THE SUFFOLK LAWYER

THE OFFICIAL PUBLICATION OF THE SUFFOLK COUNTY BAR ASSOCIATION

DEDICATED TO LEGAL EXCELLENCE SINCE 1908 www.scba.org Vol. 32, No. 10 – June 2017

INSIDE

JUNE 2017
FOCUS ON
ELDER LAW

SCBA's Annual Installation Dinner Dance One Classy Affair

By Laura Lane

The theme for the 109th Annual Installation Dinner Dance held on June 2 was "A Tradition of Professionalism & Civility." It was a perfect evening filled with camaraderie, acknowledgements for dedication and a commitment by many to serve as the Association's leaders.

At the beginning of the evening Master of Ceremonies Harvey Besunder, who is also an SCBA past president, summed up what is known about the SCBA when he said, "We are recognized as the most influential and active bar association." The latter was evident at The Larkfield by the many attorneys, judges, and friends that attended the installation.

Richard Weinblatt was honored by Past President John Calcagni with the Professionalism Award. "Richard always pursues justice for the public good," Mr. Calcagni said. "He carries himself in the true tradition of professionalism and never has too little time to help someone who needs help."

Other awards were given too. John H. Gross, a past SCBA president (1994-1995) was given a Lifetime Achievement Award, a great honor. Peter D. Tamsen was presented with the Dorothy Paine Ceparano Award by Harry Tilis, the immediate past dean. Ms. Ceparano, who passed away a few years ago, was vital to the Academy and a former editor of The Suffolk Lawyer.

Patrick McCormick was installed by Hon. C. Randall Hinrichs, the Administrative Judge for Suffolk County, as the Academy's new dean. Mr. McCormick has served for years as a frequent contributor to this publication.

Then the Hon. Hector D. LaSalle installed the new Academy directors. They included: Sean E. Campbell, Joseph A. Hanshe, Michael S. Levine and Gerard J. McCreight.

When it was time to install the officers, who will lead the

(Continued on page 22)

Photo by Jimmy Rea Photography

Patricia M. Meisenheimer was installed as the SCBA President by the Hon. Randall T. Eng on June 2.

Photo by Barry Smolowitz

Awards presented at SCBA's Annual Installation

Immediate Past President John Calcagni, left, presented Lance Pomerantz with an award at the Annual Meeting. See story and more photos on page 15.

PRESIDENT'S MESSAGE

Sharing Our Installation Dinner

By Patricia Meisenheimer

It is my pleasure to welcome our judiciary, colleagues, family and friends to the 109th Installation of the Suffolk County Bar Association. This evening is a celebration of the honored tradition of our Association's commitment to excellence, professionalism, civility and service to the community. I thank each of you for sharing this evening with us tonight.

I am humbled to stand before you and proud to serve this great Association. "You never know when one kind act, or one word of encouragement, can change a life forever." This reflects my appreciation to my colleagues who have believed in and placed their trust in me to stand before you as your president. You have enriched my life by your encouragement and kindness.

Pat Meisenheimer

I am especially grateful to Jane LaCova and the Bar Association staff who are always there for our members and whose tireless efforts made this evening a success. I wholeheartedly thank John Calcagni for his exceptional leadership, for his wisdom and most especially his friendship.

We are honored to have many distinguished guests celebrate with us this evening. The Honorable Justice

(Continued on page 22)

BAR EVENTS

Annual Golf and Fishing Outing

Monday, Aug. 14
Golf at the Rock Hill Golf and Country Club, Manorville, N.Y.

Tee off is at 1 p.m. Enjoy playing on a well maintained facility with a staff that is extremely accommodating. The course is in excellent condition and is both challenging and fair.

If you are a fishing aficionado, sail with Barry Smolowitz aboard the Osprey V out of Port Jefferson Harbor. The Road King Band will entertain members and guests and there will be prizes for the largest fish and the most caught. Call Jane LaCova for further information.

FOCUS ON
ELDER LAW
SPECIAL EDITION

CYBERSECURITY

Five Questions to Ask About Your Company's Cybersecurity Insurance Policy

By Jack Harrington

Companies of all shapes and sizes understand the importance of general commercial liability coverage. But, with the unprecedented rise in cyber attacks, particularly against businesses that collect and store the personal, medical, or financial data of their customers, how many companies have invested in the necessary cybersecurity insurance coverage? PwC estimates that cyber insurance premiums will reach $7.5 billion by the end of the decade. However, not all cybersecurity insurance policies are created equal, and companies must evaluate their unique risk profile and pay careful attention to how their insurance carrier defines key terms in their policies.

Cyber attacks resulting in customer data breaches are almost certain to invite litigation and, depending on the context, government regulatory investigation. For publicly-traded companies in particular, data breaches can prompt high-profile and costly shareholder derivative litigation that, regardless of whether the company successfully defends the litigation, is highly disruptive.

In one of the most noteworthy cases in recent years, Target Corp. was sued by shareholders over a 2013 cyber attack resulting in one of the largest data breaches ever reported. A federal judge in Minnesota dismissed the litigation in July 2016, but not before the company had reported nearly $300 million in cumulative expenses incurred since the breach, only $90 million of which was covered by Target's insurance.

Jack Harrington

So, how do you determine what cybersecurity policy is best for your business? Start by asking the following questions.

What minimum cybersecurity measures must your company implement for the policy to take effect?

So-called "minimum required practices" exclusions prevent the insured from recovering on the policy if it is determined that the insured did not implement adequate procedures and risk controls to defend against cyber attack. What constitutes "minimum required practices" can vary significantly between and among policies. Companies should clearly understand the definition of this exclusion in their policy and ensure that they are meeting or exceeding the standard.

Companies should consider policies that clearly enumerate the required practices and negotiate that language with members of the company's IT department who are more likely to understand what minimum required practices are possible given the company's existing technology infrastructure. Also, consider whether your company is subject to any industry-specific laws or regulations that your carrier could argue would set a floor in terms of cybersecurity best practices. For instance, the New York State Department of Financial Services' new rule requires certain financial services sector companies to maintain risk-based cybersecurity programs. The failure of a company to follow that rule might be considered by their insurance carrier to be a per se trigger of the policy's minimum required practices exclusion.

What types of cyber events trigger coverage and when does coverage commence?

Some cybersecurity insurance policies do not cover liability sustained from the mere breach of a company's customer data; rather, coverage applies only if that data is published or otherwise made publicly available. If your policy is triggered only in the event of publication, then also determine whether the identity of the publisher affects your coverage.

In *Zurich American Insurance Co. v. Sony Corp. of America et al.*, 651982/2011, New York Supreme Court Judge Jeffrey K. Oing ruled that Sony's insurance carrier did not have to defend the technology company in lawsuits stemming from the 2011 cyber attack on Sony's PlayStation network. In that case, the hackers had published the user data online, not Sony, and according to the court the policy required that Sony commit the act of publication. The court ruled that coverage for publication liability could not be extended to publication by third parties, including the perpetrators of the attack. Companies should also consider a retroactivity provision that covers any unknown cyber intrusion or attack that commenced before the policy was signed. In many cases, a cyber attack may have been commenced months or years before it is identified or data is stolen.

What aspects of your company's technology infrastructure are covered by your policy?

Carriers are increasingly excluding coverage for cyber attacks resulting from the loss of a cell phone or laptop,

(Continued on page 27)

LITIGATION

How to Select an eDiscovery Vendor

By Annemarie Jones

Electronic discovery (eDiscovery) is becoming an integral part of modern-day litigation. Choosing an eDiscovery vendor for storing, managing, searching, and organizing electronically-stored information (ESI) can be a daunting task. The market is flooded with vendors selling eDiscovery programs that are difficult to differentiate from one another. Despite huge variations in price, many of these programs are very similar. Some factors that should be considered before choosing an eDiscovery vendor include:

Storage of ESI: Vendors typically store ESI in the cloud. Storing ESI on a hard drive is an antiquated procedure and can be a disaster in the event of a computer crash. Storing ESI on the cloud ensures that the ESI is secure, the amount of ESI that can be stored is unlimited (subject to fees based on size), and the ESI can be accessed by password by any computer (or other electronic device) at any location.

Annemarie Jones

Number of users: It is critical the eDiscovery vendor provide the capability for the ESI to be accessible by multiple users simultaneously. This can be helpful in the event that a few lawyers need to review the ESI at the same time to meet an upcoming deadline. A multi-user function is also helpful if the review of the ESI is going to be split into different batches (i.e. electronic folders) of ESI. The majority of eDiscovery vendors that store ESI in the cloud provide a multi-user function.

De-duplication: An invaluable aspect of any eDiscovery program is the ability to "de-duplicate" the ESI. Put simply, this means the program will be able to pull out documents that are exact duplicates and either delete these duplicates or place them in a separate electronic folder. This can save hundreds of hours of review time and also eliminate the possibility that identical documents are coded differently for responsiveness and privilege.

Search Functionality: The basic search components of eDiscovery programs include the ability to search (and sort by) term, phrase, numbers, date, author, location, and/or combinations of these factors. It is also helpful if the eDiscovery program has the functionality to take a search and separate the responsive "hits" into separate electronic folders. Some of the newer sorting features on the market include: predictive coding, email threading, and grouping near duplicates.

Types of ESI: Almost all eDiscovery programs can deal with the common types of ESI – emails, word-processing documents, spreadsheets, PDFs, etc. If a case is going to involve a unique type of ESI, a higher-end vendor that is capable of processing the ESI may be necessary.

Highlighting: Many of the more expensive vendors now offer a function that highlights search terms in the text of the document. This can be especially helpful when dealing with individual documents

(Continued on page 27)

CYBER

Is Your Website Safe and Secure?

By Victor Yannacone, Jr.

Websites have now become the heart of ethical lawyer advertising. They are also a prime target for hackers and an open portal for installation of malware.

Your website can be captured by hackers and used to infect the devices which your visitors use to access your website from smartphones and tablets to laptops and office computers. When that happens, the damage to your professional reputation may be irreparable.

A quick check of website security

Some browsers now warn users when the page they are visiting may put their information at risk. In Google Chrome, that "i" symbol on the left side of the address bar indicates a site may not be secure because it is using an unencrypted connection to exchange data with your computer.

In Mozilla Firefox, when viewing a secure website, the Site Identity icon in your address bar will be a green padlock.

You should never send any sort of sensitive information to a website that is not certified secure because you cannot be sure that you are communicating with the intended website. Your data is not safe against eavesdropping unless the connection between your browser and the website is encrypted.

As you read this column, open your browser and check your own website.

Sites with secure connections encrypt data between their web servers and your computer. These sites also have a security certificate from a presumably trusted authority that verifies the website identity and protects it from being modified. You typically see a site security icon such as the Firefox padlock and the URL starts with https://.

Victor Yannacone, Jr.

Web security, your site and your network

Other than risks created by employee use or misuse of network resources, your web server and your website are your most significant cybersecurity risks. Any networks connected to the web servers are also at risk.

Web servers by design open a window between your network and the world. The care you take with server maintenance, web application updates and your web site coding defines the size of that window, limits the kind of information that can pass through it and establishes the degree of web security you will have.

Web security risk — should you be worried?

If you have importance information on your network or if anything about your website puts you in the public spotlight, then your web security will be tested. Web servers are inherently complex programs and intentionally invite interaction with the public. The opportunities for security holes are many and growing.

Your website may not be the end target at all. A common web site attack involves installing silent and concealed code that will exploit the browsers of visitors.

The world's most secure web server is the one that is turned off, but this just isn't an option for most law firms. Any system with multiple open ports, multiple services and multiple scripting languages is vulnerable simply because it has so many points of entry.

Web sites often invite visitors to load a new page containing dynamic content, search for a location, fill out a contact form, or search the site content. In each case your web site visitor is effectively sending a command to or through your web server, very likely to a database.

Websites live in a complex cyberecosystem of interconnected nodes around the internet. The Domain Name System (DNS) tells requests where to go. The web server houses various website files and the infrastructure houses various web servers. Many of these features are provided by number of service providers that make it very easy for you to create an online presence. They sell you things like domain names, hosting space, and other services designed to make operating your website easy.

Every one of these components and services has an impact on your overall security posture and can potentially contribute to how your website gets hacked.

Web security defense strategy

Security requires you to maintain constant alert. You should ensure that all patches and updates are installed as soon as they become available and have all your existing applications reviewed for security. You should maintain a tight firewall, antivirus protection and run IPS/IDS (intrusion prevention systems/intrusion defense systems).

You should also use a web scanning solution to test your existing equipment, applications and web site code to see if a known vulnerability exists. Network and web site vulnerability scanning is one of the most efficient security investments.

How to protect your website

Website security is about risk reduction not risk elimination. There is no such thing as a 100 percent solution to staying secure.

Employ *Defense in Depth* principles layers like an onion.

- Employ best practices like "Least Privileged." Not everyone needs administrative privileges.
- Protect access of your website. Use multi-factor and two-factor authentication.
- Protect against exploitation of software vulnerabilities. Use a website firewall.
- Backups are your safety net. Try to have at least 60 days available.

Security is not a singular event or action, but rather a series of actions. The responsibility begins and ends with you.

Note: Victor John Yannacone Jr. is an advocate, trial lawyer, and litigator practicing today in the manner of a British barrister by serving of counsel to attorneys and law firms locally and throughout the United States in complex matters. Mr. Yannacone has been continuously involved in computer science since the days of the first transistors in 1955 and actively involved in design, development, and management of relational databases. He pioneered in the development of environmental systems science and was a cofounder of the Environmental Defense Fund. He can be reached at (631) 475–0231, or vyannacone@yannalaw.com, and through his website https://yannalaw.com.

Directors are Deadlocked – What Happens Now? (Continued from page 10)

exists, the court looked to the existence of "genuine, good faith divisions." In the instant case, the court determined that "[t]he deadlock is the result of legitimate disagreements about the direction of [Applied] and Aharon's role." While Aharon did not want the Bioform Deal, Lafferty "wanted the Bioform Deal to succeed because he viewed it as [Applied's] only hope." Kleinberg and Herzog had lost confidence with Aharon back in 2015 and had since sought to replace Aharon as CEO. Further, the court noted that "Aharon had created the deadlock … when he appointed a third director to stop the emergent board majority of Lafferty, Kleinberg and Herzog from taking action against him."

Due the deadlock, Applied's board was unable to resolve the termination of the Bioform Deal. Moreover, Applied's board could not resolve the question of who should be CEO of Applied, a task that the court stated is "a board's most important task." Thus, the court found that "[u]nless the deadlock is broken, [Applied] has no chance of pursuing a new business plan and will become irretrievably insolvent." Without a functioning CEO and with no cash to operate its business, the court determined that Applied "has suffered and will continue to suffer irreparable harm absent the appointment of a custodian."

Finally, the court found that the stockholders are unable to break the deadlock because Applied's stockholders' voting agreement locked the board into a 3-3 tie between the two competing factions.

In exercising its power to appoint a custodian, the court cautioned that "the consequences of that deadlock for the stockholders and the enterprise must be assessed." In the instant case, the court noted that a sale of Applied or its assets would not benefit the stockholders since such sale would likely result in proceeds that is a fraction of the estimated $60 million value of the sewage processing technology.

Accordingly, the court appointed a custodian to serve as a seventh director until new investors may cause the board composition and balance of power to change, thus eliminating the need for such custodian. The court further designated that the custodian shall preside over any board meeting, oversee the discussion, set time limits for discussion, call for a vote and required the custodian's presence, together, with three other directors, to constitute a quorum in any board meeting.

As with other cases where the court appointed a custodian, the court requested the parties to submit three names for the court to consider, thus allowing the parties to retain a degree of participation on the appointment of the seventh director.

Note: Gisella Rivera, Esq., CPA, is the principal of G. Rivera Law Office, PLLC. Prior to opening her law practice, Gisella was a partner in the Corporate and Business Group of Meltzer, Lippe, Goldstein & Breitstone, LLP, a major Long Island Law firm, and worked as an associate attorney in the Capital Markets Practice of White & Case, LLP, a major Global Law Firm. Gisella worked as an accountant for over 15 years, amongst others, as the Chief Financial Officer of a prominent mental health care provider in Suffolk County and as the North-East Regional Finance Director of an assisted living company. Gisella combines her business experience with her legal training in representing and serving her clients. Contact Gisella at gisellarivera@griveralaw.com or at (631) 353-7230.

Cybersecurity Insurance Policy (Continued from page 11)

or data theft in which an employee misplaces a thumb drive or other electronic storage device. Companies where employees have remote server access or frequently work outside the office should ensure that its policy defines the origin of the cyber attack or data loss with sufficient breadth to cover all likely eventualities.

Against what types of legal actions is your company insured and how much control will your company have to respond to those actions?

In the immediate aftermath of a cyber attack or data breach it is difficult to determine exactly what types of legal liability the company will face in the coming weeks, months, and years. Depending on the gravity of the situation, it is safe to assume that companies will face civil litigation, but will the incident also result in a government investigation or even criminal charges? Do your company's existing contracts mandate that customer disputes be settled using alternative dispute resolution, such as arbitration or mediation, and will your cybersecurity policy cover those eventualities? Relatedly, does your policy require insurance carrier pre-approval before you take certain actions in defense of cyber-related claims? Time is often of the essence when it comes to cyber attack, so you want to ensure that your policy does not hamstring your company's ability to respond.

Finally, does the perpetrator or motivation of the cyber attack matter?

Even robust cybersecurity insurance policies tend to be geared toward inadvertent data breaches or cyber attacks perpetrated by criminals with financial motivations. Many insurance policies include exclusion clauses for cyber attacks committed by governments or terrorist organizations or with the intent to cause physical harm. Companies, particularly those operating in the energy and infrastructure markets, should consider whether they need protection beyond data-related liability if a cyber attack could result in physical damage or loss of life. Congress passed the Terrorism Risk Insurance Program Reauthorization Act of 2015 to extend government-backed reinsurance of terrorism coverage. However, the government program is triggered only under a limited set of circumstances.

In 2017, more and more general liability policies will include cybersecurity-related coverage, but in many cases a supplemental and tailored cybersecurity-specific policy is warranted. Companies should evaluate their risks, compare cybersecurity insurance policies, and consult with an expert before purchasing insurance for protection from cyber attacks.

Note: Jonathan "Jack" Harrington, chairs the Cybersecurity and International Regulation, Enforcement & Compliance practices at Campolo, Middleton & McCormick, LLP in Ronkonkoma and Bridgehampton. Contact Jack at jharrington@cmmllp.com or (631) 738-9100.

How to Select an eDiscovery Vendor (Continued from page 14)

that are hundreds of pages long.

Export Format: It is important to ask any eDiscovery vendor what type of export format(s) the vendor is capable of. Examples of export format include: PDF, native, TIFF, JPEG, and load files. The program must also have the capability to store and produce metadata.

Redactions: The eDiscovery program should have the ability to redact and should be capable of saving each document in its redacted and unredacted form. The program should also have the option to remove a redaction if a document is improperly redacted and/or if negotiations with opposing counsel require a change to redactions.

Vendor assistance: While a firm may be able to utilize the eDiscovery platform without the help of the vendor, in the event of an emergency (e.g. approaching deadline, rapid increase in data, complicated export format) it is important that the vendor provides the option (usually for an additional fee) of assisting in the export and organization of the production of the ESI.

Privilege Log: Most programs are capable of creating a spreadsheet of all documents that have been coded as privilege by the reviewing attorneys. This chart is typically in Microsoft Excel and contains coding fields such as author, date, recipients, subject, etc. Because this chart is in Excel, it can then be easily manipulated by an attorney into a privilege log format which meets the needs of the case and local court rules.

Cost: Vendors can charge anywhere from a few hundred dollars a year to upwards of tens of thousands of dollars a year. The cost a firm is willing to pay is typically assessed by evaluating how many cases per year the eDiscovery program will be utilized for and determining whether the cost (or a portion thereof) will be charged to clients.

After evaluating these factors and any other factors deemed relevant, the next step is to contact each vendor for a price quote tailored to meet the needs of your firm. Although daunting, after price quotes are received, and the responsiveness of each vendor can be evaluated, the field will have narrowed. At that point, it can be helpful to request references and perform background checks. If still uncertain, a great way to meet representatives of each vendor is to attend a vendor fair, such as Legaltech, which is held annually in New York City.

Note: Annemarie Jones is an associate at Lewis Johs Avallone Aviles LLP in Islandia, New York. Annemarie focuses her practice on the representation of commercial clients in complex civil litigation. Annemarie also focuses her practice on the defense of municipalities. She is the 2017 co-chair of the Public/Media Relations & Digital Strategy Committee of the Federal Bar Association, Eastern District of New York Chapter.