

The background is a dark, abstract digital landscape. It features a central perspective view of a digital corridor or tunnel, with glowing blue and white lines representing data paths. Binary code (0s and 1s) is scattered throughout the scene, some appearing as large, semi-transparent characters. The overall color palette is dominated by deep blues, purples, and bright whites, creating a high-tech, futuristic atmosphere.

Morgan Lewis

TECHNOLOGY MARATHON

**Cyberinsurance: Is Your Company
Covered?**

Mark Krotoski and Jeff Raskin

Tuesday, June 21st

Presenters



Mark L. Krotoski



Jeffrey S. Raskin

Morgan Lewis

Overview

- Cyber Risk Landscape
- Preliminary Considerations
- Cyber Investigation Issues
- Core Coverages
- Other Coverages
- Attorney-Client Privilege / Attorney Work-Product Special Issues
- The State Actor Problem
- Key Areas to Consider

CYBER RISK LANDSCAPE

The background is a dark, abstract digital landscape. It features a central vertical column of glowing blue and white binary code (0s and 1s) that appears to be rising or streaming upwards. To the right, there are horizontal streaks of light in shades of blue and purple, suggesting data flow or network activity. Various other binary digits are scattered throughout the scene, some appearing as if they are floating or falling. The overall color palette is dominated by deep blues, purples, and bright whites, creating a high-tech, futuristic feel.

Morgan Lewis

Cyber Risks and Landscape

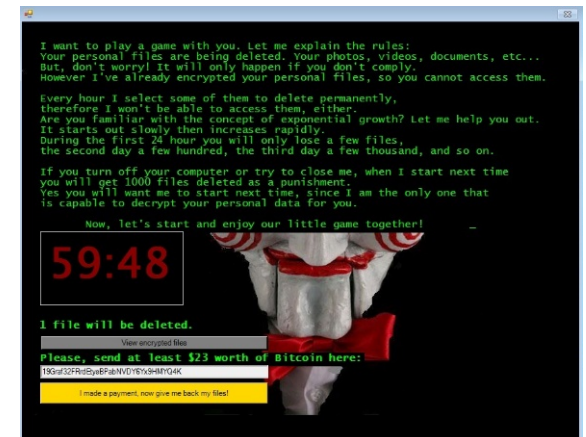
- Phishing Schemes
- Business Email Compromise
- Ransomware
- Security issues
- Password compromise
- Targeted cyber attacks
- Insider threat
- Third Party Vendors
- Stolen unencrypted laptop

Key Actors
Organized Cyber Crime
State Sponsored
Hackers for Hire
Hactivists
Third Party Vendor Attacks
Insider Threat
Inadvertence

Morgan Lewis

Ransomware Attack – Key Phases

- **Threat Actor Identifies/Exploits Vulnerability**
 - Phishing, remote desktop rotocol (RDP), compromised passwords, software vulnerabilities
- **Deploys tools, lateral movement, escalate privileges**
 - Cobalt Strike, Emotet, Trickbot
 - Credential harvesting
- **Exfiltrates data**
 - PII
 - Sensitive or proprietary information
- **Encrypts files**
 - Usually focuses on file types
- **Ransom demand**
 - Threat to leak or destroy data
 - Urgent deadline or clock
 - Double extortion?



PRELIMINARY CONSIDERATIONS

The background is a dark, abstract digital space. It features a central vertical column of glowing blue and white binary code (0s and 1s) that appears to be receding into the distance. To the right, there are several bright, horizontal streaks of light in shades of blue and white, suggesting high-speed data transfer or digital signals. Scattered throughout the scene are various floating elements, including individual binary digits, small blue cubes, and larger, fainter binary structures. The overall color palette is dominated by deep blues, purples, and bright whites, creating a futuristic and technological atmosphere.

Morgan Lewis

Preliminary Considerations

Moody's: Approximately 50% of all organizations hold cyber insurance. 65% of public sector organizations carry specialized cyber coverage, as do 57% of financial services companies.

Fitch ratings: Spending on standalone cyber insurance coverage increased by 92% to over \$3.1 billion annually in the U.S.

Cyber insurer premiums rose on average by 27.5% during the first three months of 2022.


Leading drivers of premium increases: Increased data breach litigation and cyber crime including malware and other types of extortion. Approximately 66% of mid-sized organizations worldwide suffered a ransomware attack in 2021, compared with 37% in 2020.

Approximately 8,100 cyber claims were paid in the U.S. in 2021, a 200% year-on-year increase.

Preliminary Considerations (cont'd)

The **average cost** of a data breach is approximately \$4.24 million.

Many insurers now require *at least* multifactor authentication, or the potential policyholder is deemed “virtually uninsurable”, and a quote will not be provided.



- Other requirements to obtain a quote and a policy: Stronger passwords; third-part vendor management; incident response plans; training of employees on phishing; penetration testing; system backups; endpoint detection.

- Cyber insurers often provide access to tools, assessments, consultations, and software to meet the requirements.

- Demonstrated cyber “hygiene” may be required for claims to be paid in the future. This may particularly be the case for malware and other extortion claims.

Preliminary Considerations (cont'd)

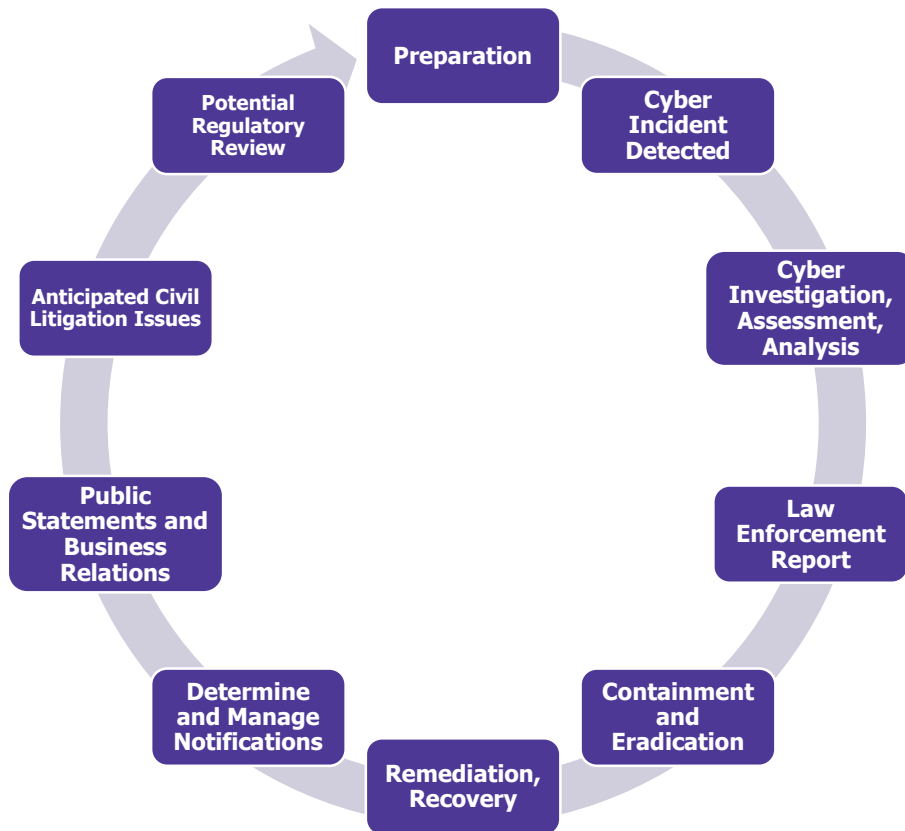
Cyber “loss ratio” -- the ratio of the claims paid by an insurer to the premiums earned -- were reported to be at 65% in 2021. That means that for every \$100 in cyber premiums received by insurers during 2021, \$65 was paid out in claims. Between 2015 and 2019, the number never rose above 48%. A loss ratio below 100% doesn't necessarily mean cyber insurers are earning profits since the number only considers direct claim payouts and not the other costs of running an insurance company like underwriting fees and legal and claims expenses.

The background is a dark, abstract digital space. It features a central vertical column of glowing blue and white binary code (0s and 1s) that appears to be receding into the distance. To the right, there are several bright, horizontal streaks of light in shades of blue and white, suggesting high-speed data transfer or network activity. Scattered throughout the scene are various digital elements, including floating binary digits, glowing cubes, and lines of code, creating a sense of depth and complexity.

CYBER INVESTIGATION ISSUES

Morgan Lewis

Legal Issues Arising During Incident Response Phases



CORE COVERAGES

The background is a dark, abstract digital space. It features a dense field of binary code (0s and 1s) in various sizes and colors, including blue, green, and white. Some digits are larger and more prominent, while others are smaller and more numerous. There are also glowing, streaky lines of light in blue and green, suggesting data flow or digital energy. The overall effect is a sense of a complex, high-tech environment.

Morgan Lewis

Core Coverages: First-Party

Breach Response

- **Security Breach**
 - Unauthorized use of the insured's computer system
 - Denial of service attack affecting the insured's computer system
 - Infection of the computer system by malicious code
- **Data Breach/Privacy Breach**
 - Theft, loss, or unauthorized disclosure of personally identifiable or third-party information in the care, custody or control of the insured or a third-party for whom the insured is liable
- **Payable policy benefits**
 - Breach response costs**
 - Lawyers to advise the insured on reporting requirements
 - Computer security expert to determine the existence, cause and scope of a breach
 - Cost of notifying potentially affected individuals
 - Cost of establishing a call center
 - Credit and identity fraud monitoring costs
 - Public relations and crisis management costs
 - Data recovery costs**
 - Reasonable and necessary costs to regain access, replace or restore lost data following a breach



Core Coverages: First-Party

Cyber Extortion

- **Responds to an extortion threat – any threat to:**
 - Alter, damage or destroy data
 - Perpetrate an unauthorized use of a computer system
 - Prevent access to computer data or a computer system
 - Steal, misuse or disclose personally identifiable information or confidential third-party information like trade secrets or magnetic strip information
 - Introduce malicious code into the insured's computer system or into a third-party system
 - Interrupt or suspend a computer system
- **Pays**
 - Extortion payment made with insurer consent to prevent or terminate an extortion event
 - Reasonable and necessary expenses incurred with insurer consent to prevent or respond to an extortion event

Business Interruption/Dependent Business Interruption

- Income loss and extra expense resulting from a security breach or an unintentional and unplanned interruption of the insured's systems
- Income loss and extra expense resulting from a security breach or an unintentional and unplanned interruption of the systems of a third-party that provides necessary products or services to the insured under a contract



Core Coverages: Third-Party Liabilities

Data/Network Liability

- Responds to claims resulting from a security breach or a data/privacy breach
- Responds to claims asserting that the insured failed to comply with its privacy policies concerning the access, disclosure or maintenance of personally identifiable information

Regulatory Defense

- Responds to requests for information, civil investigative demands or proceedings brought by any federal, state, local or foreign governmental entity resulting from a security breach or a data breach/privacy breach.
 - Includes, usually by endorsement, to proceedings brought under consumer protection statutes like the California Consumer Privacy Act or the EU's General Data Protection Regulation

OTHER COVERAGES

Morgan Lewis

Other Coverages

Errors & Omissions coverage for companies providing technology services such as data processing, internet and mobile services, email services, software as a service, platform as a service, network as a service, infrastructure as a service, hosting, computer systems analysis, custom software programming for specific clients, computer and software installation and integration, computer software support, network management services, etc.

PCI Fines and **Expenses** for companies in the credit card or payment processing business

Limited coverage for **theft**, such as by social engineering, invoice manipulation, funds transfer, computer fraud, etc. These are often covered to a much greater extent by crime policies

Bricking

Cryptojacking

Reputation loss

When an Incident Occurs or a Claim is Received

All cyber coverage is written on a “claims-made” basis. The policies typically contain “warnings” on the first page of text saying that:

- This policy’s liability insuring agreements provide claims made and reported basis and only apply to claims first made against the insured during the policy period or the optional extension period (if applicable and reported to the underwriters in accordance with the terms of the policy).

That, however, is an understatement.

- The policy’s “**first party**” coverages apply to breaches the insured first “discovers” and reports to the insurer during the policy period; and
- “**Related claims**” or “interrelated wrongful acts” provisions in the policy can bring claims “back in time” if they are “related” to prior claims.

When an Incident Occurs or a Claim is Received

Notice

Notice of "Circumstances"

- "With respect to any circumstance that could reasonably be the basis for a Claim, the Insured *may* give written notice of such circumstance to the Underwriters through the contacts listed for Notice of Claim, Loss or Circumstance in the Declarations as soon as practicable during the Policy Period."
- "Any subsequent Claim made against the Insured arising out of any circumstance reported to Underwriters in conformance with the foregoing will be considered to have been made at the time written notice complying with the above requirements was first given to the Underwriters during the Policy Period."

When an Incident Occurs or a Claim is Received

Notice of "Loss"

- "With respect to Data Recovery Costs, Business Interruption Loss and Dependent Business Loss the Named Insured *must* notify the Underwriters through the contacts for Notice of Claim, Loss or Circumstance in the Declarations *as soon as practicable* after discovery of the circumstance, incident or event giving rise to such loss."
- "With respect to Cyber Extortion Loss, the Named Insured *must* notify the Underwriters via the email address listed in the Notice of Claim, Loss or Circumstance in the Declarations *as soon as practicable* after discovery of an Extortion Threat but no later than 60 days after the end of the Policy Period. The Named Insured must obtain the Underwriters' consent prior to incurring Cyber Extortion Loss."

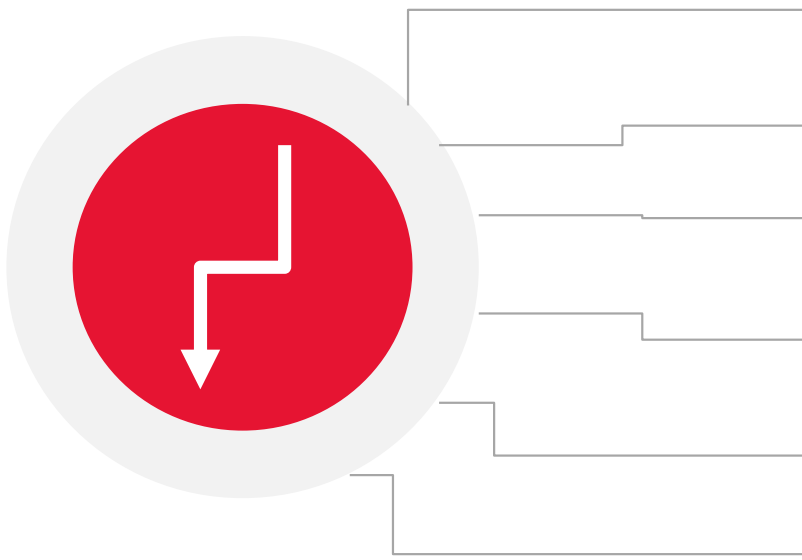
When an Incident Occurs or a Claim is Received

Notice of “Claim”

- “The Insured *must* notify the Underwriters of any Claim *as soon as practicable*, but in no event later than: (i) 60 days after the end of the Policy Period; or (ii) the end of the Optional Extension Period (if applicable).”

Real World Examples

First Party “Loss”



Insured is in the possession of a substantial amount of personally identifiable information

Insurer learns on December 29 that its prime vendor suffered a serious data breach.

Then-current cyber policy ends on December 31.

Current cyber insurer sends a notice of non-renewal on December 30

Broker places a new cyber policy with effective date as of January 1

Insurer notifies both insurers of the vendor's breach event on January 14.

Real World Examples (cont'd)

Non-renewing insurer:

- Although the policy provides an automatic 60-day extended reporting period following a non-renewal, this only applies to a third-party liability claim and not to a first-party loss.
- Notice was **not** provided during the policy period, and coverage is denied.

New insurer:

- Although notice of the claim was timely provided during the policy period, the insured knew of the existence of the vendor breach before the inception of the policy.
- Policy excludes coverage for any "loss" about which the insured knew before the inception of the policy.
- Coverage is **denied**.

No coverage is available under either policy.

Real World Examples (cont'd)

Third Party “Claim”



Definition of “claim” included a governmental audit.

Policy contained a “related claims” provision deeming multiple claims arising from the same or a series of related, repeated or continuing acts, errors or omissions to be: (i) a single claim, (ii) first made when the first of the related claims was made.

Insured is subject to what it believed to be a routine audit. Does not notify its insurer.

Three years after the audit began, the government sends the insured a notice that it owes a substantial amount of money which qualify as “damages” under its policy.

Insured notifies its insurer of the government’s claim for damages.

Real World Examples (cont'd)

Insurer:

- The audit was a “**claim**” under the policy.
- The government’s demand for money is a claim that is “related to” the prior claim.
- The date of the government’s demand for money was the date of the audit for purposes of establishing the date of the “claim.”
- Although notice of the government’s demand for money was timely provided during the current policy period, notice of the audit was not provided during the period of the then-applicable policy.
- Notice was more than two-years late.
- Coverage is **denied**.

Real World Examples (cont'd)

After “notice” of a first-party loss is provided

- The insurer may provide “**breach response services.**”
- Even if the policy does not require the insured to use the insurer’s “breach response services,” the insurer might strongly suggest (or assume) that the insured use these services.

Real World Examples (cont'd)

The services might involve the assignment of a “breach coach.” A “breach coach” is typically a lawyer specializing in cyber security and privacy issues. One insurer says the following:

- “Often, a breach coach is the first responder, coupled with the claims professionals of the carrier, to help the company triage the event. They can help companies understand what needs to take place, the timeliness of what needs to take place, also, importantly, notification requirements.”
- “A breach coach can help the company secure a trusted forensics company to investigate the data breach and determine the extent of the breach. The forensics investigation identifies the potential legal issues, which vary depending on the type of data exposed. Different notification requirements apply to Personally Identifiable Information (PII), Personal Health Information (PHI) and Payment Card Information (PCI).”
- “A breach coach can help secure crisis communications professionals to handle questions from customers, employees and the media, and establish a call center to answer inquiries from the public about identity monitoring and other questions.”

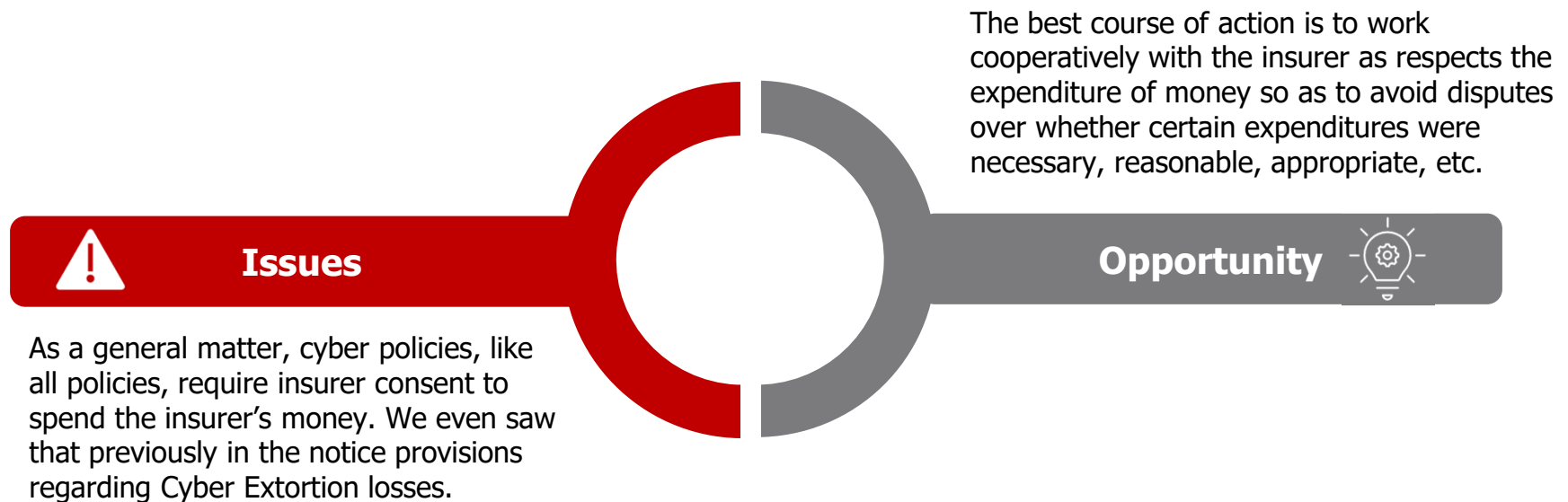
Real World Examples (cont'd)

Should an insured utilize the services of an insurer-appointed “breach coach”?

- There will not be disagreements over the rates at which the insurer will pay for the services of the “breach coach.”
- For some, or even many, breach events, the “breach coach” arrangement may be entirely appropriate, beneficial, and economical.
- Other breaches, however, involve more difficult and sensitive issues, such as public company reporting to the SEC. The services provided by an insurer-appointed “breach coach” may be too general and particularized expertise may be required.

Best course of action: Consult with independent counsel to determine rights and responsibilities under the policy and whether acceptance of services provided by an insurer-appointed “breach coach” is required or advisable under the circumstances.

Real World Examples: Consent Issues



The background is a dark, abstract digital space. It features a dense field of binary code (0s and 1s) in various sizes and colors, including blue, green, and yellow. Some digits are sharp and clear, while others are blurred, creating a sense of depth and motion. There are also glowing, streaky lines of light in blue and yellow, suggesting data flow or digital connections. The overall effect is a high-tech, futuristic aesthetic.

ATTORNEY-CLIENT PRIVILEGE / ATTORNEY WORK- PRODUCT SPECIAL ISSUES

Morgan Lewis

Are Legal Protections in Place?

Attorney-Client Privilege

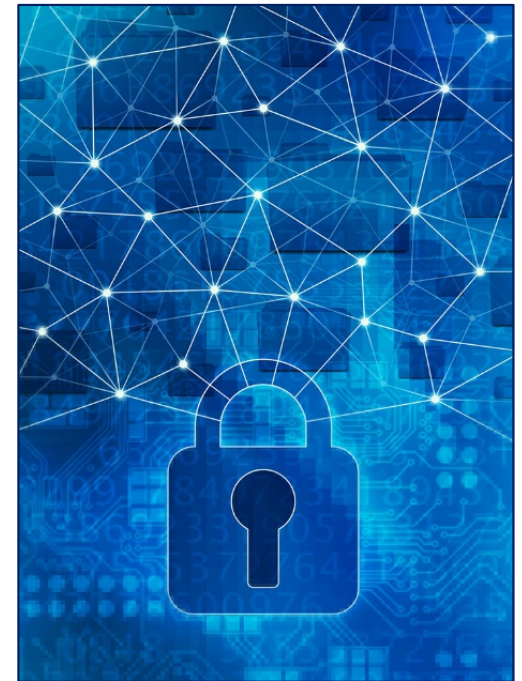
- The attorney-client privilege “purpose is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice. The privilege recognizes that **sound legal advice or advocacy** serves public ends and that such advice or advocacy depends upon the lawyer’s being fully informed by the client.” *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981).

Attorney Work-Product Doctrine

- Work prepared in anticipation of litigation by attorneys or representatives
- Mental impressions, conclusions, legal theories, opinions.
- Fed. R. Civ. P. 26(b)(3)(A)(ii)
 - May be disclosed if “party shows that it has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means.”

Range of Legal and Forensic Issues

- Was data “exfiltrated” or “accessed” or “acquired”?
- What data?
 - PII, PHI, Contractual Information?
- Did a data “breach” occur?
- What notification requirements may be triggered?
- How to mitigate loss or damages?
- Conducting a risk assessment
- Compliance issues
- Obligations during third party vendor attack
- Issues to anticipate in a regulatory inquiry or investigation
- Issues for anticipated litigation



Caution Concerning Changed Business and Legal Relationships

- “In sum, Capital One had determined that it had a **business critical need** for certain information in connection with a data breach incident, it had contracted with [a forensic provider] to provide that information directly to it in the event of a data breach incident, and after the data breach incident at issue in this action, Capital One then arranged to receive through **[a law firm] the information** it already had contracted to receive directly from [the forensic firm]. The Magistrate Judge, after considering the totality of the evidence, properly concluded that Capital One had **not established that the Report was protected work product**; and the Order was neither clearly erroneous nor contrary to law.”
 - Memorandum Opinion and Order, *In re Capital One Consumer Data Security Breach Litigation*, 2020 WL 3470261 (E.D. Va. June 25, 2020).

Common Interest Communications

- Mutual interest in a common and joint legal pursuit of resolution and handling of claims
 - Factual and legal research
 - Exchange certain Confidential Information to support the Claim
 - Cooperate in a joint legal effort
 - Avoid waiving privilege, work product, investigative privilege or allowing any confidential information to be disclosed to third parties
- Common interest extension of the attorney-client privilege and the protection afforded by the work product doctrine

THE STATE ACTOR PROBLEM

The background is a dark, abstract digital space. It features a dense field of binary digits (0s and 1s) in various sizes and colors, including white, blue, and yellow. Some digits are sharp and clear, while others are blurred, creating a sense of depth and motion. There are also glowing, streaky lines of light in blue and yellow, suggesting data flow or network connections. The overall aesthetic is high-tech and futuristic.

Morgan Lewis

The State Actor Problem

Most cyber policies have “war” exclusions under which coverage is barred if a cyber loss results from an act of war:

- The insurer is not liable for any claim or loss “alleging, based upon, arising out of, or attributable to war, invasion, acts of foreign enemies, terrorism, hijacking, hostilities, or warlike operations (whether war is declared or not), military or usurped power, civil commotion assuming the proportions of or amounting to an uprising, strike, lock-out, riot, civil war, rebellion, revolution, or insurrection.”
- A question arises as to what qualifies as a “**war**”



The State Actor Problem

Merck v. ACE American Insurance Company (N.J. Superior Court), January 13, 2022:

- Merck suffered more than \$1.4 billion in losses from the NotPetya malware attack in 2017. The attack was attributed to Russia's military intelligence agency deployed as part of its ongoing conflict with Ukraine.
- Merck's *property* insurers denied coverage based on a "war" exclusion in their policies precluding coverage for loss or damage
 - "caused by hostile or warlike action in time of peace or war, including action in hindering, combating, or defending against an actual, impending, or expected attack
 - "by any government or sovereign power (de jure or de facto) or by any authority maintaining or using military, naval or air forces"
 - "or by military, navel or air forces"
 - "or by an agent of such government, power, authority or forces"

The court held that the exclusion did not bar coverage: "Merck had every right to anticipate that the exclusion applied only to traditional forms of warfare."



The State Actor Problem

Lloyd's Market Association's Cyber Business Panel published four cyber policy exclusions in November 2021 (prior to issuance of the *Merck* decision), which significantly broaden insurers' protection against "cyber operations" launched by governments or surrogates:

- The insurer will "not cover any loss, damage, liability . . . directly or indirectly occasioned by, or happening through or in consequence of a war or a cyber operation"
- The term "war" is defined as "the *use of physical force* by a state against another state . . . whether war be declared or not."
- The term "cyber operation" is defined as "the use of a computer system by or on behalf of a state to *disrupt, deny, degrade, manipulate or destroy information* in a computer system of or in another state."
- Attribution could be difficult. The exclusion looks at whether the "government of a state (including its intelligence and security services)" makes attribution "to another state or those acting on its behalf."



The State Actor Problem

One problem is that “attribution” may be incorrect and it could change over time.

- Another problem is that the credibility of “attribution” could be in doubt. An attribution could be viewed as overly political. China and Russia, in particular, reject the legitimacy of attribution of cyber operations issued by the U.S. and allied governments as a matter of course.
- This would ultimately be a problem for the insurer, which has the burden of proving the applicability of an exclusion. In a litigated case governed by rules of evidence, the admissibility of “attribution” evidence could be challenging.



KEY AREAS TO CONSIDER

Morgan Lewis

Key Vulnerability Areas to Consider

- Risk Assessment and Management Program
- Internal Controls, Policies, Procedures and Standards
- Access Management
- Training
- Third Party Vendors
- Governance
- Managing Cyber Incident
- Address Disclosure Issues
- Address Unique Jurisdiction Standards and Requirements
- Insider Trading Controls
- Legal Review of Key Phases

Prepared for All Cyber Incident Phases

- Before, during, and after a data breach.
- Data breach-prevention guidance.
 - Implementing policies and training regarding data breaches, including governance and risk assessments, data loss prevention, and vendor management.
- Guidance on managing data breach.
 - Conducting confidential, privileged cyber incident investigations.
- Regulatory enforcement investigations and actions by federal and state regulators.
- FCA investigations and cases
- Class action litigation or other litigation that often results from a data breach.
 - Successfully defended more than two dozen data privacy class actions – either winning motions to dismiss or defeating class certifications in lawsuits brought after data breaches or based upon alleged violations of a company's privacy policy.

QUESTIONS

The background is a vibrant, abstract digital composition. It features a dark blue and purple color palette with bright, glowing light streaks and rays emanating from the right side. Scattered throughout the scene are numerous binary digits (0s and 1s) in various sizes and colors, including white, yellow, and blue. Some of these digits appear to be floating or moving, creating a sense of dynamic energy and data flow. The overall effect is reminiscent of a high-speed digital network or a futuristic data center.

Morgan Lewis

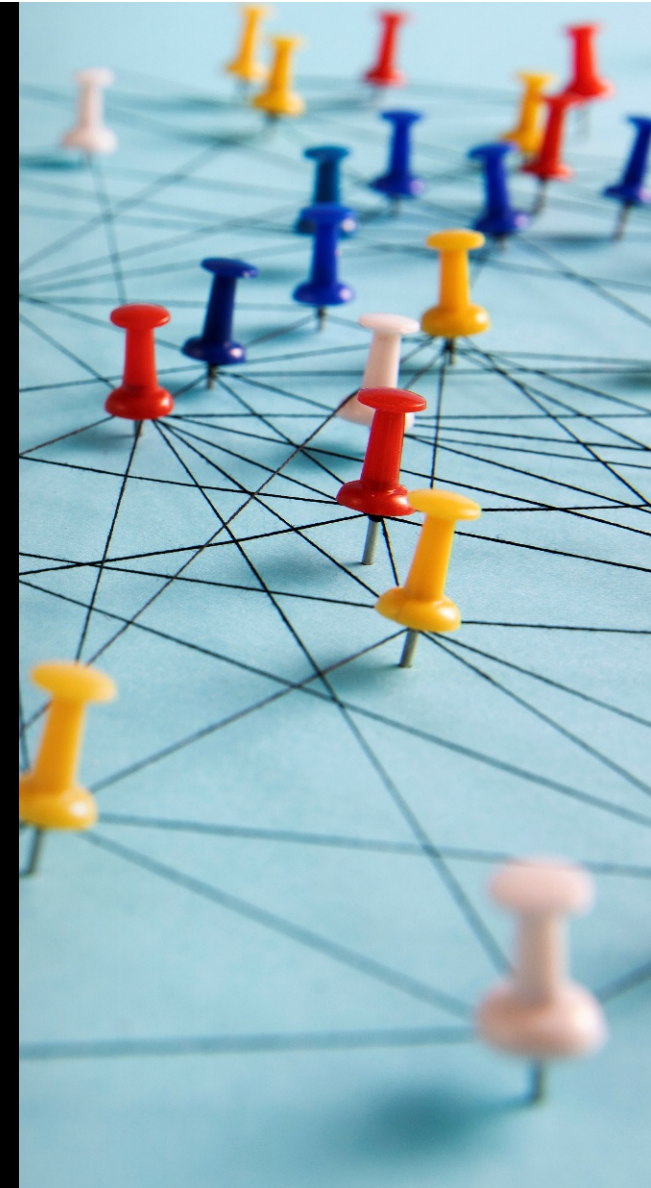
Ukraine Conflict Resources

Our lawyers have long been trusted advisers to clients navigating the complex and quickly changing global framework of international sanctions. Because companies must closely monitor evolving government guidance to understand what changes need to be made to their global operations to maintain business continuity, we offer a centralized portal to share our insights and analyses.

Morgan Lewis

To help keep you on top of developments as they unfold, visit the website at www.morganlewis.com/topics/ukraine-conflict

To receive a daily digest of all updates, please visit the resource page to **subscribe** using the "Stay Up to Date" button.



Mark L. Krotoski



Mark L. Krotoski

Silicon Valley

Washington DC

+1.650.843.7212

+1.202.739.5024

mark.krotoski@morganlewis.com

Litigation Partner, Privacy and Cybersecurity and Antitrust practices

- Co-Head of Privacy and Cybersecurity Practice Group
- More than 20 years' experience handling cybersecurity cases and issues
- Assists clients on litigation, mitigating and addressing cyber risks, developing cybersecurity protection plans, responding to a data breach or misappropriation of trade secrets, conducting confidential cybersecurity investigations, responding to regulatory investigations, and coordinating with law enforcement on cybercrime issues.
- Variety of complex and novel cyber investigations and cases
 - At DOJ, prosecuted and investigated nearly every type of international and domestic computer intrusion, cybercrime, economic espionage, and criminal intellectual property cases.
 - Served as the national coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the DOJ's Criminal Division, and as a cybercrime prosecutor in Silicon Valley, among other DOJ leadership positions.



Jeffrey S. Raskin



San Francisco

San Francisco

+1.415.442.1219

jeffrey.raskin@morganlewis.com

Jeffrey S. Raskin advises clients in litigation, mediation, and arbitration around insurance coverage matters, and intellectual property, commercial, real estate, and environmental disputes. Head of Morgan Lewis's Insurance Recovery Practice in the San Francisco office, Jeffrey counsels clients seeking recovery for catastrophic losses in securities, environmental, asbestos, silica, toxic tort, product liability, intellectual property, and employment practices cases. Jeffrey has handled first-party claims for loss covered by policies for physical damage and business interruption, title, and fidelity and crime.

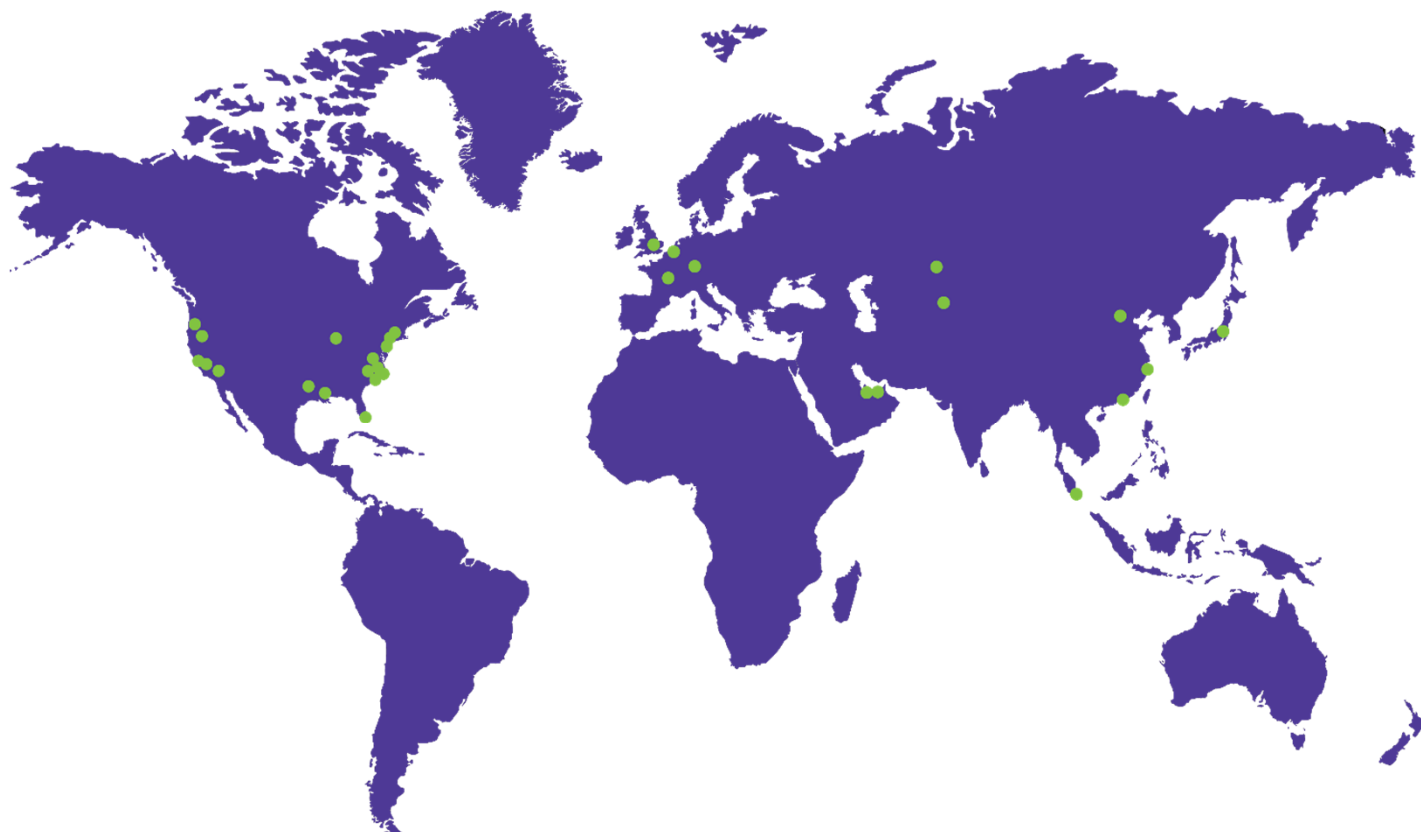


Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU

© 2022 Morgan, Lewis & Bockius LLP
© 2022 Morgan Lewis Stamford LLC
© 2022 Morgan, Lewis & Bockius UK LLP

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. Prior results do not guarantee similar outcomes. Attorney Advertising.