

Before we begin

Tech Support

If you are experiencing technical difficulties, please contact WebEx Tech Support at +1.866.779.3239.

Q&A

The Q&A tab is located near the bottom right-hand side of your screen; choose "All Panelists" before clicking "Send."

CLE

We will mention a code at some point during the presentation for attendees who requested CLE. Please make note of that code and insert it in the pop-up survey that will appear in a new browser tab after you exit this webinar. You will receive a Certificate of Attendance from our CLE team in approximately 30 to 45 days.

Audio

The audio will remain quiet until we begin at 1:00 pm ET.

You will hear sound through your computer speakers/headphones automatically. Make sure your speakers are ON and UNMUTED.

To access the audio by telephone, please click the "phone" icon below your name on the Participants Panel for teleconference information.

Morgan Lewis

TECHNOLOGY MARATHON

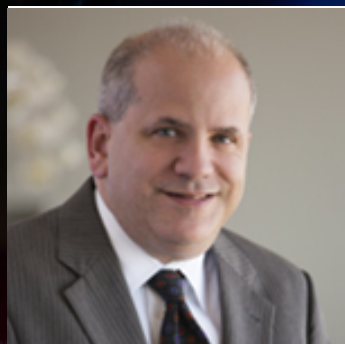
**Cyber Insurance: Is Your Company
Covered?**

Mark Krotoski and Jeff Raskin
Tuesday, June 27

Presenters



Mark L. Krotoski



Jeffrey S. Raskin

Morgan Lewis

Preliminary Note

- Comments during this presentation are based upon:
 - Publicly available information;
 - General observations and experience; and
 - ***Not*** on any specific client case information.

Overview

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

CYBER RISK LANDSCAPE

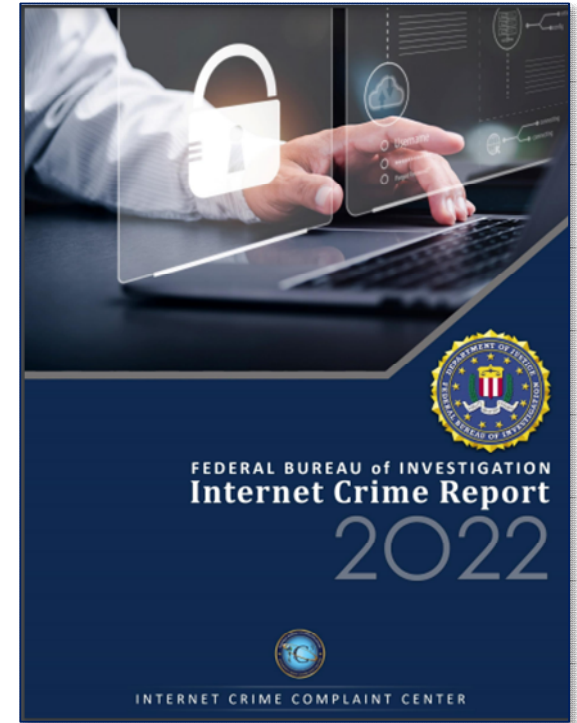
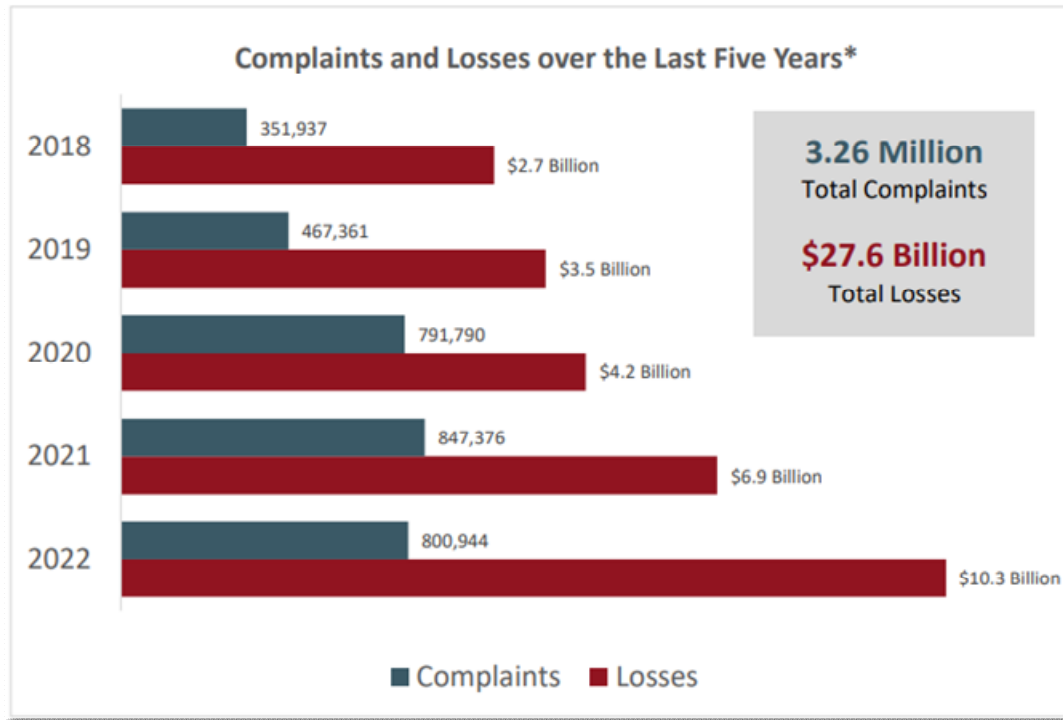


Morgan Lewis

Cyber Landscape and Risks





Internet Crime Report – Trend Last Five Years



Business Email Compromise

- Domestic and international incidents: **277,918**
- Domestic and international exposed dollar loss: **\$50,871,249,501**
- “In 2022, the IC3 received **21,832 BEC complaints** with adjusted losses **over \$2.7 billion.**”
- All **50 states, 177 countries**

Morgan Lewis



Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

June 9, 2023

Alert Number
I-060923-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field-offices

Business Email Compromise: The \$50 Billion Scam

This Public Service Announcement is an update and companion piece to Business Email Compromise [PSA I-050422-PSA](https://www.ic3.gov) posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to December 2022.

DEFINITION

Business Email Compromise/Email Account Compromise (BEC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

The scam is frequently carried out when an individual compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds.

The scam is not always associated with a transfer-of-funds request. Often times BEC variations involve compromising legitimate business email accounts and requesting employees' Personally Identifiable Information, Wage and Tax Statement (W-2) forms, and [crypto currency wallets](#).

Source: <https://www.ic3.gov/Media/Y2023/PSA230609>

Business Email Compromise

Spoofing email accounts and websites:

- Modified email address (e.g., @**company**.com to @**companygroup**.com)
- Modified domain (e.g., fullcompany.com to fu**11**company.com)

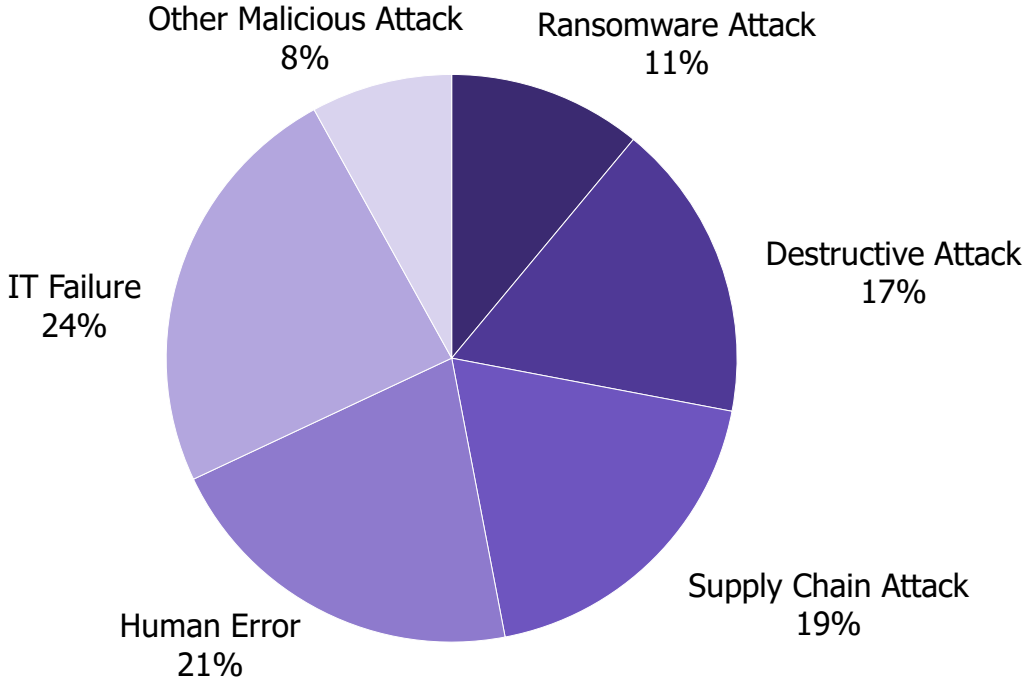
Spear-phishing

- Fraudulent email requesting confidential information

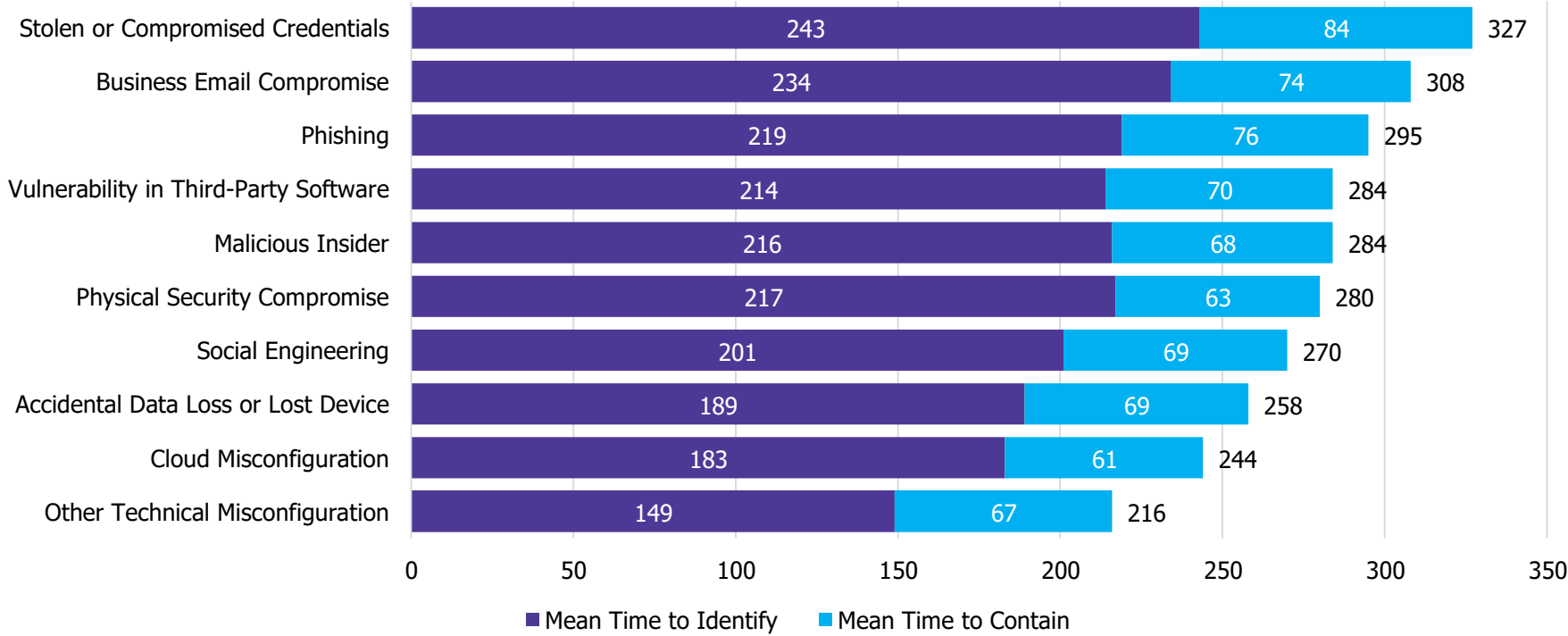
Malware

- Unauthorized access to network to review email communications about billing and invoices
- May obtain passwords to control and access email accounts
- Learn financial account information and relationships

Types of Breaches Experienced by Organizations



Average Time to Identify and Contain a Data Breach by Initial Attack Vector



Human Element

- “The human element continues to drive breaches. This year **82% of breaches involved the human element.**”
- “Whether it is the **Use of stolen credentials, Phishing, Misuse, or simply an Error**, people continue to play a very large role in incidents and breaches alike.”

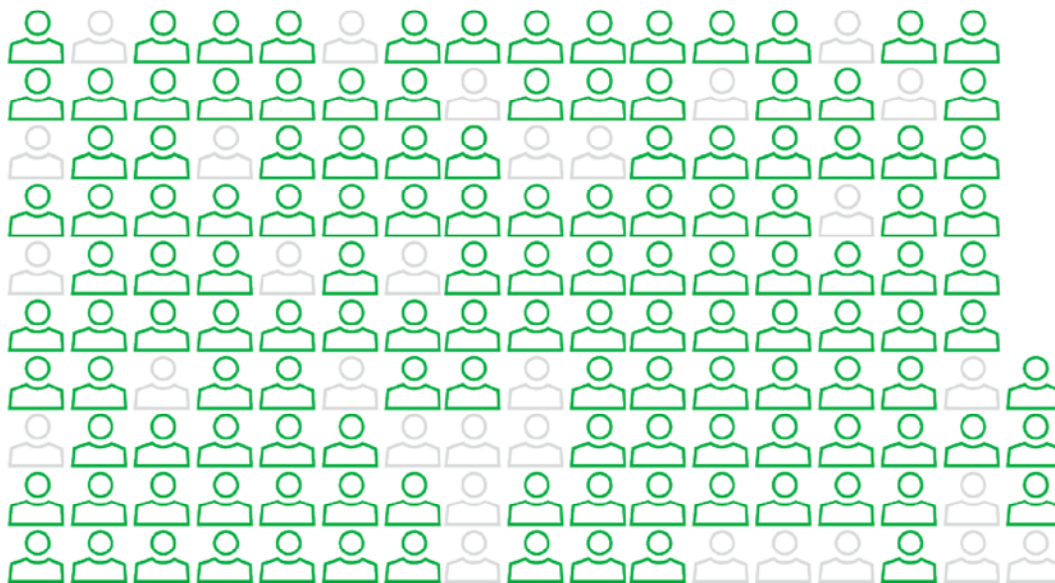
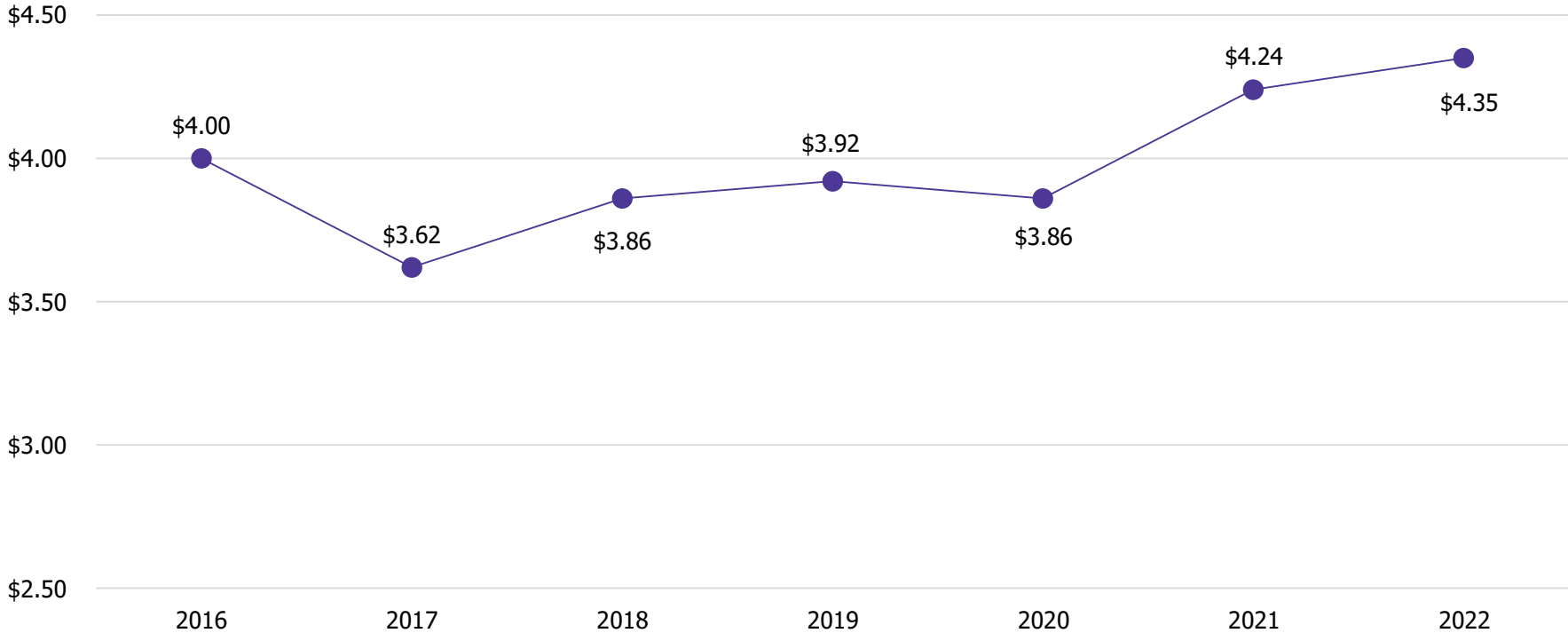
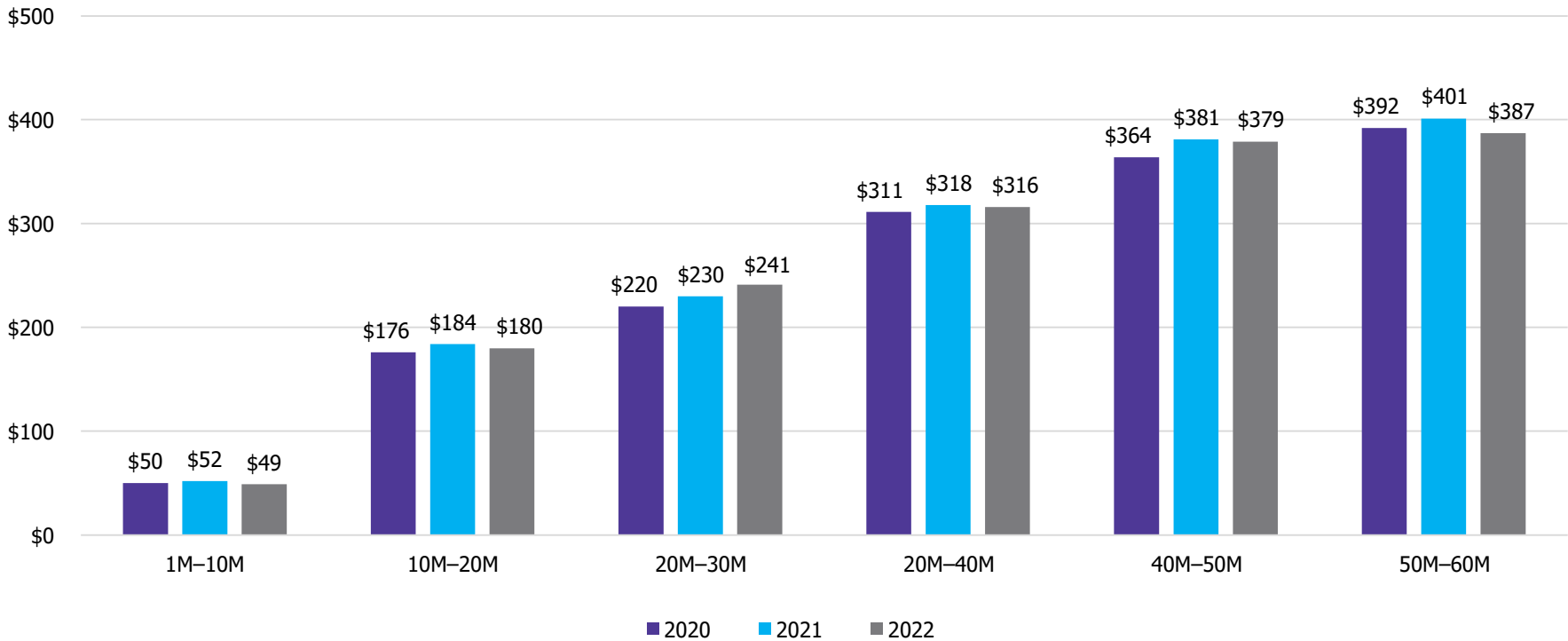


Figure 9. The human element in breaches (n=4,110)
Each glyph represents 25 breaches.

Average Total Cost of a Data Breach



Average Cost of a Mega Breach by Number of Records Lost⁽¹⁾



PRELIMINARY CYBER INSURANCE CONSIDERATIONS



Morgan Lewis

Preliminary Considerations

Cyber coverage is growing rapidly

Total premiums, 2010: \$600,000

Total premiums, 2021: \$10 Billion

Expected total premiums, 2025: \$23 Billion

But, only 55% of organizations have cyber coverage; of those, 37% lack coverage for ransomware and other forms of cyber extortion.

Ransomware attacks increased 88% in 2022 over the prior year.

Fewer than 20% of businesses have cyber limits higher than the median ransomware demand.

Preliminary Considerations

The possibility of state-sponsored cyber attacks injects substantial uncertainty in the cyber insurance market.

- Some insurers are considering retentions or deductibles for widespread cyber events
- Others are seeking to exclude acts of cyber terrorism and cyber war. The Lloyd's market asked *all* insurers using its platform to exclude state-backed cyber attacks
- Some insurers are addressing the Lloyd's-driven exclusion by introducing specific standalone cyber war coverage

Preliminary Considerations

- On May 1, 2023, a New Jersey appellate court affirmed that a standard war exclusion only barred coverage from physical warfare and not cyber attacks, thus leaving intact Merck's \$1.4 billion judgment against a group of insurers
- Despite this, there are *signs* of a more "buyer friendly" market for cyber coverage
 - Average premiums are down
 - Fewer questions are being asked during underwriting to speed the process
 - Some insurers are increasing the amount of coverage being offered
 - These developments could make it difficult for the Lloyd's market to enforce its edict that policies issued via its platform exclude state-backed cyber attacks

CYBER INVESTIGATION ISSUES

Morgan Lewis

Legal Issues Arising During Incident Response Phases



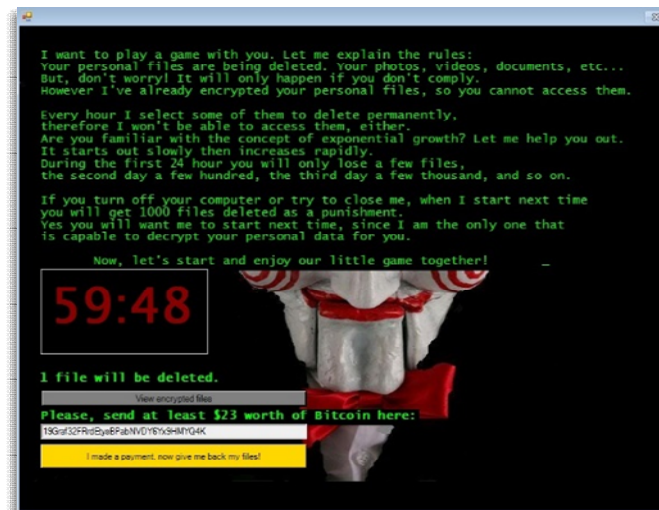
Range of Legal and Forensic Issues

- 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



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?



CORE CYBER INSURANCE COVERAGES



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 and 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 such as 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, proceedings brought under consumer protection statutes such as the California Consumer Privacy Act or the EU's General Data Protection Regulation

OTHER CYBER INSURANCE COVERAGES



Morgan Lewis

Other Cyber Insurance 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)."
- Notice should be provided **"early and often."**

Breach Coaches

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.

Breach Coaches

The services might involve the assignment of a “breach coach.” A “breach coach” is typically a lawyer specializing in cybersecurity 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.”

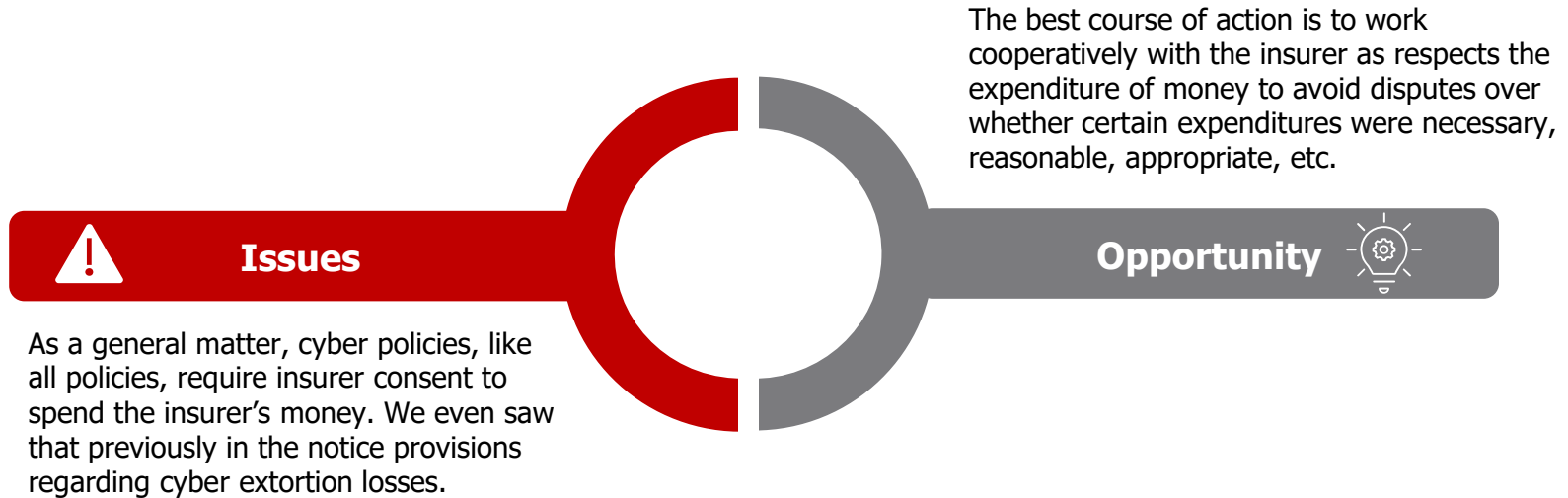
Breach Coaches

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.

Consent Issues



Your CLE Credit Information

For ALL attorneys seeking CLE credit for attending this webinar, please write down the alphanumeric code on the right >>

Kindly insert this code in the **pop-up survey** that will appear in a new browser tab after you exit out of this webinar.

THE CLE CODE IS:
TS453SA



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.”

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



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**”

State-Sponsored Cyber Attacks- Potential Systemic Risk

Merck & Co., Inc. v. ACE American Ins. Co., 475 N.J. Super. 420 (2023) (May 1, 2023)

- Merck suffered losses from the NotPetya malware/cyber attack of June 2017. It sought recovery of \$1.4 billion under 20 “all risk” property policies.
- Insurers relied on a “hostile/warlike action” exclusion in the policies. Provision excluded “loss or damage caused by hostile or warlike action in time of peace or war...(a) by any government or sovereign power.. or by any authority maintaining or using military, naval or air forces; (b) or by military, naval or air forces; (c) or by an agent of such government, power, authority or forces.”
- Per the court: The insurers “assert the word ‘hostile’ should be read in the broadest possible sense, as meaning ‘adverse,’ ‘showing ill will or a desire to harm,’ ‘antagonistic,’ or ‘unfriendly.’ According to the Insurers, any action that ‘reflects ill will or a desire to harm by the actor’ falls within the hostile/warlike action exclusion, as long as the actor was a government or sovereign power, in this case the Russian Federation.”

State-Sponsored Cyber Attacks- Potential Systemic Risk

- The court rejected this interpretation: “The exclusion of damages caused by hostile or warlike action by a government or sovereign power in times of war or peace requires the involvement of military action. The exclusion does not state the policy precluded coverage for damages arising out of a government action motivated by ill will.” *Id.* at 436.
- Insurers’ proffered interpretation conflicted with “basic construction principles requiring a court to narrowly construe an insurance policy exclusion. The specific, plain, clear, and prominent meaning of, and the clear import and intent of, a word or phrase in an exclusion does not equate to its broadest possible interpretation, but rather its narrowest.” *Id.* at 438.
- “the few cases cited by the parties reinforce our conclusion that similar exclusions have never been applied outside the context of a clear war or concerted military action and they do not support the Insurers’ arguments.” *Id.* at 439.

The Lloyd's State-Backed Cyber Exclusions

August 16, 2022 Market Bulletin

- Purpose: “To set out Lloyd’s requirements for state backed cyber-attack exclusions in standalone cyber-attack policies.”
- “If not managed properly [cyber attack cover] has the potential to expose the market to systemic risks that syndicates could struggle to manage. In particular, the ability of hostile actors to easily disseminate an attack, the ability for harmful code to spread, and the critical dependency that societies have on their IT infrastructure, including to operate physical assets, means that losses have the potential to greatly exceed what the insurance market is able to absorb.”
- “When writing cyber-attack risks, underwriters need to take account of the possibility that state backed attacks may occur outside of a war involving physical force. The damage that these attacks can cause and their ability to spread creates a similar systemic risk to insurers.”

The Lloyd's State-Backed Cyber Exclusions

- Beginning March 31, 2023, “all standalone cyber-attack policies falling within [certain risk codes] must include, unless agreed by Lloyd’s, a suitable clause excluding liability for losses arising from any state backed cyber-attack.” This applies to all new accounts and all policies renewed on that date or later.
- At a minimum, the state-backed cyber-attack exclusion must:
 - exclude losses arising from a war (whether declared or not), where the policy does not have a separate war exclusion.
 - exclude losses arising from state backed cyber-attacks that (a) significantly impair the ability of a state to function or (b) that significantly impair the security capabilities of a state.
 - be clear as to whether cover excludes computer systems that are located outside any state which is affected in the manner outlined above, by the state-backed cyber-attack.
 - set out a robust basis by which the parties agree on how any state-backed cyber-attack will be attributed to one or more states.
 - ensure all key terms are clearly defined.
- 4 *model* exclusions

The Lloyd's State-Backed Cyber Exclusions

- Actual version sent to at least one insured: "War and Cyber War Exclusion"
 - Delete original "War" exclusion in its entirety
 - Policy now excludes "War and Cyber War"
 - Does not apply to incident response costs
 - Does not apply to "that part of any claim relating to any computer systems which are physically located outside of an impacted state."
 - New definitions
 - "Cyber War": "any unauthorized access to or electronic attack on computer systems, carried out by or on behalf of a state, that directly results in another state becoming an impacted state."
 - "Impacted State": "any state that suffers a major detrimental impact on its... ability to function; or b. defense and security capabilities... as a direct result of any unauthorized access to or electronic attack on computer systems, carried out by or on behalf of another state."
 - "War": "a. war, invasion, acts of foreign enemies, hostilities or warlike operations (whether war is declared or not), civil war, rebellion, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military or usurped power; or b. action taken in controlling, preventing, suppressing or in any way relating to a. above."

The Lloyd's State-Backed Cyber Exclusions

- This version *does not comply* with the Lloyd's guidance discussed above. It lacks "attribution" language. The model attribution language provides:
 - "The primary but not exclusive factor in determining attribution of a cyber operation shall be whether the government of the state (including its intelligence and security services) in which the computer system affected by the cyber operation is physically located attributes the cyber operation to another state or those acting on its behalf."
 - "Pending attribution by the government of the state (including its intelligence and security services) in which the computer system affected by the cyber operation is physically located, the insurer may rely upon an inference which is objectively reasonable as to attribution of the cyber operation to another state or those acting on its behalf. It is agreed that during this period no loss shall be paid."
 - "In the event that the government of the state (including its intelligence and security services) in which the computer system affected by the cyber operation is physically located either:
 - takes an unreasonable length of time to
 - does not, or
 - declares it is unable toattribute the cyber operation to another state or those acting on its behalf, it shall be for the insurer to prove attribution by reference to such other evidence as is available."

The Lloyd's State-Backed Cyber Exclusions

- There are many potential problems with these provisions:
 - The definition of “impacted state” is first triggered if a state has suffered “a major detrimental impact.” How is that determined?
 - The attribution language, if adopted, is subject to political posturing from an “impacted” state.
 - The “objectively reasonable inference” of an insurer in attributing an attack to “another state” permits a large degree of variability and invites disputes.
 - The “other evidence as is available” enabling the insurer to attempt to attribute an attack to another state is also quite variable and invites disputes.

Gaslighting

The insurer that issued the “War and Cyber War Exclusion” discussed above calls this an “upgrade”

- “It introduces an explicit definition of ‘cyber war’, providing greater clarity”
- “It introduces a high threshold for what is considered to be an act of cyber war”
- “It provides cover for initial incident response support, even in the event of cyber war”
- “It provides cover for ‘collateral damage’ stemming from cyber war”

Gaslighting

- “The traditional war exclusion attaching to most insurance policies, including cyber policies, was originally intended to address physical acts of war. The language is very broad in its scope, which can create *confusion and ambiguity* as to whether the exclusion applies to certain types of cyber attack or not. Certain terms could be interpreted liberally and applied to many different scenarios, which might ultimately result in reduced cover for our policyholders. We have therefore taken steps to improve our war exclusion and bring clarity to policyholders.”
 - *Merck & Co., Inc. v. ACE American Ins. Co.*, 475 N.J. Super. 420 (2023), held that the “traditional war exclusion” does not reach cyber attacks.
- “The previous iteration of the war exclusion did not explicitly define cyber war, *creating ambiguity* for policyholders as to when a cyber attack would be considered an act of war.”
 - Ambiguities are construed against the insurer.
 - Exclusions are construed narrowly.
- “By specifically defining what an act of cyber war looks like and creating a high threshold for it, we are narrowing the scope of the war exclusion, removing ambiguity and providing greater clarity to our policyholders.”

KEY AREAS TO CONSIDER



Morgan Lewis

What Next and How to Prepare?

- Identity and access management
- Conduct risk assessments for your business operations
- Management and board role and oversight of cybersecurity risks
- Review policies, procedures, and controls
- Vulnerability management plan
- Identify primary federal and state regulators
- Update security programs consistent with regulatory expectations
- Encrypt or tokenize sensitive and critical data in transit and at rest
- Data classification program to identify sensitive and critical data



What Next and How to Prepare?

- Maintain, update, and test Incident Response and Business Continuity Plans
- Back up and secure data
 - Offline or segregated
- Review cybersecurity insurance policies
- Conduct regular employee trainings on key risk areas
- Keep security software up to date
- Address third-party vendor issues and risks
- Consider risks associated with remote work
- Address privilege and legal protection issues
- Legal guidance on compliance issues, notification requirements, security issues, and applicable legal standards

Morgan Lewis



Be 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.
- False Claims Act investigations and cases
- Class action litigation or other litigation that often results from a data breach.
 - Motions to dismiss
 - Defeating class certifications in lawsuits brought after data breaches or based upon alleged violations of a company's privacy policy.

QUESTIONS



Morgan Lewis

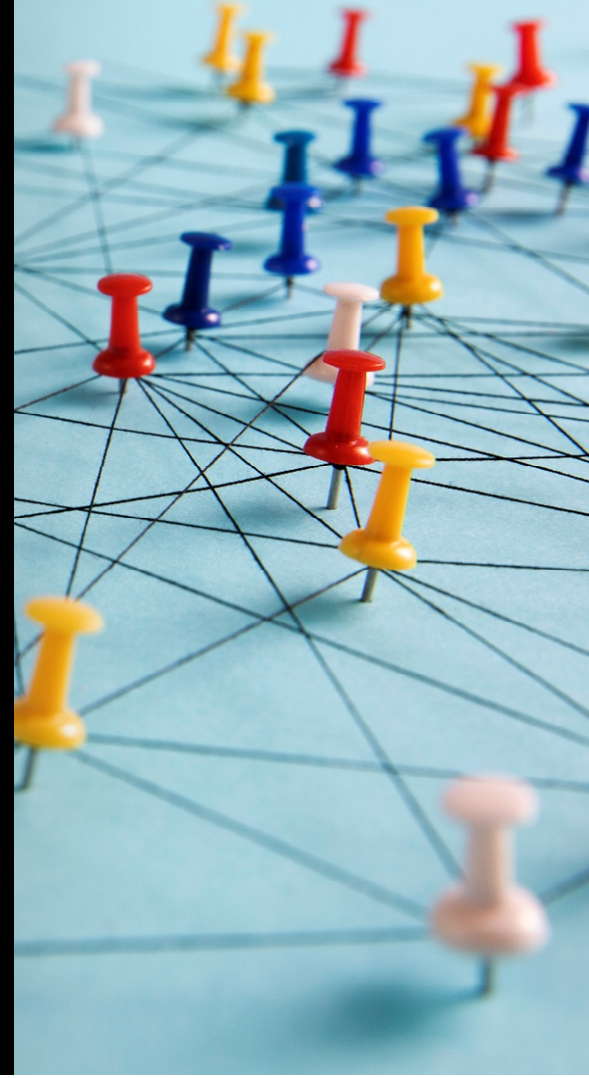
Ukraine Conflict Resources

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



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 cyber crime 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 cyber crime prosecutor in Silicon Valley, among other DOJ leadership positions.

Jeffrey S. Raskin



San Francisco
+1.415.442.1219
jeffrey.raskin@morganlewis.com

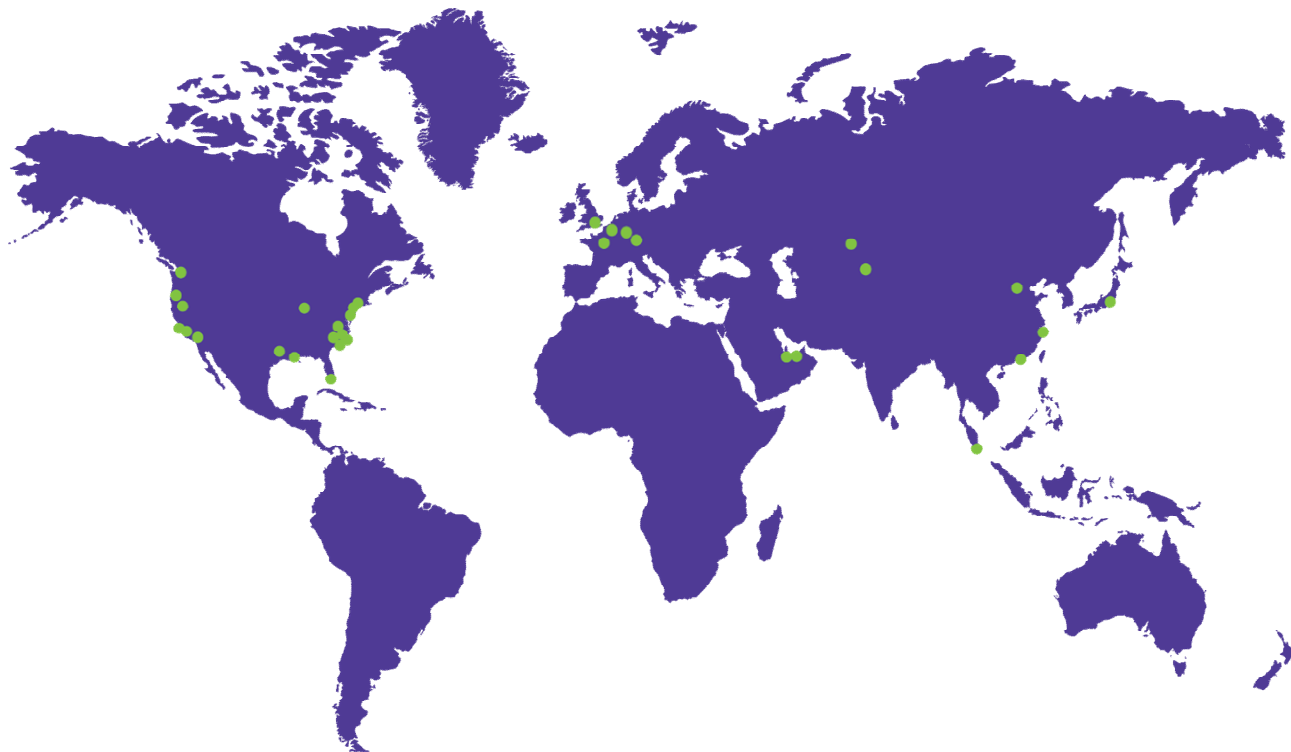
Jeffrey advises clients in litigation, mediation, and arbitration around insurance coverage matters, and intellectual property, commercial, real estate, and environmental disputes. Head of Morgan Lewis's Insurance Recovery Practice in the San Francisco office, Jeffrey counsels clients seeking recovery 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
Astana
Beijing
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong
Houston
London
Los Angeles
Miami
Munich
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Seattle
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.

THANK YOU

© 2023 Morgan Lewis

Morgan, Lewis & Bockius LLP, a Pennsylvania limited liability partnership

Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius 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.

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.