THE ROAD TO BECOMING A CERTIFIED DATA PRIVACY OR CYBERSECURITY PROFESSIONAL

By: Gretchen A. Ramos, Partner, Squire Patton Boggs LLP

Privacy and cybersecurity news seems to be everywhere we turn. A recent survey of 42,000 people around the world by the Pew Research Center found that cyberattacks were the third highest concern on people’s minds and second highest for Americans. Likewise, other surveys have pointed to data privacy and cybersecurity as being one of the main worries keeping in-house counsel up at night. These issues permeate almost every industry, with businesses across the world realizing that privacy matters to customers, and that data incidents or breaches can severely damage their brand.

Compliance with the patchwork of federal and state privacy laws in the United States can be challenging for organizations. For global organizations, compliance can be even more complex as privacy laws vary country-by-country, and in many cases are more strict than the U.S. laws. Consequently, professionals who understand these risks and how to manage them in relation to the ever-changing legal landscape are in huge demand. This is especially true right now given the looming May 25, 2018 deadline when the European Union’s new data protection law becomes effective. The General Data Protection Regulations (“GDPR”) will fundamentally change how companies handle EU personal data, whether they are based in Europe or not.

It is inevitable that at some point in your practice, if it has not already occurred, you will face a privacy and cybersecurity issue that needs to be addressed. Whether you want to become a privacy or security professional or are just interested in learning more about this area

Continued on page 11
Welcome to the New Diverse Speakers Directory Page!

Open to both ABA and Non-ABA members.

The Directory is a great way to build your resume and expand your career!

- Expand your speaking experience both nationally and internationally.
- Show off your technical skills.
- Market yourself to more than 3,500 ABA entities seeking speakers around the country and the world.

https://www.americanbar.org/diversity-portal/SpeakersDirectories.html

For more information or questions regarding the directory email: diversity@americanbar.org
Cybersecurity and Data Privacy Committee: TIPS Welcomes a New Committee

TIPS is excited to welcome our newly formed Cybersecurity and Data Privacy Committee. Cybersecurity and data privacy have become major issues for every profession and every industry. TIPS members confront cybersecurity and data privacy issues every day for clients, for their own organizations, and in addressing insurance and compliance issues. With new regulations and laws proliferating and with most companies and organizations developing policies around cybersecurity and data privacy, the new TIPS Cybersecurity and Data Privacy Committee could not be launching at a more opportune time.

Three years ago, under the leadership of then-chair Glennon Troublefield, TIPS created the Cybersecurity Task Force to examine and address the myriad and rapidly developing issues concerning cybersecurity and data privacy. The Task Force was chaired by Kathleen Strickland. The mission was to educate TIPS members about cybersecurity and data privacy and to determine the effect of these emerging risks on TIPS members and their law firms and clients. The Cybersecurity Task Force developed and sponsored significant programming. TIPS leadership recognized the need for TIPS to become a resource to its members on cybersecurity and data privacy issues. Because of the success of the Cybersecurity Task Force, the TIPS Council voted in February to turn the Task Force into the first new TIPS general committee in over a decade. The Cybersecurity and Data Privacy Committee will launch September 1, 2017. It will be Chaired by Kathleen Strickland, with Janice Mulligan as Chair Elect and Michelle Tilton as Chair-Elect designee. We encourage many of you to become members of this committee and to work with us as we confront cybersecurity issues daily in our practices and in our law firms.

The mission of the Cybersecurity and Data Privacy Committee is three-fold. First, to educate TIPS members on cybersecurity and data privacy issues affecting “clients.” Second, to educate lawyers on data security and data privacy issues arising in the context of their own legal practices and law firm operations to ensure that private, non-public, and privileged information does not become the subject of a data breach and, if it does, to have a plan to handle such a breach. Third, to educate TIPS members and clients on the insurance issues involving cybersecurity, the insurance products available, and the limitations of those insurance policies.

The Cybersecurity and Data Privacy Committee will continue the work of the Cybersecurity Task Force by planning and sponsoring, on its own and with other committees, programs on cybersecurity and data privacy, as well as continuing to host the cybersecurity page on the TIPS website, a committee webpage and the cybersecurity blog. Plans include developing a comprehensive list of links focused on cybersecurity and data privacy news and developments, an active LinkedIn group page (which already exists) and significant programming.

The new Cybersecurity and Data Privacy Committee will be composed of a majority of the Cybersecurity Task Force members and a broad cross-section of the Section’s membership with varying degrees of cybersecurity and data privacy knowledge and expertise. The Committee is a place to exchange ideas in and share experiences in dealing with cyber breaches, from both a first party and third party liability perspective as well as from a coverage perspective. If you are interested in cybersecurity and data privacy issues and would like to join this energetic, fun new Committee, please go to MyABA Profile at www.americanbar.org. There you will be able to access your committee preferences and choose Cybersecurity after September 1, 2017 and sign-up to join our committee. We welcome all of you to join us as members of the new Cybersecurity and Data Privacy Committee and look forward to greeting you at a meeting in the near future.

Kathleen Strickland
Ropers Majeski Kohn & Bentley
Dear Readers:

It is my pleasure to present the inaugural Newsletter from the ABA TIPS Cybersecurity and Data Privacy Committee. This inaugural issue features four intriguing articles regarding utilization of responsible disclosures to mitigate cybersecurity attacks, the recent WannaCry ransomware attack, the use of Bitcoin and blockchain technology in ransomware attacks, and an in-depth look at the pathway to obtaining certification as a data privacy and cybersecurity professional. I hope that you find these articles to be interesting and relevant to the every changing climate of cybersecurity and data privacy law.

We are currently looking for submissions for the next newsletter, and I encourage committee members and non-members alike to submit article proposals directly to me at jzucker@grsm.com.

Thank you to the authors who have contributed to this newsletter, and to the section members for their ongoing efforts in supporting this publication. A special thanks to committee chair, Kathleen Strickland and the Newsletter Editors, Amber Locklear, Brian Findley, and Kara Jermain for their help with this newsletter.

Enjoy the issue, and thank you for your participation in the Data Privacy and Cybersecurity Committee.

Justin A. Zucker
Gordon & Rees, LLP
Newsletter Editor-In-Chief

Brian Findley, Mulligan, Banham & Findley
Newsletter Editor

Amber Locklear, Ropers Majeski Kohn & Bentley
Newsletter Editor

* Not pictured Kara Jermain, Gallup Inc., Newsletter Editor.
RESPONSIBLE DISCLOSURE IN CYBERSECURITY: Extortion or a Valuable Weapon in the Fight Against Cyber Crime

By: Stephen J. Cosentino, Stinson Leonard Street

Your client receives what looks at first glance to be a typical demand letter. Eyebrows are raised when the client reads that it pertains to a security breach in one of the client’s most important systems. The client pauses for a moment as this seems to be quite an odd scenario. Data breaches are a common occurrence these days, but who sends a letter bragging about a cybersecurity exploit? Is this a phishing attack? No, it came in the snail mail. It does have a startling amount of detail about the client’s systems. Is it time to roll out the cybersecurity incident response plan? Upon reading further, your client’s intrigue turns to outrage. The attacker is offering to work with your client to remedy the data breach and issue a joint press release about the results of the remediation effort. Now we are in new territory.

This scenario falls under the rather innocentsounding name, “responsible disclosure.” The cybersecurity field contains a multitude of hackers and security investigators who uncover system and network vulnerabilities for a wide variety of reasons. Some are motivated by a sense of duty to make the technology community stronger, some look to make a name for themselves in the field and others may have more nefarious purposes. Given the large number of players in this game, exposing vulnerabilities can appear organized and formal or random and chaotic. Responsible disclosure is a term that defines a particular disclosure model and is often used in at least a somewhat more organized fashion that will inevitably involve guidance from a target’s cybersecurity council.

In the continuum of various vulnerability disclosure models, the relatively simple model of “non-disclosure” lies at one end of the spectrum. Non-disclosure seems relatively obvious. The person discovering the vulnerability will disclose it to a few trusted individuals so that the fix can be accomplished before word gets out about the potential threat. This model assumes that the information can be controlled. Black hat hackers and even former black hat hackers can be under significant pressure to disclose vulnerabilities to their peers, resulting in potential exploits with a relatively small number of trusted individuals working on the attack.

On the other end of the spectrum is full disclosure, whereby a vulnerability is immediately exposed with the idea that negative press from such disclosure will help motivate stronger security to avoid future attacks. These disclosures will often include the exploit code and typically do not give the target any prior warning of the release. The result can be a mad race between the target’s efforts to patch the vulnerability and the black hat community’s efforts to exploit it.

Somewhere in the middle lies responsible disclosure. Under this model the discloser notifies the target before making any public disclosure. Typically there is a grace period during which the target, sometimes with assistance from the attacker, works to resolve the vulnerability. This approach allows some time for the target to fix the problem prior to the attacker tipping off the public as to the vulnerability. Once a patch or fix is made or sometimes once the grace period expires, the attacker will disclose the vulnerability publically either with or without the cooperation of the target.

To a client receiving a demand letter relating to a responsible disclosure, it is easy to ascribe malicious motives to the attacker. While some white hat hackers are truly motivated by improving the technology community, others understandably have self-interested motivations. Security firms sometimes engage in responsible disclosure with the idea of making a name for themselves in a particular field of cybersecurity. A firm might aspire to be the Symantec of a particular growing niche of the Internet of Things field. The responsible disclosure lines could blur with extortion where the motive is signing the customer up for cybersecurity services or receiving some sort of compensation.

The motivation of the attacker doesn’t typically make a target feel a whole lot better about the incident. Why would a security firm trying to make a name as a reputable provider engage in such activities? Understanding the reasons for uncovering...
CONSIDER RANSOMWARE NOW SO YOU DON’T WANNACRY LATER

By: Roberta D. Anderson, Director, Cohen & Grigsby

On May 12, 2017, a massive wide-scale cyberattack involving a ransomware software program called Wanna Decryptor, also known as “WannaCry,” swept the globe, freezing computer systems and causing major disruptions. The attack — which is the largest ransomware infestation ever — affected tens of thousands of organizations across the globe and a wide range of industry sectors, including the United Kingdom’s National Health Service (NHS), Spanish telecom giant Telefonica, France’s car-maker Renault, Portugal’s Telecom, and the United States delivery company FedEx, among many others. The attack is reported to have claimed over 200,000 victims in over 150 countries. In the wake of WannaCry, another strain of ransomware, dubbed “NotPetya,” hit at least six countries, including the Ukraine, where NotPetya precipitated a large-scale, coordinated attack on key parts of the nation’s infrastructure.

Ransomware (a combination of the terms malware and ransom) has become an increasingly common form of cyber extortion. It often involves extortionists taking control over a computer system and locking files and data on the system by encryption, thereby rendering them inaccessible, and useless, until a demand for payment, typically in Bitcoin, is satisfied. A typical form of ransomware, WannaCry does the following: 1. locks all data on the victims’ computer systems, 2. informs victims that their files have been encrypted, 3. warns that those files will be deleted unless payment in Bitcoin is received, and 4. provides instructions for executing and sending the payment.

Ransomware has become frighteningly pervasive and increasingly serious and expensive. Ransomware attacks quadrupled from 2015 through 2016, to an estimated 4,000 per day according to the United States Department of Justice and, as punctuated by WannaCry, are projected to double yet again in 2017. These types of cyberattacks can, and do, cause significant operational disruption, often halting a business in its tracks, reputational damage and other types of losses and exposures. Every industry sector is seeing an increasing threat, with the healthcare and education sectors particularly targeted. Other forms of cyberextortion, including threats to obtain or release protected information, such as personally identifiable customer data, protected health information and confidential corporate information, or to discharge denial-of-service attacks that disrupt an organization’s networks, causing business interruption, also entail significant potential exposure to organizations.

Here we offer five insurance and other considerations for organizations to consider in the face of an enormous uptick in increasingly severe ransomware attacks and other forms of cyberextortion:

1. Consider purchasing “cyberextortion” insurance. No firewall is unbreachable, and no security system impenetrable. In the context of this reality, insurance can play a vital role in a company’s overall strategy to address, mitigate, and maximize protection against the legal and other exposures flowing from serious cybersecurity, privacy and data protection-related incidents. Importantly, almost all stand-alone so-called “cyber” insurance policies offer coverage for ransomware and other forms of cyberextortion. This type of coverage is specifically designed to cover losses and expenses that an organization incurs in the wake of a cyberextortion incident like the WannaCry software virus, together with myriad other forms of first and third-party cybersecurity and data privacy-related exposures, including coverage for crisis management (such as notification to potentially impacted individuals, credit monitoring, and call center services), data breach and network security-related claims and liability, including regulatory liability, business income loss, and digital asset loss. Cyberextortion coverage can be extremely valuable as a way for organizations to address and mitigate losses arising from mounting extortion threats, and many organizations now purchase this coverage as part of their cyberinsurance programs.

2. Closely review cyberextortion insurance terms and conditions. It is clear that cyberinsurance can be extremely valuable, but obtaining the right

Continued on page 13
BITCOIN AND RANSOMWARE: THE PEANUT BUTTER AND JELLY OF CYBER ATTACKS

By: Jeremy D. Kerman, Associate, Walker Wilcox Matousek LLP

With many calling 2014 “the year of the retail breach” and 2015 “the year of the health care breach,” the leading moniker for 2016 is “the year of ransomware.” And ransomware shows no signs of slowing down in 2017. If anything, this favorite tool of hackers seems to be gaining steam both domestically and internationally.

In a typical ransomware attack, hackers use software to block access to a computer system until party pays a ransom amount, usually in the form of “Bitcoins.” But what is a Bitcoin? And why is it so popular in ransomware attacks? The short answer is that Bitcoin has three hacker-friendly features: (1) transfers are anonymous; (2) no central bank or agency oversees the transactions; (3) and transfers are irreversible.

What is Bitcoin and How Does It Work?

Bitcoin is digitally created currency that exists electronically. Unless it is converted into another form of currency through an exchange, Bitcoin only exists on-line. Unlike typical currency, which is printed by a government, Bitcoin is created through a process called “mining.” Bitcoin “miners” solve complex math problems with randomized input data, and when the problem is solved and verified by other miners, the miner who solved the problem is rewarded with Bitcoins (usually 25, but the number can vary).

A Bitcoin miners’ work serves another function: it verifies each Bitcoin transaction. In other words, the “complex math problem,” that a miner solves is the verification of prior transactions. As a result, the verification process necessarily involves prior Bitcoin transactions as part of the data needed to solve the problem. When a series of transactions (called a “block”) occur, miners put the information in that block through a publicly available mathematical formula to convert it into a more compact, random series of numbers and letters called a “hash.” A critical portion of each hash is produced using the hash of the block that preceded it. This allows miners to track the history of transactions back to the very first Bitcoin transaction.

This entire history of Bitcoin transactions is called the “blockchain,” a public ledger for the whole Bitcoin system. Since miners can look at each block and check it against each preceding block (as well as against the entire block chain), they can confirm that each transaction is legitimate. If a transaction isn’t legitimate, it cannot not be reconciled with the blockchain. A miner who verifies a block submits his solution (called a “proof of work”) to other miners who essentially double-check the result. The other miners stamp the proof of work as a notary would stamp the recording of a deed, publicly verifying that each transaction, and therefore the whole blockchain, is trustworthy. It takes only about ten minutes for a miner to submit a proof of work and for other miners to verify it, thus finalizing the Bitcoin transaction.

Bitcoin users store their Bitcoins in a digital “wallet” on a computer or mobile device. The amount of Bitcoins in each wallet is visible to everyone since the blockchain (and every transaction within it) is public, but each user has a “private key” that only they know. The private key is what allows users to exchange or transfer the Bitcoins in their wallet. Think of the wallet as a safety deposit box made of glass so everyone can see how much is in it, but only the safety deposit box owner has the key to access the contents inside.

Importantly, the wallets do not require users to identify themselves by name or any other type of identifying information. The wallet is simply an account identified by a series of random numbers and letters. When a pure Bitcoin transaction occurs, the real names of buyers and sellers are not revealed in the wallet, or anywhere on the blockchain. The exception to the anonymous exchange occurs if someone wants to exchange Bitcoin for a good or service, or wants to convert the Bitcoin into another type of currency through an exchange.

Why Do Hackers Request Bitcoin for Ransomware Attacks?

Given the way that Bitcoin works, it is no surprise that hackers demand that ransomware be paid in Bitcoin. Since wallets do not require users to share their identities, Bitcoin is untraceable so long as a hacker...
keeps his or her ransom in Bitcoin form. And, since the blockchain only shows amounts and wallet account numbers, there is no way to tell why Bitcoin was paid for any given transaction. The appeal to criminals is obvious: simply viewing the blockchain does not reveal whether Bitcoin was paid for a legitimate reason, or for illegal purposes like purchasing drugs, funding terrorist activities, or paying off a ransomware attack.

Other appealing features of Bitcoin for criminals include:

- lack of central authority overseeing the transactions. This means that Bitcoin can be used in any country without fear of authorities attempting to freeze Bitcoin accounts suspected of funding illegal activities;
- even though the blockchain is public, the lack of a central authority means that only the user with a private key matching a specific wallet can access the Bitcoin;
- Bitcoin transactions are processed without intervention by a bank or other authority—all that is required is the ten-minute verification process by miners;
- each transaction is non-reversible and final, so a hacker is guaranteed to keep any ransom payment without fear of confiscation; and the final step for a hacker looking to cash-in is to find a “Bitcoin-to-other” currency exchange, which are often paid to launder Bitcoins.

These exchanges convert hundreds of Bitcoin transactions to other forms of currency while ignoring the identity of the criminal seeking the exchange. Ultimately, while Bitcoin was not created for criminal enterprise, it is clear why it has become a perfect vehicle for ransomware attacks. Bitcoin has many benefits, but as long as it remains untraceable, ungoverned by a central authority, and with irreversible transfers, ransomware hackers will continue to exploit its virtues.

A Recent Example: The WannaCry Attack

Preying on a vulnerability in Microsoft systems that was reportedly first discovered (but not confirmed) by the NSA, hackers recently infected hundreds of thousands of computers with interconnected ransomware attacks in almost 100 countries. The attack—dubbed the “WannaCry ransomware attack because it involved the WannaCry ransomware cryptoworm—began on Friday May 12, 2017 and spread quickly, targeting, locking out, and blackmailing a broad swath of users such as the UK’s public health system, Russia’s Interior Ministry, and FedEx in the U.S. A second-wave of attacks crippled more computers, but not at the rate seen on May 12.

The initial “ransom” cost to unlock individual computers was about $300 per computer paid in Bitcoin, with the amount doubling if the ransom was not paid within 3 days. Had most affected users paid up, the hackers would have had a good payday. But reports put their collections at about $70,000. It is still unclear how many victims paid the ransom, accepted their fate, or had back-up systems in place.

Why was WannaCry attack so effective and pervasive? Some experts point to the hackers’ use of an encrypted file that, once downloaded, allowed the ransomware to take over the host computer, locking access to data until ransom was paid. The encrypted file was a particularly crafty choice because the ransomware went undetected until opened and downloaded by the user. By that point, it was too late to react because the ransomware began replicating across the already-infiltrated network.

This latest attack one of the increasingly many and sobering wake-up calls about the vulnerability of all systems, also provides a perfect illustration of why Bitcoin is such an effective tool for ransomware hackers.
SAVE THE DATE

Join us in celebrating TIPS 85th anniversary!

TIPS SECTION CONFERENCE
May 2-5, 2018 | Loews Hotel Hollywood
Los Angeles, CA

- Learn:
  Absorb over 25 hours of CLE from distinguished panelist including prominent judges and leading in-house and corporate counsel.

- Celebrate:
  Honor 85 years of excellence and professionalism in the industry at the highlighted social event - the TIPS Gala Night.

- Network:
  Expand your circle at our complimentary nightly networking receptions.

- Join:
  Become involved with our 31 practice-specific committees for professional development and leadership opportunities.

- Enjoy:
  Explore Los Angeles and the sunshine state with colleagues, new and old.

americanbar.org/tips
THE ROAD TO BECOMING... Continued from page 1

so you can better understand your client’s or employer’s concerns, it would be wise to consider obtaining professional certification in this area. Such certification will demonstrate you are dedicated to and have a strong base of knowledge about this ever-growing area of work, provide you with access to a network of other privacy and security professionals that you can confer with, and for in-house positions might even result in an increased salary. Additionally, many organizations now require certain certifications for particular positions, since they establish that an individual has the skill set necessary for that role.

There are many types of certification, and the one you decide to pursue will depend upon your field and specialty. Most attorneys, unless they have a technology or security-related background, typically pursue certification through the International Association of Privacy Professionals (IAPP). Many years ago, I obtained my IAPP certification and became a Certified Information Privacy Professional (CIPP) in U.S. private sector privacy law and European privacy law. While unfortunately these certifications do not instantly provide me with all the answers in this fast-changing field, they do provide me with the tools necessary to identify the issues that I need to address for clients to most effectively toward a resolution.

The IAPP offers various certifications that demonstrates that a professional understands the laws, regulations, and standards of privacy in a given jurisdiction or discipline. Separate certification can be obtained in relation to the privacy laws of Canada, Europe, the United States for both the private sector and government as well as for Asia. Becoming a Certified Information Privacy Manager (CIPM) shows that an individual understands how to use process and technology to manage privacy in an organization—regardless of the specific industry or jurisdiction. The IAPP also offers training to become a Certified Information Privacy Technologist (CIPT), which is for professionals in the IT, security, or engineering, demonstrating that they know how to manage and build privacy requirements and controls into technology.

Attorneys with a background or understanding of information security and data privacy issues are in even greater demand, given the two areas work hand-in-hand in protecting an organization’s data. The International Information Systems Security Certification Consortium, Inc., or (ISC)2 is well known and offers numerous vendor-neutral security certifications with specializations in security architecture, security engineering and security management. (ISC)2 offers training to become a Certified Information Systems Security Professional (CISSP), which indicates that an individual has the knowledge and experience to design, develop, and manage the overall security posture of an organization. They also offer specialized programs to become a Certified Cloud Security Professional (CCSP), highlighting knowledge of best practices for cloud security architecture, design, operations, and service orchestration, as well as a HealthCare Information Security and Privacy Practitioner (HCISPP) certification, which shows the ability to implement, manage, or assess security and privacy controls for healthcare and patient information. In addition, for professionals involved in the Healthcare industry, Compliance Certification Board (CCB) certification programs should be considered, which are designed specifically for professionals in the healthcare industry.

The Information Systems Audit and Control Association (ISACA) also offers security certification programs. The ISACA is an independent, nonprofit, global association that engages in the development, adoption and use of globally accepted information system (IS) knowledge and practices. They offer several certification programs for security professionals including Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified in the Governance of Enterprise IT (CGEIT), Certified in Risk and Information Systems Control (CRISC), and Cybersecurity Nexus (CSX Certificate and CSX-P Certification) credentials.

If you are truly interested in steering your career in this direction, these are some of the training programs that will provide you with certifications showing your commitment to and knowledge of privacy or security issues. They will also, importantly, provide you with a community well-versed in this area. The training and the IAPP certifications that I have obtained have been well worth my time and have allowed me to practice an area of law that hardly existed when I graduated from law school. In this age of the cloud, Internet of Things and big data, such an investment is well worth your time. As I have experienced, it will surely open many doors for you in an area that impacts every industry, is intellectually stimulating, and will continue to change and adapt as technology further develops. So the time is now, don’t delay, jump in and start learning – you will certainly not regret it.
RESPONSIBLE DISCLOSURE
Continued from page 6

the vulnerability can certainly help the target in understanding what may happen next. Once a target receives notice of a vulnerability, the clock starts ticking on data breach notification requirements under various state statutes. These statutes often have some element of the likelihood of misuse of personal data or account information. It may be that after working through the process, the target can come to the conclusion that the incident was simply exposure of a vulnerability that did not result in an actual data breach with no likelihood of identity theft or fraudulent transactions.

Because of the potential for significant liability and bad press surrounding the failure to properly remediate a data security vulnerability, many targets of a responsible disclosure will choose to cooperate. By cooperating a company can gain some assistance in patching the vulnerability and try to cast the publication of the vulnerability and remediation efforts in a positive light. In today’s environment where data breach is not a question of if but when, that strategy often makes good business and legal sense under the circumstances.

There are some legal tools that can be used to try to seek some recourse over a discloser. Software code is protected by copyright, and a responsible disclosure of the original code could potentially constitute copyright infringement. A researcher may have also been subject to an end-user license agreement or a non-disclosure agreement in order to access the target’s system, giving rise to a potential breach of contract or trade secret claim. The Digital Millennium Copyright Act (17 U.S.C. § 1201) contains anti-circumvention measures that have been used, unsuccessfully, on several occasions to threaten security researchers. The Computer Fraud and Abuse Act (18 U.S.C. § 1030) prohibits accessing a protected computer without authorization. In the Internet of Things context, patent rights can also come into play where designing hardware or software to replicate a vulnerability could potentially infringe the claims of the target company’s patents.

With counterbalancing protections in the First Amendment and public policy leaning towards cooperative efforts to thwart widespread damage caused by cybersecurity threats, it is likely that responsible disclosures are here to stay. That has become more apparent with the willingness of businesses to embrace responsible disclosure. For example in January of 2016, General Motors became the first major automaker to launch a public security vulnerability disclosure program in conjunction with HackerOne, a portal that seeks disclosures and pays bounties for revealing bugs. The idea behind these programs is that through the tradeoff of agreeing not to sue the researchers, a business can take advantage of the power of multiple cybersecurity experts working together to find vulnerabilities and help limit them.

In recent years, many technology companies have negotiated contracts that shift some of the risk of cyber attacks to their customers. They rationalize that a technology company can do everything right and still be subject to an attack. Agreements often include paragraphs of exculpatory language on this point. If a customer finds itself in a less than ideal service agreement, the information technology team could use responsible disclosure as a motivational force to encourage technology vendors to increase their cybersecurity efforts. Actual damages can often pale in comparison to the reputational harm of a cybersecurity event, which harm is often excluded even in the most customer friendly contracts. Because the information technology community tends to view responsible disclosure in a more positive light than legal counsel might, anticipating this issue becomes important. Legal counsel should make information technology teams aware of the risks of using responsible disclosure in this way as it could likely violate use restrictions and confidentiality obligations in the applicable agreement.

Although responsible disclosure presents a variety of legal challenges, counsel should keep in mind the central theme of increasing security threat awareness. The ability to coordinate with the discloser and a company’s communications team on the scope and nature of the threat plays an important role in how the threat is perceived. In the context of the Internet of Things, for example, an inappropriately disclosed vulnerability can cause the public to picture a nefarious overseas actor controlling devices remotely and wreaking physical havoc on a target. A well-crafted disclosure could tailor that picture to show that the vulnerability required some physical proximity to the target or that the remediation efforts are a positive part of a program to expose and limit attacks.

While little can be done to reduce the initial shock of a cyber attack, a little training and counsel on this issue can go a long way in making the response diligent, expedient and positive.
insurance product presents significant challenges. There is a diverse and growing array of cyberinsurance products in the marketplace, each with its own insurer-drafted terms and conditions that vary dramatically from insurer to insurer — and even between cyberinsurance policies underwritten by the same insurer. In addition, the specific needs of different industry sectors, and different organizations within those sectors, are far-reaching and diverse. For these reasons, organizations purchasing cyberinsurance, and the cyberextortion components of that insurance, are well advised to closely review the terms and conditions of the coverage to ensure that the organization’s cyber extortion risk will be covered, without a protracted battle with the insurer, in the wake of an attack. Among other things, organizations are advised to consider the following:

• Scope of coverage. Cyberextortion coverage should be written to cover as broad a range of potential attacks, and potential exposure outcomes, as possible. The coverage should include any threat to negatively impact, impair access to or engage in unauthorized access to, relevant computer systems and the applications, files and data residing on those systems, together with any threat to access or divulge any sensitive information in the organization’s possession or control.

• Key definitions. Key definitions must be sufficiently broad to match the reality of risk faced by the insured organization. By way of example, in addition to definitions that define the scope of coverage, definitions governing the types of losses and expenses that are covered should be carefully reviewed. The policy should cover reasonable and necessary expenses incurred by the insured organization resulting from a covered threat, including the costs of investigating and assessing a threat (even if no ransom is paid), should expressly cover payment of cryptocurrencies (including Bitcoin), as well as, preferably, any other consideration or action that may be demanded by the extortionists, and should cover reasonable

• Conditions. Organizations are advised to pay close attention to policy conditions, including notice and consent provisions, proof of loss provisions, allocation provisions, alternative dispute resolution provisions and any requirements that the organization notify law enforcement of the incident at issue. The importance of notice provisions is addressed in further detail below. Consent provisions may be favorably amended to state that an insurer’s consent to satisfying the extortion demand “shall not be unreasonably withheld”. Other provisions, such as the requirement of involving authorities, may be deleted. As discussed more below, cyberinsurance policies are highly negotiable and very favorable amendments can often be made for no additional premium charge.

• Exclusions. It also is critical that organizations be aware of any insurance policy exclusions that may vitiate the coverage that the policy was intended to cover. By way of example, cyberinsurance policies typically contain a “bodily injury” exclusion. Such an exclusion may pose a particularly problem for hospitals and other health care providers, which rely on access to patients’ medical records to provide appropriate care and treatment. As with other exclusions, it may be possible to significantly curtail or delete bodily injury exclusions. Many other types of exclusions can be curtailed or deleted — often for no additional policy premium.

• Sublimits and retentions. It is clearly important that a cyberinsurance sublimit of liability (a ceiling on the amount of coverage available to cover a specific type of loss at issue) be sufficient to cover the organization’s potential exposure. Like other facets of cyberinsurance coverage, including coverage for losses associated with regulatory action and PCI DSS-related liabilities, cyberextortion coverage may be written subject to a relatively low sublimit, such that, for example, a $10 million limit
primary policy may provide only $250,000 or $500,000 for cyberextortion losses. In addition to policy limits, organizations are advised to pay attention to self-insurance features, such as policy retentions or deductibles, which typically range from $0 to excess of $5 million. As with the case of other cyberinsurance terms and conditions, sublimits and retentions usually are negotiable. On a related point, as discussed further below, what starts with an extortion threat can end up triggering many different modular aspects of cyberinsurance coverage. It therefore is important that the policy contain a provision stating that an extortion threat, together with any other first or third-party covered events that trigger different coverage sections of a policy, are subject only to a single retention, and that any lower retention amount applicable to a particular coverage section, such as a cyber extortion section, is met when that lower retention amount is satisfied by payment of loss under that coverage section.

- Although placing coverage in this dynamic space presents a challenge, it also presents substantial opportunity. The cyberinsurance market is competitive, and cyberinsurance policies are highly negotiable. This means that the terms of the insurers’ off-the-shelf policy forms often can be significantly enhanced and customized to respond to the insured’s particular circumstances. Frequently, very significant enhancements can be achieved for no increase in premium. Before an attack occurs, organizations are encouraged to proactively negotiate and place the best possible coverage in order to decrease the likelihood of a coverage denial and litigation. A well-drafted policy will reduce the likelihood that an insurer will be able to successfully avoid or limit insurance coverage in the event of a claim.

3. Provide notice and comply with other policy conditions. Insurance policies typically contain notification provisions stating that the insured organization must provide notice within a certain time frame, often “as soon as practicable,” even “immediately,” after the organization becomes aware of an incident. Although providing notice to an insurer may not be top of mind in a cyberattack situation, particularly where the demand is far below the policy retention or deductible, it is important for an organization to reasonably comply with notice provisions (and other policy conditions, including consent provisions) in order not to jeopardize, or delay, coverage. In the context of providing notice, moreover, it is important for organizations to recognize that what begins as a relatively low cyberextortion demand may quickly evolve into an incident or series of related events that triggers other first-party coverage sections of the insurance policy, such as the business income loss coverage (an extortion event may result in a significant loss of business income), extra expense coverage, digital asset loss recover/restoration coverage and crisis management coverage and, to the extent personally identifiable information or protected health information may have been compromised, for example, the third-party claim coverage sections of the policy, including coverage for data breach-related lawsuits and regulatory liability. Indeed, a ransom demand may be deployed as a purposeful diversion from a different, principal goal, such as stealing sensitive records. Recognizing this reality, it is important that the organization be aware of, and reasonably comply with, notice provisions in order to avoid a coverage defense based on purported late notice. In addition, providing notification can provide the insured organization with valuable coverage for costs related to the extortion threat, such as a forensics investigation, which may reveal other malware on the computer system, stop the intrusion, and block future extortion attempts, a consultant to utilize decryption keys or to recreate the files and data at issue, and, where appropriate, legal counsel. The bottom line: in the event of a cyberextortion demand, organizations are advised to provide notice under all potentially implicated policies, excepting in particular circumstances that may justify refraining to do so, and to carefully evaluate all potentially applicable coverages.

4. Maximize coverage across the entire insurance program. Although cyberextortion coverage is an obvious place to look for coverage in the wake of a ransomware attack or other cyberextortion incident, organizations are advised to consider
all potentially applicable insurance policies and coverages. As noted above, a cyberextortion incident may trigger various other coverages under the organization’s cyberinsurance program, and also may trigger other insurance policies and programs, such as computer crime policies and kidnap and ransom policies. The various types of insurance policies that may be triggered by a cyberattack likely carry different insurance limits, deductibles, retentions and other self-insurance features, together with various different and potentially conflicting provisions addressing, for example, other insurance, erosion of self-insurance and stacking of limits. For this reason, in addition to considering the scope of substantive coverage under an insured’s different policies, it is important to carefully consider the best strategy for pursuing coverage in a manner that will most effectively and efficiently maximize the potentially available coverage across the insured’s entire insurance portfolio. Absent a compelling reason, notice should be provided under all policies that potentially provide coverage.

5. Exercise business continuity and improve computer security. Insurance aside, the best protection against a ransomware attack is to have all files and data securely backed up, in a separate physical location, or at least on a separate system, so that no business-critical information that is not recoverable may be permanently deleted by extortionists. It also is important to reflect on how these types of attacks occur. Cyberextortionists must download malicious software onto a system, or a connected device, and this often is achieved through tricking employees to click on attachments or links in phishing emails, which increasingly look convincing. Therefore, improving computer security, including through antivirus programs, spam filters, firewalls, installation of software updates and security patches (early reports indicate that WannaCry appears to exploit a vulnerability in Windows that Microsoft patched on March 14, which would have automatically protected those computers with Windows Update enabled), disabling of macro scripts, and utilizing application whitelists, which only allow approved files to execute, is essential. Likewise, training employees about how to recognize and avoid social engineering exploits such as phishing emails, is key in negating or minimizing ransomware threats. Organizations also are advised to consider incorporating ransomware attack scenarios into their incident response planning.

A well-negotiated insurance program, together with solid business continuity planning and comprehensive, proactive cybersecurity policies and procedures, will position an organization to be resilient in the face of the serious and escalating threat posed by cyberextortion. For more information, please contact Roberta D. Anderson at (412) 297-4970 or randerson@cohencorp.com. To receive future news alerts, please send an e-mail to bulletins@cohencorp.com.  

This article first appeared in the May 15 edition of the Law360. Law360, Los Angeles (May 15, 2017, 10:55 PM EDT)
## 2017-2018 TIPS CALENDAR

### October 2017

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Location</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>11-15</td>
<td>TIPS Fall Leadership Meeting</td>
<td>Ritz-Carlton Key Biscayne</td>
<td>Felisha A. Stewart – 312/988-5672</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Key Biscayne, FL</td>
<td></td>
</tr>
<tr>
<td>19-20</td>
<td>Aviation Litigation Committee Meeting</td>
<td>Ritz-Carlton</td>
<td>Donald Quarles – 312/988-5708</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Washington, DC</td>
<td></td>
</tr>
</tbody>
</table>

### November 2017

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Location</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>8-10</td>
<td>FSLC &amp; FLA Fall Meeting</td>
<td>Sheraton Boston Hotel</td>
<td>Donald Quarles – 312/988-5708</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Boston, MA</td>
<td></td>
</tr>
</tbody>
</table>

### January 2018

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Location</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>24-26</td>
<td>Fidelity &amp; Surety Committee Midwinter Meeting</td>
<td>JW Marriott</td>
<td>Felisha A. Stewart – 312/988-5672</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Washington, DC</td>
<td></td>
</tr>
<tr>
<td>31-2/6</td>
<td>ABA Midyear Meeting</td>
<td></td>
<td>Felisha A. Stewart – 312/988-5672</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vancouver</td>
<td>British Columbia</td>
</tr>
</tbody>
</table>

### February 2018

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Location</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>22-24</td>
<td>Insurance Coverage Litigation Midyear Mtg</td>
<td>Arizona Biltmore</td>
<td>Donald Quarles – 312/988-5708</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Phoenix, AZ</td>
<td></td>
</tr>
</tbody>
</table>

### April 2018

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Location</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-5</td>
<td>Motor Vehicle Products Liability Program</td>
<td>Arizona Biltmore</td>
<td>Felisha A. Stewart – 312/988-5672</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Phoenix, AZ</td>
<td></td>
</tr>
<tr>
<td>6-8</td>
<td>Toxic Torts &amp; Environmental Law Meeting</td>
<td>Arizona Biltmore</td>
<td>Felisha A. Stewart – 312/988-5672</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Phoenix, AZ</td>
<td></td>
</tr>
</tbody>
</table>

### May 2018

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Location</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-6</td>
<td>TIPS Section Conference</td>
<td>Loews Hotel Hollywood</td>
<td>Felisha A. Stewart – 312/988-5672</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Los Angeles, CA</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Speaker Contact: Donald Quarles – 312/988-5708</td>
</tr>
</tbody>
</table>