text documents on file shares. Ensure security controls are implemented in accordance with the system or location.
- Record all hardware and software devices in your network. When critical vulnerabilities are announced, known devices in your environment must be updated or patched. Creating and maintaining an inventory of your hardware and software devices is key to establishing a solid cybersecurity program.
- Develop a plan to train employees and users on cybersecurity best practices. Cybersecurity is not solely an IT issue, it's a business issue that requires a culture of security adoption. Protection of sensitive data comes down to the end users who are handling it and those that manage systems containing sensitive data. Employees must be trained to recognize and report phishing attacks and baiting, and should be well-versed in password management to protect systems and data.

Cyber Security Policies & Backup Procedures

Cyber security policy should be documented, accessible, and understood by all employees. Policies should be reviewed and approved by the CISO/InfoSec Executive on an annual basis.
Backup procedures and the restoration process should be tested regularly (i.e. quarterly). Both policies and backup procedures should be reviewed, maintained and revised on a periodic basis to mitigate the impact of ransom-ware attacks.

Multifactor Authentication

Multifactor Authentication (MFA) is a method of computer access control which requires users to provide authentication methods from at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).

Security Awareness and Training

Security awareness and training should be perform at the on-set of employment and routinely tested thereafter to ensure employees understand the importance of data protection. Security awareness and training should include common threats such as phishing, malware and ransom-ware identification with documented processes consistent with the Security Incident Response plan. Employees should be provided a process that includes an electronic solution to facilitate identification, notification, treatment and remediation of threats.

Security Incident and Response Plan

Incident response is an organized approach to addressing and managing the aftermath of a security breach or cyber-attack, also known as an IT incident, computer incident or security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs. Included in the incident management plan should be the appropriate notification requirements set forth by state regulations if applicable.

Penetration and Vulnerability Testing

Vulnerability testing, includes scanning all networked devices for potential vulnerabilities, should be completed on a regular basis, as often as once a week. Remediation of discovered vulnerabilities should be considered a priority and carried out as such. Penetration testing, which tests your perimeter defenses, should be done on an annual basis at minimum.

Risk assessments

Companies should perform annual risk assessments that includes all data, to identify areas of network weakness and to ensure compliance to corporate data protection requirements and regulatory obligations

Data Loss Prevention Services

Data loss prevention, or DLP, is technology that scans documents, emails, and other types of electronically transmitted data. Data elements like Social Security Numbers, PII, PHI are identified during transmission and blocked when these types of patterns are transmitted to an untrusted location. DLP can also include scanning data going onto removable media to identify and detect loss.

Third-Party Risk Management

A formal third-party risk management framework includes IT assessment, review of policies, procedures and HR practices including background checks with criminal history. A third-party assessment should be conducted for all Contractors and third-party service providers prior to network or data access.

Intrusion Detection and Prevention Services

Perimeter defenses would include network and/or host tools to identify and prevent malicious or anomalous behavior.

Secured Data in Transit

Sensitive information transmitted electronically over public communications media is appropriately encrypted and properly authenticated by the recipient while the systems used for transmission are monitored and updated to limit the risk of unpatched or managed applications.

Full-Disk Encryption

Full-disk Encryption (FDE implies encryption at the hardware level on all equipment that contain information including mobile devices.)

System and Access Log Management

Regular log collection in applications can provide key information and indicators of security incidents, as well as provide information for audit and forensic investigations, and also help identify operational indicators regarding application failures or resource issues. Application audit trail logs, as defined below, must be active at all times and protected from unauthorized access, modification and accidental or deliberate destruction on all information resources.

System Log Management

- Executable start/stop times
- System boot/restart times
- Hardware, software, or operating system configuration changes
- Abnormal system events
- Access to, or modifications of log files
- Access by privileged accounts
- Changes in account permission or authorizations
- Critical file changes
- Port Up or Port Down

Access and System Log Management

- All successful and unsuccessful login attempts
- Additions, deletions and modifications to user accounts/privileges
- Attempts to perform unauthorized changes to critical applications
- Activities performed by Highly Authorized application accounts
- Modifications to application system configuration
- Access to Highly Restricted or Company Confidential information
- Additions, deletions and modifications to security settings
- Additions, deletions and modification to application audit log parameters

Physical Data Protection

Physical security control refers to capabilities that limit access to restricted areas. Control features are utilized at all levels of security. Controls can be mechanical, procedural, or electronic. Examples include:

- Electronic card systems
- Mechanical key locks
- Authorization by guard or receptionist
- Visitor sign-in book
- Physical access via escort

Records Management Policy

Records and retention policy should define roles and responsibilities, identify what a record is and how it must be protected. Records Management provides a framework for systematic retention and defensible record destruction practices that include electronically stored information “ESI”.

Cyber Insurance

A proper cyber security insurance policy should include reimbursement for investigation, business loss, required notification and credit monitoring to clients, legal expenses, cost of extortion and cover human error where possible.