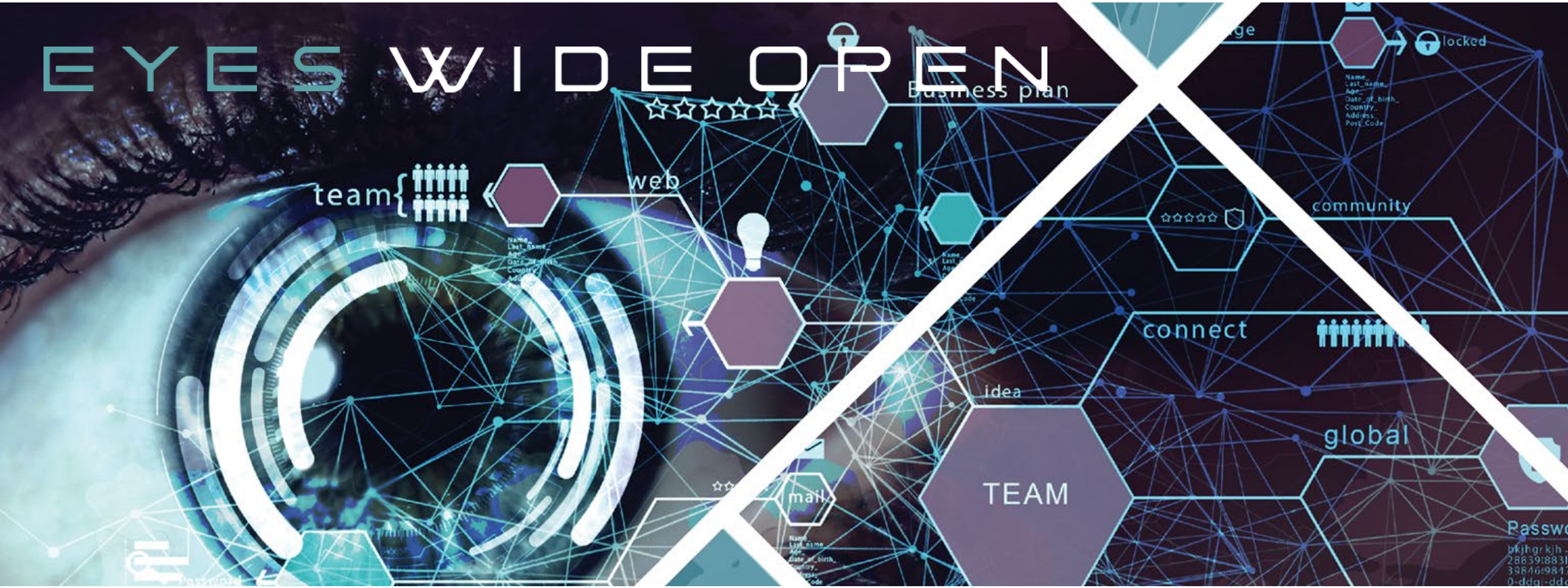
12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR

Island



Essential Contract Provisions

Eran Kahana

Cybersecurity, AI and IP
Attorney, Maslon LLP

Must-Have Security Language
key contractual themes to consider

Eran Kahana
Attorney | Maslon LLP
Research Fellow | Stanford Law School
Advisory Board Member | Stanford Artificial Intelligence Law Society
Co-Author | The Law of Artificial Intelligence and Smart Machines

October 24, 2022

Key Theme

CONFIDENTIALITY – INTEGRITY – AVAILABILITY

1. What to look for in contracts.
2. Who is providing the contract? Contracts tend to be favorable to the party drafting it.
3. What to discuss with your attorney. What to make sure you cover.
4. The CIA triad is what we maintain focus on in these agreements.
5. Most of what I talk about – you are contracting with a member of your supply chain.

Covered Systems

Identify relevant computer network systems

1. What parts of the network will the other party access?
2. Name the network/database. This helps enforcement. Policing of unauthorized access. Helps ensure both parties are on the same page insofar as what is expected.
3. Sets the tone for liability in the event of a breach of contract. Helps define a breach of contract.

Covered Systems

Restrict access through the agreement and through system settings

1. IT policy governs access controls and contractual controls should be in sync with it.
2. When the contract restricts access to a certain network environment, the IT policy should be capable of enforcing that restriction.
3. Don't rely only on the contract. Don't rely only on the IT policy. Each should work independently.

Covered Data

Data that will be used

1. Be clear. Ambiguous provisions are not your friend.
2. Identify the data you are providing access to. The more detail the better.
3. This approach helps ensure you can more effectively enforce unauthorized access.
4. This helps ensure that you are not inadvertently providing access to other confidential information.

Covered Data

Limited access

1. The party you are granting access to must have enforceable legal obligations with its employees and its subcontractors/supply chain. Everything is linked.

2. Make sure you don't have to chase the bad actors in order to obtain a legal remedy (injunction) and relief (damages).

Security Events

Attempted vs. actual: sync with incident response plan

1. Cyber incident definition is important.
2. HIPAA requires definition of a data breach if there is a compromise of PHI.
3. How does your incident response plan define a cyber incident?
4. Most incident response plans use a 3-tier approach:
    1. Level 1 = deal with it internally
    2. Level 2 = We have a breach, we need to report it, but it is unlikely to risk the future of the business.
    3. Level 3 = Same as level 2, but the future of the business is in question.

Security Events

Disclosure requirements: timing, content and scope

1. How much assistance do you need to get from the other party?
2. How much assistance will you need to provide?
3. Can you meet those requirements?
4. Make sure you don't have to pay.
5. Under HIPAA – in no event later than 60 days after discovery of the breach

Security Standard

Authorized connectivity

1. What are the approved methods for gaining access to the network?
2. Make sure the connecting party's computer systems are using the latest OS and have implemented all patches.

Security Standard

Encryption requirements

1. A frequent silver bullet remedy.
2. SHA-1 not good. SHA-256 currently ok.
3. 2-factor authentication.
4. Data at rest and data in transit.
5. If using flash drives, make sure they are encrypted.

Security Standard

Identify standards (by name)

1. Don’t hesitate to identify the standards by name.
2. ISO 27001.
3. UL 2900 – medical device cybersecurity.
4. NIST 800-53, NIST Cyber Security Framework, CIS Critical Security Controls.

Security Standard

Required certification or attestation and frequency

1. Require maintenance of certification during the contract term.
2. Failure to maintain certification = breach of contract.
3. Require the other party to provide a SOC 2 Type 2 report.
4. Make sure you don’t have to pay for it.
5. Failure to provide = breach of contract.

Security Standard

Prohibit downgrading

1. The other party cannot downgrade its cybersecurity policies and procedures.
2. This ties in with maintaining the named standards.

Security Standard

Redundancy

1. This ties into the AVAILABILITY part of the triad.
2. Make sure the other party protects against ransomware.

Audit Rights

Cooperation

1. Make sure you have access to the employees of the other party.
2. Make sure you have access to policies and procedures independently of an audit.

Audit Rights

Ensure sufficient timeframe post-termination

1. A breach is frequently something you will need to deal with for a significant amount of time
2. This amount of time can be greater than the contract term.
3. Make sure that you can continue to get cooperation contractually even if the contract is expired or terminated

Audit Rights

Consequences for non-compliance

1. Pay for your audit costs.
2. Pay liquidated damages = must be reasonable or they won't be enforced.
3. What is the window of time that is available for getting into compliance?

Insurance

WE COULD HAVE AN ENTIRE BREAKOUT SESSION JUST TO COVER CYBERSECURITY INSURANCE

1.Make sure you have coverage for incidents that involve the triad – CONFIDENTIALITY, INTEGRITY and AVAILABILITY.

2. Careful review of the policy and the endorsements is critical. Do not rely on Commercial General Liability, D&O.

3. Make sure the deductible is adequate – a large % of breaches fall below the deductible.

4. What security controls can be put in place to reduce the premium.

5. Cybersecurity insurance – sync with incidents in incident response plan.

Thank You

Eran Kahana
eran.kahana@maslon.com
612.672.8385
@cyberlawyering