2020 CLM Focus
December 3, 2020
New York, NY
Narrative

Cybersecurity in the Post-Pandemic World: Not Another Dystopian Tale?

Joshua Mooney, White & Williams, Partner, Chief Privacy Officer
Judy Selby, Hinshaw & Culbertson, Partner
Michael Phillips, Arceo, Head of Claims

I. The Current Landscape

A. Risks Associated with and Exasperated by COVID-19

Firewall and penetration defenses become more difficult. Detection becomes much more difficult, especially to the extent employees use personal devices. Device inventory/data flow tracking. It's critical for companies to (1) try to manage data privacy and security concerns through a central enterprise as much as possible, (2) inventory the new devices and workstations.

Phishing scams are always going to leverage current events to their advantage when possible. COVID-19 is a particularly attractive topic for scammers as everyone is impacted by it and are looking for authoritative information. Yet, while you need to think about the external threat landscape, you will absolutely be subject greater risks by ignoring internal threats, by not focusing on regulatory compliance, or by failing to identify internal controls and ensure control owners take responsibility for the efficacy of the controls. When you find an internal threat, give it the attention it deserves and make sure that your executives and the other teams involved in the remediation effort understand why the threat deserves the attention. This will garner further buy in to the larger program and result in a more proactive approach to implementation of controls / adherence to a framework. *Never waste a good crisis.*

B. New Value in Risk Assessments

Risk assessments also are a critical, and likely underutilized tool – especially given the economic downturn. The risk assessment process allows individuals to systematically analyze a given threat or vulnerability and attempt to quantify the probability of its occurrence and potential impacts should it occur. They should be deployed throughout all areas of a business and do not pertain solely to IT and privacy concerns. Risk assessments also should help to foster buy-in from management or any stakeholder. At their core it is simply a cost-benefit analysis. The information contained within risk assessments will allow management to make informed decisions about how to eliminate, mitigate or live with the referenced issue. It also allows an organization to properly

insure against all of the risks that must be lived with. If a company has not done a risk assessment or understands where they are with basic cyber hygiene at an organizational level.

II. Attacks on Privilege Over Cyber Incident Reports

In the action *In Re Capital One Consumer Data Security Breach Litigation*, No. 19-2915 (E.D. Va.), a Virginia federal court determined that a forensics investigation report conducted by a third-party investigator under the direction of outside counsel was not privileged and had to be produced. The essence of the court's decision is that the report was not work-product because Capital One would likely have ordered the forensic report completed even if it had not anticipated litigation. Is this decision extraordinary? This and other decisions suggest that it is becoming more difficult to shield third-party forensics reports from discovery.

So, navigating the privilege line can be difficult, especially in cybersecurity matters. In the context of a data breach response, events can move fast. Shortcuts in structure and procedure caused by time pressures can result in substantial and detrimental impacts later. It is critical for organizations to appreciate and prepare for the appropriate procedures when retaining a forensics consultant. Procedures include the context and structure of the consultant's retention, dissemination of its report, and sometimes, even the content of the report itself. In light of the *Capital One* decision, there are several steps organizations and its counsel (in-house and outside) may take to strengthen a privilege claim for a forensics report.

A. Background

To understand what should be done, it is critical to first know what happened in *Capital One*. In November 2015, Capital One entered into a Master Services Agreement (MSA) with FireEye, Inc., d/b/a Mandiant (Mandiant), which was supplemented by periodic Statements of Work (SOW) for specific services under the MSA's terms. The SOWs provided for incident response services by Mandiant, if necessary. It was undisputed that a significant purpose of the MSA and SOWs "was to ensure that Capital One could quickly respond to a cybersecurity incident should one occur." In January 2019, Capital One entered in another SOW with Mandiant entitling it to 285 hours of services including, if necessary, incident response services. Capital One designated the retainer to be paid as a "business critical" expenditure.

In March 2019, Capital One suffered what is now a well-publicized data breach that compromised the personal data of over 100 million consumers. Capital One confirmed the data breach on July 19, 2019, and the next day retained outside counsel to provide legal advice in connection with the incident. On July 24, 2019, outside counsel and Capital One signed a Letter Agreement with Mandiant, whereby Mandiant agreed to provide incident response services, including digital forensics, log and malware analysis and incident remediation. These services were to be performed under the same terms as the January 2019 SOW, but the Letter Agreement stated that the work was to be done at the direction of counsel and that deliverables would be provided to outside counsel instead of Capital One.

Mandiant preformed the services, preparing a September 2019 report "detailing the technical factors that allowed the criminal hacker to penetrate Capital One's security" (the Mandiant Report). Capital One paid Mandiant out of the retainer already given under the 2019

SOW. When the retainer amount was exhausted, Capital One paid Mandiant's additional fees from its cyber organization department. In December 2019, about three months after Mandiant had issued its report, Capital One re-designated the expenses as legal expenses and deducted them against Capital One's legal department's budget.

Pursuant to the Letter Agreement, the Mandiant Report initially was sent to outside counsel, which in turn provided the report to Capital One's legal department. Outside counsel also appeared to provide the report to Capital One's Board of Directors. Documents provided to the Capital One court showed that individuals and organization who received copies of the report included approximately fifty Capital One employees, four regulators and the accounting firm Ernst & Young. In opposing the motion to compel the report's production, Capital One did not explain why each recipient was provided with a copy of the report, or show that it had placed restrictions on further copying or dissemination of the report.

The work-product doctrine is a court-created exemption of materials from discovery under the theory that an opposing party should not have the right to discover those materials through its counsel which it has prepared for prosecution or defense of a claim.[2] Federal Rule of Evidence 502 defines work-product protection as "the protection that applicable law provides for tangible material (or its intangible equivalent) prepared in anticipation of litigation or for trial." Fed. R. Evid. 502(g)(2). "Anticipation of litigation" is a key concept – if the materials were not created in anticipation of litigation, they are not subject to the work-product doctrine protection.

Thus, materials prepared in the ordinary course of business, pursuant to regulatory requirements, or for other non-litigation purposes are not materials prepared in anticipation of litigation and fall outside the work-product doctrine protection. Courts in the Fourth Circuit, where the Capital One case is pending, examine "the driving force behind the preparation of" the document at issue to determine if the work-product doctrine applies. Under this legal standard, in the case before it, while the court agreed that when Mandiant began its "incident response services" in July 2019, there was a very real potential that Capital One would face litigation, "the determinative issue is whether the Mandiant Report would have been prepared in substantially similar form but for the prospect of that litigation."

To begin, the Capital One court established the heavy framework for the issue by stating that "the party requesting protection under the work product doctrine bears the burden of showing how it would have investigated the incident differently if there was no potential for litigation." This question was critical to its analysis. Having an investigation be done at the direction of outside counsel is not enough. In determining that the Mandiant Report was not privileged, the court noted:

- Capital One had a long-standing relationship with Mandiant and had a pre-existing SOW;

- the retainer paid to Mandiant was a business-critical expense at the time it was paid;

- the Mandiant Report was provided to four different regulators and to an accountant, showing that the results of an independent investigation was significant for regulatory and business reasons; and

- the Mandiant Report was used for Sarbanes-Oxley disclosures and was referenced in draft FAQs prepared by a senior vice president prior to the public announcement of the data breach.

The court concluded that the "only significant evidence that Capital One has presented concerning the work Mandiant performed is that the work was at the direction of outside counsel and that the final report was initially delivered to outside counsel" – evidence that was insufficient to apply the work-product doctrine protections.

Contrasting the case at hand with a similar discovery battle in the lawsuit *In re Experian Data Breach Litigation* – where the California federal court held that a report prepared by Mandiant was privileged, the court noted several differentiating factors, including the context of Mandiant's retention and use of the report:

- Experian had immediately retained outside counsel and that outside counsel had hired Mandiant to prepare a report and

- the report was not given to Experian's incident response team, noting the California federal court's conclusion that if the report had been "more relevant to Experian's internal investigation or remediation effort, as opposed to being relevant to defense of the litigation, then the full report would have been given to that team."

Most significant to the *Capital One* court was that the work to be done by Mandiant in connection with the March 2019 data breach was the same work to be performed under the MSA and SOW, without any differentiating factors other than the report was to be sent to outside counsel first.

B. Thoughts to Consider for Strengthening Privilege

There are specific processes and procedures organizations should consider when retaining a firm to conduct a forensics analysis in response to a cybersecurity incident. Different contexts provide different levels of importance for each. The critical common denominator, however, is that an organization must be prepared to produce objectively demonstrable actions that show the forensics firm's investigation, and its report, were produced and disseminated for the purpose of legal defense and not for business operations or regulatory compliance. A key consideration that courts (and plaintiffs' counsel) will focus upon is whether, in response to a cybersecurity incident, the organization would have had the forensics analysis report prepared even in absence of any anticipated litigation. Here are five things to consider.

1. The Report's Intended Use and Whether a Separate Report is Required

2. Limited Dissemination

3. Pre-Existing Agreements

4. Language Matters

5. It Needs to Be a Legal Expense

III. Enforcement Actions, Litigation, and What Have We Learned for Data Privacy and Security

A. California Consumer Protection Act

California Attorney General Xavier Becerra repeatedly made clear that enforcement of CCPA would not be delayed by the COVID-19 pandemic. While the California Office of Attorney General has not yet commenced with a barrage of enforcement actions, a wave of litigation under CCPA's private cause of action already has begun. A key issue will be the scope of that private cause of action.

Although CCPA creates a series of privacy rights enforceable only by the California Attorney General, the statute also has a private cause of action relating to data security. Cal. Civ. Code § 1798.150 authorizes consumers to institute a civil action against a business whose failure to implement and maintain reasonable security procedures resulted in the unauthorized access and exfiltration, theft or disclosure of the consumer's non-encrypted or non-redacted personal information. The definition for "personal information" in the cause of action's context is narrower than elsewhere under CCPA, and applies only to consumer's name combined with an identifying data element, such as a Social Security number, driver's license number, or medical information.

Despite the more limited nature of the private cause of action, some newly filed lawsuits seek to expand it. First, some lawsuits have used violations under CCPA as a catalyst to assert claims under other statutes, like unfair trade practices. In *Hurvitz v. Zoom Video Communications, Inc.*,[1] for instance, plaintiffs allege that defendant's purported notice violations under CCPA violate the California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.*, entitling plaintiffs to damages. In *Cullen v. Zoom Video Communications, Inc.*,[2] plaintiffs allege that Zoom's purported transfer of users' personal information without prior notice violated CCPA's private cause of action because, by permitting the transfer of data, Zoom breached its duty to implement and maintain reasonable security procedures and practices, which resulted in the unauthorized disclosure of plaintiffs' non-encrypted and non-redacted personal information. While CCPA's private cause of action was intended to be limited to data breaches, the claims asserted in *Cullen* could broaden the scope of the cause of action to any unauthorized disclosure.

B. The Dangers of Personal Devices and Older Devices

One side effect of the COVID-19 pandemic on data security is that the sudden need to convert the workplace from onsite to remote operations potentially has required many organizations to use older equipment or personal devices that lack proper encryption. The use of such devices, combined with the lack of having proper controls in place to secure workplace data, can incur significant liability. A settlement agreement entered into between the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and Lifespan Health System Affiliated Covered Entity (Lifespan ACE), subject to a July 27, 2020 OCR press release, serves as one example.

---

1 *Hurvitz v. Zoom Video Communications, Inc. et al.*, No. 20-3400 (C.D. Cal. Apr. 13, 2020).

2 *Cullen v. Zoom Video Communications, Inc.*, No. 20-2155 (N.D. Cal. Mar. 30, 2020).

Under the settlement, which arose from the theft of an unencrypted laptop containing protected health information from an employee's automobile, Lifespan ACE agreed to:

- pay a fine in excess of $1 million; and
- implement a "corrective action plan" that includes two years of OCR oversight and monitoring.[3]

Although the theft of the laptop pre-dates the COVID-19 pandemic, the penalty from the incident – which constitutes a data breach under the Health Insurance Portability and Accountability Act (HIPAA) and the various state data breach notification laws – should serve as a stark reminder of the potential cost of using unencrypted devices and the lack of controls to prevent such use. It also demonstrates a hardline stand taken by OCR against the use of unencrypted devices.

In February 2017, a hospital employee's car was broken into while parked in a public lot, resulting in the theft of a MacBook laptop used by the employee for work purposes.[4] It is unclear whether the laptop was provided by the Hospital or whether it was a personal device. The encryption settings on the hard drive had not been set – meaning the hard drive and the data stored on it were unencrypted. Lifespan ACE determined that the employee's work emails may have been cached on the device's hard drive, and that through the cached emails, the thieves could have access to patient names and medical records. In addition, the hard drive may have included information about patients across various affiliated providers. Following its investigation, OCR determined that there was "systemic noncompliance" with data privacy and security requirements under HIPAA, including "a failure to encrypt ePHI on laptops after Lifespan ACE determined it was reasonable and appropriate to do so." OCR also determined that Lifespan ACE lacked "device and media controls," and failed "to have a business associate agreement in place with the Lifespan Corporation," the healthcare provider's parent company. In particular, the consent settlement agreement noted:

> A. Lifespan did not implement policies and procedures to encrypt all devices used for work purposes (see 45 C.F .R. § I 64.312(a)(2)(iv));
>
> B. Lifespan did not implement policies and procedures to track or inventory all devices that access the network or which contain ePHI (See 45 C.F.R. § 164.3 10(d)(l));
>
> C. Lifespan did not have the proper business associate agreements in place between Lifespan Corporation and the Lifespan healthcare provider affiliates that are members of the Lifespan ACE (See 45 C.F.R. § 164.502(e)); and

---

[3] https://www.hhs.gov/about/news/2020/07/27/lifespan-pays-1040000-ocr-settle-unencrypted-stolen-laptop-breach.html

[4] https://www.hhs.gov/sites/default/files/lifespan-ra-cap-signed.pdf

D. Lifespan impermissibly disclosed the PHI of 20,431 individuals (see 45 C.F.R. § 164.502(a)).

What's notable are both the size of the fine assessed against LifeSpan ACE and that the incident spawned from the theft of a single laptop. In a post pandemic world that requires a remote workforce and virtual operations, a simple precaution of ensuring that all devices used by employees could slip through the proverbial cracks. Thus, when issuing laptops or other devices to employees, or when otherwise contemplating employees' use of personal devices for work-related functions, organizations must ensure the encryption of workplace data. Here are some simple solutions to consider:

- Use of a central enterprise program to manage data encryption of all work-issued devices.
- Managment of access tools and applications that prevent the ability to transfer data from the workplace network to a personal hard drive.
- Implementation and enforcement of policies and procedures that prohibit the storage of workplace data on unencrypted removable media.
- Teach employees how to arm encryption protocols on personal devices.

landscape of their networks and (2) identify/mitigate risk vectors identified in that new landscape.

C. After Three Long Years … N.Y. Department of Financial Services (DFS)

What do insurers need to know?

IV. Exposures in cyber and silent cyber coverage.

A. Coverage Overview

Cyber insurance policies provide first and third party coverages to policyholders in the event of a cyber or privacy event. Unfortunately, the risk of those events has soared as companies and organizations scramble to remain operational in the face of government shutdown orders and other COVID-19-related disruptions. The massive shift to work-from-home for many employees has increased exponentially their reliance on a wide variety of technologies to communicate and continue working remotely, which vastly expands the attack surface for cyber criminals. In addition, remote employees may utilize personal devices and be more inclined to adopt workarounds and bypass mandated business processes in favor of easier, but less secure, tools. Cyber criminals are further exploiting the situation by tailoring phishing scams specifically aimed at remote workers, and by posing as COVID-19 resource centers and charities. In addition to cyber-specific policies, policyholders often seek coverage for cyber-related claims under crime policies and under traditional commercial property and commercial general liability policies looking for so-called silent cyber coverage.

B. Potential Cyber-Related Claims

- A remote employee is tricked into providing his network credentials by a caller pretending to be with his company's technical support team, resulting in a ransomware or data breach event.

- An employee working on a home computer and utilizing a personal email account that auto-populates addressees inadvertently sends confidential personal health information concerning employees with COVID-19 to the wrong recipients.

- A business wires money to a foreign bank account after receiving fraudulent emails purporting to be from a vendor, advising the business of its new bank account.

C. Key Points And Select Issues

1. Notice And Claims-Made Issues Relating To Cyber Claims.

Late notice of cyber and privacy claims can significantly prejudice insurers by, among other things, potentially increasing the cost and severity of the event as well as the risk of destruction of forensic evidence. It also can reduce the chances of intercepting a wire transfer and pursuing subrogation claims. The potential for late notice may be increased by disruption caused by work-from-home situations.

2. Compliance With Policy Requirements.

Cyber policies often require the insured to obtain the insurer's written consent before expending funds or retaining professionals to respond to an incident. The instinct of many insureds, however, is to take matters into their own hands and try to immediately address the situation on their own (often retaining less experienced, and non-approved vendors/agents), and, in doing so, incur significant costs before putting the carriers on notice. Many policies also have requirements concerning utilization of pre-approved incident response professionals and verification of requests to transfer funds. Insurers should examine all such policy requirements in connection with any claim.

3. Carefully Review All Policy Terms, Including Definitions.

There is wide variation in coverages under cyber policies due, in part, to the absence of standardized forms and the widespread use of manuscript policies and endorsements. Depending on the terms of the policy at issue, for example, coverage for regulatory claims may be limited to data breach or security events. In some polices, coverage for breach of a third-party holding the policyholder's confidential information may depend on the status of the third-party as an independent contractor or its contractual relationship with the policyholder. In addition, some policies limit coverage to events arising out of computer systems and any associated devices or equipment operated by and either owned or leased to the insured organization. It is crucial, therefore, to carefully review the entire policy including endorsements when considering any COVID-19 claim.

4. Cyber Exclusions And Limitations In Commercial Property And Liability Policies.

As mentioned above, policyholders sometimes seek coverage for cyber claims under traditional commercial property and general liability policies. These claims are often referred to as "silent cyber" claims, since the policies may not affirmatively grant or exclude coverage for cyber and privacy claims.

Over the years, insurers have introduced various exclusions to address silent cyber claims that were not intended for coverage under non-cyber policies. For example, CGL policies typically exclude coverage for bodily injury and property damage claims for damages arising from any "access to or disclosure of any person's or organization's confidential or personal information, including . . . trade secrets, . . . customer lists, . . . credit card information, health information or any other type of nonpublic information . . . ." For Personal and Advertising Injury Liability, coverage may be excluded on claims arising from any access to or disclosure of non-public information. For first-party property policies, the 2012 ISO Businessowners Policy ("BOP") form excludes computer-related losses that, by definition, includes malicious code, and the 2012 BOP form excludes loss caused by viruses or malware. Some insurers also have recently asserted that silent cyber claims might be excluded under War Exclusions in connection with ransomware events under commercial property policies.

Non-cyber policies may be endorsed with coverage grants for social engineering or business email compromise events. Those coverages typically are subject to sublimits and may contain internal verification requirements as a condition precedent to coverage.

Policyholders, however, have had some success in seeking coverage for silent cyber claims under non-cyber policies, most recently in *Nat'l Ink & Stitch, LLC v. State Auto Prop. & Cas. Ins. Co.*, 435 F. Supp. 3d 679 (D. Md. 2020), where the court ruled that a ransomware claim was covered under the specific terms of the BOP at issue. Insurers should therefore carefully examine choice of law considerations in connection with their consideration of COVID-19-related silent cyber claims.

5. UK Silent Cyber Developments

Spurred on by a mandate from the UK Prudential Regulation Authority to either affirmatively cover or exclude cyber acts (malicious acts) and cyber incidents (accidental or operational error) by January 1, 2020, two UK insurance industry associations have released new cyber exclusions to eliminate or substantially limit potential coverage for cyber-related claims.

In November 2019, the Lloyd's Market Association issued two exclusion for property policies, although they can be utilized in other forms as well. The first, LMA 5400, excludes coverage for any loss arising out of a cyber act or a cyber incident, but contains a carve out for ensuring fire or explosion from a cyber incident only. All other resultant damage from a cyber act or incident is excluded. There is coverage for the cost of repair or replacement of damaged data processing media and the cost of copying data from backups or from originals of a previous generation. The exclusion states:

> *Notwithstanding any provision to the contrary within this Policy or any endorsement thereto this Policy excludes any:*
>
> *1.1 Cyber Loss, unless subject to the provisions of paragraph 2;*

1.2 loss, damage, liability, claim, cost, expense of whatsoever nature directly or indirectly caused by, contributed to by, resulting from, arising out of or in connection with any loss of use, reduction in functionality, repair, replacement, restoration or reproduction of any Data, including any amount pertaining to the value of such Data, unless subject to the provisions of paragraph 3; regardless of any other cause or event contributing concurrently or in any other sequence thereto.

2 Subject to all the terms, conditions, limitations and exclusions of this Policy or any endorsement thereto, this Policy covers physical loss or physical damage to property insured under this Policy caused by any ensuing fire or explosion which directly results from a Cyber Incident, unless that Cyber Incident is caused by, contributed to by, resulting from, arising out of or in connection with a Cyber Act including, but not limited to, any action taken in controlling, preventing, suppressing or remediating any Cyber Act.

3 Subject to all the terms, conditions, limitations and exclusions of this Policy or any endorsement thereto, should Data Processing Media owned or operated by the Insured suffer physical loss or physical damage insured by this Policy, then this Policy will cover the cost to repair or replace the Data Processing Media itself plus the costs of copying the Data from back-up or from originals of a previous generation. These costs will not include research and engineering nor any costs of recreating, gathering or assembling the Data. If such media is not repaired, replaced or restored the basis of valuation shall be the cost of the blank Data Processing Media. However, this Policy excludes any amount pertaining to the value of such Data, to the Insured or any other party, even if such Data cannot be recreated, gathered or assembled.

4 In the event any portion of this endorsement is found to be invalid or unenforceable, the remainder shall remain in full force and effect.

5 This endorsement supersedes and, if in conflict with any other wording in the Policy or any endorsement thereto having a bearing on Cyber Loss, Data or Data Processing Media, replaces that wording.

DEFINITIONS

6 Cyber Loss means any loss, damage, liability, claim, cost or expense of whatsoever nature directly or indirectly caused by, contributed to by, resulting from, arising out of or in connection with any Cyber Act or Cyber Incident including, but not limited to, any action taken in controlling, preventing, suppressing or remediating any Cyber Act or Cyber Incident.

7 Cyber Act means an unauthorised, malicious or criminal act or series of related unauthorised, malicious or criminal acts, regardless of time and place, or the threat or hoax thereof involving access to, processing of, use of or operation of any Computer System.

8 Cyber Incident means:

> *8.1 any error or omission or series of related errors or omissions involving access to, processing of, use of or operation of any Computer System; or*
>
> *8.2 any partial or total unavailability or failure or series of related partial or total unavailability or failures to access, process, use or operate any Computer System.*

9 Computer System means:

> *9.1 any computer, hardware, software, communications system, electronic device (including, but not limited to, smart phone, laptop, tablet, wearable device), server, cloud or microcontroller including any similar system or any configuration of the aforementioned and including any associated input, output, data storage device, networking equipment or back up facility, owned or operated by the Insured or any other party.*

10 Data means information, facts, concepts, code or any other information of any kind that is recorded or transmitted in a form to be used, accessed, processed, transmitted or stored by a Computer System.

11 Data Processing Media means any property insured by this Policy on which Data can be stored but not the Data itself.

The second exclusion, LMA 5401, is an "absolute" exclusion that bars coverage for both malicious cyber acts and non-malicious cyber incidents, with no carve out. There is no coverage for repair or replacement of data or for data loss caused by any physical peril. That exclusion provides in relevant part:

1. Notwithstanding any provision to the contrary within this Policy or any endorsement thereto this Policy excludes any:

> *1.1 Cyber Loss;*
>
> *1.2 loss, damage, liability, claim, cost, expense of whatsoever nature directly or indirectly caused by, contributed to by, resulting from, arising out of or in connection with any loss of use, reduction in functionality, repair, replacement, restoration or reproduction of any Data, including any amount pertaining to the value of such Data;*

regardless of any other cause or event contributing concurrently or in any other sequence thereto.

2 In the event any portion of this endorsement is found to be invalid or unenforceable, the remainder shall remain in full force and effect.

3 This endorsement supersedes and, if in conflict with any other wording in the Policy or any endorsement thereto having a bearing on Cyber Loss or Data, replaces that wording.

The International Underwriting Association of London also released two exclusions, an absolute and a limited cyber loss exclusion. The Cyber Loss Absolute Exclusion Clause, IUA 01-081, provides:

1. Notwithstanding any provision to the contrary within this contract, this contract excludes any Cyber Loss.

2. Cyber Loss means any loss, damage, liability, expense, fines or penalties or any other amount ***directly or indirectly caused*** *by:*

2.1 the use or operation of any Computer System or Computer Network;

2.2 the reduction in or loss of ability to use or operate any Computer System, Computer Network or Data;

2.3 access to, processing, transmission, storage or use of any Data;

2.4 inability to access, process, transmit, store or use any Data;

2.5 any threat of or any hoax relating to 2.1 to 2.4 above;

2.6 any error or omission or accident in respect of any Computer System, Computer Network or Data.

3. Computer System means any computer, hardware, software, application, process, code, programme, information technology, communications system or electronic device owned or operated by the Insured or any other party. This includes any similar system and any associated input, output or data storage device or system, networking equipment or back up facility.

4. Computer Network means a group of Computer Systems and other electronic devices or network facilities connected via a form of communications technology, including the internet, intranet and virtual private networks (VPN), allowing the networked computing devices to exchange Data.

5. Data means information used, accessed, processed, transmitted or stored by a Computer System.

6. When this clause forms part of a reinsurance contract, Insured shall be amended to read Original Insured. (bolding added)

IUA 09-082, the Cyber Loss Limited Exclusion Clause, is identical to the Absolute Exclusion Clause except that it does not contain the words "and indirectly" in Paragraph 2.

Individual insurers are also taking steps to address silent cyber exposures. Allianz and AIG, for example, announced initiatives to either affirmatively cover or exclude physical and non-physical cyber exposures across traditional policies. Over the past several years, the Insurance Services Office (ISO) also has issued cyber exclusions for various lines of traditional policies.

As the pace and severity of cyber risks continue to create wreak havoc for enterprises across every industry vertical, we can expect to see more insurers take steps to address related coverage concerns and channel those exposures to dedicated cyber policies