WHITE PAPER:
WHAT EVERY CISO NEEDS TO KNOW ABOUT
CYBER INSURANCE

Industry Experts Report:

What Every CISO Needs to Know About Cyber Insurance

Who should read this paper

CISOs and other leaders involved in cyber insurance decisions

Contributors

AIG HUNTON & WILLIAMS LEWIS BRISBOIS BISGAARD & SMITH LLP LOCKTON NetDiligence INFORM Global Integrated Communications THE COUNCIL

Symantec

Content

Introduction: The Evolving Threat Landscape

Written by: Samir Kapuria - Symantec

Decades ago, a group of merchants created a concept of general average—which is when all parties in a maritime venture share in losses resulting from a sacrifice of cargo in an emergency. What this group fashioned in 1890 was a method for merchants to insure their shipped goods. Upon landing, merchants whose cargo landed safely were expected to contribute a portion to merchants whose goods had been lost at sea. With this, an early form of insurance was born.

If we look at cybersecurity today, our information could be lost in a digital ocean we call the worldwide web. From a threat lens, the volume of attacks continues to rise as adversaries become more determined, persistent, and hostile with cyber attacks. Attackers will continue to:

- move faster and more efficiently,
- breach organizations with targeted campaigns,
- focus on consumers across social media, mobile, and connected platforms, and
- aim to take advantage of the emerging Internet of Things.

The impact of a cyber attack to an organization's brand, reputation, and business operations can be catastrophic.

The impact of a cyber attack to an organization's brand, reputation, and business operations can be catastrophic. Therefore, organizations need to plan proactively but prepare for the reactive, which includes insurance for goods, intellectual property (IP), and commerce—the assets sailing across the digital landscape. Welcome cyber insurance.

Symantec has partnered with key cyber insurance thought leaders to shed light on essential cyber insurance tenets and frequently asked questions we've received when engaging with organizations around the world. The business relevance of cyber is here to stay, and Symantec is here to help you lessen that risk for yourself and your organization.

Legislative and Regulatory Update

Written by: Amy Roberti - Council of Insurance Agents and Brokers

Where there's smoke there's fire—and where there's a crisis, there are state and federal lawmakers and regulators trying to be helpful. Major data breaches are in the news every day in both the private and public sectors. Experts are telling us we could experience a massive cyber terrorist event that could cause major market disruptions, and even physical damage to property and critical infrastructure. The general public is at the mercy of villainous cyber criminals who could cripple society with one malicious click of a mouse. So it makes sense that Congress and state and local governments would take a look at this risk and explore ways to help prevent cyber crime. They've even been looking at the burgeoning cyber insurance market and how cyber insurance could—as insurance has done throughout history with every type of coverage—encourage better, safer cyber behavior. To add to the frenzy, jurisdiction over cyber issues is broad. While legislation with the greatest chances of success has come out of the House and Senate Intelligence and Homeland Security Committees, approximately 15 committees in Congress have claimed at least some jurisdiction over cybersecurity issues. These include House Energy & Commerce and Senate Commerce; House Financial Services and Senate Banking; Science, Agriculture, Armed Services; and others…not to mention the Administration and the States. Here's a little taste of what they've been up to.

Congress

Since January 2015, the 114th Congress has seen a flood of data and cybersecurity bills introduced; however, most have failed to gain traction. The bills that are currently in play with the most potential to move forward are the cybersecurity information sharing bills—two have been passed by the House and one is under consideration in the Senate. In late April, the House voted on and passed two information sharing bills: HR 1560, the Protecting Cyber Networks Act, sponsored by Rep. Devin Nunes (R-CA), chair of the Intelligence Committee, and HR 1731, the National Cybersecurity Protection Advancement Act, sponsored by Rep. Mike McCaul (R-TX), chair of the Homeland Security Committee.[1] The goal of information sharing legislation is to help the public and private sectors, through a reciprocal process of sharing cyber threat indicators, improve their cyber defenses.

Progress on information sharing legislation has been slower in the Senate. The legislation with the greatest chance of success is S. 754, the Cybersecurity Information Sharing Act (CISA), which passed the Senate Intelligence Committee in April. CISA is sponsored by Intelligence Committee Chairman Richard Burr (R-NC) and has bipartisan support. This legislation would establish a process for reciprocal sharing of cyber threat indicators between the public and private sectors through the Department of Homeland Security.

This legislation would provide liability protections for private entities that share and/or receive such cyber threat indicators through this process and exempts that data from Freedom of Information Act (FOIA) requests.[2] CISA faces opposition from privacy advocates who fear that this is essentially a surveillance bill that allows the federal government to collect even more sensitive personal information on individuals.[3]

The goal of information sharing legislation is to help the public and private sectors, through a reciprocal process of sharing cyber threat indicators, improve their cyber defenses.

In June, Senate Republican leadership tried to add CISA to the National Defense Authorization Act (NDAA). That move was blocked, however, when the Senate voted 56-40 in favor of opening debate on CISA as an amendment to the NDAA, four votes short of the 60 needed to invoke cloture.[4] In a final attempt to vote on CISA before the August recess, Senate Majority

1- Eric A. Fischer and Stephanie M. Logan, Cybersecurity and Information Sharing: Comparison of H.R. 1560 and H.R. 1731 as Passed by the House (CRS Report No. R43996) (Washington, DC: Congressional Research Service, 2015), 1-29, http://fas.org/sgp/crs/misc/R43996.pdf.
2- Cybersecurity Information Sharing Act of 2015, S.754, 114th Congress, 1st Sess. (2015).
3- Nadia Kayyali, "Stop CISA: Join EFF in a Week of Action Opposing Broad "Cybersecurity" Surveillance Legislation," Electronic Frontier Foundation, July 27, 2015, accessed September 1, 2015, https://www.eff.org/deeplinks/2015/07/stop-cisa-join-eff-week-action-opposing-cyber-spying-0.
4- Cory Bennett, "Senate Democrats block cyber amendment," The Hill, June 11, 2015, accessed June 11, 2015, http://thehill.com/business-a-lobbying/244723-senate-moves-to-end-debate-on-cyber-amendment.

Leader McConnell filed cloture on CISA on August 3. Ultimately, Republican and Democratic leadership were unable to agree on a finite number of amendments, the clock ran out, and CISA was pushed to September or later.

Legislation creating one uniform, national standard for data breach notification would be a likely next candidate for action once information sharing is addressed.[5] Lawmakers could also attempt to attach a data security bill to a larger cybersecurity bill. There is considerable support from the business community to create such a standard, because the 47 disparate state reporting laws and regulations can make compliance burdensome and confusing for companies that have experienced a breach that affects consumers across multiple states. The House Energy and Commerce Committee passed a data breach bill, HR 1770, the Data Security and Breach Notification Act, which provides rules for how companies must protect personal data and notify customers if it is stolen. Republicans are still fine-tuning the measure, trying to win Democratic support. Notably, the bill passed out of committee on a party line vote, without the support of its only Democratic cosponsor. Any legislation that pre-empts state law, however, always faces a steep uphill battle in Congress and we are not likely to see action on such legislation this Congress.[6]

Hearings on cyber threats and the state of data security in the United States in various sectors, including two hearings on the breach at the Office of Personnel Management that exposed personnel records of tens of millions of federal employees, have continued throughout the year. Over two dozen cyber and data security-related bills have been introduced. We can expect to see many more cyber-related bills and hearings, as the issue straddles an astounding 15 committees in the House and Senate.

White House

The White House has been active on the cyber front as well. On January 13, 2015, President Obama sent three cybersecurity and data breach legislative proposals to Congress. Those included Enabling Public-Private Sector Information Sharing; Modernizing Law Enforcement Authorities to Combat Cyber Crime; and Creating a National Standard for Data Breach Notification.[7] In early February, the President announced the creation of the Cyber Threat Intelligence Integration Center (CTIIC)—based out of the Office of the Director of National Intelligence—which will "be a national intelligence center focused on 'connecting the dots' regarding malicious foreign cyber threats to the nation and cyber incidents affecting U.S. national interests, and on providing all-source analysis of threats to U.S. policymakers."[8]

On February 13, President Obama also convened a summit on "Cybersecurity and Consumer Protection" at Stanford University where he signed an Executive Order (EO). The EO, *Promoting Private Sector Cybersecurity Information Sharing,* encourages the development of Information Sharing and Analysis Organizations (ISAOs); develops a common set of voluntary standards for information sharing organizations; clarifies the Department of Homeland Security's authority to enter into agreements with information sharing organizations; streamlines private sector companies' ability to access classified cybersecurity threat information; and "ensures that information sharing enabled by this new framework will include strong protections for privacy and civil liberties."[9]

Department of Homeland Security

For the past several years, the Department of Homeland Security (DHS) has been bringing together insurance carriers, brokers, consumers, Chief Information Security Officers, and critical infrastructure to talk about cyber threats and how cyber insurance can and should play a role

5- Amy F. Davenport and Norma M. Krayem, "Data Breach Legislation Continues To Be A Congressional Priority," The National Law Review, May 11, 2015, accessed September 1, 2015, http://www.natlawreview.com/article/data-breach-legislation-continues-to-be-congressional-priority.
6- National Association of Attorneys General to the Congressional Leadership, July 7, 2015, http://www.naag.org/assets/redesign/files/sign-on-letter/Final%20NAAG%20Data%20Breach%20Notification%20Letter.pdf.
7- "Securing Cyberspace - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts," The White House, accessed January 20, 2015, https://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat.
8- The White House, Fact Sheet: Cyber Threat Intelligence Integration Center, February 25, 2015, https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center.
9- The White House, Executive Order -- Promoting Private Sector Cybersecurity Information Sharing, February 13, 2015, https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

in both mitigation and recovery. During the first four workshops, there was talk about creating a cyber incident repository to meet the industry's need for data on cyber risk. Despite the interest, DHS has no intention of establishing such a repository and instead hopes that by facilitating discussion among the private sector, some sort of private sector repository (or several repositories) may emerge.

In February of this year, the National Protection and Programs Directorate (NPPD) at DHS established a Cyber Incident Data and Analysis Working Group (CIDAWG), comprised of CISOs and CSOs from various critical infrastructure sectors, insurers, and other cybersecurity professionals, to deliberate and develop key findings and conclusions about:

1. The value proposition for a cyber incident data repository;
2. The cyber incident data points that should be shared into a repository to support needed analysis;
3. Methods to incentivize such sharing on a voluntary basis; and
4. A potential repository's structure and functions.

In July, the NPPD circulated a white paper entitled "The Value Proposition for a Cyber Incident Data Repository." The white paper is the culmination of the first charge. The CIDAWG will explore and report on the other three topics next.[10]

Treasury Department

The Treasury Department and the Federal Insurance Office (FIO) convened a meeting in November 2014 of mid-market carriers and brokers to talk about cyber insurance. FIO Director Michael McRaith proposed two ideas: (1) FIO wants to develop underwriting "principles" for cyber insurance policies; and (2) FIO wants to get more involved in risk mitigation. Director McRaith has stated that the federal government fully supports the insurance industry as they try to better protect themselves and quickly adapt to the ever-changing cyber threat landscape. Another Treasury official also indicated that Treasury is concerned there are no underwriting standards for cyber insurance. Given this concern, Treasury and FIO have been paying close attention to the burgeoning cyber insurance market.[11] Cyber is a regular topic of discussion at the Federal Advisory Committee on Insurance.

State Insurance Commissioners

The National Association of Insurance Commissioners (NAIC) formed a new Cybersecurity Task Force at their November 2014 meeting. This was the first foray into cybersecurity for the state regulators as a whole. The NAIC has been mainly focused on three areas:

1. Protecting their own data
2. Making sure that the entities they regulate are adequately protecting their own data
3. Monitoring the development of the cyber insurance market

The Cybersecurity Task Force, chaired by North Dakota insurance commissioner Adam Hamm, drafted a "Cybersecurity Bill of Rights" which outlines consumer "rights" regarding their personal, private information, how it should be handled, and what they are entitled to in the event that information is compromised.[12]The Task Force anticipates that the Bill of Rights will be distributed to consumers by their state insurance commissioners, but many companies and trades in the insurance industry have concerns that it could create consumer confusion by

10- Department of Homeland Security, The Value Proposition for a Cyber Incident Data Repository: Enhancing Resilience Through Cyber Incident Data Sharing and Analysis, June 2015, http://www.dhs.gov/sites/default/files/publications/dhs-value-proposition-white-paper-2015.pdf.
11- Mark Hollmer, "Feds Support Insurers Seeking Protection From Cyber Attacks," Claims Journal, April 9, 2015, accessed April 14, 2015, http://www.claimsjournal.com/news/national/2015/04/09/262735.htm.
12- "Cybersecurity Bill of Rights," The National Association of Insurance Commissioners, http://www.naic.org/documents/committees_ex_cybersecurity_tf_exposure_draft_cybersecurity_bill.pdf.

outlining so-called "rights" that are not codified in every (or any) state laws or regulations. The NAIC also intends to use portions of the Bill of Rights to update their model laws on privacy.

On April 16, the Cybersecurity Task Force adopted the "Principles for Effective Cybersecurity Insurance Regulatory Guidance." These twelve principles outline the types of safeguards regulators expect insurers and producers to have in place to protect consumer information from cybersecurity breaches.[13]

States

Forty-seven states, plus the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, have established "data breach notification" laws to better inform consumers when their personal information has potentially been stolen or compromised. While each statute varies, the laws generally require entities that own, license, or process personal information to notify affected parties when personal information is, or is believed to be, acquired without authorization. Many states make exceptions to notification requirements if the breach is not believed to have caused the affected party harm. State data breach notification laws establish standards on who gives and receives the notice, what information is considered personal or private information under the law, methods and timing for conveying the notice, content requirements that must be contained in the notice, and provides penalties for non-compliance of the law. California was the first state to implement a state date breach notification law, and many states have utilized its model to implement their own law. Below, we have highlighted three states as an example of the variance found in the individual state data breach notification laws.

Forty-seven states have established "data breach notification" laws to better inform consumers when their personal information has potentially been stolen or compromised.

California

Covered entities under California's state data breach notification law are any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information. California defines a "breach of the security of the system" as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." The law does not contain a specific risk of harm analysis whereby an entity would not have to give notice should no harm be done to the person whose information was compromised. A notice of breach must be made in the most expedient time possible and without unreasonable delay. Notice may be provided via written, electronic, or a substitute notice. Substitute notices can be utilized if the breached company can demonstrate that the cost of providing breach notices exceed $250,000 or more than 500,000 individuals were impacted. Substitute notices require the breached entity to send email notices to any individual for whom they have an email address, post on its website, and notify major statewide media. California allows a private right of action for affected individuals to recover damages.[14]

New York

Covered entities under New York's state data breach notification law are any person or business which conducts business in New York state, and that owns or licenses computerized data that includes private information. Service providers are also covered. Any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization is required to be notified. The law does not contain a specific risk of harm analysis, although the definition of "breach" may incorporate risks. A notice of breach must be provided "in the most expedient time possible and without unreasonable delay." Further, the notice can be provided to the affected person via written, electronic (if consent is given), or telephone notice. A "substitute notice" is allowed if the cost to provide notice

13- Caitlin Bronson, "Regulators issue cyber security guidelines for insurers and producers," Insurance Business America, April 21, 2015, accessed April 22, 2015, http://www.ibamag.com/news/regulators-issue-cyber-security-guidelines-for-insurers-and-producers-22176.aspx.
14- Cal. Civ. Code §§ 1798.29, 1798.80 et seq.

exceeds $250,000 or over 500,000 individuals are involved in the breach. New York does not allow a private right of action for affected individuals.[15]

Florida

In Florida, covered entities include any sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. In the event of a breach at a third-party service provider (i.e., credit card processing company), the third-party is required to notify the covered entity within ten days. The covered entity is then required to provide breach notifications to the affected individuals. Florida does not require breach notifications "if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed." Notices must be made "as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach or reason to believe a breach occurred." A notice to an affected individual can be sent via written notice or via email. Florida allows substitute notices similar to California and New York. Florida's statute allows state enforcement for violations of the breach notification law but does not allow private rights of action.[16]

These are just three examples out of more than 47. Unless and until there is a single, uniform national standard for data breach notification, the variances in each state law make it absolutely essential that an entity that has experienced a breach of consumer data consult with legal counsel and law enforcement to ensure they are complying with the law in every state in which there are affected consumers.

Abroad

Although many cyber insurance policies are written out of Lloyd's of London, the majority of UK businesses lack proper cyber insurance protection. According to a report by The Corporate Executive Programme, only 13% of large and mid-sized businesses in the UK have cyber insurance, compared to 40% in the United States.[17] Additionally, a joint report by Marsh and the government found that only 2% of all businesses in the UK had cyber insurance, although 81% of companies reported that they have suffered a breach in the past 12 months.[18]

In the United Kingdom, the government, in partnership with the insurance sector, launched a Cyber Essentials Scheme intended to make the UK the global leader in cyber insurance while also encouraging better cybersecurity practices among businesses. A pillar of the Cyber Essentials scheme would see brokers adopt Cyber Essentials (CE) accreditation while performing risk assessments for small and mid-sized businesses. Similar to the NIST Cybersecurity Framework in the US, Cyber Essentials is a foundation for basic cyber hygiene best practices for all types of organizations to adopt and build upon.[19]

Take up rates among UK businesses have remained low even while the average cost associated with a data breach for large companies has doubled since 2014, from $2.2 million to $4.7 million according to a June Pricewaterhouse Coopers report.[20] Increased costs have led a number of industry experts to call for a government backstop for the sector. In July, Tom Bolt of Lloyd's outlined the need for a backstop to limit the threat to insurer's solvency if multiple businesses

The average cost associated with a data breach for large companies has doubled since 2014, from $2.2 million to $4.7 million.

15- N.Y. Gen. Bus. Law § 899-aa
16- Fla. Stat. Ann. §501.171
17- Warwick Ashford, "UK lags US in cyber insurance, study shows," Computer Weekly, February 9, 2015, accessed February 17, 2015, http://www.computerweekly.com/news/2240239989/UK-lags-US-in-cyber-insurance-study-shows.
18- HM Government and Marsh Ltd, UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk, March, 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf.
19- HM Government, Cyber Essentials Scheme (London: Crown Copyright, 2014), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317480/Cyber_Essentials_Summary.pdf.

across multiple industries were to suffer a cyberattack at once.[21] Bolt's statements were further substantiated by an August report from *Long Finance*, which argued that a public/private reinsurance scheme should be implemented to manage growing cyber threats.[22]

The European Union (EU) has been working on a data breach protection law, which would require organizations to notify those affected by a breach within 72 hours. Additionally, the proposed legislation would make it possible for organizations to be fined if it is concluded that negligence was the cause of the data breach.[23]

20- HM Government, PwC and InfoSecurity Europe, 2015 Information Security Breaches Survey (London: Crown Copyright, 2015), http://www.pwc.co.uk/assets/pdf/2015-isbs-executive-summary-02.pdf.
21- "Government cyber backstops needed: Lloyd's," Reactions, July 13, 2015, accessed July 16, 2015, http://www.reactionsnet.com/Article/3470524/Government-cyber-backstops-needed-Lloyds.html?ArticleID=3470524.
22- "Public, private cyber catastrophe reinsurance scheme would add clarity to U.K.'s cyber insurance market, encourage take-up: report," Canadian Underwriter, July 31, 2015, accessed August 5, 2015, http://www.canadianunderwriter.ca/news/public-private-cyber-catastrophe-reinsurance-scheme-would-add-clarity-to-u-k-s-cyber-insurance/1003742884/?&er=NA.
23- Sarah Veysey, "European Union gets serious about data protection," Business Insurance, August 2, 2015, accessed August 5, 2015, http://www.businessinsurance.com/article/20150802/NEWS06/308029995/upcoming-european-union-data-protection-law-tightens-cyber-breach?tags=|75|83|302.

Cyber Insurance: What You Should Know

Written by: Robert Jones - AIG

No matter how strong or sophisticated an organization's IT defenses are, how thorough the vetting of an organization's vendors may be, or how well an organization trains or plans in preparation to respond to a data breach or other incident, there will still be network security and privacy failures. Relying on IT defenses alone can provide a false sense of security. Recognizing that some risks cannot be eliminated, organizations have increasingly turned to cyber insurance as a method of mitigating and transferring the risk of exposure to cyber events.

Cyber insurance is particularly effective when the cost of additional information security controls do not reduce the risk enough to make the investment in such controls practical. Cyber insurance itself is not a defense; without a rudimentary information security management system, cyber insurance can be prohibitively expensive, and represents an unsustainable solution (for both insurers and companies). It is the application of cyber insurance as another layer—complimenting the efforts IT and other information security oriented functions—where its greatest value is realized.

Cyber Insurance Coverage—A Brief History

The first iterations of today's "cyber" policies appeared in the late 1990s, as the insurance industry began to develop errors and omissions policies to respond to exposures arising out of emerging technologies: the internet and e-commerce. These "internet insurance" policies reflected their E&O roots in that they: i) were limited to responding only to security failures of an insured's computer system, and ii) did not provide coverage for first-party costs of mitigating a data breach (one of the potential outcomes of security failure). The coverage did not extend to non-electronic records or accidental disclosure. Underwriters were starting to offer first-party coverages the value of lost data and business interruption (the cyber analog to property insurance), but first-party coverage was not typically underwritten or brokered by members of the E&O insurance community, and these coverages were not widely utilized.

In the mid-2000s, these early cyber policies evolved into forms more recognizable today: coverage was amended to include "privacy incidents", which expanded the policies' response to accidental disclosure of sensitive data in both electronic or paper form; liability coverage was expanded beyond civil actions to also include regulatory investigations; coverage started to appear for contractual fines paid to payment card brands for security non-compliance (contractual liability being generally excluded by E&O policies); and new first-party coverages were created to respond to the costs of investigating and mitigating a security or privacy incident.

Two factors in concert contributed to cyber insurance's growth: i) new regulations which obligated companies to do more to respond to information breaches, such as the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the early electronic breach notification laws like California's SB 1386; and ii) organized crime's increasing awareness of the profitability of payment fraud, identity theft and other crimes made possible by stolen information. Whereas victim companies were previously protected from the fallout of security incidents by the public's lack of awareness of what transpired, these new regulations forced companies to be responsible for data breaches which were caused—or at least exacerbated—by poor security. As cybercrime increased, cyber insurance grew and evolved to meet the exposure.

The cyber insurance marketplace continues to evolve in several different ways:

- Available limits for in-demand coverages continue to increase, both in terms of per carrier and total marketplace capacity;
- Coverage continues to evolve to match emerging technologies—an example being the creation of "Cloud Failure Extensions" to respond to the migration to the cloud and the exposure of dependent business interruption;

- The underwriting requirements are changing in response to the increasing loss developments; and
- Some insurance carriers are partnering with information security service and product providers so as not only to be able to accept risk from companies, but also assist companies in evaluating and augmenting their information security or "cyber" resiliency.

While pricing, capacity and underwriting requirements are changing, it is clear after more than a dozen high profile breaches that cyber insurance is a risk management tool for information security that is as important as a company's security training or intrusion prevention systems. In fact, cybersecurity oversight is now rightfully viewed as a responsibility of a board of director's enterprise-wide risk management. The Commissioner of the Securities and Exchange Commission noted in June 2014 that "there can be little doubt that cyber-risk also must be considered as part of board's overall risk oversight." Board members are increasingly polling their company's risk managers and IT professionals to confirm that cyber insurance coverage is in place and to better understand the policy offerings in the event that coverage is triggered.

What Does Cyber Insurance Cover?

Generally, most insurers offer cyber policies with coverage on an a la carte basis; a company can choose which coverages are right for it. The main coverage components are:

1. Defense and indemnity for alleged liability due a cyber or privacy incident ("Liability")
2. Coverage for investigating and mitigating a cyber or privacy incident ("Event Response")
3. Coverage for business interruption due to a cyber incident ("Business Interruption")
4. Coverage for the response to threats to harm a network, or release confidential information ("Cyber Extortion")

The "triggers" of the coverages are important to understand as well: a "cyber incident" typically means the failure of the insured's computer system security, while a "privacy incident" is any failure to protect "confidential information". The distinction is a subtle, but important, one: a failure of a company's computer security can result in a privacy incident, but some privacy incidents don't arise out of a failure of company's computer security. Generally, there is a lower threshold for "privacy incidents" to trigger the policy. Coverages and wordings vary from carrier to carrier. Some carriers split the liability coverage for cyber and privacy incidents, so insureds can buy only one of the two if they choose; other carriers have chosen to combine some of the coverages for marketing purposes; and all of the carriers have slightly different definitions for what "computer system", "failure of security", and "confidential information" mean.

It should be noted that the vast majority of cyber policies exclude three key types of loss, which a layman might—understandably—find confusing, but which are a product of the borders between different types of insurance. Those three types of loss are: i) tangible property damage (data not being considered tangible property), ii) bodily injury (bodily injury not including emotional distress), and iii) loss of the company's funds. Coverage for bodily injury and property damage is usually found in traditional property or casualty insurance, and coverage for stolen funds is usually the domain of Crime coverage. The availability of coverage for a cyber incident under a traditional property or casualty program is often not explicit; insurance carriers are grappling with whether such policies are priced and structured appropriately for this new risk. As technology advances—the Internet of Things, computer controlled medical devices, etc.—and the increasing potential for a cyber incident to result in BI/PD, some carriers are starting to exclude this coverage under traditional property and casualty programs. Other insurers are addressing this gap, offering policies that are geared to respond specifically to cyber-related bodily injury and property damage. It remains to be seen how this growing exposure will be addressed.

The "Liability" or Third Party coverage provided by typical cyber insurance applies to claims first made during the relevant policy period involving allegations of damages due to a cyber or privacy incident. Liability cyber insurance functions much in the same manner as

traditional third-party errors and omissions insurance. Like other professional liability forms, a cyber policy's liability insurance typically covers the following liability expenses: the costs of the legal fees to defend third-party lawsuits; costs of electronic discovery; class action administration costs; and judgments and settlements, often including substantial plaintiff attorney fees. For companies defending a third-party cyber lawsuit, a sound defense strategy will contemplate indemnity rights and recovery efforts.

Two noteworthy extensions exist to the Liability coverage. First, "Regulatory Coverage" extends the Liability coverage so as to also respond to investigations brought by regulators—such as the Office of Civil Rights at the Department of Health and Human Services, the Federal Trade Commission, the Securities and Exchange Commission, and state attorneys general—arising out of a cyber or privacy incident. With this extension, defense costs are covered not only for civil actions, but also for an investigation by such regulators. Coverage may also extend to any fines and penalties to the extent they are insurable under State Insurance Law. As regulators are becoming more aggressive in investigating data breaches and levying fines on affected companies, this coverage has become increasingly important.

The other extension to the Liability coverage is coverage for the assessments of contractual fines by credit card brands for failure to comply with the Payment Card Industry Data Security Standards ("PCI-DSS"). Such fines include the costs of reissuance of affected credit cards and the reimbursement for fraudulent transactions to affected consumers. This coverage is becoming more important as it becomes evident that breaches affecting large amounts of consumer payment card information will result in mass reissuance of cards and substantial reimbursement of fraudulent transactions to the consumers by the card brands, which pass those costs back to the liable party.

First party "Event Response" coverage usually applies in response to an actual or suspected cyber or privacy incident first discovered during the policy period. Typical first party coverage includes coverage for the following: forensic investigators to determine the scope of the cyber or privacy incident; a law firm to act as breach counsel to advise the insured of its obligations arising from any breach of sensitive data; costs of notifying affected individuals; a public relations firm to provide advice on whether and how to make public statements, credit and/or identity monitoring; and call center support. Cyber policies will help to stem an event but do not pay for the expenses incurred to correct or remediate technical problems or provide the upgrades necessary to prevent future data breaches.

Cyber insurance is evolving just as fast as technology. What is considered core coverage today was not available as little as three years ago, and enhancements to coverage are being negotiated in the marketplace every day.

"Business Interruption," also referred to as Network Interruption, covers lost net income and extra operating expenses resulting from a material interruption of an insured's business as caused by a security failure. The business interruption coverage usually applies after the greater of: i) a dollar amount of loss (the retention), or ii) a "waiting period" has elapsed.

"Cyber Extortion" will cover the costs to assess the cause and validity of privacy and security related threats and any monies paid to end such threats. Privacy threats involve attackers who claim to be able to disclose confidential information. Security threats involve attackers who claim to be able to commit or further an attack against a network.

Cyber insurance is evolving just as fast as technology. What is considered core coverage today was not available as little as three years ago, and enhancements to coverage are being negotiated in the marketplace every day.

Increasing Front-End, Pre-Breach Loss Prevention Services

To provide valuable and differentiating policy enhancements, a number of insurers currently offer preventative tools and consultative solutions to insureds that bind a cyber policy. Loss prevention services may include (i) infrastructure vulnerability scanning, (ii) cybersecurity risk assessment, (iii) "dark net" mining and monitoring, (iv) generation of third-party vendor security ratings, (v) isolation and "shunning" of malicious IP addresses, (vi) mobile apps which provide news, claims data, and related information and (vii) online employee education and

training. These preventative tools, when properly implemented and utilized, provide an additional line of defense in the prevention and mitigation of cyber incidents.

How Much Coverage Is Appropriate?

Almost every purchaser of cyber insurance buys the liability and the first-party coverage for the value of data; the majority—about four-fifths—also buys the first-party coverage for the costs of investigating an incident and coverage for extortion demands. Roughly half of buyers are purchasing the business interruption coverage. As companies evaluate the current and future dependency on computer systems to run their business, they should re-evaluate whether they are purchasing the right types of cyber coverage, not only the right amount.

Almost every purchaser of cyber insurance buys the liability and the first-party coverage for the value of data; the majority also buys the first-party coverage for the costs of investigating an incident and coverage for extortion demands.

Based on the variance of the above factors, the costs of cyber insurance will vary from organization to organization. Nevertheless, reports estimating the costs of data breach—the leading type of loss in the cyber insurance space—are relatively easy to find. Many estimates assess costs in relation to records exposed. The NetDiligence 2014 Cyber Claims Study pegs the maximum cost per record at $33,000 (the average was $956.21, and the median $19.84). In May 2014, the Ponemon Institute published a report entitled, “Cost of Data Breach Study,” a global survey of 1,690 information technology, information security, and compliance professionals from 314 organizations, all of whose companies had experienced cyber breaches. The widely cited Ponemon report concluded that the average per-record cost of a breach in the U.S. was $201 in 2014, up from $188 in 2013. The report went on to peg the average cost of a U.S. data breach at $5.85 million.

These figures should be used as a reference point for potential median data breach losses, and they should be part of a broader review of the risk a company has to cyber exposure from both unavailability of its computer system/data and repudiation of its computer based communications.

While there is no simple answer to the amount of cyber insurance an organization should buy, some important factors to consider include: the size of the insured entity; the amount of sensitive data stored; the industry; the degree of potential reputational risk; organizational resiliency; the degree of regulatory attention paid to the company; threat vectors—for example, state actors, or cyber activists (also referred to as “hacktivists”)—and of course the company’s own risk appetite.

The evolving nature of the cyber insurance marketplace means the adequacy of cyber insurance should be evaluated on an annual basis and that new insurance tools and offerings should be fully considered. Companies should work with their brokers or other specialized insurance professionals to consider the differences in insurance products offered across the market at the time of placement. Consideration should be given to the differences in coverages and offerings between carriers, the availability and strength of any loss prevention services offered by the carriers, and each carrier’s commitment to a company’s sector.

Privacy Attorney: Lynchpin to Success

Written by: John Mullen, Esq. and Jennifer Coughlin, Esq. - Lewis Brisbois Bisgaard & Smith, LLP

What Is a Privacy Attorney's Role In an Incident?

Attorneys, like doctors, should know when specific expertise is required to address a specific situation. Crisis management in the context of data privacy is not an area a generalist can adequately navigate. Proper legal handling of a data privacy event requires counsel with significant and frequent data privacy experience. Those few attorneys who focus their practice in this rapidly growing and developing area are the key to an organization's successful response to a data privacy event.

The legal framework surrounding data security incidents is not one-size-fits-all and changes constantly. Events can implicate state, federal and international laws, and contractual relationships. Outside privacy counsel possess repeated and significant experience with jurisdictional and definitional considerations, knowledge of pending amendments and regulator interpretations, and intimate familiarity with required vendors, regulators, and applicable insurance issues. As an event unfolds, privacy counsel use this knowledge to ensure the safety of their client's systems and data, identify an organization's resultant legal obligations, generate a response plan that will bring an organization into timely compliance with applicable laws and contracts, and prepare the organization for regulatory inquiry and/or litigation.

The legal framework surrounding data security incidents is not one-size-fits-all and changes constantly.

Outside privacy counsel play a pivotal guiding role during the initial response to an investigation of a data security incident. Simply put, external counsel must quickly and efficiently identify the likely nature of the event and retain appropriate external vendor support (forensic, public relations, etc.) immediately. It is counsel's job to quickly evaluate the organizational structure and the threat, and take steps to ensure any threat is neutralized. As this is happening, counsel must concurrently analyze all possible legal and public/client relation's issues, prepare the organization to take aggressive steps to satisfy any legal obligations, and address public and client issues. Privacy counsel should coordinate with law enforcement as necessary. Failing to retain experienced privacy counsel quickly can result in an untimely and non-compliant response that weakens the defensibility of an organization and exposes it to additional liability arising from mishandling the event, not to mention lessens the ability of the organization to retain its clients. Proceeding without required expertise can result in ongoing data exposure, inadequate legal issue coverage, insurance coverage difficulties, failure to properly prepare for regulatory inquires, and even disclosure of a non-reportable event causing unnecessary damage to the organization.

External privacy counsel knows who to call (and has already established pre-event contracts, rates and availability with forensic, public relations, and other vendors). Privacy counsel relies on the evolving findings of qualified third-party forensic experts to confirm the precise nature and scope of an event. The retention of a forensic investigator is a perfect example of a critical early step in the response process that, if mishandled, may result in delay and further exposure to the organization. The findings of a forensic investigation engaged and directed by counsel should be covered by privilege and protected from disclosure, particularly if litigation is anticipated. If forensic investigators are not retained and directed by external privacy counsel, an organization may retain the wrong investigators for the wrong reasons, without privilege, who are not otherwise qualified to ensure that the company's data and systems are truly safe and that all necessary facts are determined and date preserved.

Relying upon inexperienced counsel will likely result in untimely disclosures followed by heightened regulator inquiries that may have otherwise been avoided. A second round of disclosures to individuals to accommodate regulator follow up requests often results, as well. For example, an experienced data privacy attorney knows which regulators "request" an organization to provide its residents with two years of

credit monitoring service despite no requirement in the law to do so, and which regulators interpret its law to require notice to both its office and its impacted residents within 30 days of discovery of a data security incident, despite the law requiring such notice be provided merely without unreasonable delay. This knowledge is essential to limiting additional regulatory inquiry.

Dedicated privacy counsel has teams of attorneys, with years of experience, focusing their practice only on data security incident response services. They know which vendors offer services crucial to an effective and efficient response (forensics, public relations, mailing vendors, call center vendors and credit/I.D. monitoring vendors) as opposed to vendors trying to penetrate that market without sufficient experience. They know what vendors can ramp up quickly to mail hundreds or thousands of letters, if not more, and to make sure each letter recipient has timely access to representatives able to answer questions about the incident and enroll the individual to receive credit or identification monitoring services being offered. Failing to retain vendors that have the ability to properly service both the client and the impacted population may result in a public relations nightmare and reputational damage to an organization that might otherwise have been avoided if the right vendors were engaged in the first place.

There are many times when solid local counsel is sufficient to handle legal issues. Data privacy events do not fall into that category.

Proactively Limiting Data Privacy Liability: A Quick Summary

A data security incident poses significant and time-sensitive challenges to an organization. Preparation, insurance and appropriate experts will go a long way in minimizing the pain. An organization can limit liability it may have as a result of a data security incident both before and when an incident occurs.

Before an incident, the organization can assess (both internally and by using a qualified outside specialist) its policies, procedures, information security, and business relationships (business-to-business and business-to-customer). There are several, non-exhaustive questions the organization should ask, including:

A data security incident poses significant and time-sensitive challenges to an organization. Preparation, insurance, and appropriate experts will go a long way in minimizing the pain.

- **What information does the organization collect, and does it need this information to conduct its business?** An organization may suffer an incident, such as an intrusion into its network, which results in unauthorized access to or exfiltration of information it had no need to retain or collect in the first place. The organization should focus on collecting and retaining only information that it has a legal obligation to retain or that it uses during the normal course of its business. If it does this, the number of individuals impacted by an event, and the organization's legal obligations and overall risk exposure will be narrower and more manageable.
- **Who has access to the information?** Organizations often permit access to sensitive information to too many employees, regardless of whether there is a legitimate need-to-know. Allowing access to protected information by individuals and/or vendors with no legitimate need increases the risk that the information will be compromised or misused. An example is when a bad actor maliciously acquires the employee's access credentials. An organization should only allow access to data by employees and vendors with a legitimate business need. All access should be closely monitored.
- **What type of internal training does an organization provide regarding information security, and are policies and procedures enforced?** An organization's staff is unlikely to appreciate the importance of information security without appropriate policies, regular training, and constant reinforcement on the subject. Educating staff will invite free discussion with upper management on an organization's policies and risks (such as saving information locally on company-issued laptops), and ensure timely event reporting. If a

laptop is lost or stolen, for example, an employee trained in information security will know how critical it is that the theft be reported internally immediately.

- **Does the organization have cyber insurance?** Multiple carriers have comprehensive cyber insurance products that provide coverage for both first-party and third-party expenses an organization may incur to investigate and respond to a data security incident and defend against regulator, business partner, or class action litigation. These products often provide indemnification for fines, penalties, and judgments. Depending upon the magnitude of the event and the population, an organization can easily spend hundreds of thousands of dollars (sometimes millions) investigating or responding to an incident, defending against claims, and funding settlements or judgments. Many organizations are shifting some of this significant risk through insurance. By obtaining cyber insurance, organizations have immediate access to experienced privacy counsel, forensic investigators, public relations firms, and other response vendors who focus on this discrete business challenge.

- **Does the organization contractually shift risk to its business partners?** If an organization utilizes the services of a third-party vendor to collect or store protected information, its contract with this service provider should address data privacy. For example, if an organization utilizes a payroll service provider to pay its employees via direct deposit and employee names and bank account information are exfiltrated from the payroll service provider's systems, the organization may have the legal obligation to disclose the incident to employees, regulators, and consumer reporting agencies. Having a contract in place whereby the third-party service provider—at its own cost—is required to disclose the incident to necessary audiences and otherwise address the issues raised by the event limits the financial impact of the event on the organization. An organization can further shift the risk to a third-party vendor by including a provision whereby the third-party vendor agrees to indemnify an organization for costs incurred to investigate and respond to a data privacy event for which the third-party vendor is partially or completely at fault.

- **Is someone at the organization in charge of the response and empowered to act?** Too often, organizations have hierarchical structures requiring multiple levels of briefing and decision-making. This is not an optimal way to address a crisis management data privacy event. Rather, an organization should empower one executive (with the support of other required departments) to act and make binding organizational decisions. If the person/team that is in place cannot make decisions after hours or on weekends, the organization does not have the proper structure in place.

When an incident happens the most important thing to know about limiting liability is that a data privacy security incident is a crisis. Experts are needed immediately after discovering that there may have been a data security incident. There will be many moving parts and timelines are short. Communication will be key. There is little time or room for missteps. Avoid the temptation to rely on internal and existing business partners. Even one misstep in confirming the nature and scope of an incident, and implementing an incident response, can be disastrous for an organization, its reputation, and its bottom line. The likelihood of missteps dramatically increases when experts are not retained to assist in responding to a data security incident, potentially exposing the organization to liability. Mishandling the post-incident response can result in lost or unavailable evidence, incorrect or inconsistent messaging, incomplete investigations, and defensive communications which may result in public scrutiny, lost business, regulator inquiry, litigation, assessments or fines, as well as brand and reputational harm. If done properly, the appropriate approach will mitigate brand and reputational damage and limit third-party or regulatory exposure.

Insurance Brokers: More Than Just Your Sales Contact

Written by: Ben Beeson - Lockton Companies

Contrary to the perception of many people, the insurance industry does not have all the answers today in terms of identifying and quantifying cyber risks. Just as companies struggle to understand the size and type of investment needed to be made in risk mitigation, so too insurers remain hamstrung by the lack of actuarial data available to model risk.

Choosing to transfer risk from the balance sheet by way of insurance is a daunting task. Key questions that buyers struggle to answer include:

1. Does my current insurance program, which might include Directors and Officers Liability, Errors and Omissions, Property and General Liability products, address all my corporate assets at risk?
2. If not, do I need to consider a specific cyber insurance policy?
3. What specifically will cyber insurance cover and how do I seek to avoid material contractual clauses and exclusions?
4. How much cyber insurance should I buy, from whom should I buy it, and how do I know that I am paying a competitive price?

To answer these questions requires engaging an insurance broker. Unlike certain other classes of the industry, a broker represents the interests of you, the buyer. It is not the insurance company's agent. First class brokers work with their clients to understand the assets at risk and how best to address them either under the existing insurance program or through a new dedicated product. An existing Directors and Officer's policy form (D&O) addressing management liability from a cyber event probably offers sufficient coverage today. More often than not, though, liability to the enterprise requires a new dedicated product. However, choosing the right broker means more than simply identifying an understanding of your specific risks. Larger companies who operate in more than one territory around the world will want to understand the broker's own distribution network and the ability to be "local" where needed. A global platform will also mean understanding how liability to your organization may change depending on local data security and privacy regulation and legislation, for example. A broker's relationship to insurers is also key. The amount of business transacted with insurers and the ability to access the most senior decision makers can both be key factors in achieving a competitive outcome.

Increasingly, first class brokers are bringing more to the table than simply the ability to negotiate and transact insurance. Building resilience against cyber events means adopting an enterprise wide risk management approach. Many companies who have purely focused on investment in the IT department have begun to realize that the process of acquiring cyber insurance can be the catalyst for change. A higher quality of broker can act as facilitator, bringing all relevant stakeholders in the enterprise together to drive collaboration. Finally, appropriate risk mitigation also requires engagement from a number of service providers such as outside counsel, forensics, and crisis communications. Broker differentiation also exists in the relationships with other service providers that they can bring to the table as you look to build a strong readiness and response structure.

The Broker's Role In Acquiring Coverage

Building resilience against cyber events means adopting an enterprise wide risk management approach.

A good broker understands that insurers seek to understand the security culture of a firm and will work to position their clients as best as possible. For many larger organizations, this does not involve completing a written questionnaire and staying divorced from the process. Rather, an investor-style presentation to the insurance marketplace by key stakeholders in IT, legal, and risk management in particular—which involves questions and answers—ensures the best possible results. Top-tier insurance underwriters appreciate that cybersecurity is not a "tick box" exercise. They understand that the risk is dynamic and will not necessarily penalize a buyer today for shortcomings if a roadmap is spelled

out as to how these shortcomings will be addressed in the next 12 months. An experienced broker will be able to anticipate the information that insurers will want to know, working with their client to ensure that relevant answers are embedded in the presentation and Q&A kept to a minimum.

Upon completion of the underwriting presentation, the broker—following client agreement—must set out the coverage terms that insurers should address during a competitive bid process. More often than not, this will require manuscripted changes from an insurer's standard product. Examples include the ability to delete or at least narrow war and terrorism exclusions with the emergence of the nation state as a threat actor. The challenge in detecting an Advanced Persistent Threat (APT) also raises alarm bells regarding whether an insurer will or will not cover an act that occurred prior to the start of the insurance policy but without the policyholder's knowledge. A broker will negotiate with each insurer, ultimately recommending the most competitive option.

Depending on the amount of insurance required, a broker's job may not be done. Typically each insurer will offer a maximum $10,000,000 aggregate limit of insurance. As the risk severity has grown many companies buy much higher limits and a broker in some instances may work with ten or more insurers to build the required amount. Typically this is structured on an "excess of loss" basis where each insurer stacks one above the other to indemnify financial loss once the underlying insurer has paid out.

Considerations Prior To a Breach

There is no doubt that the insurance marketplace today is moving towards a basis that rewards buyers for strong security through discounted premium, lower deductibles, or broader coverage. However, the dynamic nature of the risk and the lack of actuarial data have limited the growth of the market and it remains somewhat embryonic today. As the frequency and severity of corporate data breaches in particular have grown over the last two years, insurers have raised the minimum security standards needed simply to acquire insurance. In some instances, this can be a pass/fail exercise. A good example is how you secure PII and payment card data in particular. If you do not encrypt or use an alternative control such as tokenization, you will struggle to find insurance. The good news is that insurers have started to seek partnerships with security firms that can provide intelligence and monitoring capability and in some instances the ability to measure security levels. Insurers will leverage these tools as they evolve to more accurately price risk as well as incentivize buyer adoption through competitive pricing and coverage.

Incident Response: Why Planning for Failure Can Lead to Success

Written by: Bob Shaker - Symantec

A major part of every cyber insurance claim is Incident Response. A well-built and regularly tested Incident Response program is an important component of a comprehensive risk management plan. Each claim requires investigation and—depending on how that investigation is performed—can mean the difference between a minor incident and a major breach that requires PR, Legal, and External Notification.

Symantec's Incident Response Services Team has worked closely with customers and the different players in the cyber insurance market. Insight from one of the world's largest civilian security intelligence databases gives Symantec a unique view and allows us to help customers select cyber insurance or analyze their existing coverage—to be prepared and informed before they have a compromise.

Understand Your Options: *Not all investigators are alike*

Live response and traditional forensics have a lot in common, in that they are both looking for similar artifacts on a system. The differentiator is that with live response the artifacts are being discovered on a live running system against an active adversary; with traditional forensics images are taken of volatile memory and disks before being analyzed. Imaging alone can take hours, and then the images need to be processed and indexed to allow for keyword searches.

Obtaining and processing the image can easily take a day or longer with large capacity discs. With live response, there is no imaging or processing; everything is in real time. This dramatically improves the response time in identifying and quantifying a threat—and the quicker the threat is identified, the quicker it can be contained and remediated. Having live response provides better and faster results against attacks. You can read more about Live Response vs. Traditional Forensics written by Jamie Porter, Lead Investigator, Symantec.

Having live response provides better and faster results against attacks.

Proactivity is Key: *Preparedness leads to more successful response*.

Another focus point is the need for an incident response program, rather than just a plan. We have seen that our most successful engagements came from customers who had a strong incident response readiness program. Everyone involved in the ecosystem wants to see the customer preparing for an incident, and—if an incident occurs—leveraging the lessons learned to incorporate a stronger readiness component. Keep the following in mind when beginning to build out an Incident Response program for your organization.

- **Dedicate Project Management Resources**. An IR PM is responsible for coordinating all areas of the Incident Response process including:
  - The triage of incoming requests for assistance from the NOC, the Helpdesk, SIEM/MSSP alerts, and Security Operations.
  - Coordinating resources and planning.
  - Managing third-party vendor engagement and contracting when needed.
  - Driving completion of milestones outlined in your IR process.
  - Managing each incident within a Case Management tool.
  - Sending out status updates and communications to internal stakeholders.
  - Documenting lessons learned and driving/tracking learnings into implementation.
  - Updating IR plans and policies based on new learnings from prior incidents.
  - Escalating changes to the project scope or plan to appropriate IT resource owners and business owners.
  - Proactively disseminating project information to all stakeholders.

- **Implement Case Management**. Eighty percent of CISOs that we have spoken to say they were not using any sort of Case Management tool. Case Management tools are a critical component of any IR program. This is what we've learned from our experience working with customer for years in this space. Case Management can:
  - Document status and maintain a timeline of events.
  - Correlate across incidents, over time, to identify persistence campaigns.
  - Track evidence for litigation needs.
  - Evaluate performance of the IR plan over time.
  - Generate reports for auditors, law enforcement, and management.
- **Conduct and Maintain an Investigation Skills Inventory**. The heat of an incident is not when you want to realize that you don't have the skills you need. Will IR investigations in your environment require SCADA expertise? Mobile platforms? Embedded Systems? IoT devices? It's highly recommended that you maintain an up-to-date skills assessment of your internal investigation team and place 3rd party vendors on retainer to cover the gaps.
- **Purchase a Retainer**. Consider putting a third-party vendor on retainer. This not only helps to back up your own teams in the case of an activity surge, it can also provide specialty expertise during a data breach—such as crisis communication and legal support—that is difficult to maintain internally.
- **Create and Maintain Incident Playbooks**. A playbook is a document with specific guidelines for given scenarios. It defines specific steps to follow unique to DDoS, APT, malware outbreaks, web server compromise, and so on.
- **Understand Business Context of Systems and Applications**. As part of an investigation, it may be necessary to take systems and applications offline for analysis. When investigating a system for potential compromise, it is critical to consider the business impact and know what confidential data is known to be stored on, or passed through, the system. Leverage Data Loss Prevention solutions to map out the important data flows in your organization.
- **Cross-Organizational Buy-In**. Success in IR often requires cross-functional buy-in from both IT owners of an array of systems and the business owner of the data in those systems. Don't wait until an incident to engage key stakeholders and obtain their buy-in on how your IR plan would be implemented.
- **Practice, Practice, Practice**. Just like Disaster Recovery plans, IR plans need to be tested. This can be as simple as regular tabletop exercises or as thorough as using "cyber range" solutions that simulate attack scenarios.
- **Create and Maintain an Incident Response Plan**. Though we are discussing the need to evolve your plan into a program, this doesn't mean to downplay the need for a plan. Plans define and document things like internal stakeholders, vendor, and support contact lists required to ensure success of the program.

Learn more about Turning an Incident Response Plan into a Program written by Clint M. Sand, Sr. Director, Global Cyber Readiness & Incident Response Services at Symantec.

Build a Partnership With Your IR Provider: *Choose the right incident response partner*

When you choose a third-party vendor, look for someone with global insight into security threats and incidents who can also provide in-region security experts. This gives your organization the best of both worlds. Regardless of your size and geographic dispersion, you want a worldview that aids in understanding the attack actors and their motives, with the in-region response needed to react quickly.

Many customers have an incident response company they prefer to work with. You and this third-party vendor already understand one another's operations, and you have a trust that has been built over time. If this trusted vendor is not on the carrier's preferred vendor list, ask

your broker to have them added as a supplemental provider. They can provide you with significant improvements in the efficiency of your engagements. An incident response provider chosen by your carrier knows nothing of your organization and its operations.

A well thought-out and well-designed incident response program and partnership can mean the difference between disaster and success. This is something you need to plan and execute long before you get into a compromising situation—ultimately leading to quicker response times and allowing you to expedite a return to normal business operations, minimizing potential data, and monetary loss.

Be sure to consider these points when you purchase a policy. Getting the partner you want when you need them is instrumental in determining cyber insurance policy terms and critical to the overall success during an incident.

Crisis Communications In a Data Breach Event

Written by: Melanie Dougherty Thomas - Inform

Guidelines and Tips for Communicating Through A Crisis

The number of cyber security attacks being waged today has grown exponentially. In fact we're experiencing an increase of over 200% on a compound annual basis, notably from state-sponsored actors.[24] The sophistication of both the attacks and, increasingly, the public require an equal level of sophistication, expertise, coordination, and rapidness in the communication response. A crisis communications practitioner with experience in data breach and privacy is arguably the only professional with the subject matter knowledge, process know-how, and partner relationships that can adequately service an organization during a data breach. They are critical members of the incident response team. They mold the public-facing communication strategy that determines how stakeholders who are critical to the company's survival ultimately perceive the data breach event. But, that is far more intricate and delicate a process than one might expect.

Companies have many different audiences they must reach through their communications response during a breach: the general public, news media, employees, regulators, analysts, partners, contractors, suppliers, and Wall Street each have their own particular engagement with a company and different concerns. Consumers and employees might worry about their PII, PCI, or PHI, while Wall Street will be concerned with business interruption and a company's ability to meet its quarterly earnings. Regulators will want to know if you conformed with legal obligations to notify consumers, while the media will want to know the basic facts of the breach and who is to blame. Creating accurate, concise messages that meet the concerns of each of your company's stakeholders is difficult to be sure. Ultimately, your messages must anticipate a myriad of questions during the crisis, such as: Is the attack still happening? Was my identity stolen? Was it PII? Will the company be downgraded? Will the stock price take a sharp decline? Will a state Attorney General, or the Federal Trade Commission decide to investigate the company? Will consumers lose faith in the company and retreat to its competitors? Will the CEO be forced to resign? Will a class action suit be brought against the company? All of the aforementioned propositions have occurred for multiple organizations that have experienced highly public data breaches over the past few years. They are not conjecture, but fact. Recall the devastating impact of cyber attacks and resulting breaches for once stalwart brands like Anthem, Target, Sony, Chase, Home Depot, Neiman Marcus, Michael's, CVS, the Wall Street Journal, the NYSE, and even our Federal Government agencies, like DOE and OPM, to name a few. These organizations were rendered powerless to stop the damage that resulted from the breaches they endured. And endure they did. A cyber attack can leave an organization helpless and its brand damaged. They are forced to fight for control through their incident response team and, at times, only able to communicate the delicate situation to stem the bleeding. This is crisis communications.

A solid communications response to a cybersecurity attack may lead consumers to feel a sense of sympathy and even loyalty to the target company as a victim of a criminal organization, or enemy of the state, eliciting support. A weak response may result in tumult like that experienced by Sony, which was literally taken to its knees by the North Koreans; became the focus of negative media, Congressional, and regulatory attention, and made lead defendant in a class action suit by some of its employees. The scenarios presented are all too common today. They are, in fact, modern day corporate warfare, to be sure.

A cyber attack can leave an organization helpless and its brand damaged.

Effective Crisis Communications: *Still Eluding Many Organizations*

How does an organization survive a breach while maintaining its brand integrity, reputation, and market position? Companies must employ an effective, strategic crisis communications plan and response. Consider the highly publicized breaches of late. Their public relations

24- 2015 PWC Global State of Information Security Survey.

responses failed to adequately, and in some cases accurately, explain the events in a manner that assuaged its critical stakeholders. What ensued was critical news coverage, public outcry through the press and on social media, Congressional hearings, a loss of public trust, increased regulatory scrutiny, Wall Street downgrades, drops in stock price, lost earnings, and damaged brands. The mistakes were many and entirely unnecessary. Poor messaging and timing was to blame for one retailer's very public humiliation. Consumers and ultimately the company's own Board of Directors were given the impression that its' leadership was unaware of what type of data and number of files had been exfiltrated. They came out with public statements too early and with inaccurate information, which forced multiple restatements. In addition, the tone of the initial spokespeople (yes, there were a few) was defensive, aggressive, unapologetic, insensitive, and even a bit arrogant, making many customers almost apologetic for wanting to know if their data had been breached. Then, the regret felt by many consumers quickly turned to confusion, and then to anger. For many, the aforementioned breach was a crash course in data security and our right to data privacy. Consumers quickly became a well-informed, determined audience demanding more from corporations in their promise to protect personal data.

Lesson: Release a holding statement that acknowledges a breach event has, or is occurring, with a promise to regularly update the public, in a contrite tone. Then let the forensics team complete a thorough, accurate assessment of the attack and loss, and allow time for them to conduct their remediation before making announcements prematurely.

Messaging: *What's In a Word? Everything*

Effectively messaging a breach event is one of the most challenging aspects of the response and something that still eludes many organizations. How do you present the details of a breach event in a manner that conveys control over a situation you really have little control over? How do you explain a highly technical event to a public that, while desperate to know, may not be fully capable of understanding? How do you convince critical stakeholders that your organization can be trusted after you have failed to protect their most sensitive data? In a recent social networking site breach, 37 million people who placed their trust in the company which existed solely to provide a platform for confidential romantic relationships woke up to find their email addresses on the web and their identities as philanderers revealed to their loved ones. The resulting carnage included families destroyed, employment resignations and firings, and even suicides. The CEO of the company used messaging that was so arrogant and offensive it left little room for empathy from the media and consumers. Ultimately, he was forced out of the company he created. What is equally surprising is the tone the company has taken since the removal of its CEO. They have actually been boasting of an explosion in membership since the breach, which begs the question of how accurate that statement really is. Ask yourself this: would you want to do business with a company that failed to protect its consumers' personal information, caused unthinkable damage to the lives of so many, then had the gall to brag about a spike in new membership?

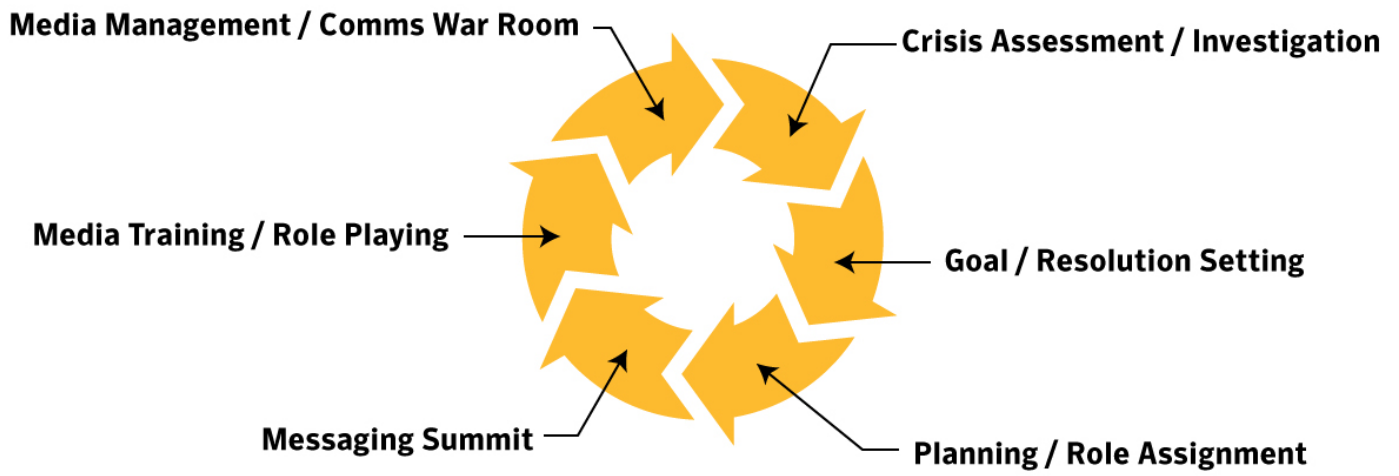
Lesson: Don't boast about your failure. It makes a fool of you and your audience. Use simple, accurate messaging that conveys only what consumers and regulators need to know and do so with a humble, contrite tone. The public wants to forgive you, so don't make it difficult for them to do so.

Crisis Communications Planning: *The Time Has Probably Already Come and Gone*

When is the best time to buy flood insurance? Probably before the flood has occurred. While that is a somewhat overused adage, it very simply conveys the critical nature of crisis communications planning. With the wrath of highly publicized breaches over the previous few years, one would think every company has created a crisis communications plan. Surprisingly, far too many have not. Communications planning, like data breach incident response planning, is your flood insurance. There is simply no reason not to have a plan. A good plan will allow you to be prepared for any crisis situation and ensure your response is swift and well-coordinated. A crisis communications plan should include the following:

1. **Strategy**: Plan for every conceivable crisis scenario. Take a cue from the intelligence provided by your forensics firm and the trends in your market sector.
2. **Procedure**: Determine the first, second and third thing that will likely happen when a crisis occurs, your response, and alternative actions to those responses should the crisis render them impossible.
3. **Roles and responsibilities**: Choose your crisis team members, determine their roles in the response, have their mobile and home numbers, and choose alternates should any of your team members become unavailable. **NOTE**: Incident response teams should include representatives from the executive team, corporate counsel, privacy counsel, CISO, IT, forensics consultants, crisis communications, corporate communications, marketing, human resources, customer service, notification, and credit monitoring.
4. **Messaging:** Develop language you will use for every likely crisis scenario. The challenge is to use words that convey the event and meaning in a manner that a broad audience can understand, with specific messaging to each audience (for example, financial, consumer, industry, government, employees, and media). Provide only information that is necessary, while not revealing that which could be used in litigation. The legal teams, both in-house and privacy counsel, should approve your messaging. Marketing should also give their approval to ensure the language and tone adhere to the brand guidelines of the organization.
5. **Content/collateral material**: Develop a generic holding statement, press release, web statement, social media language, and Q&A sheet for every conceivable scenario, which can be quickly adapted during the crisis.
6. **Media training**: Test both your messages and spokesperson on camera to prepare both for the time of crisis. Standard media training will not suffice for a crisis event. Even the most unflappable among us loses his or her cool during a crisis.

Crisis Communications Planning Process



Reputation Management: *Earning the Trust You've Lost*

Once the crisis has subsided, it's imperative to hold an assessment session with your team to explore what went right and what went wrong with your crisis response. In most cases, the organization has sustained some degree of brand damage. In such a case, companies will often initiate a Reputation Management (RM) campaign, which allows for damage control through several tools used in traditional public relations

campaigns. This is your opportunity to tell your story, through your messages, and in your brand voice, to win back the trust of the stakeholders critical to your survival. A RM campaign usually consists of the following tools:

- **Messaging session:** How you talk about the event moving forward, what you've done to prevent such a crisis in the future
- **Internal communications campaign:** Employee outreach
- **Critical stakeholder engagement:** Partners, vendors, analyst, government; win them back
- **Corporate social responsibility campaign:** Charitable campaigns, Public Service Announcements (PSA)
- **Media and analyst roadshow:** Travel to meet with journalists and analysts; make the effort
- **Op-eds, Letters to the Editors, blogs and white papers:** Push out positive content to suppress the negative news coverage and social media chatter
- **Earned media campaign:** Shift focus to positive corporate stories, programs, and services-pitch news coverage
- **Digital advertising campaign:** Promote the corporate brand

Note: Move from the negative to the positive. Remind the marketplace why they respected your brand prior to the incident.

Crisis Communications Specialist: *Your External Team Member*

More often than not, organizations are wrongly entrusting crisis response to PR generalists, which is a very dangerous gamble. Cybersecurity and breach response is fraught with legal and regulatory landmines that if not understood and respected will likely result in regulatory investigations, law suits, and most definitely damage to the brand. This is evidenced by the afore mentioned retailer, which is facing more than a few class action suits and action by the Federal Trade Commission, including audits for the next 20 years. Consider making a crisis communications specialist a part of your organization's extended corporate communications team for breach response. That expertise comes with years of experience working crises, which requires a unique understanding. And, as a specialist in data privacy, the specialist understands the complexities of the legal and regulatory landscape that guides the organization's response. He or she is also versed in the roles of the incident response team, likely has good working relationships across the IR industry and, thusly, knows how to effectively engage them and can even act as a bridge between the internal and external response team members.

More often than not, organizations are wrongly entrusting crisis response to PR generalists, which is a very dangerous gamble.

An experienced crisis communications professional will also have a deep understanding of recent breach responses due to their singular focus on the area. We monitor the media for breach response cases exploring what has been effective and what has been damaging to organizations. We stay informed about changing legislation and regulatory rules, which vary by state and on the Federal and Congressional level. We also tend to have very deep relationships in the cybersecurity and business media that allow us to guide the media engagement for our clients, position the spokesperson with the most appropriate, favorable journalist, and at times even prevent truly damaging news coverage.

Establish a relationship with a crisis communications professional today to help you create or review your crisis communications plan and make that person a trusted part of your extended incident response team. And don't forget: plan and train, and plan and train, and plan and train some more. When the inevitable crisis occurs, you won't regret it.

Legal Viewpoint: Critical Next Steps to Avoid Litigation, Notifying Law Enforcement, and Choosing Response Vendors

Written by: Lisa Sotto and Contribution by: Ryan Logan - Hunton & Williams LLP

You've Been Breached. What's Next?

Companies should contact outside counsel as soon as they discover an information security breach or receive notice that a potential breach has occurred. Under most state data breach notification laws, the moment an organization discovers that a breach has occurred is the time the clock starts ticking for the company to meet its legal obligations. Several states impose tight timing requirements on companies to provide legally required notifications. For example, Vermont's breach notification law requires affected companies to provide a preliminary description of the breach to the Vermont Attorney General within 14 business days following discovery or notification. Florida's law requires companies to notify affected individuals and the Florida Department of Legal Affairs no later than 30 days after the determination of the breach or there is reason to believe a breach occurred.

Notifying outside counsel can help ensure that a company both meets its deadlines for making legally required notifications and takes other necessary actions that counsel may be able to facilitate. Those actions may include hiring a forensic investigator (and cloaking the investigator's work in privilege), engaging an identity theft protection service provider, setting up a call center to answer the inevitable questions about the breach, and developing a public relations strategy in connection with the incident.

Depending on the nature of the information security breach, it may also be important to report the issue to law enforcement authorities. Some potential breaches, such as those involving an employee who emails a file containing sensitive personal information to unintended recipients, likely won't require outreach to law enforcement. Other events, however, may necessitate reaching out to different levels of law enforcement based on the factual circumstances surrounding the incident. These authorities may be local police, such as in the case of a stolen laptop or other portable electronic device, or the FBI, or U.S. Secret Service if, for example, a company suspects that a crime has occurred or that foreign entities or national security issues may be involved. It is important to note that most state breach notification laws allow companies to delay notification to affected individuals and regulators if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation. This may be critical in incidents where an external third party has accessed a company's systems without authorization but it is unclear if that third party exfiltrated any personal information. Other vagaries in the state breach laws include requirements such as those in New Jersey, where an entity that has suffered a breach is required to notify law enforcement prior to notifying affected individuals.

With respect to insurers, a company should notify its cybersecurity insurer quickly after learning of an incident. An organization suffering a breach should immediately review its cyber insurance policy to determine whether the policy covers the specific incident the company experienced and whether the policy contains provisions on when and how to notify the insurer. In the event a company does not have cybersecurity insurance coverage, it might seek to evaluate its other types of insurance coverage, such as its comprehensive general liability policy or general crime policy, to determine whether that coverage can apply to an information security breach.

Avoiding Litigation

In the current environment, private litigation following a revelation about an information security breach seems inevitable. Class-action lawsuits often are filed days after an information security breach is made public, even if the company itself has not publicly acknowledged the breach. Those bringing the suits have recently had a number of legal successes and, therefore, we do not anticipate that this trend will subside. A company's ability to discern quickly the true impact of an attack will put it in the best position to counter allegations at the

appropriate stage of litigation. A company should also be well-versed in the legal arguments that can be used to pare down the suits and potentially prevent the putative class from being certified, which would blunt the economic impact to the company.

Companies might first focus on defeating a potential litigant's claim of standing. To establish standing in breach litigation that is based on the alleged negligence of the company that experienced the information security breach, a plaintiff must demonstrate that (1) he or she has suffered a concrete and actual or imminent "injury in fact," (2) the injury can be causally linked to the company's actions and (3) it is likely that the injury can be redressed with a favorable decision.

The "injury in fact" requirement to establish standing is often challenged in the information security breach context because many breaches involve situations in which a plaintiff's information may have been exposed but not necessarily misused. In other words, a breach may have caused an increased risk of harm, but not actual misuse of, an individual's personal information. Though courts are divided on whether a plaintiff's increased risk of future identity theft can confer standing, companies should map out their best arguments for why standing fails in that jurisdiction given the facts and circumstances of their particular case. The development of these arguments will assist the company throughout the life of the litigation.

Many plaintiffs choose to avail themselves of unfair and deceptive trade practice statutes under which it is often easier to counteract defenses about the lack of an injury-in-fact. Plaintiffs often utilize certain state unfair competition laws asserting that they purchased a company's product on the basis of a representation in a company's privacy statement.

Companies should also be prepared to attack the claims on causation grounds. This is a fact-specific argument that depends on a plaintiff connecting the injury (i.e., the identity theft) with the information security breach. Because of the unfortunate prevalence of identity theft in our society, it will be increasingly difficult for a plaintiff to demonstrate harm that was caused by a particular information security breach. For example, if an individual plaintiff was a consumer of both a retailer and a large financial institution that experienced breaches in roughly the same time frame, it might be difficult to directly tie the plaintiff's injury to either entity.

As alluded to above, because most claims arising from an information security breach are class actions, companies should focus on demonstrating that such cases do not meet the legal requirements for class actions. Specifically, companies could maintain that class certification is not appropriate due to individualized issues related to causation that predominate over common questions. Again, this is a fact-specific inquiry for which a company may not be able to prepare until after an information security breach has occurred.

Because of the unfortunate prevalence of identity theft in our society, it will be increasingly difficult for a plaintiff to demonstrate harm that was caused by a particular information security breach.

Service Providers: *Choosing the Best Incident Response Team*

Companies should select service providers that demonstrate they have appropriate privacy and security safeguards in place to protect the personal information they will use or process on behalf of the company. This is not just a good business practice; it is required by law. For example, Massachusetts' information security regulations require companies to take "reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect…personal information" and to contractually obligate those service providers to implement and maintain such appropriate security measures. The Gramm-Leach-Bliley Act ("GLB") and its implementing regulations, which focus on financial institutions, and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations, which address certain health care entities, also impose specific obligations on companies that use service providers that have access to personal information.

To evaluate a service provider, companies should develop a due diligence questionnaire to gather information about the service provider's privacy and information security practices. The questionnaire should (1) ask specific questions about privacy and data security issues and (2) request that the service provider provide privacy and security-related materials such as information security policies. The questionnaire might touch on the following key areas:

- **General privacy and information security questions** – such as the types of personal information used or processed by the service provider and the purposes for such processing;
- **The service provider's privacy and information security framework and documentation** – such as whether the company has dedicated, senior-level privacy and information security professionals, an information security policy or an incident response plan;
- **Employee training and management and auditing** – such as whether the service provider conducts background screening of employees and contractors who may access personal information, trains relevant personnel on handling personal information, or conducts regular information security audits; and
- **Technical safeguards** – such as whether the service provider requires the use of security tokens or unique user IDs and strong passwords to access personal information, uses automatic log-off features on its computers or uses anti-virus, anti-spyware scanning and intrusion detection software.

After reviewing the completed questionnaire, the company can better understand the attributes of the service provider's privacy and information security status. Ideally, a service provider should have a written, comprehensive privacy and information security program that complies with industry best practices. If there are gaps in the service provider's responses to the questionnaire, the company may want to consider bolstering privacy and information security provisions in its contract with the service provider. The provisions could range from a general obligation that the service provider develop and implement administrative, physical and technical safeguards to protect personal information to more prescriptive obligations, such as requiring that all company-issued devices be encrypted before the service provider is engaged. Finally, as with any solid compliance program, ongoing monitoring of the service provider may be necessary.

Contributor Biographies, Company Descriptions, and Contact Information

Samir Kapuria - Symantec

Samir Kapuria is Senior Vice President and General Manager of Symantec's Cyber Security Services business unit. In this role, he leads engineering, product management, business development, delivery and operations worldwide for the business, including Symantec's DeepSight Intelligence, Managed Security Services, Incident Response, and Simulation Platform.

During his tenure at Symantec, Samir has held several executive leadership positions and built many successful teams, including the organization responsible for building Symantec's Global Intelligence Network. He also led the Security Intelligence Group, which created Symantec's CyberWar Games and Cyber Readiness Challenge, in addition to forward-looking technologies and intelligence programs to proactively address cyber threats.

Samir joined Symantec in 2004 through the acquisition of @stake, a leading cyber security consulting firm, where he served as an executive advisor for global enterprise customers, and led the business strategy and services organization. As a recognized industry authority, Samir regularly counsels high-level government officials worldwide on cybersecurity issues and emerging threats to critical infrastructure. He serves on corporate advisory boards, and provides guidance on next generation business and security strategy initiatives.

About Symantec

For more than 30 years, Symantec has made the online world safer, giving customers peace of mind and making the world around us a better place. Symantec, a Fortune 500 company, operates one of the largest global data-intelligence networks and provides leading security technologies where vital information is stored, accessed, and shared.

Amy Roberti - Council of Insurance Agents and Brokers

(amy.roberti@ciab.com)

Amy Roberti is Vice President of Industry Affairs at the Council of Insurance Agents and Brokers. She is responsible for analyzing commercial property/casualty and group health insurance market conditions, macro and micro events, and issues and trends impacting insurance brokers. Prior to joining the Council, Roberti spent 10 years in Liberty Mutual's Office of Federal Affairs, working as one of their top lobbyists in Washington, DC. She has worked on an extensive portfolio of federal and international issues including international regulation and trade, terrorism risk insurance, flood insurance, workers' compensation, health care and employer-sponsored benefits plans, surety bonding and cybersecurity. A graduate of Penn State University, Roberti holds a MBA from Georgetown University and earned the Chartered Property Casualty Underwriter (CPCU) designation in 2011.

About the Council of Insurance Agents & Brokers

The Council of Insurance Agents & Brokers is the premier association for the top regional, national and international commercial insurance and employee benefits intermediaries worldwide. Council members are market leaders who annually place 85 percent of U.S. commercial property/casualty insurance premiums and administer billions of dollars in employee benefits accounts. With expansive international reach, The Council fosters industry wide relationships around the globe by engaging lawmakers, regulators and stakeholders to promote the interests of its members and the valuable role they play in the mitigation of risk for their clients. Founded in 1913, The Council is based in Washington, DC.

Robert J. Jones - AIG

(Robert.Jones@aig.com)

Robert J. Jones is the Global Head of Financial Lines, Specialty Claims, at AIG. Robert is responsible for claims within the Cyber, Technology, Media, Fidelity and Kidnap & Ransom lines of business. Robert has developed Financial Lines expertise through a variety of technical and managerial roles in Claims, Reinsurance and Underwriting. Robert began his career at The Travelers in 1989 and joined AIG in 1992. Robert received a B.S. from the State University of New York at Binghamton.

About AIG

American International Group, Inc. (AIG) is a leading international insurance organization serving customers in more than 100 countries and jurisdictions. AIG companies serve commercial, institutional, and individual customers through one of the most extensive worldwide property-casualty networks of any insurer. In addition, AIG companies are leading providers of life insurance and retirement services in the United States. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit ourwebsite at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds.

Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance | LinkedIn: www.linkedin.com/company/aig

John Mullen - Lewis Brisbois Bisgaard & Smith LLP

(john.mullen@lewisbrisbois.com)

John F. Mullen is the Managing Partner of the Philadelphia Regional Office and Chair of the US Data Privacy and Network Security Group with Lewis Brisbois Bisgaard & Smith. Mr. Mullen concentrates his practice on first- and third- party privacy and data security matters, and (with his team) serves as a data breach coach/legal counsel for entities coping with data privacy issues. Mr. Mullen is well-versed in the complex state, federal, and international rules and laws governing data collection, storage and security practices and breach response obligations. Mr. Mullen has been on the forefront of developing the cyber market in the insurance industry, and continues to assist insurers, brokers, risks managers, underwriters, product specialists and professional claims personnel in navigating this rapidly-developing territory.

Mr. Mullen holds a B.S. from Pennsylvania State University (1987) and a J.D. from Arizona State University, College of Law (1991).

Jennifer Coughlin - Lewis Brisbois Bisgaard & Smith LLP

(Jennifer.Coughlin@lewisbrisbois.com)

Jennifer Coughlin is a partner in the Data Privacy and Network Security Practice, and sits in the Philadelphia, Pennsylvania office. Jennifer focuses her practice on the representation on entities that have suffered or may have suffered a data breach. As part of representing this specific clientele, she works with law enforcement and independent forensic investigators in identifying the cause and scope of a data breach, identifies and engages vendors necessary to offer breach response services to both her clients and the affected population, identifies and satisfies state, federal, and international legal obligations entities may have as a result of a data breach, and defends entities against third-party and regulatory actions arising from the data event. Jennifer also represents clients looking to proactively protect against a data breach by identifying state, federal, and internal legal obligations an entity may have if a breach were to occur, assisting clients in identifying data for which it is responsible, and preparing information management plans and incident response plans geared towards efficient and effective breach response.

Jennifer is a frequent lecturer on privacy and data security matters, and was previously employed as Claim Counsel with a CyberRisk insurer, where she assisted CyberRisk insureds in first- and third-party security breach response. Prior to her employment with the CyberRisk insurer, she was employed as a Breach Coach.

Ms. Coughlin holds a B.A. from Cabrini College (2002) and a J.D. from Widener University School of Law (2005).

About Lewis Brisbois

Established in 1979, Lewis Brisbois Bisgaard & Smith LLP is a national, full-service law firm with more than 1,000 attorneys and 35 offices in 22 states and the District of Columbia. Our national practice is sophisticated, multi-faceted and well-versed in current legal trends, while our individual state practices provide vast resources and knowledge of procedural and legal nuances. Lewis Brisbois offers legal practice in more than 30 specialties and a multitude of sub-specialties associated with each practice area. Our attorneys have broad knowledge, expertise, and sensitivity to their clients' unique needs. Through interaction among its practices, Lewis Brisbois provides a wide range of legal services to each client with a continuity of representation over multiple disciplines. We have built longstanding relationships with corporate and institutional clients based on our ability to provide comprehensive service on a national scale. Lewis Brisbois is known for its commitment to principled advocacy, an unflinching work ethic, and unyielding recognition of our duty to provide the highest level of service to our clients, who choose us because we take the time to understand their business interests and philosophies. We have developed sophisticated

proprietary risk evaluation and litigation management processes that many of our clients have incorporated into their business practices, and we help them manage and defend claims and litigation. As a result, they are avoiding and reducing losses that impact their bottom line. We are truly client-driven and result-oriented.

For more about Lewis Brisbois, please visit us at LewisBrisbois.com.

Ben Beeson - Lockton

(bbeeson@lockton.com)

Ben Beeson is Senior Vice President and Leader of the Cybersecurity Practice at Lockton Companies. Based in Washington, DC, he advises organizations on how best to mitigate emerging cyber risks to mission critical assets that align with the business strategy. As insurance continues to take a greater role in a comprehensive enterprise cyber risk management program, Ben also designs and places customized insurance solutions to fit an organization's specific needs. Ben's experience ranges from addressing data privacy issues in the utility, financial, healthcare, retail, and hospitality industries to identifying emerging property damage and bodily injury risks from a cyber attack in energy, transportation, and manufacturing.

Prior to moving to Washington DC, Ben was based in Lockton's London office for seven years, where he cofounded and built one of the leading cybersecurity teams in the industry.

Ben holds a B.A. (Hons) degree in modern languages from the University of Durham, UK, and a certification in cybersecurity strategy from Georgetown University, Washington DC.

About Lockton

More than 5,300 professionals at Lockton provide 41,000 clients around the world with risk management, insurance, and employee benefits consulting services that improve their businesses. From its founding in 1966 in Kansas City, Mo., Lockton has attracted entrepreneurial professionals who have driven its growth to become the largest privately held, independent insurance broker in the world and 10th largest overall. Independent researcher Greenwich Associates has awarded Lockton its Service Excellence Award for risk management for large companies. For six consecutive years, Business Insurance magazine has recognized Lockton as a "Best Place to Work in Insurance."

To see the latest insights from Lockton's experts, check Lockton Market Update.

Robert J. Shaker II - Symantec

Bob Shaker is a Director of Strategic Operations in Symantec's Cyber Security Services organization. Bob spends his days working with teams on ways to protect customers and prepare for the future. Growing dynamic teams of people and helping to eliminate obstacles in the way of success are his primary goals. By doing this, Bob is able to help Symantec customers identify, contain, and eradicate increasingly sophisticated attackers as part of Symantec's Incident Response Service.

Mr. Shaker's prior role was as CTO for the Security Business Practice, an organization that provided deep technology specialization in support of field sales efforts; strategic guidance to Symantec security business unit leaders on security market trends and opportunities; and increased security industry visibility for the Americas. He also led a team of Security Strategists focused on direct interactions with CISOs to understand real-world IT security challenges and help them drive internal change.

Prior to joining Symantec, Mr. Shaker worked for Wellington Management Company, LLP for nine years, where he served as Vice President, Director, Information Security and Internal Controls. He was a global Incident Commander, responsible for developing and executing global incident response plans that included Security, DR and BCP. He also drove the strategic direction of information security for the firm, including policy, architecture, engineering and the internal controls program. He was also the central resource for Information Services for all client, regulatory, and internal due diligence and audit requests, including SAS 70, OCC, SEC, etc.

Before joining Wellington, Mr. Shaker worked in leadership roles for several consulting organizations where he developed, sold, and executed security solutions with a team of security professionals.

Mr. Shaker earned his Bachelor of Science degree from the University of Massachusetts.
LinkedIn Profile: www.linkedin.com/in/rshaker2

Melanie Dougherty Thomas - Inform

(mthomas@informtheagency.com)

Melanie is the CEO at Inform, and has over 25 years of experience in marketing and communications, beginning at just 17 years old, when she worked for the Washington, DC affiliate of NBC News. She continued to work in network news for organizations like CNN, NewsLink, Conus, and Fox while earning her BA in journalism from George Washington University. In 1996, Melanie began her career in public relations representing clients in cyber security, data privacy, technology, healthcare, finance, homeland security, defense, consumer markets, public affairs, and foreign governments, in both an in-house and firm capacity. Her experience transcends traditional communications, with expertise in strategy, media relations, crisis communications and integrating new media tools to leverage exposure for her clients. Melanie started Capitol Communications (now Inform) over a decade ago to meet the growing need for highly specialized public relations talent in Washington, D.C. The firm now has nearly a dozen communications veterans, each with over 25 years experience, in Washington D.C., New York, and San Francisco. In addition to leading her firm, Melanie spends a considerable amount of time speaking and blogging about crisis communications and branding.

About Inform

Inform is a public relations firm that specializes in crisis communications with a unique expertise in privacy, data breach, and cybersecurity. We help companies prepare for and respond to security events and breaches through our Inform (RED) Crisis Communications, ™ which includes Inform Crisis Response Planning. Our program helps organizations create and test a comprehensive plan, which includes: strategy development, procedure, messaging for various scenarios, content creation, media training, media management, reputation management, and brand rehabilitation. We also deploy a rapid response engagement through our Inform Crisis Response Group, ™ to manage the communications response of a data breach event within 24 hours, as a part of the incident response team. Our team of professionals each has over 25 years of public relations and professional news industry experience. We have deep experience working breach responses for small businesses, Fortune 100 companies, and global conglomerates. Inform has offices in Washington, D.C., New York, and San Francisco.

You may view our company and professionals at: www.InformTheAgency.com, reach us through our INFORM BREACH HOTLINE at: 844-678-8866, or contact the company's CEO, Melanie Dougherty, at: mthomas@informtheagency.com

Lisa Sotto - Hunton & Williams LLP

(lsotto@hunton.com)

Lisa J. Sotto is the managing partner of Hunton & Williams LLP's New York office and chair of the firm's top-ranked Global Privacy and Cybersecurity practice. Lisa was named among *The National Law Journal's* "100 Most Influential Lawyers," was voted the world's leading privacy advisor in *Computerworld* magazine, and was recognized by Chambers and Partners as a "Star" performer for privacy and data security. She was recognized as a leading lawyer by *The Legal 500 United States* for cyber crime and data protection, and was featured as "The Queen of Breach" in *New York Super Lawyers Magazine*. Lisa serves as Chairperson of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. She speaks frequently at conferences, testifies regularly before the U.S. Congress and other legislative and regulatory agencies, and is the editor and lead author of the legal treatise entitled *Privacy and Data Security Law Deskbook*, published by Aspen Publishers. Lisa received her JD from the University of Pennsylvania Law School, and her BA from Cornell University, with distinction in all subjects.

Ryan Logan - Hunton & Williams LLP

(rlogan@hunton.com)

Ryan P. Logan is an associate in the New York office of Hunton & Williams LLP, and he is a member of the firm's Global Privacy and Cybersecurity practice. His practice focuses on privacy, cybersecurity and records management. Ryan assists clients in conducting privacy and information security assessments, developing and implementing records management programs, and drafting privacy notices, contracts, policies and procedures. He counsels clients on the impact of various privacy laws, including the Gramm-Leach-Bliley Act, HIPAA, CAN-SPAM, and other state, federal and international privacy requirements. Ryan received his JD from Vanderbilt University Law School, where he was a Chancellor's Scholar, and his BA from Stanford University.

About Hunton & Williams LLP

Since our establishment more than a century ago, Hunton & Williams has grown to 800 lawyers serving clients from 19 offices worldwide. We have a strong industry focus on consumer products and retail, energy, financial services, and real estate. Our global experience extends to myriad legal disciplines, including bankruptcy, commercial litigation, corporate transactions and securities law, intellectual property, international and government relations, regulatory law, privacy and cybersecurity, and products liability.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings – anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 19,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2015, it recorded revenues of $6.5 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com