“The Internet of Buildings”: Insurance of Cyber Risks for Commercial Real Estate

Thomas D. Hunt

Follow this and additional works at: https://digitalcommons.law.ou.edu/olr

Recommended Citation

This Article is brought to you for free and open access by University of Oklahoma College of Law Digital Commons. It has been accepted for inclusion in Oklahoma Law Review by an authorized editor of University of Oklahoma College of Law Digital Commons. For more information, please contact darinfox@ou.edu.
“THE INTERNET OF BUILDINGS”: INSURANCE OF CYBER RISKS FOR COMMERCIAL REAL ESTATE

THOMAS D. HUNT

“I know I’ve made some very poor decisions recently, but I can give you my complete assurance that my work will be back to normal. I’ve still got the greatest enthusiasm and confidence in the mission.”

I. Introduction

The technological advances of the twenty-first century have led modern societies to reap previously unheard of advantages, including the now ubiquitous “Internet of Things” (IoT).

IoT refers to the connection of ordinary objects to the internet—e.g., smart phones, smart TVs, smart

* Thomas D. Hunt is a Risk Management Associate at Robert M. Currey & Associates. He is a member of the Massachusetts and Maine bars and a graduate of Suffolk University Law School (J.D., 2017, magna cum laude) and Boston University (B.A., 2013). For helpful discussions and edits, thank you to Tom Vincent II of the law firm GableGotwals as well as the entire staff of the Oklahoma Law Review.

1. 2001: A SPACE ODYSSEY (MGM 1968) (statement of a HAL 9000 computer, following its malfunction and murder of all but one of the crew of the spacecraft Discovery One, and immediately prior to being disconnected by the lone remaining mission pilot, Dave Bowman).


Most people are now familiar with the Internet of Things (IoT), the network of physical objects, embedded sensors, connections and computers that permeates much of our everyday life. Encompassing the mundane (smart refrigerators and toasters), the vital (medical devices), the amusing (smart toilets) and the creepy (tracking and shopping monitors), the IoT has become both a buzzword and a way of life.

Id. IoT has been defined as “the connection of systems and devices with primarily physical purposes (e.g., sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems.” U.S. DEP’T OF HOMELAND SEC., STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS 2 n.1 (2016), https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf.
buildings, and soon enough smart cities. In recent years, commercial real estate (CRE) owners, operators, builders, and developers have embraced IoT technology by gradually integrating artificial intelligence into the critical infrastructural components of buildings. This helps generate advances in data analytics, open up new revenue streams, and ensure long-term efficiency and sustainability.

Although these developments undoubtedly connote progress, it is almost axiomatic that whenever the internet and computers become more involved with any aspect of our lives, the possibility of a system failure or data breach increases correlatively. One prominent professor at Carnegie Mellon University and member of the Institute of Electrical and Electronics Engineers opined that “security and privacy are the biggest hurdles to overcome to realize” the reality of a “smart city.”


4. Totty, supra note 3 (discussing sensors being implemented in locations such as streetlights and water pipes).


6. See Andrew McGill, The Inevitability of Being Hacked, ATLANTIC (Oct. 28, 2016), https://www.theatlantic.com/technology/archive/2016/10/we-built-a-fake-web-toaster-and-it-was-hacked-in-an-hour/505571/ (demonstrating such risk through an experiment wherein a “smart toaster” suffered a first hack attempt within an hour of creation). This principle has massive implications for the commercial real estate sector, as experts predict 30.7 billion IoT devices will be installed in building bases by 2020. Mihalic, supra note 5.

7. Jimmy H. Koo, Views on Smart Cities and Indoor Localization from Bruno Sinopoli, Associate Professor, Carnegie Mellon University, BLOOMBERG LAW PRIVACY &
Some research and analysis has demonstrated that the risks of system failures and data breaches (hereinafter, collectively, “cyber events”) are especially large for the hotel and retail sectors. However, cyber events can affect all businesses, and especially where entire buildings are becoming computerized, no real estate asset is safe from a cyber attack. This article will argue that CRE stakeholders involved across all sectors must weigh the costs and benefits of purchasing cyber insurance as part of their larger risk management programs, and that the cyber carriers must accordingly tailor their products to better benefit CRE insureds. This article explores (1) the nature of cyber insurance; (2) the types of risks that CRE should consider when shopping for coverage; (3) whether such risks are adequately covered by other more “traditional” types of insurance; (4) a concrete example of a real estate cyber event and how these principles might apply in a real-world scenario; and ultimately, (5) how CRE stakeholders and their insurers should approach the cyber market going forward.

Professor Sinopoli elaborated:

Security is a difficult property to achieve as, unlike in computer networks, many devices will be deployed in the field with little physical protection and are bound to be tampered with. Several nodes of the network will be low-cost and simple, and therefore incapable of running layers of security that require more powerful and sophisticated devices. In addition, ICT will support the operation of physical systems, some of which may be safety-critical. Attacks, either of integrity or denial-of-service, can potentially lead to catastrophic consequences, even so far as loss of human life. One such example is connected vehicles—one can only imagine what could happen if an attacker can wirelessly take control of a number of cars on the road at the same time, as was recently demonstrated by the hackers Charlie Miller and Chris Valasek.

Id. (citation omitted).


9. See infra Section II.A, Part VI.
10. See infra Part II.
11. See infra Parts III, IV.
12. See infra Part V.
13. See infra Part VI.
14. See infra Part VII.
II. Rise of Cyber Insurance

A. Nature of the Risk

The list of recent cyber events in the news is nearly endless—they happen on an almost daily basis, such that it now almost seems banal. In 2017, one of the “Big Three” U.S. credit reporting firms suffered a data breach (allegedly resulting from a mistake by a single employee) that resulted in the exposure of 146 million Americans’ sensitive personal information.\(^\text{15}\) In 2014, the third largest U.S. retailer experienced one that saw 40 million credit and debit card records and 70 million other customer records stolen, leading to a reported $61 million in related losses to the company.\(^\text{16}\) That same year, malware wiped out and exposed for public review massive amounts of data from the corporate computers of one of Hollywood’s largest film studios in an attack that U.S. officials attribute to North Korea.\(^\text{17}\) The Federal Bureau of Investigation (FBI) has suggested that the very integrity of U.S. elections has been threatened and will continue to be threatened by cyber attacks from malevolent foreign actors.\(^\text{18}\) Reports estimate that cyber-crime costs the global economy over $400


billion per year, with one Munich Re subsidiary’s survey finding that almost one-third of U.S. businesses suffered a data breach in 2017 alone.

CRE, for its part, has historically avoided purchasing cyber insurance, but as smart buildings, cloud based computing, electronic wire transfers, and other “internetizing” phenomena have become more prevalent, CRE stakeholders no longer feel so immune from cyber risks, nor should they. In the past, CRE owners may have rested assured that much of the risk surrounding cyber events was borne with their tenants or property managers. Because the tenants and property managers were the entities actually operating whatever computer or digital technology existed at the premises, together with storing any related data, any liability arising

cost.


21. See Mihalic, supra note 5; Walter Andrews & Jennifer White, Real Estate Is Not Above the (Cyber Attack) Risk, COM. OBSERVER (Aug. 9, 2017, 3:58 PM), https://commercialobserver.com/2017/08/real-estate-is-not-above-the-cyber-attack-risk/ (noting that at least one-third of real estate firms have experienced a cybersecurity event in the last two years). As one director from the Real Estate Financial Advisory practice at Deloitte summarizes:

Industries like retail, travel and hospitality, and the financial services industries have long been dealing with cyberattacks, and have not only matured their response capability but also positioned cybersecurity as a core element of their businesses. In contrast, [CRE] . . . considers itself to be relatively less at risk from a potential cyberattack. This is because CRE firms typically maintain relatively less consumer personally identifiable information (PII) and valuable intellectual property (IP) directly on their own technology systems. However, due to the rise of smart buildings where tenants have building management systems on their smart phones, new opportunities for cyberattacks will emerge within the sector. The interconnectedness of real estate owners’ systems and tenant IT systems form a potential cyber risk for both parties. As a consequence to this heightened risk we predict IT and CRE will become more intertwined during the coming year to face these new cyber threats.

Donkers, supra note 5.
therefrom logically rested with them. Now, however, computers can be intertwined with the very shell or structure of the building itself, and while CRE owners frequently attempt to pass off all liability risks to others via triple-net leases, indemnity agreements, and other contractual remedies, the buck often stops with the landlord when it comes to insuring the shell of the building. This not only means that vast amounts of personal data may be incidentally or purposefully stored in CRE owners’ buildings, but also that critical, core components of the building itself are put at risk of system failure because a cyber event could disrupt the computers that operate them.

Moreover, much like all other businesses, the corporate offices for CRE companies tend to hold “tax records, federal identification numbers, social security numbers and other [sensitive private] information” in their computer systems. Their corporate teams frequently (1) conduct complex operations,

---

22. See Practical Law Real Estate, Cyber Security Insurance for Commercial Real Estate (May 5, 2016), Westlaw W-002-1978 [hereinafter Cyber Security Insurance for Commercial Real Estate]. Critical parts of modern building systems are remotely accessible through digital means, including closed-circuit TV; security systems; utilities; fire alarms; servers; voicemail; fax; and email. Id. In industrial real estate, expensive pieces of industrial hardware such as “switches, valves, pumps and other heavy machinery” are controlled by or with the assistance of computer technology. Cash, Doot & Blackburn, supra note 2.

23. See, e.g., Practical Law Real Estate, Office Lease Agreement (Multi-Tenant Net Lease) (Pro-Landlord Short Form) (2018), Westlaw W-005-8336 [hereinafter Office Lease Agreement]. This particular Westlaw form office lease includes the following pertinent language:

   (d) Landlord shall purchase and maintain: (i) a standard policy of “all-risk” insurance with customary exclusions covering the Building in the full replacement cost of the Building, together with rent loss insurance and windstorm coverage (on a full replacement cost basis); and (ii) broad form commercial general liability insurance with a minimum combined single limit of liability of at least [NUMBER IN WORDS] Dollars ($[NUMBER]), written by companies authorized to do business in the State of [STATE].

   Id.; see also Stephen Raptis & Donna Wilson, Bloomberg BNA/Manatt Webinar, Navigating the Evolving World of Cyber Insurance (2016) (on file with author) (“Indemnity agreements typically have limitations, and are only as good as the entity providing the indemnity.”); Matthew R. Slakoff, Commercial Insurance Update—Managing Real Property Exposures, Cavignac & Associates (Aug. 2007), http://www.cavignac.com/publications/publications-commercial-client-commercial-insurance-update/commercial-insurance-update-managing-real-property-exposures/ (“In most cases, landlords should buy their own insurance covering the leased property.”).

transactions by electronic means (e.g., completing closings through wire transfers), (2) utilize cloud servers, and (3) ask employees to use their own smartphones and tablets at work, all of which potentially expose massive amounts of personal and financial information to malicious actors. A CRE owner may purport to assign management of some of its data to a third party operator or property manager, but there still undeniably remains a massive amount of data that is in the care, custody, and control of the owner, whether it be connected to the underlying asset or on the corporate computers. Thus, it would be the owner’s insurance that would need to respond to cover any economic losses related to such data.


corporate information in their systems, such as pending transactions for public-traded companies that have not yet been disclosed.
B. Growth of Cyber Insurance

The earliest iterations of cyber insurance arrived on the market in the 1990s under the auspices of errors and omissions coverage, generally covering computer virus or malware-related events, with the first cyber policy being underwritten in 1997 by AIG agent Steve Haase. These early policies afforded coverage only for third-party lawsuits arising from data breaches caused by outsiders of the insured company. The problem was that, in reality, over fifty percent of these breaches were coming from disgruntled employees inside the company. As the internet has grown, so too has the coverage. The market for stand-alone cyber policies has seen an explosion over the last decade because cyber risks have become so difficult to ignore both for businesses and their insurance carriers.


28. Lauri Floresca, Cyber Insurance 101: The Basics of Cyber Coverage, WOODRUFF-SAWYER (June 19, 2014), https://woodruffsawyer.com/cyber-liability/cyber-basics/ (noting that in cyber insurance’s earliest days, the coverage was generally only purchased by technology companies).


30. Id.

31. Id.

32. Id.

2016, insurers collected $3.25 billion in cyber premiums, up from $2.75 billion in 2015 and $2.5 billion in 2014, with the market expected to triple by 2020 and quadruple by 2025.\(^\text{34}\) The relative novelty of cyber insurance presents both a challenge and an opportunity for risk managers and counsel because on the one hand, it is among the most negotiable (and thus the most malleable) types of coverage on the market, but on the other hand, it is among the most uncertain because of the dearth of court interpretations of cyber policy language and the lack of standardized forms.\(^\text{35}\)

The cyber risk insurance market has evolved significantly since it first emerged approximately two decades ago and is expected to continue experiencing rapid growth. A 2016 report on cyber insurance noted that 19 different categories of coverage are available to a greater or lesser extent in the cyber insurance market, including first and third party coverage related to data breaches, cyber extortion, business interruption, data and software loss, physical damage, and death and bodily injury.

\(\text{Id. (footnotes omitted).}\)


\(^{35}\) See Micah E. Skidmore, \textit{Negotiating Coverage & Pursuing Claims Under Cyber-Security & Privacy Insurance}, 14 J. TEX. INS. L. 27, 28 (2015) (noting lack of court guidance on meanings of wrongful acts, “incidents,” “events,” and “breaches” in cyber policies); see also Raptis & Wilson, \textit{supra} note 23. There have been only a few cases discussing the scope of cyber policies. See, e.g., P.F. Chang’s China Bistro, Inc. v. Fed Ins. Co., No. CV-15-01322-PHX-SMM, 2016 WL 3055111, at *8-9 (D. Ariz. May 31, 2016) (holding policy excluded coverage for fees required to be paid to credit card processor following breach); Travelers Prop. Cas. Co. v. Fed. Recovery Servs., Inc., 103 F. Supp. 3d 1297, 1302 (D. Utah 2015) (holding no errors and omissions coverage under cyber policy where third party complaint alleged knowledge, willfulness, and maliciousness); Columbia Cas. Co. v. Cottage Health Sys., 2:15–CV–03432, 2015 WL 4497730, at *1-2 (C.D. Cal. July 17, 2015) (wherein insurer argued that a “minimum required practices” exclusion and condition barred coverage, but no substantive ruling was made as it was dismissed to go to mediation per the policy language). The insurer’s complaint in \textit{Columbia Casualty} is especially troubling, as it asserted it had no obligation to fund any of a $4.125 million class action settlement resulting from a group of hospitals’ data breach, solely due to the fact that the insured did not follow some “Minimum Required Practices” set forth in its application for the insurance. Compl. ¶
C. Nature of Cyber Insurance

An adequate cyber insurance policy covers both an insured’s first-party losses and third-party losses. First-party coverage may include payment for lost income resulting from the breach; administrative safeguards; recovery of lost data; hiring of experienced professionals for investigative and responsive purposes; notification to affected parties (by mail and through call centers, etc.); and credit monitoring for affected parties, if applicable. Third-party coverage includes payment for regulatory defense, fines, and punitive damages; costs of litigation defense; and litigation damages. The policies often have separate definitions for the “trigger events” of these coverages—e.g., under JLT Asset Management Cyber Policy wording, a “System Event” (with respect to the first-party costs) as opposed to a “Privacy Breach Event” (with respect to the third-party costs). Under the JLT policy, “System Event” is defined as:

- any intrusion, modification, damage inability to access, service degradation, corruption, or failure of the Company’s Computer System due to:
  - (i) a denial of service attack, a malicious code, computer virus, or hacker attack
  - (ii) any negligence, or mistakes, in operating, maintaining or upgrading the Company’s Computer System
  - (iii) Programming errors or software bugs in fully operational and integrated programs or software
  - (iv) Malfunction or failure of the Company’s Computer System.


37. See generally RAND Study, supra note 27; see also CYBER SECURITY INSURANCE FOR COMMERCIAL REAL ESTATE, supra note 22; Ins. Servs. Office, Information Security Protection Endorsement Form, supra note 36.

38. See sources cited supra note 37.

39. See JLT Asset Management Cyber Policy, supra note 26, Definitions 34 and 39.

40. See id. at Definition 39.
“Privacy Breach Event” is then defined as:

the actual or alleged unauthorised disclosure, access, or transmission of:

(i) personally identifiable information (PII), including an individual’s name, address, telephone number, health information, or credit card, debit card, and bank account information

(ii) any Third Party’s trade secrets, data, designs, forecasts, formulas, practices, processes, records, reports, documents subject to legal privilege or other item of information that is not available to the general public for which the Company is responsible.\textsuperscript{41}

The JLT policy also covers “Cyber Extortion” (i.e., ransomware, discussed below) and “Digital Media Liability” (liability from alleged torts committed during the course of the insured’s website or social media operations) under still more separate definitions.\textsuperscript{42}

These distinct definitions can be critical. To take just one example, cyber policies typically assign “waiting periods” whereby the insurer will only provide coverage for any business interruption losses that occur after a certain number of hours, and the moment when that waiting period begins

\textsuperscript{41} \textit{See} JLT Asset Management Cyber Policy, \textit{supra} note 26, Definition 34; \textit{see also} Am. Int’l Grp., Security and Privacy Coverage Section, \textit{supra} note 26, Definition 2(l). The AIG policy defines “Privacy Event” as follows:

(1) any failure to protect Confidential Information (whether by "phishing," other social engineering technique or otherwise) including, without limitation, that which could result in an identity theft or other wrongful emulation of the identity of an individual or corporation;

(2) any failure to disclose an event referenced in Sub-paragraph (1) above in violation of any Security Breach Notice Law;

(3) any unintentional failure of an Insured to comply with those parts of a Company's privacy policy that (a) prohibit or restrict the disclosure or sale of Confidential Information by an Insured, or (b) require an Insured to allow an individual to access or correct Confidential Information about such individual; or

(4) any violation of a federal, state, foreign or local privacy statute alleged in connection with a Claim for a failure described in Sub-paragraphs (1) or (2) above.

\textit{Id.}

\textsuperscript{42} JLT Asset Management Cyber Policy, \textit{supra} note 26, Additional Coverage Sections C(1)-(2); \textit{see also} Am. Int’l Grp., Cyber Extortion Coverage Section, \textit{supra} note 26.
is determined by which “event” starts the clock. In the JLT example, the triggering event is a “System Event,” and thus the insured need only self-insure losses for ten hours after “any intrusion,” which presumably would mean the moment a phishing e-mail is sent, even if it is not opened until hours or even days later. If the triggering event were a “Privacy Breach Event,” however, the waiting period clock would start when “the actual or alleged unauthorised disclosure, access, or transmission” occurs, which could mean that the insurer might cover significantly less in the first party context, because many of the costs associated with a data breach arise almost simultaneously with the disclosure, access, or transmission. The JLT definition offers a favorable outcome in terms of counting up losses relative to the waiting period, but not so favorable in that only a “System Event” will actually trigger business interruption coverage, whereas Privacy Breach Events and Cyber Extortion events will not.

D. Negotiability of Cyber Insurance

Unlike traditional lines of insurance, cyber insurance is difficult to price because it is difficult for carriers to quantify the risks involved. Underwriters can predict, for example, by operating on some reasonable factual assumptions, which counties are more likely to suffer damage from a hurricane, but the scope and scale of the danger of cyber events is more difficult to pin down. Some data supports the assertion that hackers target

---

43. See JLT Asset Management Cyber Policy, supra note 26, Business Interruption and System Restoration A(1); Evolve MGA Cyber Policy, supra note 33, Insuring Clause 3, Section B; Am. Int’l Grp., Network Interruption Coverage Section, supra note 26, Section 1 (Insuring Agreement).

44. See JLT Asset Management Cyber Policy, supra note 26, Definition 39.

45. See id. at Definition 34; see also infra Section IV.A-B.

46. See sources cited supra note 43; see also infra Section III.B, Part VI.

47. PricewaterhouseCoopers, supra note 34, at 9. Underwriters struggle with the lack of historical data as well as the constantly changing nature of cyberattacks when pricing cyber insurance. Id.; see also RAND Study, supra note 27, at 23 (“In only a few cases were carriers confident in their own experience to develop pricing models.”). In response to this issue, insurers are lobbying government regulators to allow them access, at least on an anonymized basis, to any cyber-related data collected in enforcement actions. See William Shaw, GDPR’s Reporting Mandate May Fuel Fledgling Cyber Market, Law360 (Mar. 7, 2018, 9:58 PM GMT), https://www.law360.com/articles/1019400/gdpr-s-reporting-mandate-may-fuel-fledgling-cyber-market.

48. See Shaw, supra note 47. As Russ Johnston, CEO of QBE North America, summarized: “Most major cat exposures tend to have a season. To the extent you have sophisticated models, the market can expect events and project magnitudes. Cyber does not have a season and can cross multiple lines of business and customer segments.” Rebecca
smaller businesses because of their weaker cybersecurity measures, but other data suggests that it is larger companies that suffer much greater losses. Hackers may show no rhyme or reason as to which companies they target. The ransom amount cyber attackers request in a ransomware attack varies; the business interruption losses are unpredictable because one does not know how long systems will remain shut down, and the response by governmental authorities like the FBI is often inadequate as the hacker(s) frequently escape scot-free. All of these variables, on the one hand, make pricing of cyber insurance challenging, but on the other hand, they make it heavily negotiable. The market price can fluctuate massively depending on the robustness of the insured’s cybersecurity practices, the insured’s line of business, the amount of and types of coverages purchased, the amount of the deductible or retention, and whether the insurance is intended to sit primary or excess.


50. PricewaterhouseCoopers, supra note 34, at 8.

51. See Mihalic, supra note 5. For example, the perpetrators of the ransomware attack on Hollywood Presbyterian Medical Center were never found. Id. The email “spoofing” scam artists who tricked a company employee into wiring $4.8 million to a Chinese bank account in the underlying facts of Medidata Solutions Inc. v. Federal Insurance Co. were never found or even identified. See Jeff Sistrunk, Email Scam Not a Covered Fraud, Insurer Org. Tells 2nd Circ., LAW360 (Nov. 29, 2017, 9:49 PM EST), https://www.law360.com/articles/989344/email-scam-not-a-covered-fraud-insurer-org-tells-2nd-circ; see also discussion infra Section V.C. The U.S. federal government itself suffers from cyberattacks on a regular basis and thus surely cannot be counted upon to prevent or remedy cyberattacks on private companies or citizens. See Julie Hirschfeld Davis, Hacking of Government Computers Exposed 21.5 Million People, N.Y. TIMES (July 9, 2015), https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html (reporting on massive hacking of government computer systems leading to compromise of SSNs and other sensitive information); Michelle Price, U.S. SEC Says Hackers May Have Traded Using Stolen Insider Information, REUTERS (Sept. 21, 2017, 6:26 AM), https://www.reuters.com/article/legal-us-sec-intrusion/us-sec-says-hackers-may-have-traded-using-stolen-insider-information-idUSKCN1BW1K0 (discussing hacking of SEC’s “EDGAR” database and subsequent insider trading resulting therefrom).

52. See Siemens & Beck, supra note 27, at *10; Raptis & Wilson, supra note 23; L.D. Simmons II, A Buyer’s Guide to Cyber Insurance, MCGUIREWOODS LLP (Oct. 2, 2013),
III. First Party Cyber Risks

CRE stakeholders need to ensure that they have proper coverage for direct loss of assets resulting from a cyber event. This part of the Article discusses three of the most significant “first-party” concerns in the cyber arena from a CRE perspective and how typical cyber insurance policies respond: (1) loss of tangible property, money, or important data from system failures or cyberattacks; (2) business interruption from data breaches or cyberattacks; and (3) money paid out due to ransomware attacks.

A. Loss of Tangible Property, Money, or Important Data

Cyber attacks and system failures at smart buildings could lead to significant physical damage because the computer systems involved are interconnected with the utilities and basic functions of the buildings. They also can lead to the loss of or damage to important electronic data that is critical to the smooth operation of the company. This might include valuable customer account information, employee information, trade secrets or other intellectual property, or confidential internal correspondence, any of which might be stolen in a data breach. Additionally, malicious actors may seek to obtain money from the company by re-routing wire transfers or by conducting so-called “spoofing” schemes, or “social engineering,” where they pretend to be a person entitled to payment of funds via a convincing email, and a company employee obliges them by wiring funds to the account instructed. To the extent possible, CRE insureds should ensure that they have first-party coverage for property, dollars, and data that could be lost in a cyber event, including money paid out to scams, investigation of the hacking incidents, incident response, notification and credit monitoring of affected parties, and data and software restoration.

Unfortunately, most cyber policies will not cover physical damage to property or equipment resulting from a cyber event, which is one of the

https://www.mcguirewoods.com/Client-Resources/Alerts/2013/10/Buyers-Guide-to-Cyber-Insurance.aspx. Factors that can drive up the cost of coverage include whether the insured is involved in the healthcare or retail industries and whether the insured has a history of data breaches. Raptis & Wilson, supra note 23; see also RAND Study, supra note 27, at 23 (“[I]t was not unseen for carriers to examine their competitors in order to define rates.”).

53. See supra note 21 and accompanying text.
54. See id.
55. See O’Brien & Kejriwal, supra note 5.
most significant risks a smart building owner faces.⁵⁶ Many policies will also carve out or exclude coverage for lost value of intellectual property, which eliminates even more of the policies’ alleged value.⁵⁷ Additionally, as discussed in Part V, courts continue to wrestle with the issue of whether commercial crime insurance already covers email scammers who engage in “spoofing” or “social engineering” schemes.⁵⁸ Often the only novel coverage the cyber policy does provide on the first party side is the costs associated with lost electronic data and software restoration, e.g., “repairing, restoring, re-collecting or reconstructing any data or software applications hosted on the Company’s Computer System.”⁵⁹ Such costs are likely to be relatively insignificant when compared to the potential damage to physical and intellectual property, as well as loss of money, that may inflict CRE insureds. The CRE owner might be left wondering whether cyber coverage is worth purchasing at all.⁶₀

⁵₆. See RAND Study, supra note 27, at 14-15; Evolve MGA Cyber Policy, supra note 33, Exclusion 21 (excluding any payment “for any tangible property repair or replacement including the cost of repairing any hardware or replacing any tangible property or equipment”); id. at Exclusion 5; JLT Asset Management Cyber Policy, supra note 26, Exclusions 8, 14 (excluding “(i) any loss or destruction of tangible property other than Data” and “(ii) any repair or replacement of hardware or equipment which forms part of the Company’s Computer System”); Raptis & Wilson, supra note 23; Chubb Cyber Policy, supra note 33, Exclusion 6, (excluding, under property damage definition, losses related to “physical injury to, or loss or destruction of, tangible property, including the loss of use thereof whether or not it is damaged or destroyed”). The property damage exclusion should at least be negotiated to carve out damage to intangible property, i.e., electronic data, one of the very reasons the cyber policy is meant to exist in the first place. See, e.g., JLT Asset Management Cyber Policy, supra note 26, Exclusion 14(i) (excluding, inter alia, “any loss or destruction of tangible property, other than Data”).

⁵⁷. See Shawn Tuma & Katti Smith, Risky Business: Why Lawyers Need to Understand Cyber Insurance for Their Clients, 78 Tex. B.J. 854, 855 (2015); RAND Study, supra note 27, at 14-15; JLT Asset Management Cyber Policy, supra note 26, Exclusion 9; Chubb Cyber Policy, supra note 33, Exclusion 13. Given the amount of unique technology systems that can be in place in smart buildings due to the innovative designs by the engineers and IT professionals, this could be a significant issue. This gap in coverage is especially critical for engineers and architects who design smart buildings, as their intellectual property relating to this new technology is becoming increasingly valuable. See Mihalic, supra note 5. Similarly, and as a side note, CRE should ensure that any contracting architects and engineers carry errors and omissions coverage separately from cyber coverage to ensure that any defective designs in the smart buildings are insured.

⁵⁸. See Spoofing, INVESTOPEDIA, https://www.investopedia.com/terms/s/spoofing.asp (last visited Oct. 16, 2018); see also infra Section V.C.

⁵⁹. See JLT Asset Management Cyber Policy, supra note 26, Business Interruption and System Restoration A(3).

⁶₀. But see infra Section V.A (casting doubt on this notion).
B. Business Interruption

Business interruption is “a time-element coverage offered under first-party property policies” that covers the costs associated with a necessitated shutdown of business operations on the premises caused by a direct physical loss or specified cause of loss under the policy. CRE policyholders should be concerned about business interruption costs accompanying cyber events, including the lost rent and other revenue that might stem from a system failure, as well as the potential loss of customers, investors, tenants, reputation, and goodwill resulting from a data breach and resulting public concern. For example, in the smart building context, if a hacker breaks into a building’s electricity system (which is operated by a centralized computer) and turns it off for a month, the building owner might have trouble collecting rent from its tenants because of disruptions in their respective businesses. Furthermore, if highly publicized data breaches affecting commercial tenants at the property lead to a drop in business, it is conceivable that those tenants will become insolvent or otherwise incapable of continuing to pay rent.

Cyber insurance may cover the lost rental income and extra expenses associated with a cyber event. This coverage should include reputational harm and loss of future revenue (although how one can calculate such a number is another intriguing question altogether). Most policies will predicate business interruption coverage on there being a “System Event”
rather than a “Privacy Breach Event,” which can be a problem in and of itself.\textsuperscript{66} For example, if a hacker intrudes upon a building’s computer systems in order to gather massive amounts of personally identifiable information (PII) to sell, but does not deny any critical building services, then businesses may not actually cease operations.\textsuperscript{67} Still, when the PII is ultimately released or sold, bad publicity could cause the tenants’ revenues to suffer over time, which could ultimately lead to lost rental income to the landlord/owner.\textsuperscript{68} Policies that do not cover this risk ought to be avoided because this indirect loss in revenue is a significant concern for CRE owners whose financial salubriousness originates in no small part from that of their tenants.\textsuperscript{69} Thus it is critical that CRE insureds carefully read the business interruption language in all cyber policies available to them, as the decision on which policy to buy could come down to which language offers the broadest type of coverage and is most easily triggered.

\textbf{C. Ransomware Attacks}

Cyber events do not always happen in isolation—they may come with ransom messages, demanding payment of Bitcoin or payment by electronic wire transfer to an attacker’s bank account in exchange for a return to normalcy in computer systems or for neglecting to sell or reveal individuals’ PII on the dark web.\textsuperscript{70} These are generally referred to as

\\[\text{Published by University of Oklahoma College of Law Digital Commons, 2019}\]
“ransomware”\textsuperscript{71} or “Cyber Extortion”\textsuperscript{72} events. One disturbing example of a ransomware event in the real estate world occurred in February of 2016 at Hollywood Presbyterian Medical Center, where hackers turned off all hospital computer systems, including emergency systems, thereby inducing a panic and eventually a ransom payment by the hospital of $17,000 worth of Bitcoin.\textsuperscript{73} To curb the possible pitfalls of events like this, CRE insureds need first-party coverage not only for the property damage, data restoration, and business interruption costs associated with cyber events, but also for the dollars actually paid out to cyber criminals. This is one area where most cyber policies should theoretically provide coverage.\textsuperscript{74}

\begin{itemize}
\item \textsuperscript{71} The FBI defines “ransomware” as follows in their Internet Crime Complaint Center report:
\begin{itemize}
\item a form of malware targeting both human and technical weaknesses in an effort to deny the availability of critical data and/or systems. Ransomware is frequently delivered through various vectors, including phishing and Remote Desktop Protocol (RDP). RDP allows computers to connect to each other across a network. In one scenario, spear phishing emails are sent to end users resulting in the rapid encryption of sensitive files on a corporate network. When the victim organization determines they are no longer able to access their data, the cyber actor demands the payment of a ransom, typically in virtual currency such as Bitcoin. The actor will purportedly provide an avenue to the victim to regain access to their data. Recent iterations target specific organizations and their employees, making awareness and training a critical preventative measure. In 2016, the IC3 received 2,673 complaints identified as ransomware with losses of over $2.4 million.
\end{itemize}
\end{itemize}

\begin{itemize}
\item \textsuperscript{72} The FBI discusses “extortion” separately in the same Internet Crime Complaint Center report:
\begin{itemize}
\item Extortion is defined as an incident when a cyber criminal demands something of value from a victim by threatening physical or financial harm or the release of sensitive data. Extortion is often used in various schemes reported to the IC3, including Denial of Service attacks, hitman schemes, sextortion, Government impersonation schemes, loan schemes, and high-profile data breaches. Another tactic exploited in extortion schemes is the use of virtual currency as a payment mechanism. Virtual currency provides the cyber criminal an additional layer of anonymity when perpetrating these schemes. The IC3 continues to receive complaints regarding various extortion techniques. In 2016, the IC3 received 17,146 extortion-related complaints with adjusted losses of over $15 million.
\end{itemize}

\begin{itemize}
\item \textsuperscript{73} \textit{Id.} at 13; \textit{see also} JLT Asset Management Cyber Policy, \textit{supra} note 26, Additional Coverage Section C(2).
\item \textsuperscript{74} \textit{See} Mihalic, \textit{supra} note 5.
\item \textsuperscript{74} \textit{See supra} Section II.C (discussing cyber policy’s coverage of “cyber extortion”).
\end{itemize}
To add a further layer of complexity, however, several high-profile ransomware attacks have come from rogue foreign governments. Look no further than the infamous WannaCry ransomware that affected over 200,000 victims in 150 countries, which is widely attributed to the North Korean government. The sponsorship of such a rogue foreign actor, in and of itself, may create a gap in coverage because cyber liability policies often exclude not only war (an insurance policy staple), but also broader perils like “act[s] of foreign enemy, hostilities or warlike activities.” Such language could preclude coverage for events like North Korea’s sponsored cyberattack on Sony. Even if the insured successfully convinces the carrier that North Korea is not a “foreign enemy” or engaging in “hostilities” (a dubious premise), cyberwarfare could certainly be construed to be a “warlike activity.” Such language may provide the insurer a convenient excuse to deny coverage.

This reasoning for denial may be further bolstered by the commonly incorporated “Terrorism” exclusion, defined as including “the use of force or violence . . . whether acting alone, on behalf of or in connection with any


77. JLT Asset Management Cyber Policy, supra note 26, Exclusion 23; see also Evolve MGA Cyber Policy, supra note 33, Exclusion 28(a) (excluding losses arising directly or indirectly out of “war, invasion, acts of foreign enemies, hostilities or warlike operations (whether war is declared or not)”; Maynard, supra note 19, at 17; RAND Study, supra note 27, at 15 (noting “expenses for extortion or from an act of terrorism, war, or a military action [are] covered in rare cases, but mostly noted as exclusions” in cyber policies); Raptis & Wilson, supra note 23 (noting prevalence of these exclusions and thus absence of coverage for incidents similar to North Korea’s hacking of Sony).

78. See Cyber Attack Hits 200,000 in at Least 150 Countries: Europol, supra note 76; see also Volz, supra note 76.
organization(s), committed for political, religious, ideological purposes.”

The Terrorism exclusion paints with a fairly broad brush, and could also be argued to exclude ransomware attacks. Although ransomware attacks are not typically violent, there is always some effort to “force” payment of currency, and the insurance carrier could always argue that any living and breathing person has some kind of “ideological purpose.” Insurers could attempt to use both the War and the Terrorism exclusions, if they are worded broadly enough, to deny ransomware or “Cyber Extortion” coverage under certain circumstances.

IV. Third Party Cyber Risks

CRE stakeholders also need to carry adequate insurance coverage that obliges the insurer to defend against claims arising out of a data breach (whether an accidental breach by the insured or one by a hacker). This part discusses the different sorts of “third-party” concerns in the cyber arena from a CRE perspective and how typical cyber policies respond, namely: (1) contract and tort liability, (2) government enforcement actions, and (3) derivative/shareholder litigation.

A. Contract and Tort Liability

Cyber events can result in costly litigation in the form of class action lawsuits. Although it may be dubious whether the plaintiffs have suffered an injury-in-fact in data breach cases, courts remain divided on whether

79. JLT Asset Management Cyber Policy, supra note 26, Exclusion 21; see also Evolve MGA Cyber Policy, supra note 33, Exclusion 28(b) (excluding “any act or threat of force or violence . . . , whether acting alone or on behalf of or in connection with any organization or government, committed for political, religious, ideological or similar purposes”); RAND Study, supra note 27, at 15 (noting “expenses for extortion or from an act of terrorism, war, or a military action [are] covered in rare cases, but mostly noted as exclusions” in cyber policies); Raptis & Wilson, supra note 23.

such plaintiffs have standing to sue depending on the facts and circumstances.\textsuperscript{81} A release of PII can give rise to privacy-related litigation under a variety of legal theories such as invasion of privacy,\textsuperscript{82} breach of contract,\textsuperscript{83} plain vanilla negligence,\textsuperscript{84} and liability under state privacy statutes.\textsuperscript{85} These lawsuits pose a far greater danger to CRE in the age of smart buildings. The owner of the building may no longer be able to hide behind its contractual risk transfers to tenants because private data is being stored and transferred either in the shell of the building itself or on a network system indistinguishably connected to the owner.\textsuperscript{86} Similarly, even

\textsuperscript{81} See, e.g., \textit{Remijas}, 794 F.3d at 691-92 (analyzing customers' putative class action claims against Neiman Marcus following a cyber-attack in which the attackers obtained the plaintiffs' credit card information). The Seventh Circuit in this case reversed and remanded an Illinois district court ruling that the plaintiffs lacked standing, finding that “injuries associated with resolving fraudulent charges and protecting oneself against future identity theft” were sufficient to constitute injuries in fact for Article III standing purposes. \textit{Id.} at 696-97. This reversal ultimately led to a $1.6 million settlement in favor of the plaintiffs in 2017 after years of litigation. Suevon Lee, \textit{Neiman Marcus to Pay $1.6M in Shopper Data Breach Suit}, LAW360 (Mar. 17, 2017, 10:15 PM EDT), \url{https://www.law360.com/articles/903573/neiman-marcus-to-pay-1-6m-in-shopper-data-breach-suit}; see also \textit{In re Target Corp. Data Sec. Breach Litigation}, 66 F. Supp. 3d 1154 (D. Minn. 2014); Corona v. Sony Pictures Entm’t, Inc., No. 14-CV-09600 RGK (Ex), 2015 WL 3916744 (C.D. Cal. 2015) (plaintiffs survived motions to dismiss for lack of standing); \textit{Galaria v. Nationwide Mut. Ins. Co.}, 663 F. App’x 384 (6th Cir. 2016) (reversing and remanding an Ohio state court decision finding that plaintiffs’ increased risk of harm following a data breach at Nationwide and plaintiffs’ expenses to guard against such risks were insufficient to establish injuries in fact for standing purposes); \textit{Flores, LLC}, 2:17-CV-08503; \textit{Ruiz v. Gap, Inc.}, 540 F. Supp. 2d 1121, 1126 (N.D. Cal. 2008) (holding plaintiff had standing to sue based on an alleged increased risk of identity theft). But see \textit{Clapper} v. Amnesty Int’l USA, 133 S. Ct. 1138 (2013) (holding plaintiffs lacked standing to sue National Security Administration because they did not show the threat of interception of their personal communications to be “certainly impending to constitute injury in fact”); Beck v. McDonald, 848 F.3d 262, 274-76 (4th Cir. 2017) (holding precise opposite of \textit{Galaria} court); \textit{Santana v. Take-Two Interactive Software, Inc.}, 717 F. App’x 12, 17-18 (2d Cir. 2017) (affirming the Southern District of New York’s dismissal of Illinois Biometric Information Privacy Act class action for lack of standing).

\textsuperscript{82} See, e.g., \textit{Restatement (Second) of Torts} § 652B (Am. Law Inst. 1977) (discussing intrusion upon seclusion as invasion of privacy); \textit{id.} § 652D (discussing publicity given to private life as invasion of privacy).

\textsuperscript{83} See \textit{Remijas}, 794 F.3d at 690.

\textsuperscript{84} See \textit{id}.

\textsuperscript{85} See, e.g., \textit{Wis. Stat.} § 995.50 (2014).

\textsuperscript{86} See supra Section II.A; see also Mike Weston, “\textit{Smart Cities} Will Know Everything About You,” \textit{Wall St. J.} (July 12, 2015, 6:36 PM ET), \url{http://www.wsj.com/articles/smart-cities-will-know-everything-about-you-1436740596}. Journalist Mike Weston ominously prophesizes:
where the plaintiffs place blame solely on the tenants, those same tenants could then turn around and look to the owner for indemnification for any litigation costs and sue for negligent maintenance of the building’s computer systems.\textsuperscript{87}

While privacy tort liability defense is usually included in the limits of a market-competitive cyber policy, contractual liability arising out of data breaches generally is not.\textsuperscript{88} For example, the definition of “damages” in the sample JLT policy discussed in this Article excludes “costs or other amounts that the Insured is responsible for under a merchant services agreement, unless they are liable for such amounts in the absence of such agreement.”\textsuperscript{89} This definition would arguably include payments to credit card companies for failure to comply with terms of the credit card services agreement,\textsuperscript{90} which can be one of the most significant costs arising out of a

\begin{quote}
In a fully “smart” city, every movement an individual makes can be tracked. The data will reveal where she works, how she commutes, her shopping habits, places she visits, and her proximity to other people. . . . [T]his data will be centralized and easy to access. . . . Private companies could know more about people than they know about themselves.
\end{quote}

\textit{Id.} This increased interconnectedness exponentially increases the liability exposure for CRE.

\textsuperscript{87} See generally O’Brien & Kejriwal, \textit{supra} note 5.


Many policy forms in the marketplace directly exclude contractual indemnities and liability, including that which stems from merchant service agreements. Some policy forms initially grant coverage for breach of contract claims, but then add exclusions concerning key components of this coverage. In addition, some policy forms exclude breach of contract claims with some very narrow carvebacks to the exclusionary wording that may not help the insured much in the event of a payment card breach. Although most privacy/security insurance policies grant the insured coverage for situations in which they need to incur the first-party costs to notify individuals and extend insureds credit monitoring services, not all will directly respond to the breach of, or the indemnities contained in, a merchant services agreement.


\textsuperscript{89} JLT Asset Management Cyber Policy, \textit{supra} note 26, Definition 11.

data breach. Additionally, some cyber policies have exclusions or restrictions on payments for liability arising out of consumer protection statutes, which are a substantial source of privacy-related litigation across the United States.\textsuperscript{91} Accordingly, cyber policies may be helpful for responding to some civil lawsuits, but they generally leave much to be desired in the breadth of such coverage.

\textbf{B. Government Enforcement Actions}

Beyond pure traditional contract and tort liability, privacy liability has also increasingly taken the form of government enforcement actions. All fifty states, along with the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands, have enacted data breach notification laws requiring private entities to notify individuals of data breaches involving certain PII within a specified period of time.\textsuperscript{92} Some of these statutes allow

---

\textsuperscript{91} See, e.g., Evolve MGA Cyber Policy, supra note 33, Exclusions 2, 27; see also Raptis \& Wilson, supra note 23; RAND Study, supra note 27, at 15-16; infra note 98 and accompanying text.

injured persons to recover damages and attorney’s fees through a private right of action, while others authorize state administrative bodies to assess fines based on number of persons affected by the breach or based simply on the government’s discretion. In addition to state laws, the Federal Trade

---


93. See, e.g., ALASKA STAT. §§ 45.48.080(b), 45.50.471-45.50.531 (2016); CAL. CIV. CODE §§ 1798.29, 1798.80, 1798.82, 1798.84 (Deering Supp. 2018); D.C. CODE § 28-3853(a) (2013); HAW. REV. STAT. ANN. § 487N-3(b) (West 2008); 815 ILL. COMP. STAT. §§ 530/20, 505/10 (2016 & Supp. 2017); ILL. STAT. ANN. § 51/3075 (2013); MD. CODE ANN., COM. LAW §§ 13-408, 14-3508 (West Supp. 2017); NEV. REV. STAT. ANN. 603A.900 (2017); N.C. GEN. STAT. §§ 75-16, 16.1, 65(i) (2017); N.H. REV. STAT. ANN. § 359-C:21(f) (2009); N.J. STAT. ANN. 56:8-19 (West 2018); S.C. CODE ANN. §§ 1-11-490(G), 39-1-90(G) (2017); TENN. CODE ANN. §§ 47-18-2105(d), 47-18-2107(h) (2013 & Supp. 2017); VA. CODE ANN. §§ 18.2-186.6(1) (Supp. 2018); WASH. REV. CODE §§ 19.255.010(13)(a)-(c), 42.56.590(12)(a)-(c) (2016). For concerns about privately brought lawsuits brought against the insured, see supra Section IV.A.

94. See, e.g., MASS. GEN. LAWS. ch. 93A § 4, 93H § 6 (2013) (entitling attorney general to injunctive relief or $5,000 for each violation along with reasonable costs and attorney’s fees); N.Y. GEN. BUS. LAW § 899-aa (LexisNexis Supp. 2018) (entitling court to impose up to the greater of $5000 or $10 per failed notification [not to exceed $150,000] in fines where knowledge or recklessness is found). See generally supra note 92 and accompanying text.

95. Included among state privacy laws are the notice statutes, discussed supra note 92, as well as other privacy regulations outside the scope of this article, like the New York
Commission (FTC) has authority to enforce the identity theft and privacy requirements of the Gramm Leach Bliley Act (GLBA)\(^96\) and the Fair Credit Reporting Act (FCRA),\(^97\) as well as those found to be implicit in the prohibitions on unfairness and deception in the Federal Trade Commission Act (FTCA).\(^98\) Where healthcare information is involved, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act also come into play.\(^99\)

Furthermore, public outcry after breaches like Equifax’s has instigated renewed interest in cyber risk from regulators, meaning that still more enforcement might loom on the horizon.\(^100\) Members of Congress have repeatedly remarked upon the importance of addressing cyber risks in committee hearings.\(^101\) Recent activity and rumors suggest that the

---


\(^{97}\) Id. §§ 1681-1681x.

\(^{98}\) Id. §§ 41-58. The Act allows the FTC to investigate and pursue actions against an organization whose activity qualifies as a practice that “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.” Id. § 45(n).


\(^{101}\) Rep. Joe Barton (R-TX), for example, called on Congress to “put some teeth” into cybersecurity enforcement by creating federal statutory data breach penalties. Bernard & Cowley, supra note 15. At a congressional hearing on the Equifax breach, Barton lamented,
Consumer Financial Protection Bureau (CFPB) may begin to enforce privacy standards against financial firms as part of its broad statutory authority. Perhaps most significantly, the European Union (EU) recently rolled out its much-anticipated General Data Protection Regulation (GDPR), which threatens CRE insureds with properties in EU countries with incredibly stringent and harsh penalties for data breaches. Despite


103. See Council Regulation 2016/679, 2016 O.J.(L 119) 1 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [hereinafter GDPR]. The GDPR took effect on May 25, 2018. Id. art. 51(4), at 65. Noncompliance with the GDPR can result in fines of up to four percent of a company’s global revenue or €20 million, whichever is greater. Id. art. 83(5); see also Mitzi Hill, GDPR: Good Defense = Prepared + Responsive!, TAYLOR ENGLISH DUMA LLP (Sept. 26, 2017), https://www.taylorenglish.com/blogs-emerging-markets,gdpr-good-defense-prepared-responsive. Disturbingly, it is mostly unknown whether GDPR fines could actually be covered by insurance, as coverage may depend on whether local regulators or courts deem that such fines are
the occurrence of Brexit in 2016, the Data Protection Act in the United Kingdom may be enforced with similar rigor.\(^{104}\)

CRE insureds must confirm that costs related to compliance with these statutes and any subsequent enforcement thereof are covered under their policies. Fortunately, many cyber policies currently offer coverage for the regulatory investigations and fines, fees, and penalties associated with the above,\(^{105}\) where standard commercial general liability policies fall short.\(^{106}\)

**C. Derivative and Shareholder Litigation**

In the case of publicly traded REITs or any publicly traded companies with real estate, the disclosure of customer or tenant information, valuable trade secrets, or other sensitive commercial information that leads to a drop in the company’s stock price could spawn fiduciary or shareholder derivative litigation\(^{107}\) or securities class actions\(^{108}\) against the company and


105. Evolve MGA Cyber Policy, *supra* note 33, Insuring Clause 1, Section B. Note, however, that costs related to *industry-wide* regulatory investigations are excluded under the JLT policy. See JLT Asset Management Cyber Policy, *supra* note 26, Exclusion 18 (excluding “any industry-wide, non-firm specific, inquiry or action by any governmental, regulatory or statutory body”). Small wrinkles such as this underscore the omnipresent importance of reading each specific policy word by word.

106. *See discussion infra* Section V.B.


108. *See generally* Complaint, Yuan v. Facebook, Inc., No. 3:18-cv-01725, 2018 WL 1400036 (N.D. Cal. Mar. 20, 2018). Guidance from the SEC Division of Corporation Finance warns that compliance with existing disclosure requirements under the securities laws (e.g., Exchange Act Rules 12b-20, 14a-9 and 10b-5) may require disclosure of:

1) Risk factors relating to a potential cyber incident, including known or threatened attacks;

2) Costs or other consequences associated with known cyber incidents or the risk of potential incidents, where the costs of such incidents individually or
its individual directors and officers. Although the intent of cyber insurance is generally to provide coverage on behalf of the company and not individuals, some policy forms include directors and officers under the definition of “insured persons”—but troublingly, many cyber policies often exclude securities claims altogether.109 Depending on the policy language, many directors’ and officers’ (“D&O”) liability policy forms could provide defense and indemnity regardless of whether the claims against the directors and officers arise out of a cyber event.110

V. Traditional Insurance Solutions

There are five types of policies that could conceivably provide coverage for some of the risks discussed here: property, commercial general liability, crime, terrorism, and D&O. This part will discuss the possible cyber coverages (or lack thereof) provided by all five.

A. All-Risk Property Insurance

A layperson might believe that property insurance should cover direct losses resulting from system failures (e.g., loss of tangible property and data, and related business interruption costs).111 All-risk (also called “special form”) property policies offer insureds coverage for physical

collectively represent a material event, through disclosure in the Management Discussion and Analysis section of the registrant's annual report;

3) Cyber incidents that materially affect a registrant’s products, services, or relationships with customers and suppliers;

4) Material legal proceedings involving cyber incidents; and

5) Any material impact of cyber security, both pre- and post-incident, on the registrant’s financial statements.


110. See discussion infra Section V.E.

111. See supra Section IV.A (describing nature of first party cyber risks).
damage to their property and, if purchased, related business interruption costs. Yet these policies generally do not provide coverage for loss of electronic data, and moreover, they usually contain cyber exclusions specifically precluding coverage for any losses arising from, inter alia, system failures, corruption of data, and loss of use of any computer. Historically, property insurance responded to costs relating to a computer virus infecting a business’ network. But beginning in 2002, insurance carriers began adding exclusionary language like the NMA 2914 endorsement to their policies, which makes their intent to exclude such events from coverage relatively clear:

This Policy does not insure loss, damage, destruction, distortion, erasure, corruption or alteration of ELECTRONIC DATA from any cause whatsoever (including but not limited to COMPUTER VIRUS) or loss of use, reduction in functionality, cost, expense of whatsoever nature resulting therefrom, regardless of any other cause or event contributing concurrently or in any other sequence to the loss.


113. See PR 9514 (on file with author). This endorsement states that the insurer will not pay for Damage or Consequential Loss directly or indirectly caused by, consisting of, or arising from:

1. Any functioning or malfunctioning of the internet or similar facility, or of any intranet or private network or similar facility,
2. Any corruption, destruction, distortion, erasure or other loss or damage to data, software, or any kind of programming or instruction set,
3. Loss of use or functionality whether partial or entire of data, coding, program, software, any computer or computer system or other device dependent upon any microchip or embedded logic, and any ensuing liability or failure of the Insured to conduct business.

Id.; see also Ins. Servs. Office, Inc., Form No. CP 01 70 (standard endorsement introduced to exclude electronic data from ISO standard Building and Personal Property coverage form).


115. See NMA 2914A Electronic Data Endorsement C (2015) (endorsement created by London’s Non-Marine Association) (on file with author) (emphasis added); see also NMA
This language signifies a straightforward elimination of coverage for first-party electronic data losses that could be covered under a property policy. Some property policies can be endorsed to provide limited coverage for first-party losses resulting from cyber events. In most cases, however, a data intrusion would likely neither constitute a direct physical loss nor a covered cause of loss, thereby making the possibility of business interruption coverage for cyber events on a property policy very slim.

2915A Electronic Data Endorsement D (2015) (on file with author) (excluding “loss, damage, destruction, distortion, erasure, corruption or alteration of [electronic data],” and any “loss of use, reduction in functionality, cost, expense of whatsoever nature resulting” from that loss of data); NMA 2912 (on file with author) (excluding losses arising out of the “(i) loss of, alteration of, or damage to, or (ii) a reduction in the functionality, availability or operation of” computer systems, hardware, programs, software, data information repository, microchip, integrated circuit or similar devices in computer equipment or non-computer equipment); NMA 2928 (on file with author); CL 380 (on file with author) (excluding all loss, damage and liability directly or indirectly caused by, contributed to by, or arising from, the use or operation “as a means for inflicting harm” of any computer, computer system, computer software program, malicious code, computer virus or process or any other electronic system); Michael Rossi, The End of Computer Virus Coverage as We Know It?, INT’L RISK MGMT. INST., INC. (May 2002), https://www.irmi.com/articles/expert-commentary/the-end-of-computer-virus-coverage-as-we-know-it/.

116. See Computer Systems Damage, Zurich EDGE-100-B (2010) (on file with author). This Zurich policy form states:

The Company will pay for direct physical loss of or damage to the Insured's Electronic Data, Programs, Software and the actual Time Element loss sustained, as provided by this Policy, during the Period of Interruption directly resulting from mysterious disappearance of code, any failure, malfunction, deficiency, deletion, fault, Computer Virus or corruption to the Insured's Electronic Data, Programs, Software at an Insured Location. The Company will also pay for such loss or damage that may arise out of or result from any unauthorized access in, of, or to any computer, communication system, file server, networking equipment, computer system, computer hardware, data processing equipment, computer memory, microchip, microprocessor, integrated circuit or similar device.

This Coverage will only apply when the Period of Interruption exceeds the time shown as Qualifying Period in the Qualifying Period clause of the Declarations section. If the Qualifying Period is exceeded, then this Policy will pay for the amount of loss in excess of the Policy Deductible, but not more than the limit applying to this Coverage.

Id. Note, however, that this coverage is typically subject to a low sublimit (e.g., $1,000,000) as well as a “Qualifying Period” whereby the insured self-insures for a specified period of time until the coverage kicks in (e.g., forty-eight hours). See id.

With respect to data restoration or system recovery costs, even if the endorsements excluding electronic data can be successfully removed during negotiations, the associated premium increase would likely be cost-prohibitive. Further, policy forms’ exclusion of “electronic data” from the definition of covered property would still render potential coverage for cyber risks an unsettling question mark at best. Given all these difficulties, an all-risk property policy is likely not a good place to turn for any meaningful cyber coverage.

Cyber policies, as discussed above, generally do cover the restoration of any lost or corrupted data accompanying a cyber event, as well as some business interruption costs related thereto. Given that business interruption is one of the most critical and necessary aspects of cyber coverage for CRE insureds, this represents one of the reasons cyber policies could be a worthwhile purchase. On the other hand, many cyber policies exclude or attempt to sublimit reimbursement for reputational harm, loss of future revenue, and tangible property damage arising out of cyber events. Given the interconnectedness of the infrastructure of a smart building with the computer system and data therein, CRE insureds should want coverage for those risks in particular. CRE insureds must carefully inspect their policy language in order to determine whether the stand-alone cyber policy offers any meaningful value or protection at all over the standard “all-risk” property policy.

B. Commercial General Liability Insurance

The commercial general liability (CGL) policy may be another place to turn for coverage of cyber risks. CGL policies pay, under “Coverage A,” for sums that an insured becomes legally obligated to pay due to an occurrence that results in property damage or bodily injury, with property damage being defined as “[p]hysical injury to tangible property, including all resulting loss of use of that property.” Most CGL forms now state that

---

118. See supra Section III.A, III.B.
119. See supra note 115 and accompanying text.
120. See supra Section III.B; 2 STUART A. PANENSKY, DATA SECURITY & PRIVACY LAW § 14:6, Westlaw (database updated June 2018) (noting the gap in available coverage for physical property damage caused by a data breach).
121. See supra note 21 and accompanying text.
“electronic data is not tangible property,” and explicitly exclude “Damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.” While courts have accordingly been reluctant to categorize electronically stored data as “tangible property” for purposes of triggering a CGL policy,

effectively eliminating the “Computer Fraud” coverage which in preceding years was an additional coverage that could be purchased and endorsed to the CGL form. See Virginia N. Roddy, Expanding Risks, Growing Market: Cyber Insurance Today, DRI For Def., Oct. 2017, at 80. Computer Fraud coverage is still available in the market, but only on commercial crime policies. See infra Section V.C.


124. See, e.g., Ins. Servs. Office, 2012 Commercial General Liability Coverage Form, supra note 124, Exclusion (p). This policy form excludes:

- Damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data. However, this exclusion does not apply to liability for damages because of “bodily injury”. As used in this exclusion, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CDROMs, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.


insureds have occasionally found an effective way around this by arguing that because computer hardware is clearly tangible property, any lawsuits relating to losses anent physical components of the computers themselves must be covered under Coverage A.\textsuperscript{126} Therefore, if a real estate cyber attack physically damages a building’s computer systems, any lawsuits deriving therefrom could trigger the insurer’s duty to defend on a CGL policy. Nevertheless, it likely would be a grave mistake to rely on this loophole for all cyber liability coverage, given that (1) the insurer likely will fight on this point, and (2) much of the liability risk stems from privacy lawsuits rather than tangible property damage.\textsuperscript{127}

CGL policies also insure “personal and advertising injury” resulting from offenses such as violation of the right to privacy under Coverage B.\textsuperscript{128} Included within this scope of coverage is liability arising out of an “[o]ral or written publication, in any manner, of material that violates a person’s right of privacy.”\textsuperscript{129} Some courts have suggested or held that a disclosure of PII resulting from a data breach constitutes a “publication” and, consequently, that CGL carriers owe a duty to defend and potentially indemnify from lawsuits arising out of such disclosure.\textsuperscript{130} Unfortunately, stored computer data is not “direct physical loss”); Warner v. Fire Ins. Exch., 281 Cal. Rptr. 635 (Cal. Ct. App. 1991) (using the same analysis as America Online).

126. \textit{See, e.g.}, Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797, 802 (8th Cir. 2010) (holding that “[t]he plain meaning of tangible property includes computers, and the Sefton complaint alleges repeatedly the ‘loss of use’ of his computer” and “conclud[ing] . . . the allegations are within the scope of the General Liability policy,” despite the policy’s exclusion of electronic data from the definition of “tangible property”); Centillium Commc’ns v. Atl. Mut. Ins. Co., 528 F. Supp. 2d 940, 948-49 (N.D. Cal. 2007) (applying California law and holding that allegations that semiconductor chips physically injured other components of routers triggered insurer’s duty to defend); State Auto Prop. & Cas. Ins. Co. v. Midwest Computs. & More, 147 F. Supp. 2d 1113, 1116 (W.D. Okla. 2001) (“Because a computer clearly is tangible property, an alleged loss of use of computers constitutes ‘property damage’ within the meaning of plaintiff's policy.”); Retail Sys., Inc. v. CNA Ins. Cos., 469 N.W.2d 735, 737 (Minn. Ct. App. 1991) (holding data on computer tape containing results of a political survey constituted tangible property because “[t]he data on the tape was of permanent value and was integrated completely with the physical property of the tape.”).

127. \textit{See supra} Section IV.A and accompanying text.


129. \textit{Id.} at Definition (14)(e) (emphasis added).

130. Travelers Indem. Co. of Am. v. Portal Healthcare Sols., LLC, 644 F. App’x 245, 247-48 (4th Cir. 2016) (holding that data breach constituted “publication” under CGL personal and advertising coverage); \textit{see also} Am. States Ins. Co. v. Capital Assocys. of Jackson Cty., 392 F.3d 939, 941 (7th Cir. 2004) (stating in dicta that “[t]he language reads

Published by University of Oklahoma College of Law Digital Commons, 2019
widely circulated endorsements first introduced in 2014 now exclude liability arising out of “Access Or Disclosure Of Confidential Or Personal Information” from both Coverages A and B. Although there is not a substantial amount of case law interpreting these endorsements, it seems clear that the intent is to negate coverage for invasion-of-privacy lawsuits as part of a renewed effort to force insureds to purchase a separate cyber insurance product. Followers of the insurance industry understand that whenever there is increased regulatory scrutiny for an exposure (as with cyber), insurers look to exclude and segregate the risk from the broadly worded general like coverage of the tort of ‘invasion of privacy,’” and “[p]erhaps the language reasonably could be understood to cover improper disclosures of Social Security numbers, credit records, email addresses, and other details that could facilitate identity theft or spamming”); Hartford Cas. Ins. Co. v. Corcino & Assocs., No. CV 13–3728 GAF (Jx), 2013 WL 5687527, at *3 (C.D. Cal. Oct. 7, 2013) (endorsing, tacitly, Hartford’s choice not to dispute that accidental posting of confidential information on website was “publication”); Tamm v. Hartford Fire Ins. Co., No. 020541BLS2, 2003 WL 21960374, at *4 (Mass. Super. Ct. July 10, 2003) (holding that revealing private correspondence of the insured and its executives via email to outside attorneys constituted “publication” under Coverage B). But see Innovak Int'l, Inc. v. Hanover Ins. Co., 280 F. Supp. 3d 1340, 1349 (M.D. Fla. 2017) (holding that because third party hackers and not the insured caused the data breach, coverage was barred because lawsuit did not arise out of the insured’s oral or written publication); Recall Total Info. Mgmt. v. Fed. Ins. Co., 115 A.3d 458, 460 (Conn. 2015). In Recall Total, Connecticut’s highest court found that coverage was barred where computer tapes fell out of the insured’s transportation contractor’s van and were subsequently stolen. 115 A.3d 458 at 459-60. This case presented a unique set of facts because there was no computer hack, but rather a loss of physical tapes, and also no evidence existed that anyone ever accessed the confidential information on the stolen tapes. Id. at 459.


133. See infra note 135 and accompanying text; see also Big 5 Sporting Goods Corp. v. Zurich Am. Ins. Co., 635 F. App’x 351 (9th Cir. 2015) (holding CGL insurer had no duty to defend lawsuit against insured brought under Song–Beverly Act of 1991 because all underlying claims arose from the “alleged violation of the statutory right to privacy,” which was excluded under the CGL policy).

134. See supra Section IV.B.
liability policy in order to force policyholders to pay additional premium for a separate policy to insure the risk.\footnote{135}

CRE stakeholders can attempt to negotiate the re-inclusion of electronic data in the definition of “tangible property” with brokers and carriers via endorsement.\footnote{136} It is uncertain how willing carriers are to remove the “Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability” exclusions from Coverage B, and even if they are willing, the premium might be cost-prohibitive. Further, even if such exclusions are left off of policies at a reasonable price, there remains some

---

\footnote{135}{We know this to be true because the insurance industry has publicly acknowledged the fact. \textit{See} Bole, supra note 48 (noting that uncomfortable insurers will “take a ‘hard look’ at where cyber cover could appear in [other non-cyber] policies”); Jeffrey P. Klenk, \textit{Emerging Coverage Issues In Employment Practices Liability Insurance: The Industry Perspective On Recent Developments}, 21 W. NEW ENG. L. REV. 323 (1999) (explaining dawn of employment practices exclusion on CGL policy and subsequent policy segregation resulted from, \textit{inter alia}, the Civil Rights Act of 1991); E. Joshua Rosenkranz, \textit{The Pollution Exclusion Clause Through The Looking Glass}, 74 GEO. L.J. 1237 (1986) (explaining dawn of pollution exclusion on CGL policy and subsequent policy segregation resulted from, \textit{inter alia}, the RCRA, CERCLA, and other new statutory schemes). Bob O’Leary, president and CEO of Philadelphia Insurance Companies even openly predicted and admitted that underwriters of traditional lines of insurance will ramp up their exclusionary language as it relates to cyber, stating that “[s]ilent cyber cover will be closed down across the industry via exclusionary language . . . \textit{We did this with pollution cover and saw a quicker take-up rate of standalone pollution cover as a result.”} Bole, supra note 48 (emphasis added). This is one of the economic realities of the insurance industry that on the one hand cannot be overstated, but that on the other hand lawyers and academics still struggle to accept as it relates to cyber coverage. \textit{See}, e.g., Erik S. Knutsen, & Jeffrey W. Stempel, \textit{The Techno-Neutrality Solution To Navigating Insurance Coverage For Cyber Losses}, 122 PENN ST. L. REV. 645 (2018) (arguing that insurance industry should fold cyber coverage into already-existing traditional coverages such as CGL and property). Countless academic writings on cyber insurance simply emphasize possible existing cyber coverages on traditional policies rather than acknowledging the reality that soon all such coverage will be excluded. \textit{See} Seaman & Schulze, supra note 131; Larry Bowman, Kenneth Johnston, Dan Klein & Shae Keefe, \textit{Data Breach: The Aftermath – Insurance Coverage Under CGL Policies for Cyber Security Breaches, Hacks, and Malware Attacks}, KANE RUSSELL COLEMAN LOGAN PC (Oct. 18, 2016), \url{https://www.krcl.com/articles/litigation-update/data-breach-aftermath-insurance-coverage-cgl-policies-cyber-security-breaches-hacks-malware-attacks/}; James H. Kallianis, Jr., \textit{Read The Fine Print – Insurance Coverage Issues Implicated in Data-Breach Claims}, DRI FOR DEF., Mar. 2015, at 56.}

\footnote{136}{Published by University of Oklahoma College of Law Digital Commons, 2019}
question s as to (1) whether a cyber event resulting from intentional conduct would qualify as an accident or an occurrence to trigger the CGL policy;\(^{137}\) and (2) whether a CGL policy would cover a publication initiated by a third party (i.e., a hacker) rather than the insured itself.\(^{138}\) Accordingly, in terms of mitigating third-party liability risk, the cyber policy will likely be a necessary avenue of defense for all contract and tort lawsuits and government enforcement actions arising out of cyber events for CRE, except in circumstances where the insured successfully argues that the lawsuit arises out of “physical damage” to “tangible property.” Even then, the cyber policy must be carefully reviewed for coverage gaps, because bodily injury and property damage are often excluded with critically worded carvebacks, leaving an opening for insurance carriers to argue that claims like allegations of emotional distress are excluded as a type of “bodily injury.”\(^{139}\)


\(^{139}\) See Chubb Cyber Policy, supra note 33, Exclusion III(A)(5) (excluding bodily injury except in the case of the liability coverage part with respect to “mental injury, mental anguish, mental tension, emotional distress, pain and suffering, or shock resulting from an Incident”); Evolve MGA Cyber Policy, supra note 33, Exclusion 5 (excluding bodily injury and property damage altogether with no carveback). The bodily injury carveback (or lack thereof) can be critical because a carrier could use a plaintiff’s assertion of emotional distress (together with whatever other privacy claims they are bringing) as an excuse to deny defense or deny coverage. Even the risk of death and more physical bodily injury should not be disregarded when it comes to cyber insurance. See, e.g., Nicole Perlroth & Clifford Krauss, A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try, N.Y. Times (Mar. 15, 2018), https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html (discussing how attempted hacking of a petrochemical manufacturer appears to have sought “to sabotage the firm’s operations and trigger an explosion”).
C. Commercial Crime Insurance

Commercial crime insurance\textsuperscript{140} may be purchased on a stand-alone basis or as part of a CRE insured’s package policy.\textsuperscript{141} The policy typically provides coverage for “Computer Fraud,” which is usually defined as:

\[
\text{[L]oss of or damage to “money,” “securities” and “other property” resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the “premises” or “banking premises:” (a) To a person (other than a “messenger”) outside those “premises;” or (b) To a place outside those “premises.”}^142
\]

Crime policies typically also cover “Funds Transfer Fraud,” often stating something to the effect of: “We will pay for the loss of ‘funds’ resulting directly from a ‘fraudulent instruction’ directing a financial institution to transfer, pay or deliver ‘funds’ from your ‘transfer account.’”\textsuperscript{143}

Under New York law, these two provisions cover dollars lost to “social engineering” or “spoofing” schemes.\textsuperscript{144} In Medidata Solutions v. Federal Insurance Co.,\textsuperscript{145} a New York federal judge held that Chubb subsidiary Federal Insurance Co. had to pay the money that an employee in the accounts-payable department of Medidata paid to a malicious party that had posed as the company president via email, despite Federal’s argument that coverage was negated by the fact that the transfer of money was done by an employee with authorization to transfer the funds and that there was no “entry or change of data to Medidata’s computer system.”\textsuperscript{146} Federal


\textsuperscript{143}. \textit{Id.} at Section 7.


\textsuperscript{145}. \textit{Id.}

\textsuperscript{146}. \textit{Id.} at 476-80. On appeal, an insurance trade group filed an amicus brief siding with Federal, arguing from a prudential perspective that “[i]f ‘computer fraud’ insurance is construed so overbroadly to cover losses resulting from e-mails that fool the insured’s employees, who do not take commercially reasonable steps to confirm the substance of the e-mails, such insurance will become much harder to obtain and substantially more expensive.” Brief for the Sur. & Fid. Ass’n of Am. as Amicus Curiae Supporting Appellant...
appealed the judgment to the Second Circuit, who subsequently affirmed the lower court’s decision. A few unpublished opinions by the Fifth and Ninth Circuits align more with the insurer’s argument that because victims of these schemes instruct their own bank to transfer the funds via an agent with “authorization,” there cannot have been any computer fraud or funds-transfer fraud under the above definitions because the loss did not “result directly” from a fraudulent instruction using a computer. Other courts tend to agree more with Judge Carter’s reasoning in Medidata.

The Second Circuit’s decision is incredibly significant in the context of this Article because of the vast number of CRE companies based in New York and insurers based in Connecticut, two Second Circuit jurisdictions.

at *14, Medidata Sols., Inc. v. Fed. Ins. Co., 729 F. App’x 117 (2nd Cir. 2018). Of course, an interest group’s vague cautionary threat that a certain ruling might make coverage more expensive has no bearing on what the law dictates a result to be.

148. See Taylor & Lieberman v. Fed. Ins. Co., 681 F. App’x 627 (9th Cir. 2017); Apache Corp. v. Great Am. Ins. Co., 662 F. App’x 252 (5th Cir. 2016); Posco Daewoo Am. Corp. v. Allnex USA, Inc., No. CV 17-483, 2017 WL 4922014 (D.N.J. Oct. 31, 2017); Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., No. 16-12108, 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017), rev’d, 895 F.3d 455 (6th Cir. 2018); Brick Warehouse LP v. Chubb Ins. Co. of Can., 2017 ABQB 413 (Can.). Posco Daewoo is a somewhat distinct case because it involved a “reverse” social engineering scheme, wherein the intended payee of the funds, not the payor, asserted a claim under its own crime policy for recovery of funds that a malicious actor had tricked the payor into paying out. 2017 WL 4922014, at *1-2. The court then understandably held that because the claimant had no actual property interest in the money (at least, not yet), they then had no good claim under the crime policy. Id. at *6-7. Therefore, the Posco Daewoo holding does not necessarily portend New Jersey courts’ or the Third Circuit Court of Appeals’ alignment with the view of the Fifth Circuit and the Michigan court.


In the meantime, the rest of the country should follow Judge Carter’s lead, as the divergent contemporaneous case law simply defies reason. The court in Apache Corporation v. Great American Insurance Co., for example, based on similar facts as Medidata, used the following pretzel logic to justify its ruling that the loss did not “result directly” from computer fraud:

The email was part of the scheme; but, the email was merely incidental to the occurrence of the authorized transfer of money. To interpret the computer-fraud provision as reaching any fraudulent scheme in which an email communication was part of the process would . . . convert the computer-fraud provision to one for general fraud.151

As Judge Story of the Northern District of Georgia pointed out in Principle Solutions Group LLC v. Ironshore Indemnity Inc., “If some employee interaction between the fraud and the loss [i]s sufficient to allow [the insurer] to be relieved from paying under the provision at issue, the provision would be rendered ‘almost pointless’ and would result in illusory coverage.”152 This conclusion is correct because the nature of fraud is that a misrepresentation by a malicious party induces action by an innocent party (i.e., action that the innocent party would not have taken but for the misrepresentation).153 To suggest that an “authorized” action by the insured’s agent(s) somehow would negate fraud coverage essentially renders the computer fraud coverage useless, as it undercuts the very definition of fraud itself.154 The email is not “incidental” to the occurrence

151. Apache Corp., 662 F. App’x. at 258.
152. Civil Action No. 1:15-CV-4130-RWS, 2016 WL 4618761 at *5 (quoting Apache Corp., No. 4:14-CV-237, 2015 WL 7709584, at *3 (S.D. Texas Aug. 7, 2015)). In finding that money paid to a spoofing scammer was covered under a crime policy’s Funds Transfer Fraud provision in Medidata, Judge Carter echoed this sentiment, summarizing the scenario succinctly and accurately:

It is also undisputed that the accounts payable personnel would not have initiated the wire transfer, but for, the third parties’ manipulation of the emails. The fact that the accounts payable employee willingly pressed the send button on the bank transfer does not transform the bank wire into a valid transaction. To the contrary, the validity of the wire transfer depended upon several high level employees’ knowledge and consent which was only obtained by trick. As the parties are well aware, larceny by trick is still larceny.

153. See Fraud, BLACK’S LAW DICTIONARY (10th ed. 2014) (“fraud n. (14c) 1. A knowing misrepresentation or knowing concealment of a material fact made to induce another to act to his or her detriment.” (emphasis added)).
154. See id.; see also Knutsen & Stempel, supra note 135, at 663-64.
of the money transfer in any of these cases, but rather the direct cause. Blend this common-sense rationale with the bedrock insurance-law principle that any policy ambiguities are to be construed in favor of the insured, and one reasonably could conclude that future court decisions will side more with Judge Carter and Judge Story rather than the unpublished Fifth and Ninth Circuit opinions.

Theft and fraudulent transfer of funds by malicious actors is a significant concern for CRE because a substantial amount of acquisitions, dispositions, and financing of properties occur through web transactions, ripe territory for computer scam artists. If the insured purchases the coverage for theft by non-employees, it seems undisputed that commercial crime policies would cover a hacker’s unlawful entry into a computer system whereby the hacker unlawfully transfers funds himself directly (standard larceny). Under Medidata and related cases, moreover, the related computer-fraud coverage also should cover money lost to a “social engineer” or “spoofing” scam artist, and the purchase of certain computer-fraud riders can even cover related losses arising out of such incidents, including credit card fees.
and public-relations expenses. Crime policies, on the other hand, do not cover Cyber Extortion. Thus the cyber policy must step in to insure this exposure, but it should be noted simultaneously that some cyber policies may not cover fraudulent instructions such as the one discussed in Medidata where larceny by trick is involved. Accordingly, CRE insureds should ensure that their crime and cyber coverages work in concordance with one another in order to fill these respective gaps, as well as to avoid overpayment of premiums for “double coverage.”

D. Terrorism Insurance

In the absence of help from crime coverage, CRE insureds might seek refuge from ransomware attacks through terrorism coverage. Under the

158. Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa., 691 F.3d 821, 824, 833-34 (6th Cir. 2012) (holding that under computer crime rider’s “resulting directly from” language, a proximate cause standard controlled, necessitating coverage for “incurred expenses for customer communications, public relations, . . . charge backs, card reissuance, account monitoring, and fines imposed by VISA/MasterCard”).

159. See Ins. Servs. Office Inc., Form No. CR 00 23 05 06, Commercial Crime Policy (Loss Sustained Form), Exclusions (f)(1)(a)-(e) (2005). This policy form states:

Insuring Agreements . . . do not cover . . . (1) Loss of or damage to property after it has been transferred or surrendered to a person or place outside the “premises” or “banking premises”; . . . (c) As a result of a threat to do damage to any property; (d) As a result of a threat to introduce a denial of service attack into your computer system; (e) As a result of a threat to introduce a virus or other malicious instruction into your computer system[.]

160. See Am. Int'l Grp., Cyber Extortion Coverage Section, supra note 26, Exclusion 3(a) (excluding from coverage “any payment for Loss: (a) arising out of, based upon or attributable to any dishonest, fraudulent, criminal or malicious act, error or omission, or any intentional or knowing violation of the law, if committed by any . . . (2) past or present employee . . . ”); JLT Asset Management Cyber Policy, supra note 26, Exclusion 16 (excluding “monetary value of any electronic fund transfers or transactions by or on behalf of the Insured which is lost, diminished or damaged during transfer from, into or between accounts”); JLT Asset Management Cyber Policy, supra note 26, Additional Coverage Section C(2), Definition 18 (tying Cyber Extortion coverage solely to “Extortion Demand(s),” which by definition must include a “threats” or a “series of threats”). But see Am. Int'l Grp., Event Management Coverage Section, supra note 26, Definition 2(1) (including “social engineering” within definition of “Privacy Event”); Evolve MGA Cyber Policy, supra note 33, Insuring Clause 2, Section A(e) (covering under Cyber Crime “any phishing, vishing or other social engineering attack against any employee or senior executive officer that results in the transfer of your funds to an unintended third party”).

Published by University of Oklahoma College of Law Digital Commons, 2019
Terrorism Risk Insurance Act of 2002 (TRIA), \(^{161}\) as extended through 2020 by the Terrorism Risk Insurance Program Reauthorization Act of 2015 (TRIPRA), \(^{162}\) insurers must offer terrorism insurance with coverage at least as broad as the property or casualty policy being offered provides, and for its part, the federal government offers a financial backstop for the insurers in case a large loss does occur. \(^{163}\) The Terrorism Risk Insurance Program (TRIP) only provides this reinsurance, however, for certified “acts of terrorism,” which require, inter alia:

- a violent act dangerous to human life, property, or infrastructure;
- occurring within the United States (or at a U.S. mission or U.S. air carrier/flag vessel);
- committed by an individual(s) as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the United States Government by coercion;
- and property and casualty losses exceeding $5,000,000. \(^{164}\)

Because many insurers tie their coverage to this federal certification, the question of whether terrorism insurance will respond to a cyber event frequently revolves around whether the event meets the above definition. \(^{165}\)

U.S. Treasury Department guidance has confirmed that stand-alone cyber liability policies are subject to TRIA requirements because they generally are categorized as “property and casualty” rather than “[p]rofessional [e]rrors and [o]missions” policies, and therefore insurers must “make available” terrorism


\(^{163}\) See id. §§ 103(c), 105(a). TRIA requires insurers to offer terrorism coverage that “does not differ materially from the terms, amounts, and other coverage limitations applicable to losses arising from events other than acts of terrorism.” Id. § 103(c)(1)(B); see also Edward M. Bloom & Michael S. Strauss, Massachusetts CLE, Inc., LEASE DRAFTING IN MASSACHUSETTS–INSURANCE, SUBROGATION, AND INDEMNITY (4th ed. 2017).

\(^{164}\) See 31 C.F.R. §§ 50.4(b), 50.60 (2017) (setting forth the definition of “act of terrorism” and the process under which an act is certified as an act of terrorism).

coverage in connection with their sale of such policies. This requirement does not answer the question of whether terrorism coverage necessarily applies to a cyber event, however. It would be difficult in many cases to argue that certain cyber scammers are attempting “to coerce the civilian population of the United States or to influence the policy or affect the conduct of the United States Government by coercion” with their actions, although there are surely conceivable exceptions. Even in the event of the rare exception, cyber events are seldom “violent” acts, absent special facts—indeed, part of the appeal of being a hacker is being able to make money while still hiding safely behind a computer screen without facing any threat of violence. To add another wrinkle, many terrorism forms contain endorsements excluding losses arising out of the malfunctioning, theft, corruption, or loss of use of or access to electronic data, just as property and CGL insurers now have done, leading to the final conclusion that seeking cyber coverage under the standard terrorism coverage offered with CGL and property policies is at best an uphill battle.


167. See id. Such ambiguity is a pervasive problem for TRIA and related terrorism legislation, as a few practitioners have noted: “Terrorism legislation of all sorts defy cohesive analysis by their sheer volume. Even if one finds the pertinent statute, there are numerous other authorities, such as enactments specific to certain countries or even specific court cases, executive orders, and regulations.”

168. 31 C.F.R. § 50.4(b)(2017); see Daniel Wilson, ISIS-Linked Hacker Pleads Guilty In Cyberterror Case, LAW360 (June 17, 2016, 2:41 PM EDT), https://www.law360.com/articles/808220/isis-linked-hacker-pleads-guilty-in-cyberterror-case (“Kosovo man pled guilty in Virginia federal court to charges that he hacked the personal details of around 1,300 American troops and government personnel and put them at risk by posting that information on a Twitter account controlled by the Islamic State group, commonly called ISIS.”).

169. See John Winn & Kevin Govern, Identity Theft: Risks and Challenges to Business of Data Compromise, 28 Temp. J. Sci. Tech. & Envt’l. L. 49, 51 (2009) (“Cyber-theft is usually non-violent, has high profit margins, and incurs little or no risk of detection or prosecution.”).

170. See, e.g., UKP 602 1213 Endorsement (on file with author). This endorsement excludes:

any loss, damage, cost or expense directly or indirectly caused by, consisting of, or resulting from any of the following, regardless of any other cause or event contributing concurrently or in any other sequence thereto:

1. Any functioning or malfunctioning of Electronic Data (including but not limited to any issues related to dates or date processing), the internet, an intranet, a private network, or any similar facility;
ransom, and extortion” insurance policies do not necessarily cover ransomware.171

E. Directors’ & Officers’ Insurance

Directors’ and officers’ (D&O) liability insurance policies provide coverage for claims against directors and officers that allege wrongful acts that those officials committed in their capacity as directors and officers of the insured company.172 Some D&O policy forms exclude coverage for claims arising out of “damage to or destruction of any data or tangible property, including loss of use thereof; [provided this exclusion does] not apply to Loss on account of any Claim arising from damage to, destruction of, loss of, or loss of use of, client records in an Insured’s possession.”173 This exclusionary language is not nearly as far-reaching as that of the “Access Or Disclosure Of Confidential Or Personal Information” endorsement found in almost all CGL policies (discussed supra Section V.B), as it only excludes “damage to” or “destruction” of data, which does not necessarily occur during the course of a Privacy Breach Event. However, many D&O policies specifically exclude coverage for “invasion of privacy,” and courts generally enforce such exclusions, which could

2. Any corruption, destruction, distortion, erasure, alteration, theft, or other loss or damage to Electronic Data;
3. Loss of use, access to, or functionality, all whether partial or entire, of Electronic Data, any computer or computer system, or any other device dependent upon any microchip or embedded logic, and any ensuing liability or failure of the Insured to conduct business.

Id.

171. See Jeffrey Weinstein & Bruce Kaliner, Will Crisis Management Insurance Cover Ransomware?, LAW360 (Jan. 17, 2018, 4:44 PM EST), https://www.law360.com/insurance/articles/1002995/will-crisis-management-insurance-cover-ransomware-. Although many of these policies have updated their language to expressly include computer-related events, there may be coverage hiccups in some instances where the following policy conditions are not met: (1) the threat is “communicated to the insured by person(s) who demand a ransom as a condition for not carrying out or ending the extortion incident”; and (2) “the insured is the intended victim of the triggering event.” Id. These conditions can be difficult because during these events the malware encryption often has already taken place before any threat is made; there is no “human” threat but rather only a computer message; and the “intended victim” is often not precise, as the ransomware does not necessarily target certain individuals but rather is designed to spread and infect. Id.


present a problem if a securities-law or fiduciary-duty claim arose out of a Privacy Breach Event.  

The insured has prevailed in obtaining D&O coverage for a Privacy Breach Event when it (the insured) specifically purchases “Electronic Risk Liability” coverage. In First Bank of Delaware, Inc. v. Fidelity and Deposit Co. of Maryland, the insured subcontracted with Data Access Systems (DAS) to process certain credit card payments. Malicious actors hacked DAS’s servers, which led to millions of unauthorized withdrawals from customer accounts, placing First Bank out of compliance with the “Payment Card Industry Data Security Standard (‘PCI DSS’).” First Bank sought coverage under a provision of its D&O policy that covered electronic-risk liability, defined as “any unauthorized use of, or unauthorized access to, electronic data or software with a computer system.” The insurer argued that there was no covered “loss event” because the computer system was “not used to transact business on behalf of First Bank” (an element of the policy’s definition of “Computer System”), and that coverage should be denied under an exclusion for claims “based upon or attributable to or arising from the actual or purported fraudulent use by any person or entity of any card or in any credit, debit, charge, access, convenience, customer identification or other card, including, but not limited to, the card number.” The court sided with the insured, finding that a loss event did occur because DAS’s computers were used to conduct credit card transactions, fees from which were indeed part of First Bank’s “business.” It determined that every unauthorized use of or access to the insured’s electronic data or software would almost necessarily involve fraud, and thus a literal reading of the policy’s exclusion would render the electronic-risk coverage illusory.

---

176. Id. at *1-2.
177. Id. at *2, 5.
178. Id. at *4-8.
179. Id. at *5.
180. Id. at *5-9. With respect to the latter point, the court summarized:

The Court finds that applying Exclusion M would swallow the coverage granted under Section 4.III(L)(1) for “any unauthorized use of, or unauthorized access to electronic data . . . with a computer system.” It is theoretically
VI. A Nightmare Scenario

As one might be able to glean from this Article, there are myriad cyber scenarios that could present problems for CRE insureds. However, it is useful to walk through an example of a potential cyber event and provide a step-by-step explanation of the dangers involved and how insurers would respond. Drawing upon the real events as well as the policy form and endorsement language discussed in this Article, the following represents a possible cyber event for which CRE insureds should be sufficiently prepared. Although the example utilizes a multi-tenant office asset (and makes a number of other assumptions) for simplicity’s sake, it should be noted that there are nearly limitless distinct applications and exposures that could be discussed, all of which could have varying outcomes.

Suppose Owner leases a Chicago office building to various entities, including Tenant. In the Lease, Tenant warrants that it is a small startup company that sells widgets and that it will use its portion of the leased premises as a corporate office. Tenant covenants that it will obtain and maintain various traditional insurance coverages during the Lease Term, including general liability insurance and insurance for its own personal property. Owner covenants that it will carry “all-risk” property insurance for the building, and Owner also happens to carry its own CGL, crime, terrorism, D&O, and cyber insurance. The Lease provides that Tenant will indemnify, defend, and hold Owner harmless for any and all claims and losses “in connection with or arising from the use or occupancy or manner of use or occupancy of the Premises or any injury or damage caused by Tenant.”

Suppose further the Lease states that the HVAC at the building is to be handled through a centralized system that is ultimately controlled possible that an example of non-fraudulent unauthorized use of data exists. However, in the context of this Policy, all unauthorized use could be, to some extent, fraudulent. The abstract possibility of some coverage surviving the fraud exclusion is not sufficient to persuade the Court to apply an exclusion that is almost entirely irreconcilable with the Loss Event coverage.

Id. at *9. Note that Judge Johnston’s logic here is entirely consistent with this Article’s position on Medidata and related cases of computer fraud, discussed supra in Section V.C of this Article (“Commercial Crime Insurance”). The Fifth Circuit has also ruled in favor of the D&O insured in a case involving a hacking of credit card information leading to non-compliance with the PCI DSS. See Spec’s Family Partners, Ltd. v. Hanover Ins. Co., No. 17-20263, 2018 WL 3120794 (5th Cir., Jun. 25, 2018) (holding insurer wrongfully refused to defend insured because contractual liability exclusion did not explicitly excuse duty to defend).

181. See supra Sections III-IV.
182. See, e.g., OFFICE LEASE AGREEMENT, supra note 23.
2019] INSURANCE OF CYBER RISKS FOR REAL ESTATE 443

by the Owner, but that Tenant will be charged proportional costs related to maintaining the HVAC as Additional Rent. Owner contracts with a third-party HVAC vendor to handle all the heat and air conditioning and maintenance thereof.

The HVAC system is “smart”—i.e., it includes various environmental sensors that monitor the system for abnormalities, energy consumption, and the need for service checkups and routine maintenance. Accordingly, the HVAC vendor that operates the system retains access rights to Owner’s computer network for carrying out these tasks. One day, malevolent hackers breach the HVAC system through a security vulnerability, thus giving them a foothold in Owner’s network and allowing them to exercise control of not only the HVAC systems, but also the building electrical systems, the Tenant’s Wi-Fi, and Tenant’s customer-payment systems. The intrusion has thus occurred. That day, Owner and Tenant both receive messages from the hackers indicating that if they do not transfer $10,000 in Bitcoin to the hackers within forty-eight hours, the hackers will turn off the HVAC and electricity at the office building and release on the dark web the information of 10 million individuals found in Tenant’s payment-systems database.

Unsure of whether this message is some kind of bluff or joke, Owner and Tenant work together during the next two days to address the problem by consulting law enforcement and hired computer experts. They begin the process of obtaining enough Bitcoin to pay the hackers in the event they end up needing to pay, but they assume the issue will be fixed and that


185. This sort of breach through the HVAC system is exactly how the Target cyber attack was accomplished. Id.

[T]hieves sent phishing emails to Fazio Mechanical Services, a third-party HVAC vendor that had access to Target’s computer systems, according to court documents. The emails were designed to trick users into clicking a link to download password-stealing malware. That gave Fazio’s Target network passwords to the hackers, who then used them to steal the retail giant’s customer data.

business will continue smoothly\(^{186}\) (and furthermore, they are told that their Bitcoin transaction will take a few days to process).\(^{187}\) Unfortunately, the message is not a bluff, and the hackers do exactly as they threatened after forty-eight hours. The building’s HVAC and electricity are turned off, and the hackers release the personal data of millions of individuals over the dark web, the long-term effect of which is immeasurable. While there is no electricity, heat, or air conditioning, Tenant is unable to conduct business operations. At this point, data breach notification statutes are triggered, and Owner immediately retains a lawyer who specializes in data security and privacy, meanwhile putting all Owner and Tenant insurance carriers on notice of the issue.

On the day of this calamitous occurrence, computer experts are quickly able to compile all of the names of the people potentially affected. Owner and Tenant both incur significant expenses notifying all affected parties of the breach, in compliance with all relevant data breach notification statutes,\(^{188}\) which is in addition to the fees they are paying the lawyer and the computer experts. The stakeholders agree at this point that it is probably best to just pay the hackers so that the building will be placed back into service. Owner pays the hackers that same day with the understanding that insurance likely will reimburse the cost, and failing that, Tenant’s indemnity obligations should kick in. Sadly, once the payment is made, the hackers do not turn the HVAC and electricity back on, but rather, demand another ransom payment. Owner and Tenant are both (understandably) incredibly frustrated at this point and refuse to pay out any more money to these awful hackers. After about three more weeks, the computer experts discover the vulnerability, fix it, and make changes sufficient to ensure that the hackers no longer have access to any of the computer systems. Normalcy is restored.

The return of the HVAC and electricity is all well and good, but in the meantime, Owner has lost a month’s worth of rental income from each of its angry tenants whose lawyers advised that they withhold rent payments because Owner failed to maintain the building in a tenantable manner for nearly an entire month due to its failure to adequately secure the HVAC

\(^{186}\) One survey found that only “24.6% of companies would be willing to pay a ransom to hackers.” Cloud Sec. All. & Skyhigh, The Cloud Balancing Act for IT: Between Promise and Peril 2 (2016), http://info.skyhighnetworks.com/rs/274-AUP-214/images/WP%20CSA%20Survey%20Cloud%20Balancing%20Act%200116.pdf.


\(^{188}\) See supra Section IV.B.
for which it was responsible under the Lease) and maintain the electricity.\textsuperscript{189} Tenant, a small startup company, is unable to withstand the deadly combined blow of one month without widget-selling and the tarnished reputation from the release of its customers’ PII, so it eventually files for bankruptcy. Predictably, it also breaks the lease, and Owner now must find a replacement tenant, not to mention the expenses incurred through the ineffective Bitcoin payment, data breach notification compliance, attorneys’ fees, and payment for the computer experts. To make matters worse, plaintiffs’ lawyers have discovered that the breach that caused the release of PII originated in the HVAC, which was the Owner’s responsibility under the Lease. Given that Tenant is rendered insolvent and that the HVAC vendor does not have pockets as deep as the Owner’s, the plaintiffs’ lawyers organize a big-money class action lawsuit against Owner.

Tenant’s insurance policies would not assist with any of these costs because (1) the class action is not against Tenant, so the insurer has no duty to defend (not to mention the applicability of the Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability exclusion); (2) the HVAC is not Tenant’s personal property, but rather, it is Owner’s property, so Tenant’s property policy would not respond (not to mention any applicable electronic data exclusions); and (3) Owner did not require Tenant to carry any cyber insurance, so there would be no cyber coverage. Furthermore, Tenant is insolvent, so any attempts by Owner to attain satisfaction on Tenant’s indemnity obligations will inevitably be relegated to the back of the line with the other unsecured creditors in bankruptcy. Even if Tenant had remained solvent, it is certainly arguable whether a hacking of Owner’s HVAC would give rise to any obligations on behalf of Tenant under the Lease language.\textsuperscript{190} Could Owner seek any defense or indemnification from its own insurance? Let us assume that throughout this whole process, Owner dutifully and accurately has kept its insurance carriers abreast of everything with the hope of obtaining coverage for all of these expenses.

\textsuperscript{189} See supra Section III.B; note 62 and accompanying text.

\textsuperscript{190} See OFFICE LEASE AGREEMENT, supra note 23 (stating in lease language that Tenant will indemnify for claims and losses “in connection with or arising from the use or occupancy or manner of use or occupancy of the Premises or any injury or damage caused by Tenant”) (emphasis added). Here, the breach of the HVAC did not arise out of Tenant’s use or occupancy or manner of use or occupancy, and all losses were arguably caused by the acts or omissions of Owner or his HVAC vendor, not Tenant.
The business interruption coverage on Owner’s all-risk property policy would likely not provide any coverage for lost rent or income, because although building systems were turned off, there was no specified covered peril or physical damage to trigger the policy.\textsuperscript{191} The CGL carrier would not tender a defense in relation to the class action, as the action arises out of “Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability.”\textsuperscript{192} Owner’s crime and terrorism carriers will deny the claim for the massive Bitcoin payment because standard crime policies do not cover Cyber Extortion, and absent other facts, it is unlikely that this hacking would be deemed a certified act of terrorism.\textsuperscript{193} If shareholders sued Owner’s officers and directors for breach of duty of care, then theoretically Owner’s D&O coverage could provide defense and possibly indemnity depending on the policy language, but only as to that particular lawsuit.\textsuperscript{194} Thus, Owner’s cyber policy would almost certainly be the last resort for indemnification for these losses.

First, any adequate cyber policy should cover all of Owner’s data breach notification costs, as well as the fees paid to the computer experts.\textsuperscript{195} The Cyber Extortion coverage provisions of most cyber policies should cover the eventual payment of the Bitcoin.\textsuperscript{196} Defense of the class action lawsuit should also be covered, assuming the policy does not have a blanket exclusion for consumer-protection class actions that the carrier uses to deny the claim.\textsuperscript{197} So, under the average cyber policy, the insured Owner would likely recoup some of the costs associated with this unfortunate event.

As to the lost rental income stemming from the angry tenants and the insolvent Tenant, however, it is likely that many cyber insurers would deny coverage for all the costs related thereto because many of the business-interruption costs here arguably were caused by a “Privacy Breach Event”

\textsuperscript{191} See supra Section V.A.
\textsuperscript{192} See supra Section V.B.
\textsuperscript{193} See supra Sections V.C-D.
\textsuperscript{194} See supra Sections V.E. Owner would have to ensure that its D&O policy does not contain any relevant exclusion, such as one for “invasion of privacy.” See supra Section V.E.
\textsuperscript{195} See RAND Study, supra note 27, at 13; Am. Int’l Grp., Event Management Coverage Section, supra note 26, Definition 2(h); Am. Int’l Grp., Reputation Guard Coverage Section, supra note 26, Definition 2(f); Evolve MGA Cyber Policy, supra note 33, Insuring Clause 1, Sections A, B; JLT Asset Management Cyber Policy, supra note 26, Privacy Breach, Privacy Breach Management B.1; Chubb Cyber Policy, supra note 33, Cyber Incident Response Expenses Definition.
\textsuperscript{196} See Chubb Cyber Policy, supra note 33, Extortion Expenses Definition.
\textsuperscript{197} See sources cited supra note 195.
or a “Cyber Extortion Event” rather than a “System Event.” Although the hackers did shut systems down in this hypothetical, they also threatened release of PII through ransomware, giving the insurer plenty of room to argue that business-interruption coverage was never triggered at all. Given that the building at issue is a multi-tenant office building in Chicago, the amount lost to Owner if the insurer denies this coverage is likely in the millions of dollars. Furthermore, if it ever becomes apparent that the hackers in question were operating at the behest of North Korea or a terrorist group, the insurer could deny coverage altogether if the policy contained broad terrorism or war exclusion wording. As the reader undoubtedly now recognizes, traditional insurance policies are not adequate to cover events like these, and indeed even the cyber policy coverage itself can be tenuous, a reality that underscores the importance of buying the right policy with the most expansive possible coverage.

This hypothetical obviously presents something of a nightmare scenario, but it is not terribly far-fetched. All of the events in this hypothetical are drawn from actual cyber events and related litigation, most of which were discussed in this Article. CRE insureds would do well to take these threats seriously and attempt to address them with robust cybersecurity, contractual risk transfer, and well-negotiated cyber insurance. Until more case law comes down to determine what types of events are really covered by cyber insurance, rigorous diligence before policies are bound and before claims arise is the best risk mitigation approach. For example, the Lease in this hypothetical should have included a cyber insurance requirement for all tenants as well as indemnification language indicating that tenants would indemnify, defend, and hold Owner harmless for any costs arising out of any cyber events, including those related to the HVAC. Further, Owner’s cyber policy should have adequately addressed the provision of indemnity for business interruption caused by Privacy Breach Events and Cyber Extortion Events rather than only System Events.

198. See supra Sections II.C, III.B; JLT Asset Management Cyber Policy, supra note 26, Definitions 34, 39; see also Am. Int’l Grp., Network Interruption Coverage Section, supra note 26, Section 1 (Insuring Agreement), Definition 2(k) (tying business interruption coverage to “Security Failure”); Am. Int’l Grp., Security and Privacy Coverage Section, supra note 26, Section 1 (Insuring Agreement), Definitions 2(l) and 2(p) (tying liability coverage to either “Security Failure” or “Privacy Event”); but see Evolve MGA Cyber Policy, supra note 33, Insuring Clauses 1 & 3, Definition 11 (tying both first- and third-party coverages to broadly defined “cyber event”).

199. See supra Section III.C.
VII. Conclusion

Given the acuteness of cyber threats, it is critical that risk managers and insurance counsel analyze any and all potential gaps between current policies and the market’s available cyber options when shopping for coverage. CRE insureds involved with the construction or ownership of smart buildings are likely to be most concerned about property damage, business interruption, and liability to third parties arising from cyber events. Insurance coverage for these dangers that might have historically existed under property, CGL, crime, terrorism, and D&O policies (i.e., “silent cyber”) has already been or soon will be phased out from those policies and segregated into cyber insurance products. Regrettably, many of the cyber solutions that the insurance industry offers can also be too narrow in their scope in that they too do not guarantee sufficient coverage for these risks. From a smart building owner’s perspective, broadly worded exclusions relating to property damage, bodily injury, contractual liability, war, intellectual property, and other terms collectively serve to obfuscate the advantages of many cyber policies in the market.

Still, CRE stakeholders must ensure that a risk assessment and coverage gap analysis takes place, using the analysis thereof as the basis for their negotiations with cyber carriers to obtain coverage to fill those specific gaps and obtain the necessary coverage to the extent available. Insureds must also emphasize stronger negotiation and contractual risk transfer to ensure that any tenants or property managers maintaining the data at smart buildings purchase cyber insurance and agree to indemnify the owner for losses arising out of any cyber events. Cyber insurance carriers, meanwhile, should focus their efforts on offering products that are more narrowly tailored to CRE needs and the risks associated with smart

200. See supra Section V.
201. See supra Sections III-IV.
202. See supra Sections V-VI; see also supra note 135 and accompanying text.
203. See supra Sections III-IV.
204. See supra Section III.A; note 56 and accompanying text.
205. See supra Section V.B; note 139 and accompanying text.
206. See supra Section IV.A.
207. See supra Section III.C.
208. See supra Section III.A; note 57 and accompanying text.
209. See supra Sections III-IV.
210. This is possible because cyber insurance is relatively negotiable due to its difficulty in pricing. See supra Section II.D.
211. See supra Sections V-VI.
buildings, so that they can actually offer additional protection that is worth purchasing as these new perils continue to emerge. Otherwise, CRE might continue to stay away from cyber insurance products where there is little to no articulable benefit to purchasing them.\textsuperscript{212} Nevertheless, because the insurance industry has already begun the process of excluding any possible “silent cyber” from the traditional policies, obtainment and maintenance of cyber insurance will soon undoubtedly become more of a necessity, and less of a luxury, for all businesses.\textsuperscript{213}


\textsuperscript{213} See supra note 135 and accompanying text.
Appendix

Cyber Coverage Checklist for CRE\textsuperscript{214} Based on Current Case Law and Prevalent Policy Forms and Endorsements

\begin{itemize}
\item LOST INCOME, REVENUE, REPUTATION / BUSINESS INTERRUPTION INCLUDED\textsuperscript{215}
\item BUSINESS INTERRUPTION WAITING PERIOD IS 8 HOURS OR LESS\textsuperscript{216}
\item NO EXCLUSION FOR BODILY INJURY, OR IF THERE IS AN EXCLUSION, CARVEBACK FOR MENTAL ANGUISH/EMOTIONAL DISTRESS\textsuperscript{217}
\item EXCLUSION FOR PROPERTY DAMAGE CARVED BACK TO ALLOW COVERAGE FOR BRICKING AND DAMAGE TO INTANGIBLE PROPERTY (I.E., ELECTRONIC DATA)\textsuperscript{218}
\item EXCLUSION FOR CONTRACTUAL LIABILITY CARVED BACK TO PROVIDE COVERAGE FOR PCI FINES, LIABILITY THAT WOULD HAVE ARISEN IN ABSENCE OF CONTRACT, AND CONTRACTUAL OBLIGATION TO SECURE/MAINTAIN PHI\textsuperscript{219}
\item SECURITIES CLAIMS/BREACH OF SECURITIES LAWS EXCLUSION CARVED BACK TO ALLOW COVERAGE FOR SUCH CLAIMS THAT ARISE OUT OF CYBERSECURITY/ CYBER LIABILITY\textsuperscript{220}
\item NO TERRORISM EXCLUSION DEFINING TERRORISM AS BEING ANY ATTACK CONNECTED TO AN “IDEOLOGY” OR OTHER VAGUE TERMS\textsuperscript{221}
\item WAR EXCLUSION DOES NOT APPLY TO CYBER TERRORISM\textsuperscript{222}
\item AUTOMATIC COVERAGE FOR MERGERS & ACQUISITIONS\textsuperscript{223}
\end{itemize}

\textsuperscript{214} Please note that depending on the size and nature of the various exposures to the insured, as well as the costliness of adding/removing certain items, some of these terms should not necessarily be “deal breakers” during the negotiation process for every insured. Rather, this list is an attempt to provide considerations insureds should seek to confirm with their insurance brokers and carriers as part of the negotiation and decision-making process when signing up with a cyber insurance program.

\textsuperscript{215} \textit{See supra} Section III.B.

\textsuperscript{216} \textit{See supra} Section II.C. Note, the shortest waiting period the author has seen offered is six hours.

\textsuperscript{217} \textit{See supra} note 139 and accompanying text.

\textsuperscript{218} \textit{See supra} Section III.A.

\textsuperscript{219} \textit{See supra} Section IV.A.

\textsuperscript{220} \textit{See supra} Section IV.C.

\textsuperscript{221} \textit{See supra} Section III.C.

\textsuperscript{222} \textit{See supra} Section III.C.

\textsuperscript{223} Although not discussed in this Article at great length, this is a critical component of proper cyber coverage for real estate companies because new assets are going to need to be added to the policy throughout the term. A CRE insured does not want a negotiation to occur or have a substantial additional premium be charged every single time a new property is
CONFIRM GDPR COVERAGE (TO THE EXTENT ENFORCEABLE)\textsuperscript{224}

RETENTION/DEDUCTIBLE NOT GREATER THAN $25,000\textsuperscript{225}

VIOLATION OF CONSUMER PROTECTION STATUTE NOT EXCLUDED (OR, IF EXCLUDED, SUCH EXCLUSION IS SPECIFICALLY CARVED BACK FOR SUITS/ACTIONS BROUGHT UNDER THE FEDERAL TRADE COMMISSION ACT)\textsuperscript{226}

CRYPTOCURRENCY PROVIDED AS PART OF CYBER EXTORTION/RANSOMWARE COVERAGE (WITH NO WAITING PERIOD)\textsuperscript{227}

\textsuperscript{224} See supra note 103 and accompanying text.
\textsuperscript{225} This is the market standard as of this writing.
\textsuperscript{226} See supra Section IV.A.
\textsuperscript{227} See supra note 187 and accompanying text.