

Global Cyber Newsletter



Table of Contents

Notable Cyber Breaches & Threats PAGE 3

- Equifax data breach compromises 143M customers
- HBO Series of unfortunate cyber events
- 4M Records Exposed in Time Warner Cable Leak
- Maersk Reports \$300M Impact from NotPetya
- CopyCat Adware Hits 14M Devices
- Nationwide Settles over 2012 Data Breach
- UniCredit SpA Banking Records Breached
- 1.8M Illinois Voter Records Exposed
- Philadelphia OB/GYN Practice Breached
- Kansas Department of Commerce Hacked
- Health Portal data breach in Singapore
- “Big Four” accountancy firm hacked

Regulatory & Legislative Update PAGE 8

- Internet of Things Cybersecurity Act of 2017 bill drafted by U.S. Senate

Global Cyber Security PAGE 11

- Power Grids Across Europe and the U.S. Breached
- Bitcoin Insurance Goes Live in Japan
- Erie County Medical Center Invests \$10M to Rebuild Systems following Cyber Attack
- FTC Reviewing Privacy Complaint about Google
- Medical Device Vulnerabilities

Guest Column PAGE 14

- The Ever Expanding Scope of Cyber Risks: All Policy Lines Beware by Laurie A. Kamaiko

Litigation News PAGE 18

- CareFirst Class Action Suit Reinstated
- Yahoo Data Breach Litigation to Proceed
- U.S. District Court of Eastern Michigan: Whaling Attack
- Canada – Queen’s Bench of Alberta: Whaling Attack
- Three Class Action Lawsuits Spring from COPPA

Cyber Studies & Trends PAGE 21

- Cisco Midyear Cyber Security Report
- IBM/Ponemon 2017 Cost of Data Breach Report
- Advisen Cyber Security Conference
- Net Diligence Cyber Security Conference

Notable Cyber Breaches & Threats

Equifax Breach Compromises 143M US Customers



Described as one of the largest data breaches in US corporate history, [hackers](#) are said to have exploited a US website application vulnerability to access social security numbers and other personal information of 143m US consumers. The Atlanta based consumer credit agency said credit card numbers of 209,000 consumers were accessed. The breach is said to have occurred between May and July this year. [Equifax shares fell 35%](#) following the breach, with analysts predicting additional losses. [Lawsuits](#) have already been initiated in the US, [and multiple federal agencies](#), including the Dept. of Justice, SEC, and Senate Finance Committee are investigating.

The impact will be felt in the UK as well: as many as [400,000 UK customers](#) were affected. Equifax provide services for companies including BT, British Gas and Capital One.

HBO in a Series of Unfortunate Cyber Events



In early August, [hackers](#) approached media outlets with news that they had accessed HBO's networks and released previously unseen episodes of a number of popular shows plus the script of an upcoming episode of Game of Thrones. The hackers claimed to have stolen 1.5 terabytes of data.



In a separate incident a few days later an episode of Game of Thrones was leaked by [Star India](#), a distribution partner. Later in the month, [HBO's twitter accounts](#) were taken over by a notorious hacking group, OurMine.

4M Records Exposed in Time Warner Cable Leak



A security company, Kromtech, [found 600 GB of unprotected data](#) on an Amazon server while investigating another breach for World Wrestling Entertainment. The data included user account names and numbers. No bank, credit card or other personal data was exposed.

Maersk Reports \$300M Impact From NotPetya

Following June's massive, worldwide NotPetya attack, global shipping giant Maersk reports that the total fallout [could cost as much as \\$300M](#). The bulk of the financial impact is from business interruption in the form of lost bookings in the weeks following the attack. Maersk has reportedly added "different and further protective measures" following the attack.

Similarly, [Mondelez International Inc](#), the world's second largest confectionary company reported a 5 percent quarterly drop in sales due to shipping and invoicing delays and [Reckitt Benckiser](#), the consumer goods giant informed shareholders that 2Q revenues would be down 2% as a result of the attack.

CopyCat Adware Hits 14M Devices



Although reported in July, the peak of the [CopyCat attack](#) was in the second quarter of 2017, infecting an estimated 14M Android devices, mainly in Asia. The malware uses the infected device to report fraudulent app-downloads and / or actually download apps to the device, earning the malware's creators false ad revenue. Google addressed the malware through the Android store.

Nationwide Settles with 32 States Over 2012 Data Breach



[Nationwide recently settled](#) with the Attorneys General of 32 states regarding the 2012 data breach that exposed the data of ~1.2M individuals. In addition to the monetary penalty, Nationwide and their subsidiary Allied P&C Insurance Company will [implement several new security practices](#). The data breach was also the subject of two class action lawsuits that were consolidated, dismissed, but has now been reinstated by a federal appeals court in Ohio.



UniCredit SPA Banking Records Breached

A cyber breach at Italy's top bank [exposed the records of 400,000 accounts](#), and hackers appear to have captured personal and loan data, as well as some international bank account numbers. Notably, the earliest in this series of breaches took place in September 2016, nearly a year before disclosure. Such large gaps in reporting will be impermissible once the EU GDPR goes into effect in May 2018.

1.8M Illinois Voter Records Exposed

Election Systems & Software – one of the largest suppliers of voting machines in the U.S. – [failed to secure the personal information for 1.8M voters in Illinois](#). Whitehat hackers at Upguard discovered the cache of information on an unsecured Amazon Web Services device. This is the second major incident concerning U.S. voting records in 2017 (see, [TransRe 2Q2017 Cyber Newsletter, p. 4](#)).



Philadelphia OB/GYN Practice Breached

The medical records of at least [300,000 patients were breached](#) at Women's Health Care Group of Pa, LLC in what is the 3rd largest healthcare breach of the year according to the HHS' [Wall of Shame](#). Patients were notified in July, but the malware was identified at least two months earlier. The Pennsylvania breach notification statute requires notification "without unreasonable delay"—it remains to be seen whether the Group is deemed to have complied with that requirement.

6.5M Records Hacked Through the Kansas Department of Commerce



A [massive hack of the Kansas Dept. of Commerce](#) was discovered in March 2017 and disclosed in July. Out of the 6.5M records compromised, 5.5M included social security numbers for individuals across 10 states. The state of Kansas has retained at least two private breach response companies to assist in dealing with the repercussions, and affected individuals are to receive a variety of compensation according to their own states' laws.

Health Portal Data Breach in Singapore



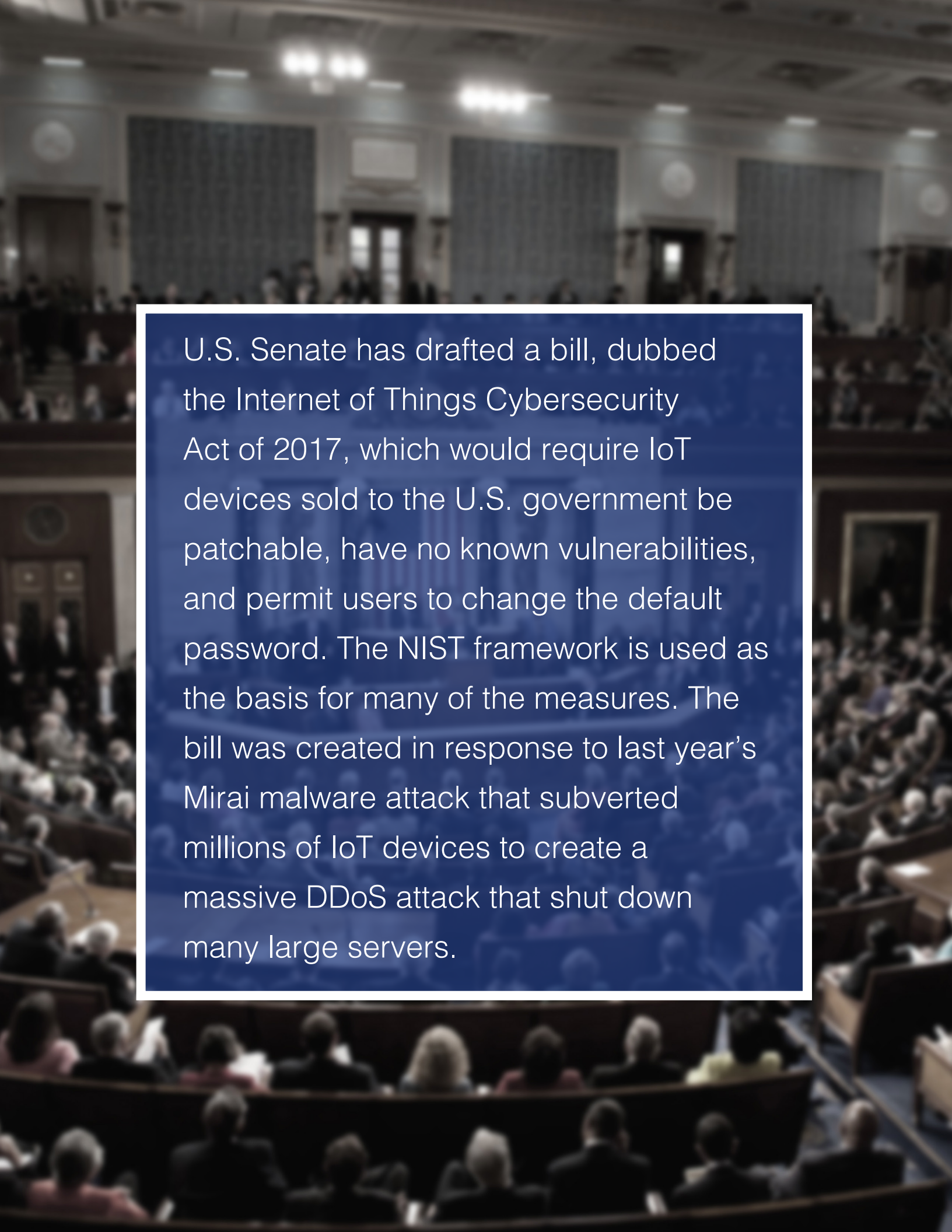
Email addresses, mobile numbers & dates of birth of 5,400 customers (past and present) were exposed when [Axa Insurance's health portal](#) was breached in Singapore. No financial or health data was compromised and AXA has addressed the vulnerability in its system.

"Big Four" Accountancy Firm Hacked



[Deloitte](#) has been the victim of an attack on its global e-mail server which may have compromised client information. The attack is said to have been discovered in March this year although, the breach may have occurred months earlier. Deloitte confirmed that only a small number of clients had been affected.

Regulatory & Legislative Update



U.S. Senate has drafted a bill, dubbed the Internet of Things Cybersecurity Act of 2017, which would require IoT devices sold to the U.S. government be patchable, have no known vulnerabilities, and permit users to change the default password. The NIST framework is used as the basis for many of the measures. The bill was created in response to last year's Mirai malware attack that subverted millions of IoT devices to create a massive DDoS attack that shut down many large servers.

UK Regulator Expresses Concern About Silent Cyber



The Prudential Regulation Authority released its [Supervisory Statement SS 4/17](#) on Cyber insurance underwriting risk requiring a robust assessment of insurance products with specific consideration of silent cyber risk exposure. The statement is relevant to all UK non-life insurance and reinsurance firms.

Kaspersky Lab Antivirus Software Ordered Off US Government Computers



[Federal agencies](#) have been ordered to develop plans to remove Kaspersky software from government systems within 90 days over concerns of links with Russian intelligence services.

ICO Fines Talk Talk Again



[Talk Talk](#) has been fined £100,000 by the Information Commissioner's Office for not providing appropriate technical or organizational measures to keep personal data secure. In particular, employees of an IT services provider, Wipro based in India, had access to between 25,000 and 50,000 customer's data.

Wipro accounts had been used to gain unauthorized and unlawful access to personal data of 21,000 customers. Names addresses, phone numbers and account numbers were compromised resulting in customers receiving scam calls.

The fine represents the second fine issues to the telecommunications company in 10 months following the record £400,000 penalty issued for a data breach exposing 150,000 customers in 2015.

Nationwide Settles With 32 States Over 2012 Data Breach



Nationwide recently settled with the Attorneys General of 32 states regarding the 2012 data breach that exposed the data of ~1.2M individuals. In addition to the monetary penalty, Nationwide and their subsidiary Allied P&C Insurance Company will implement several new security practices. The data breach was also the subject of two class action lawsuits that were consolidated, dismissed, but has now been reinstated by a federal appeals court in Ohio.



Global Cyber Security

Bitcoin Insurance Goes Live in Japan



In a significant step for the leading cryptocurrency, Bitcoin transactions in Japan [can now be insured](#) against fears of failed transactions. The leading Japanese Bitcoin exchange, bitFlyer, partnered with Mitsui Sumimoto to offer the product. Although the need for the product speaks to its perception as an unreliable currency, Bitcoin has continued its gradual move into the mainstream.

Power Grids Across Europe and the U.S. Breached

A hacking campaign by a group being called “Dragonfly” identified by the researchers at Symantec who discovered the breach has [penetrated power grid control systems across two continents](#). The purpose of the hack appears to have been information-gathering to gain familiarity with the systems. The identity and geographic location of the hackers is unknown at this time.

Erie County Medical Center Invests \$10M to Rebuild Systems Following Cyber Attack



[Erie County Medical Center](#) in Buffalo, NY, was hit by ransomware in April and was forced to return to handwritten medical records after it declined to pay the attackers \$30k to unlock their system. They were forced to purchase new hardware, software, and retain expert assistance to recover. ECMC had only recently increased their technology insurance coverage from \$2M to \$10M, and so expects to recoup much of the cost of upgrading their systems, but also anticipate a \$250k - \$400k monthly expense for continued upgrades.

China Central Cyber Attack Repository

[China's Ministry of Industry and Information Technology](#) (MIIT) is to create a national database for the purpose of sharing information on cyber-attacks.



FTC Reviewing Privacy Complaint About Google

The Electronic Privacy Information Center has lodged a [complaint](#) alleging that [Google uses credit card data to track whether online ads lead to in-store purchases](#). Google has partnered with as-yet-un-named partners to obtain customers offline shopping records, which it then links to online activity. The linking of online activity to offline purchases would be an advertising boon, but there is significant concern with the lack of transparency and consent.

ICO's International Focus

The [ICO](#) is seeking close ties with the newly created European Data Protection Board (EDPB) post Brexit. The EDPB will oversee enforcement of the General Data Protection Regulations (GDPR) which becomes law in May 2018 across Europe including the UK.

Medical Device Vulnerabilities

In August 2017, [Siemens reported](#) that several of its CT imaging products contained vulnerabilities that could allow a hacker to execute improper actions. Siemens has updated the code and issued a patch. In an echo of our news item "[Pacemakers Remain Vulnerable](#)" in the 2Q2017 update, the U.S. Food and Drug Administration issued an alert in August regarding a [vulnerability in pacemakers manufactured by Abbott Labs](#) (formerly St. Jude Medical). The vulnerability affects 465k devices in the U.S. and 280k devices elsewhere in the world. These flaws could cause the devices to pace too quickly, or to run down their battery. A firmware update has been issued, and every person with an effected device must see their physician to receive the update. At the University of Washington in Seattle, [researchers successfully hacked DNA](#) by inserting a short stretch of malware into a piece of DNA, then using it to gain full control of a computer that was processing the genetic data. They warn that any such technology could be similarly hacked to change DNA / blood / saliva test results.



Guest Column

The Ever Expanding Scope of Cyber Risks: All Policy Lines Beware

By Laurie A. Kamaiko

What exactly is a cyber risk, and in particular a risk that is covered by insurance, is a constantly evolving concept. Insureds, insurers and reinsurers are continually faced with new types of risks and claims that fall within the rubric of “cyber.” What is a cyber risk is often broadly construed as anything related to the use of a computing device or network. As cyber risks expand, so do their impact on insurance lines, both those designed to apply to them and those that are impacted inadvertently in what has become known as “silent cyber” coverage. Thus, insurers in all lines need to become familiar with identifying and addressing cyber risks.

The types of events that can trigger cyber coverage, and the scope of coverage afforded by cyber policies, still vary considerably. In the early 2000’s, in the wake of the enactment of data breach notification laws that began in the U.S. in 2003 in California (and now are present in 48 states in the U.S. and worldwide), most cyber policies focused on payment of breach investigation and notification costs for events that involved the loss or theft of protected personal information maintained in electronic formats. That is still a fundamental coverage afforded by almost all cyber policies, and is often a coverage added on to other types of policies. However, in

recent years, there has been an expansion of the type of cyber events to which businesses, and their insurers, are subject. Some of the current cyber events do not even involve an actual breach of computer systems, but merely the threat of one.

Even the basic exposure of businesses to theft and loss of protected personal information has increased in scope. Laws and regulations in the U.S. are expanding the definition of what constitutes protected personal information, for example increasingly including on-line log-in credentials and biometrics. Jurisdictions outside the U.S., many of which already had a broad definition of protected personal information, are adopting notification requirements, such as the EU’s General Data Protection Regulation (“GDPR”) that will go into effect in May 2018. This has increased the exposure to businesses, and to their insurers who provide coverage for the costs of investigating and responding to a data breach. While cyber insurers offering stand-alone cyber coverage are likely aware of these developments, insurers offering breach response add-on coverage to “traditional” lines of coverage such as professional liability and other E&O insurance may not be fully taking into account the impending increase in exposure presented by these developments.

Moreover, there has been expansion of cyber risks well beyond the theft or loss of information. As demonstrated by recent news stories, cyber events now include denial of service attacks and attacks directed at destruction of information and systems. This is in addition to the rapid increase in cyber extortion and ransomware, funds transfer frauds utilizing social engineering and electronic communications to trick business employees into making wire transfers to bank accounts controlled by criminals (often referred to as business email compromise), and similar events that may not include a theft of information or breach of a business's own computer systems. Often, the resulting damages are well beyond investigation and notification costs, and include economic losses resulting from denial of access to systems, property and data damage, bodily injury (particularly when medical devices are affected) and an array of third party claims by corporate and individual customers, business partners, and others affected by the event.

These days, just the vulnerability to a cyber-attack, even if an attack or breach has not occurred, can generate claims against a business by regulators, customers, and shareholders. Increasingly, there are regulatory and legal proceedings that allege failure by a business to comply with the growing number of laws and regulations that require cybersecurity protection to be in place or require disclosure of

data collection and security practices, with resulting fines, injunctive relief and potentially other damages awarded for non-compliance. Recent lawsuits against a law firm and a medical device developer, while so far unsuccessful, generated substantial legal defense costs. Regulatory proceedings investigating businesses compliance with security and disclosure requirements for cyber risks can also be expensive to defend. Vulnerabilities in cybersecurity have led to finger pointing by businesses to their cybersecurity vendors and other business parties. Vulnerabilities in software that increase the risk of cyber-attacks of any kind, be it auto theft, data compromise, or privacy violations, can also generate claims even before a breach or loss occurs.

Businesses faced with such losses and claims often look not only to stand alone cyber insurance policies to pay, but also to other types of policies they may have in their insurance arsenal. Many "traditional" lines of insurance have expanded to include add-on coverages for breach response or other designated cyber risks to first party property, third party professional liability and other types of E&O lines, and even general liability.

However, often other lines less deliberately, and often inadvertently, get caught up in claims that arise from cyber risks, and are faced with requests to cover claims of economic losses, property damage or

bodily injury. Virtually every insurer has been faced with a claim they never anticipated, which arose from what can be described as a cyber event because it involved use of or affected a computer system even tangentially.

Crime insurers are now facing the increasing number of funds transfer frauds that involve usage of computers, resulting in a series of conflicting court decisions as to coverage. D&O insurers have been faced with claims by shareholders against boards of companies that sustained data breaches for their role in alleged inadequate cyber security or breach response. Employer's liability insurers may see claims from employees disciplined or terminated because of cyber events and perceived fault. Media liability insurers (and cyber insurers offering media coverage as part of stand-alone cyber policies) are faced with claims arising from the content of statements on business websites and social media. Products liability and product recall insurers are likely to see claims arising from allegedly defective cyber security in devices connected to networks, which these days include a broad range of consumer and health-related products. Property insurers have long dealt with claims arising from events ranging from stolen computers to network outages, resulting in property damage and business interruption claims both direct and contingent. Some insurers on these lines have embraced extensions of coverage that

knowingly encompass such cyber risks. Others have relied on cyber exclusions that can be difficult to fashion to exclude all possible exposures from all possible cyber related events. Personal lines insurers, such as homeowner insurers, are not immune, as individuals as well as businesses are at times faced with claims, as demonstrated by those against families who have a member accused of cyberbullying.

Thus, it is increasingly important for insurers to train both underwriters and claims handlers involved in other lines of insurance than cyber stand-alone policies to recognize the risk of cyber exposures when drafting coverage forms and exclusions, underwriting prospective insureds, and receiving notice of a claim. Often, identifying a potential cyber related claim and consulting with internal talent experienced in addressing such risks can be key to controlling the risk and exposure both on an individual and aggregate basis for the insured, the insurer, and the reinsurer.



Litigation News

Canada –Queen’s Bench of Alberta: No Coverage in Whaling Attack

In a social engineering case similar to the ATC case above, the Court of Queen’s Bench of Alberta reached a comparable decision in the case of [The Brick Warehouse v. Chubb Insurance of Canada](#). There, a hacker convinced The Brick’s accounting department to change the account information for an existing vendor so that the hacker received a number of payments. The court essentially found the same lack of direct causation as above.

U.S. District Court of New York (S.D.N.Y): Coverage in Whaling Attack

In Medidata Solutions, Inc. v. Federal Insurance Co., the New York District Court found coverage on nearly identical facts to the ATC and Brick cases above. Similarly, email was used to trick an employee into transferring funds (in this case, over \$4M) to the hacker. The distinguishing fact was that the insured used the Google email service Gmail, which the hackers tricked into displaying the appropriate credentials / photo to the Medidata employee. The presence of that malware being used to deceive the computer system, as opposed to the hackers simply deceiving the employees was enough for that court to find coverage.

U.S. District Court of Eastern Michigan: No Coverage in Whaling Attack

In March 2015, American Tooling Center (ATC) [received an email](#) purportedly from a business partner, updating their banking information and requesting payment. The email was in fact from a hacker, using an email address that appeared to be legitimate, but in actuality replaced an “m” with “rn”. ATC wired \$800k to the hackers account, later discovered the error, and made a claim to Travelers on the Computer Fraud section of their Crime Policy. The Court found a lack of direct causation: the policy protects against the use of a computer to fraudulently transfer money, but the fraudulent emails had not directly caused the transfer of funds, and it was in fact the insured themselves who transferred the money.

CareFirst Class Action Suit Reinstated, to be Appealed

In August, 2017, a three-judge panel of judges for the U.S. Court of Appeals in D.C. declined to affirm the District Courts' dismissal of the lawsuit, which arises from a June 2014 breach affecting the data of 1.1M users. The District Court dismissed the case in September 2016 on familiar grounds in this arena: the mere theft of data did not amount to an actual, present injury, or a likely future injury. The Circuit Court - following the trend of more recent decisions - [did not dismiss the case at this stage](#). Thus, the circuit split on the issue continues as the courts struggle to define what the Supreme Court intended in this arena by requiring a "concrete and particularized" injury in their Spokeo decision. Now, the Supreme Court will have an opportunity to clarify that stance: CareFirst filed an appeal on August 31st and the [Circuit Court as stayed their ruling](#) pending a decision from the Supreme Court whether they will hear the case.

Three Class Action Lawsuits Spring From COPPA

[Three new class action suits](#) have been filed based on alleged violations of the Children's Online Privacy Protection Act (COPPA). All three were brought in the Northern District of California, and push the envelope of existing case law: COPPA provides no private right of action, so the allegations focus on violations of reasonable expectations of privacy. As courts have been seen to soften the requirements for Article III standing in data breach cases, more of these types of "test" cases are being filed.

Yahoo Data Breach Litigation to Proceed

The U.S. District Court for Northern California ruled that the plaintiff's in the long-standing class action lawsuit had alleged risk of future ID theft as well as the loss of value of their personal information, such that they [satisfied Article III standing](#). The breaches occurred between 2013 and 2016 and exposed information on over 1 billion users. The breach was first exposed in 2016, coming to light amid Verizon's purchase of Yahoo and causing a significant drop in the purchase price.

YAHOO!



Cyber Studies & Trends

- Cisco Midyear Cybersecurity Report
- IBM / Ponemon 2017 Cost of a Data Breach report



Contacts

Kara Owens

Global Head of Cyber Risk
1.212.365.2340
kowens@transre.com

Lauren Markowski

Cyber Risk Underwriter
1.212.365.2301
lmarkowski@transre.com

Miguel Canals

Cyber Risk Underwriter
1.212.365.2266
mcanals@transre.com

Calum Kennedy

Vice President
44 (0) 20 7204 8645
ckennedy@transre.com

Rhett Hewitt

Cyber Risk Underwriter
44 (0) 20 7204 8676
rhewitt@transre.com

Peter Cridland

Assistant Vice President
1.212.365.2032
Pcridland@transre.com

Alex Bustillo

Cyber Risk Underwriter
1.212.365.2379
abustillo@transre.com

*To receive future editions of the TransRe Cyber Newsletter,
please [CLICK HERE](#) and include your name, title,
and organization in the body of the email.*

Disclaimer

The material and any conclusions contained in this document are for information purposes only the authors offer no guarantee for the completeness of its contents. The statements in this document may provide current expectations of future events based on certain assumptions. These statements involve known and unknown risks, uncertainties and other factors which are not exhaustive. The authors of this document undertake no obligations to the publicity revise or update any statements, where as a result of new information, future events or otherwise and in no event shall TransRe or any of its affiliates or employees be liable for any damage and financial loss arising in connection with the use of the information relating to this document. Although TransRe makes reasonable efforts to obtain reliable content from third parties, TransRe does not guarantee the accuracy of or endorse the views or opinions given by any third party. This document may point to websites or other documents; however TransRe does not endorse or take responsibility for the content on such websites or other documents.