VERITEXT LEGAL SOLUTIONS

Are You and Your Insurer Connecting on Cyber Risk?

HB LITIGATION CONFERENCES

Northeast Corporate Counsel Forum 2016

April 21, 2016 | Atlantic City

Speakers

Kate Browne
Swiss Re
Kate_browne@swissre.com

Evan Fenaroli
Philadelphia Insurance Companies
Evan.fenaroli@phly.com

Laura Foggan
Wiley Rein LLP
lfoggan@wileyrein.com

Vince Vitkowsky
Seiger Gfeller Laurie LLP
vvitkowsky@sgllawgroup.com

We will address the principal “cyber” risks faced by businesses, which are lost data, network disruption, data breaches of personal and confidential information, and fraudulently induced electronic funds transfers.

- Potential coverage under CGL policies
- Potential coverage under crime and fidelity policies
- Coverage under cyber insurance and related products
- The Role and Importance of the Policyholder Advocate
- Current developments in technology and the evolving nature of cyber risks
- Gray areas concerning war and terrorism

VERITEXT
LEGAL SOLUTIONS

Potential Coverage Under
CGL Policies

HB LITIGATION CONFERENCES

General Liability – Overview

- Policyholders seek to obtain CGL coverage for private suits following a data breach, as well as for their substantial exposures under agreements that may allow credit card processors such as Visa, Discover and MasterCard to impose charges on them in the event of a data breach.
- Courts have split on these issues.
- Both Coverage A (Property Damage) and Coverage B (Personal and Advertising Liability) are being tested in litigation.

General Liability – Coverage A: (cont'd)

- Most CGL policies afford coverage for "those sums that the insured becomes legally obligated to pay as damages because of … 'property damage' to which this insurance applies."

- "Property damage" is defined to mean "physical injury to tangible property, including all resulting loss of use of that property" and "loss of use of tangible property that is not physically injured."

General Liability – Coverage A: (cont'd)

- Under CGL policies issued before 2001, a split of authority existed as to whether electronic data constituted "tangible property."
  - Am. Online, Inc. v. St. Paul Mercury Ins. Co., 207 F. Supp. 2d 459, 466 (E.D. Va. 2002) ("Computer data is not tangible property."), aff'd, 347 F.3d 89 (4th Cir. 2003).
  - State Auto Prop. & Cas. Ins. Co. v. Midwest Computers & More, 147 F. Supp. 2d 1113, 1116 (W.D. Okla. 2001) ("Alone, computer data cannot be touched, held or sensed by the human mind; it has no physical substance. It is not tangible property.").
  - Computer Corner, Inc. v. Fireman's Fund Ins. Co., 46 P.2d 1264 (N.M. Ct. App. 2002) (finding coverage for suit for loss of data from reformatting hard drive; "computer data is tangible property").
  - Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc., No. CIV. 99-185 TUC ACM, 2000 WL 726789 (D. Ariz. Apr. 18, 2000) (concluding that loss of data on computer network constituted "property damage").
- More recently-issued CGL policies specifically provide that "electronic data is not tangible property." See ISO Form No. CG 00 01 10 01 (added in 2001).

General Liability – Coverage A: (cont'd)

- However, more recent CGL policies eliminate coverage for "[d]amages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." See ISO Form No. CG 00 01 12 04 (added in 2004).

- Assuming this exclusion is applied as written, Coverage A should not afford coverage under post-2004 policies with this exclusion regardless of how the definition of "property damage" is construed.

General Liability – Coverage B

- Policyholders have also sought coverage under “Coverage B,” which covers “those sums that the insured becomes legally obligated to pay as damages because of ‘personal and advertising injury.’”

- “Personal and advertising injury” is defined to include “injury … arising out of one or more of the following offenses: … [o]ral or written publication, in any manner, of material that violates a person's right of privacy.”

General Liability – Coverage B (cont'd)

- Policyholders are testing whether at least some types of claims arising from a data breach (e.g., alleged failure to secure private data adequately) can fall under the "personal or advertising injury" coverage found in CGL policies.

- There are many coverage issues posed by these cases, and the early court rulings are mixed.

General Liability – Coverage B (cont'd)

- ISO issued a set of exclusions to be included in CGL policies in May 2014 that bar coverage for claims "arising out of any access to or disclosure of any person's or organization's confidential or personal information" as confirmative of the intent that CGL policies are not written to cover suits arising from data breaches.

- However, these exclusions may take some time to make their way into CGL policies and – even after they have been utilized – and policyholders likely will seek to litigate the scope of this exclusion in specific instances.

General Liability – Coverage B (cont'd)

- The early cases addressing data breach, privacy and other cyber claims under CGL coverage are mixed.

- To the extent coverage is found, it has been limited to certain fact settings and to certain types of exposures. CGL coverage plainly does not encompass all data breach, privacy and cyber losses – even when courts find some coverage.

General Liability – Coverage B (cont'd)

- Hartford Cas. Ins. Co. v. Corcino & Assocs., No. CV 13-3728 GAF (JCx), 2013 WL 5687527 (C.D. Cal. Oct. 7, 2013).
  - Insured allegedly posted "private, confidential, and sensitive medical and/or psychiatric information" on a public website, which remained online for almost a full year. Patients brought class actions which sought, among other relief, statutory damages of $1,000 per person under the California Confidentiality of Medical Information Act ("CMIA") and statutory damages of up to $10,000 per person under the California Lanterman Petris Short ("LPS") Act.
  - Insurers contended coverage was barred under an exclusion for "Personal And Advertising Injury ... [a]rising out of the violation of a person's right to privacy created by any state or federal act." However, the court found that "the plaintiffs in the underlying cases seek remedies for breaches of privacy rights that were not themselves 'created by any state or federal act,'" but which exist under common law and the California state Constitution.
  - The court also rejected Hartford's argument that the statutory penalties were not covered "damages" because of "personal and advertising injury," finding that "[t]he statutes … permit an injured individual to recover damages for breach of an established privacy right, and as such, fall squarely within the Policy's coverage."

General Liability – Coverage B (cont'd)

- Travelers Indem. Co. v. Portal Healthcare Solutions LLC, 14-1944 (4th Cir. Apr. 11, 2016) (unpublished).
  - Insured allegedly failed to safeguard confidential medical records from being viewed on a public website, and two patients (who later sued) alleged that they were able to access their own records by way of a Google search.
  - Trial court found a duty to defend based on potential coverage for "unreasonable publicity" to and "disclosure" of information about patients' private lives. It found "publication" to arguably include records "place[d] before the public," and a potential for coverage based on the underlying allegations, even though the insured took no steps designed to disclose or publish the information and there was no evidence it was viewed by any third party.
  - The Fourth Circuit affirmed the trial court's determination that the complaint at least potentially or arguably alleged conduct covered under the Policies.

General Liability – Coverage B (cont'd)

- Zurich Am. Ins. Co. v. Sony Corp. of Am., No. 651982/2011 (N.Y. Sup. Ct. Feb. 21, 2014).
  - Sony's PlayStation Network was hacked in April 2011. The hackers stole personally-identifiable information of over 77 million users, one of the largest data breaches in history.
  - Sony argued that hackers' theft of personal information fell within the Coverage B offense of "oral or written publication in any manner of material that violates a person's right of privacy."
  - The court ruled that coverage was not triggered where the alleged "publication" was not an intentional act committed by the insured, but instead was the result of a criminal act of a third party hacker. The "oral or written publication" offense requires "an act by or some kind of act or conduct by the policyholder in order for coverage to be present," it held.
  - The case settled on appeal to New York intermediate appellate court.

General Liability – Coverage B (cont'd)

- Recall Total Info. Mgmt., Inc., v. Federal Ins. Co., 115 A.3d 458 (Conn. 2015)
  - Insured transport vendor allegedly lost data tapes containing sensitive data on a large number of employees. Those tapes allegedly were recovered by a third party, but there was no evidence that the information on the tapes was ever accessed. The main "damages" sought were the costs of notification and remedial measures allegedly taken by the party who owned the data tapes.
  - Court ruled that there was no "publication" absent evidence that information on the tapes was ever accessed, noting that the communication of information to a third party was required to trigger coverage.
  - The court also held that triggering a breach notification statute does not demonstrate personal injury as such statutes "merely require notification to an affected person so that he may protect himself from potential harm."

VERITEXT
LEGAL SOLUTIONS

Fidelity and Crime Policies

HB LITIGATION CONFERENCES

- Fidelity and crime policies often expressly exclude coverage for the theft of data or information.

- They are sometimes broadened to include computer crime. When they are, coverage is often limited to the recollecting or restoring damaged or corrupted data

- The interpretation of crime policies which also insure against computer fraud has arisen in several cases in which employees have been tricked into making improper transfers of funds or assets through “social engineering, i.e., the manipulation of humans into performing acts or divulging confidential information. These are sometimes referred to as Business Email Compromises, or B.E.C.s.

- Apache Corporation v. Great American Ins. Co., 2015 WL 7709584 (S.D.Tex. Aug. 7, 2015) .
  - Found coverage for a social engineering induced transfer of funds under a Crime Protection Policy which insured against “loss . . . resulting directly from the use of any computer to fraudulently cause a transfer of [money] from inside the premises”
  - Texas law
  - Rationale: the phrase “resulting directly from” is synonymous with a “cause in fact,” which in turn means the act in question “was a substantial factor in bringing about the injuries, and without it, the harm would not have occurred.” The court rejected the argument that only fraud perpetrated through a direct “hacking” would be covered. This case is on appeal to the Fifth Circuit.

- Pending case: Medidata Solutions, Inc. v. Federal Ins. Co., No. 1:15-cv-00907 (S.D.N.Y., filed February 6, 2015).
  - Also involves a claim for social engineering induced transfer under a crime policy providing coverage for Computer Fraud, defined as “fraudulent entry of data into . . . a Computer System” or a “fraudulent change of data elements . . . of a computer system.”
  - Insurer argues that there was a voluntary transfer by authorized users. It says its policy only covers manipulation or unauthorized entry into a computer system, and involuntary transfers effected by hackers, forgers or impostors.
  - Last month, the court denied cross-motions for summary judgment, and granted leave to conduct expert discovery. The discovery is “to be limited to establishing the method in which the perpetrator sent its emails to [Mediator] and discussing what changes, if any, were made to [Mediator’s] computer systems when the emails were received.”
  - If the case proceeds to a further decision, it could provide significant insight into the facts and analysis that would inform future computer-related coverage disputes.

- Universal Am. Corp v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA, 25 N.Y. 3d 675 (2015).

  - Found no coverage under a financial institutions bond for losses arising when authorized users allegedly submitted over $18 million in fraudulent claims directly into an insurer's computer system.
  - New York law
  - Rationale: The Bond provided coverage for losses incurred through unauthorized access to the computer system, i.e., deceitful and dishonest acts of outside hackers, but not to fraudulent information entered by authorized users.

Coverage for social engineering funds transfers losses are addressed in various ways.

- Voluntary Parting exclusions
- Coverage provided by endorsements to crime policies
- Cyber insurance underwriters are considering options

- Data Breach Case: Retail Ventures, Inc. v. National Union Fire Ins. of Pittsburg, Pa., 691 F.3d 821 (6th Cir. 2012)

  - Found coverage under a Blanket crime Policy with a Computer Fraud Rider for $5.3 million in first-party costs arising from a hacker's data breach of a retailer. Damages included visa and MasterCard assessments and fines.
  - Ohio law
  - Rationale: The insurer did not dispute that the unauthorized access and copying of customer information involved the "theft of an insured property by Computer Fraud," It disputed whether the losses resulted "directly from the theft . . . By computer fraud. The court applied a proximate cause standard, meaning the losses were covered even if they did not result "solely" or "immediately" from the theft itself. The court also declined to apply an exclusion for the loss of "other confidential information of any kind."

VERITEXT
LEGAL SOLUTIONS

Coverage Solutions
Cyber Products and Beyond

HB LITIGATION CONFERENCES

Coverage Solutions

- Cyber or Data Breach endorsements to traditional package/CGL policies generally provide limited coverage and low sub-limits

- Dedicated coverage for a variety of cyber perils and privacy risks can be found in the following types of products, which are sometimes combined into a single policy:
    - Technology Errors & Omissions
    - Media Liability
    - Crime/Fidelity
    - Cyber

Tech E&O

- May be covered on a stand-alone policy or as part of a comprehensive cyber risk policy
- Addresses exposures arising from an entity's technology services (consulting, customer software development, etc.) and products (software and hardware)
- Coverage is triggered by claims or suits arising out of an actual or alleged negligent act, error or omission
- Coverage for both defense costs and damages, judgments, or settlements

Media Liability

- Media policies are typically written on a “named perils” basis and cover defamation, intellectual property infringement (copyright, trademark, domain name, etc.), invasion of privacy and plagiarism. Patent infringement is usually excluded from standard products.

- Traditional stand-alone Media policies may be written to cover only specific content such as written works or films, but may also cover a full range of content, whether written or electronic.

- When included as part of a cyber liability product, media coverage may only apply to “electronic media,” often defined as content displayed on an insured’s website or via social media.

Crime/Fidelity

- Most stand-alone crime products include coverage for Computer Fraud and Funds Transfer Fraud, although these insuring agreements may also be included in a cyber product.

- Coverage for first party loss of money or securities as a result of Social Engineering may also be addressed by or endorsed onto Crime or Cyber policy.

- With respect to Social Engineering, it is important to understand that it can be used to include individuals to divulge information (including login credentials, PII or other sensitive information) or to transfer funds. Insurance coverage is available for both risks, but typically within different insuring agreements or even on different policies.

Cyber Insurance Products

- While stand-alone cyber products may include the aforementioned Tech E&O, Media and Crime coverage, most forms have evolved to include the following “core” coverage:
  - First Party Loss, including:
    - Data Breach Response / Security Event Costs
      - Attorney/”Breach Coach” fees, forensic review, notification costs, credit monitoring, public relations etc.
    - Business Interruption / Contingent Business Interruption
    - Data Loss / Data Restoration
    - Cyber Extortion
  - Third Party Liability, including
    - Network Security & Privacy Liability
    - Regulatory Defense / Fines / Penalties

Where else may coverage exist?

- Professional Liability / Miscellaneous E&O
  - Whenever the safeguarding of sensitive or private client/customer data is inherent to the professional services being rendered, coverage may exist in the event of an actual or alleged privacy breach (i.e. Accounting Firms, Law Firms, Financial Advisors)
  - Important to look for data or privacy breach exclusions, sub-limits or other limitations; for example, unless specifically endorsed, first party breach response costs are not likely to be covered

- Directors & Officers Liability (D&O)
  - Possibility that negative fallout from a cyber breach could trigger class actions and other D&O claims, especially if and when stock prices are affected.
  - Increasing need for boards to be aware of enterprise cyber security and take reasonable steps to mitigate risks

The Role and Importance of the Policyholder Advocate

VERITEXT
LEGAL SOLUTIONS

A Whole New World

HB LITIGATION CONFERENCES

Hacking 101

- Active Hacking Via Network Penetration – Software attack on a computer system that looks for security weaknesses, potentially gaining access to the computer's features and data.
- Active Hacking – Social Engineering
    - Baiting with “free” items
    - Phishing/spearphishing
    - Physical access, old printers, and the Raspberry Pi
    - Badge cloning
- Passive Hacking –Using information about a target that is on the internet with or without the target’s knowledge “googleDorks”

Cracking Wi-Fi passwords, spoofing accounts, and testing networks for exploits is all fun enough, but if you want to take the show on the road, you'll want an easily portable rig. Enter Kali Linux and the Raspberry Pi.

Why and Who Are the Weak Links?

- Lack of training
- Incredibly sophisticated attacks i.e. fake Chinese law firms and banks with web sites identical to what you find in the US and Canada
- Insufficient Controls/Override of Controls
- Email Technology and Lack of Workflow
- Verizon's 2015 Data Breach Investigations Report found that a company's legal department was "far more likely to actually open [a phishing] e-mail than all other departments."
- People are trusting. We regularly form relationships of trust with our clients, our colleagues and other lawyers. So we respond freely to an e-mail that looks like it comes from that trade group or that bank.
- People are responsive. We don't always think before we click.
- We may sometimes overestimate our tech skills — humility is not always our strong suit and stopping to ask our IT departments for advice isn't always our first response.

Not a Good day at the Office

- Hollywood Hospital CEO Allen Stefanek: “The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key.”
- The hospital that had its electronic patient records hacked and held hostage chose to pay $17,000 in bitcoin to retrieve the ransomed records.
- According to the Christian Science Monitor, one variety of ransomware called CryptoWall collected nearly $2 billion worth of ransoms by 2015.
- According to a report by antivirus software creator Symantec, ransomware attacks in 2013 rose from 100,000 per month to 600,000 a month by the end of the year.

When Are You “Using a Computer”

- InComm Holdings Inc., a provider of prepaid cards and payment networks sued Great American Insurance Company in a Georgia federal court claiming the insurance company wrongfully denied coverage for a cyberattack on its systems that resulted in more than $11 million in losses.
- InComm contends that its $10 million crime protection policy with Great American provides coverage for computer fraud.
- InComm customers can add money to their cards by buying a chit from a retail store, which is then redeemed online. Once the chit is redeemed, InComm transfers the funds to a bank account that’s held in the name of the third-party issuer of the card, which makes the funds available to the customer.
- In May 2014, InComm discovered that hackers were breaking into its system and fraudulently submitting multiple, simultaneous requests to redeem individual chits. “Due to the reload chit fraud, InComm incurred a loss of $11,471,407 as a result of approximately 25,521 duplicate fraudulent redemptions of 2,396 individual reload chits.”

- InComm said that its policy with Great American provides coverage for losses from computer fraud, According to InComm, “.., the reload chit fraud was in fact carried out through the use of a computer because InComm’s ... system is computer-based and serves as a gateway to the core transaction processing system at InComm for the transactions at issue. Because this transaction processing system is meant to process chits only once, the multiple, simultaneous requests submitted by the hackers constituted an unauthorized use of InComm’s system.”
- InComm claims its seeking coverage for its own, first-party loss — the amounts transferred and stolen because of the reload chit fraud
- Great American’s denial letter contends that the loss wasn’t caused by “the use of any computer."
- Great American also argued that the fraud scheme did not cause money to be transferred to an outside party and InComm’s losses were not caused by the fraud, but instead its contractual liability to Bancorp to fund the customer accounts.
- InComm Holdings Inc. et al v. Great American Insurance Company, in the U.S. District Court for the Northern District of Georgia.

“Fraudulently Causing a Transfer” v “Causing a Fraudulent Transfer”

- BitPay CFO Bryan Krohn received an email from a hacker claiming to be David Bailey, an executive for prominent digital currency publication yBitcoin, requesting a comment for an article. Mr. Krohn was directed to a website controlled by the hacker and provided credentials for his corporate email account, which the hacker then used to steal 5,000 bitcoins through three fraudulent transfers.
- By reading Krohn’s emails, the hacker learned that bitcoin purchaser Second Market didn’t require advance payment for bitcoin transfers. The hacker then posed as Krohn in messages to the CEO of Second Market, whom the hacker persuaded to make transfers into an account he controlled.
- In its denial letter, Massachusetts Bay told BitPay that its policy’s computer fraud provision only covers money lost as a direct result of a cyberattack using BitPay’s computer system to fraudulently cause a transfer, and claimed the $1.85 million BitPay lost was actually the indirect result of a hack targeting Bailey, the yBitcoin executive.
- Massachusetts Bay distinguished between fraudulently causing a transfer and causing a fraudulent transfer, the latter of which the insurer said more accurately described the chain of events leading to BitPay’s losses, and said the bitcoins weren’t covered because they weren’t physically in BitPay’s offices.

- BitPay responded that it had suffered a direct financial loss due to the attack, and sharply criticized its insurer for using the digital currency's lack of physical properties as a means of denying coverage.
- "Unlike traditional money, bitcoin does not exist in physical form in any location or premises, and it cannot be transferred from or to any physical location," BitPay said in a letter to the insurer. "Accordingly, any agreement to insure bitcoin that purportedly requires bitcoin to be on BitPay's premises is illusory."
- BitPay Inc. v. Massachusetts Bay Insurance Co., case no. in the U.S. District Court for the Northern District of Georgia.

Columbia Casualty v Cottage Health

- Do you check for security patches on your systems at least weekly and implement them within 30 days?
- Do you replace factory default settings to ensure your information security systems are securely configured?
- Do you re-assess your exposure to information security and privacy threats at least yearly, and enhance your risk controls in response to changes?
- Do you outsource your information security management to a qualified firm specializing in security or have staff responsible for and trained in information security?
- Whenever you entrust sensitive information to third parties do you…

  a. contractually require all such third parties to protect your information with safeguards at least as good as your own,

  b. perform due diligence on each such third party to ensure that their safeguards for protecting sensitive information meet your standards (e.g., conduct security/privacy audits or review findings of independent security/privacy audits),

c. audit all such third parties at least once per year to ensure that they continuously satisfy your standards for safeguarding sensitive information,

d. require them to have sufficient liquid assets or maintain enough insurance to cover their liability arising from a breach of privacy or confidentiality?

- Do you have a way to detect unauthorized access or attempts to access sensitive information?
- Do you control and track all changes to your network to ensure it remains secure?
- Cottage Health suffered a breach involving 32,500 confidential medical records between Oct 8, 2013, and Dec. 2, 2013. The breach allegedly occurred because Cottage and/or its third-party vendor stored medical records on a system that was fully accessible to the Internet but failed to install encryption or take other security measures to protect patient information.
- Paid 4.1M to settle class actions

- Columbia Casualty issued a NetProtect360 claims-made policy to Cottage that was in effect from Oct. 1, 2013, to Oct. 1, 2014. The policy provided coverage for privacy injury claims and privacy regulation proceedings, with limits of $10 million per claim and in the aggregate, subject to a $100,000 deductible. The policy contains an exclusion that precludes coverage for “failure to follow minimum required practices.”
- According to CNA, Cottage's Internet servers “permitted anonymous user access, thereby allowing electronic personal information to become available to the public via Google's Internet search engine”.
- The hospital system failed to “continuously implement the procedures and risk controls identified” in its insurance application.
- The data breach was caused by its “failure to regularly check and maintain security patches on its system, its failure to regularly reassess its information security exposure and enhance risk controls, its failure to have a system in place to detect unauthorized access or attempts to access sensitive formation stored on its servers and its failure to control and track all changes to its network to ensure”.

Rise of the Bitcoin

- Developed in 2009, Bitcoin is the most widely used digital currency in the world.
- Exists only as a long string of numbers and letters in a user's computer file, using public and private key encryption and a network of computers to conduct and verify transactions.
- As of November 1, 2013 there were over $11.8M bit coins in circulation
- February 2011: 1 BTC=$1
- Nov. 13, 2013: 1 BTC=$392
- January 7,2014-1 BTC=$1,093
- February 24,2014-1 BTC= $560
- May 4, 2015 -1 BTC=$241
- Sept 2015- 1BTC= $289

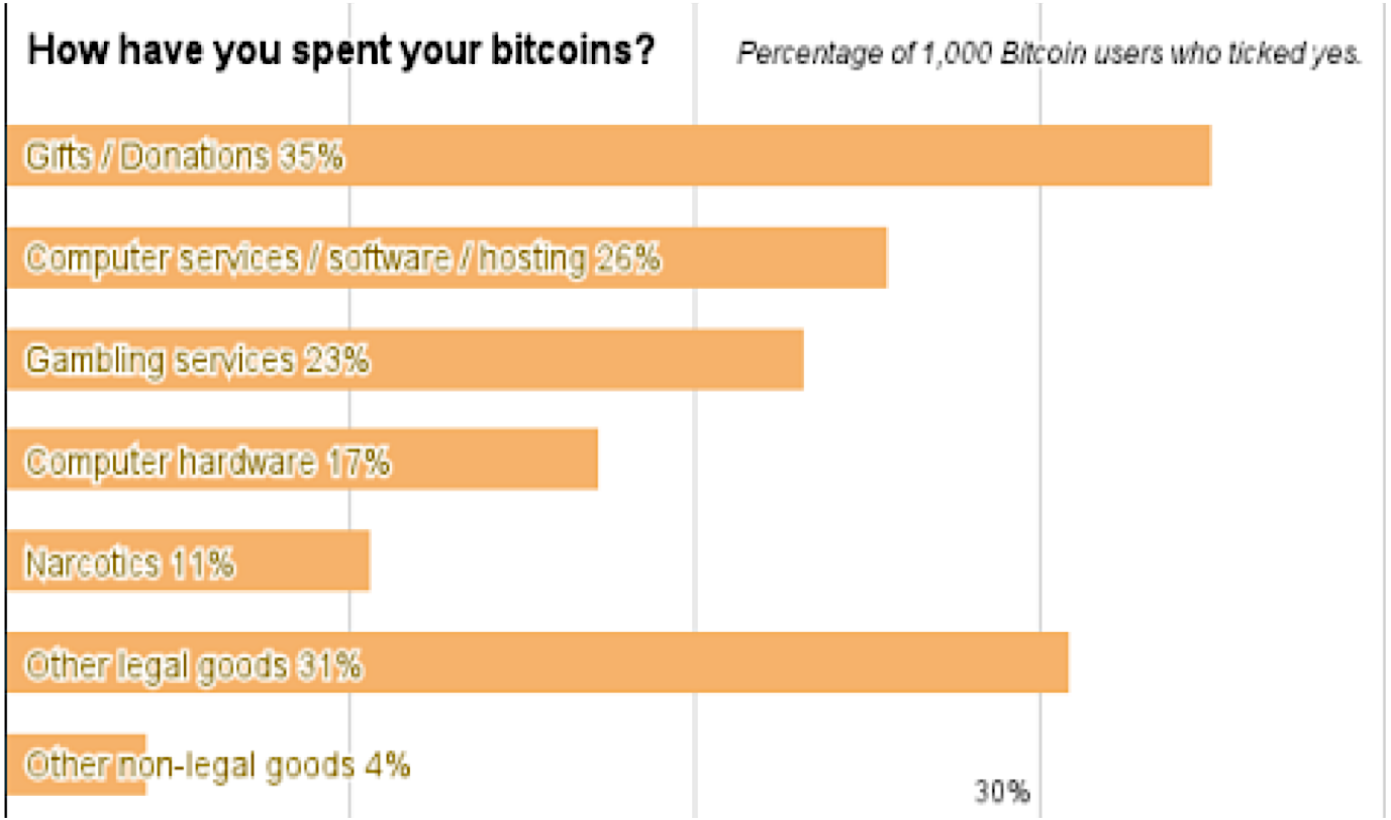
How Do You Mine a Bitcoin?

- Bitcoins are created and entered into circulation through a process called "mining“, performed by members of the bitcoin network.
- Miners download software used to solve extremely complex mathematical problems, which verify the validity of past bitcoin transactions to insure there is no double spending.
- When a miner's computer solves an equation, the Bitcoin network creates 25 new bitcoins and awards them to the miner.
- There can only be a maximum of 21 million bitcoins in circulation, with the last one scheduled to be mined in 2140.
- The rate of mining is controlled by the complexity of the mathematical problems.

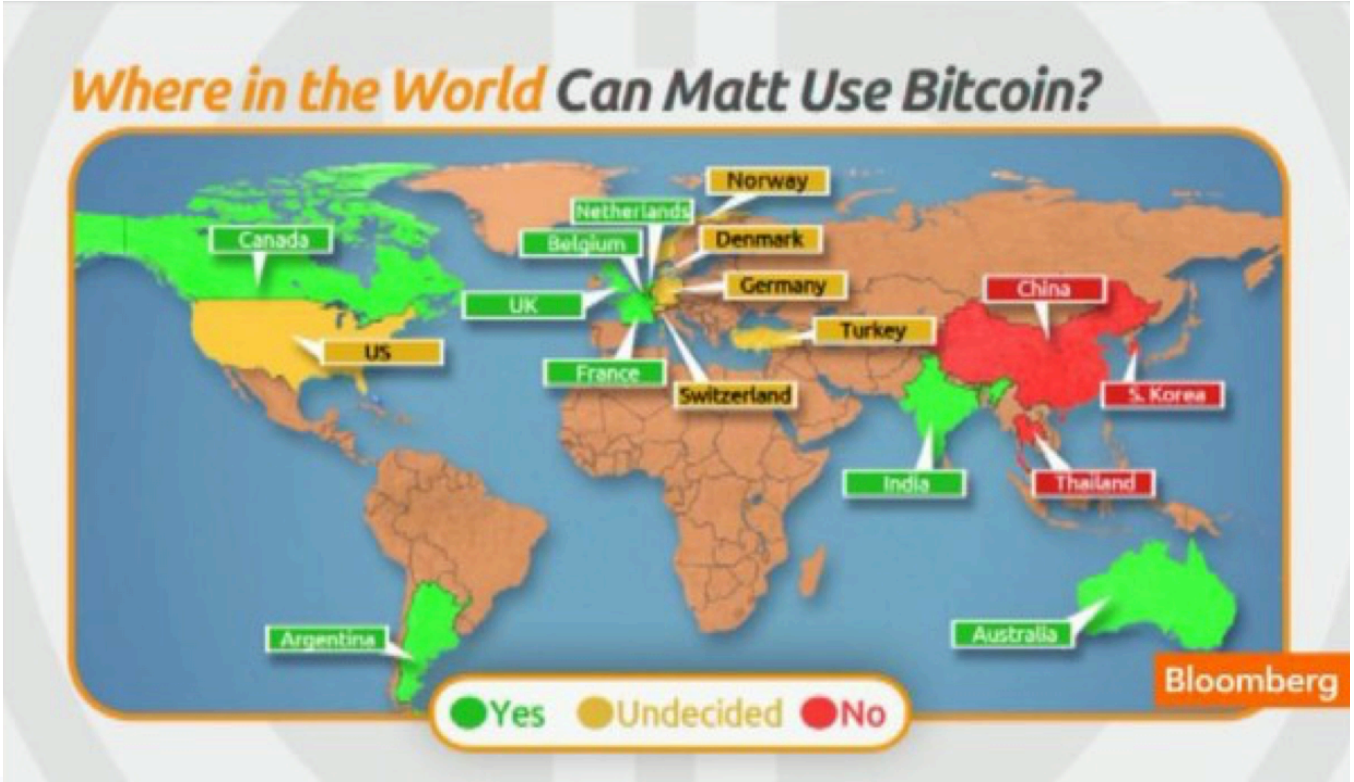
It’s the Blockchain that Matters!

- Bitcoins are sent from a "bitcoin wallet" to the Bitcoin address of the other person via computer or smartphone. Recipients need a private key to access their bitcoins.
- After a transaction has been conducted, the Bitcoin network verifies the transaction and ensures that the same bitcoin has not been spent twice.
- A decentralized peer-to-peer payment network and a virtual currency that essentially operates as online cash.
- The block chain allows people to reliably exchange funds on the Internet without relying on a third party, such as a bank or PayPal.

Anonymous – Public Transactions!!!!


How have you spent your bitcoins?
Percentage of 1,000 Bitcoin users who ticked yes.
Gifts / Donations 35%
Computer services / software / hosting 26%
Gambling services 23%
Computer hardware 17%
Narcotics 11%
Other legal goods 31%
Other non-legal goods 4%
30%

Where?


Where in the World Can Matt Use Bitcoin?
Norway
Netherlands
Canada
Belgium
Denmark
Germany
China
UK
Turkey
US
France
Switzerland
S. Korea
India
Thailand
Argentina
Australia
Bloomberg
Yes
Undecided
No

Regulations

- Germany – bitcoin is "a unit of account" officially recognized it as money taxable under capital gains laws
- Hong Kong – bitcoin is virtual currency can be traded privately or online but is not electronic currency or a form of money
- Canada – bitcoin is virtual currency that can be used to buy or sell goods and can be taxed (1) transactions for goods & services taxed as barter transaction rules (2) profits on commodity transactions are income or capital
- Isle of Man – "… banks, service providers, landlords and technology companies on the island can all be confident that digital currency development has full government support and the FSC is not going to penalize anyone for engaging in the sector."
- Spain – "bitcoins are cash"
- UK – Bank of England "interesting technology"

Will It Be Covered?

- Is a virtual currency an asset, a security, a commodity or a medium of exchange?
- Is the loss of a crypto coin – "loss of tangible property"?
- "We will pay for loss or damage to ‘money, securities or other property’"
- We will pay for loss of "funds."
- Money means "currency, coins and bank notes in current use and having a face value".
- Funds means "monies or securities"
- Securities means "negotiable and non-negotiable instruments or contracts representing either money or property and includes tokens, tickets, revenue and other stamps… evidence of debt issued in connection with credit or charge cards”


6
Cold
Cold

Virtual Stores Are The New Business Model in Asia

- South Korea was first in 2011 – Homeplus, the nation's second largest discount chain, offered 500 images of items at its "store" at Seolleung subway station. Shoppers download app on their smartphone and make purchases by taking photos of the barcodes. Products delivered to home or office same day.
- Hong Kong – 5500 types of goods are available in aeoncity.com.hk mobile site for shoppers to choose from.
- Indian online retailer Yebhi.com has opened virtual stores at 30 Cafe Coffee Day outlets in Delhi and Bangalore.
- Costco will open a single "virtual" store in China and only sell its items online. Costco will sell items on Tmall, a website operated by Alibaba.
- A new report from the McKinsey Global Institute (MGI) on China's digital transformation: "The Internet's impact on productivity and growth projects that new Internet applications could fuel some 7 to 22 percent of China's incremental GDP growth through 2025, depending on the rate of adoption. That translates into 4 trillion to 14 trillion renminbi in annual GDP in 2025".
- Frost and Sullivan – Singapore was the largest e-commerce market in South-east Asia last year, generating revenues of US$1.7 billion (S$2.1 billion)

Possible Impact

- No bricks & mortar means no need for first party property insurance
- No worries about slips and falls or labor relations
- Major boost to residential parcel delivery services
- Retail shippers need to have at multiple freight carriers on the lanes they're moving freight. If they elect to leverage intermodal for larger products, they need to make sure that they have a distribution center (DC) that's served by rail so they can cross-dock and locally transfer freight as needed.
- Disputes in cyberspace? Its been decades and we still don't know:
  - Which law applies to the e-transaction? Which authority has jurisdiction over the dispute? Which forum is competent to hear dispute? Is the decision enforceable?
- Does the world need international agreements and transborder or dispute settlement mechanisms designed specifically for electronic transactions?
- Still confusion over diverse areas as taxation and customs duties, the legal status of e-signatures and the distinction between products and services.

Legal Notice

The information and opinions contained in the presentation are provided as at the date of the presentation and are subject to change without notice. Although the information used was taken from reliable sources, Swiss Re does not accept any responsibility for the accuracy or comprehensiveness of the details given. All liability for the accuracy and completeness thereof or for any damage or loss resulting from the use of the information contained in this presentation is expressly excluded. Under no circumstances shall Swiss Re or its Group companies be liable for any financial or consequential loss relating to this presentation.

VERITEXT
LEGAL SOLUTIONS

Potential War and Terrorism Scenarios

HB LITIGATION CONFERENCES

Scenarios to Consider

- Personal information of two million customers of a large retailer is revealed online. A hacktivist collective claims credit and says that it has customer information from five more retailers. Unless the USG allows Edward Snowden back into the US with a promise not to prosecute, it will reveal the rest. The USG does not comply, and the data is made available.

- Same scenario, except the act is to disable medical devices in hospitals throughout the country, resulting in deaths.

- The USG learns that the Syrian Electronic Army is planning to try to shut down the New York Stock Exchange. It preempts the attack by inserting a malicious code into the hostile computers. The malicious code inadvertently spreads to private commercial computers of Western banks in Dubai, rendering them permanently inoperable.

Scenarios to Consider

- Cyber Fighters of Izz ad-Din al-Qassam effectuates a series of fraudulent wire transfers from US banks to protest US assistance in developing and maintaining Israel's Iron Dome technology.

- Nightmare engages in data breaches, sells the information and gives the proceeds to ISIS. In response, a hacktivist group steals and releases data from the US branches of banks in Turkey and Quatar, countries they assert are funding Nightmare.

- A cyberattack on a communication network or emergency system greatly exacerbates the death and destruction from a traditional physical terrorist attack.

Speakers

Kate Browne
Swiss Re
Kate_browne@swissre.com

Evan Fenaroli
Philadelphia Insurance Companies
Evan.fenaroli@phly.com

Laura Foggan
Wiley Rein LLP
lfoggan@wileyrein.com

Vince Vitkowsky
Seiger Gfeller Laurie LLP
vvitkowsky@sgllawgroup.com