DATA BREACH NOTIFICATION LETTER

Under California law, state agencies and businesses have an obligation to notify *any* California resident whose unencrypted personal information (as defined by the statute) was acquired, or reasonably believed to have been acquired, by an unauthorized person. (California Civil Code § 1798.82(a)).

California also provides specific requirements for what the notification must look like in order to comply with the law. The notice must be in plain language and shall be formatted to all attention to the nature and significance of the information it contains. Specifically, the font of the notice must be no smaller than 10-point size and use clear and inconspicuous headings, including "Notice of Data Breach" at the top. The notice must also provide the following information:

- Who is issuing the notification;
- The date of the notification;
- What happened, including the date range affected by the breach;
- Identification of what information was involved in the data breach;
- Whether there was a delay in providing the notification due to an investigation by law enforcement;
- What the business is doing to resolve the problem;
- What the recipient of the notice can do to protect themselves;
- Where to find more information about the data breach.

Thus, the notification should provide information under the following headings:

"What Happened,"

"What Information Was Involved,"

"What We Are Doing,"

"What You Can Do," and

"More Information."

Any business that is required to issue a notification to more than 500 California residents as a result of a single breach must also electronically submit a sample copy of that security breach notification to the Attorney General (California Civil Code § 1798.82(f)). Online submissions to the Attorney General are made here: https://oag.ca.gov/privacy/databreach/report-a-breach. Sample breach notices submitted to the Attorney General are found here: https://oag.ca.gov/privacy/databreach/list.

[ABC, LLC / LOGO] _____ _____ Date: April 16, 2019

NOTICE OF DATA BREACH

Dear Robert Smith:

We take the privacy and security of your information very seriously and we are writing to provide you with information about a data incident involving ABC, LLP. It is possible that the security of your information may have been compromised as a result of the unauthorized activity of a third party.

What Happened?

After noticing some unusual activity on our network including a possible ransomware attempt on November 17, 2018, we hired a specialized forensic IT firm to investigate. On November 27, 2018, the specialized forensic IT firm determined that there was unauthorized access to our main network drive from a foreign IP address between September 13, 2018 and October 23, 2018.

What Information Was Involved?

The information on our system may have included your: first and last name, home address, date of birth, and Social Security information.

What are we doing.

In addition to the steps outlined above, we notified the FBI, the IRS, the FTB, all three credit bureaus, and the applicable state agencies of this incident. Further we are reviewing our office policies and procedures to ensure all security measures are taken to avoid such an incident from occurring again. In this endeavor, we hired IT specialists to determine what happened and confirm the security of our network. Lastly, we are working with law enforcement in their investigation of the criminals.

What you can do.

Given the nature of the information potentially exposed, we strongly recommend that you monitor your accounts. Further, we strongly recommend that you contact the three credit bureaus and place a free fraud alert and/or security freeze on your credit files. Their contact information is:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241 Atlanta, GA 30374 1-888-766-0008	P.O. Box 2104 Allen, TX 75013 1-888-397-3742	P.O. Box 2000 Chester, PA 19022 1-800-680-7289

You are also entitled to a free credit report every year from each of these agencies at: www.annualcreditreport.com.

As an added precaution, we have also arranged to provide you with 12 months of complimentary credit monitoring from Credit Monitor Program. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on

immediate identification and resolution of identity theft. This service is completely free to you and enrolling in this program will not hurt your credit score. For more information on identify theft prevention and Credit Monitor Program, including instructions on how to activate your complimentary one-year subscription, please call Credit Monitor Program Company at 1-XXX-XXX-XXXX, or visit the website [LINK].

For More Information

If you have further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 1-800-XXX-XXXX, or write to us at 123 Main Street, AnyTown, USA. The response line is staffed with personnel familiar with this incident and knowledge about what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9 am to 9 pm, Eastern Time.

Please accept our apologies that this incident occurred. We are committed to protecting the privacy of personal information provided to us and have taken many precautions to safeguard it. We strive to continually evaluate and modify our practices to enhance the security and privacy of your personal information.

Sincerely,

Jane Smith, CEO

ABC, LLP

FULFILLING THE ETHICAL DUTY OF COMPETENCE: DEVELOPING AN INCIDENT RESPONSE PLAN FOR A CYBER ATTACK

By Procopio Partner and General Counsel, Carole J. Buckner

Every attorney's ethical duty of competence requires a lawyer to provide competent representation to a client, applying the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation. This in turn requires that a lawyer keep abreast of technology, including associated risks and benefits, including continuing study and education. As a matter of best practice and preparation, lawyers should proactively develop an incident response plan with the objectives of both stopping the breach and restoring systems, with "specific plans and procedures for responding to a data breach." Because a data breach requires a rapid response, the plan should be developed prior to the time the lawyer is swept up in an actual breach. Developing a thorough and thoughtful incident response plan creates the ability to respond to data breach incidents systematically, employing the appropriate personnel with appropriate experience, with a careful methodology, in a coordinated manner.

Once an incident occurs, mitigating damage and minimizing legal exposure requires a quick response on multiple levels. Undertaking the process of creating an incident response plan before it is needed allows for the development of strategy by a diverse team with the appropriate range of expertise and knowledge. A strong and comprehensive incident response plan will consider a range of issues including communications, legal rights and remedies, mitigation of loss and business disruption and preservation of evidence in an appropriate manner. Approval of the incident response plan should be obtained from senior management.

Training

In anticipation of litigation, structure the incident response plan so that the response is covered by the attorney client privilege and work product doctrine to the maximum extent possible. Everyone involved should be trained to communicate in a manner that preserves the application of both privilege and work product to the maximum extent possible. Once the plan is prepared, team members should practice running through a mock incident response. Training should be repeated periodically through a variety of simulated data breach situations. Tabletop exercises, in which members of the incident response team address a hypothetical incident and explain proposed responses, may reveal gaps in the plan and can be used to improve the incident response plan.

An incident response plan should be designed to address any type of security incident, including both internal incidents and external incidents such as exfiltration that may involve theft of information or ransomware attacks that block use of systems.

There are many formulations for incident response plans. Such plans share several common key components:

- Identification of all team members and their backups.
- Definition of the role of each team member in the event of an incident.
- 24/7 contact information for each team member and backup.
- An outline of all steps to be taken at each stage of the incident response process.
- Guidelines for external and internal information sharing in handling an incident response.
- Designation of each team member responsible for each step in the process.

Communications

Planning for communications without use of compromised systems should be addressed in the incident response plan. Ideally, the compromised system should not be used for communications. If the compromised system must be used to address the incident response, encryption should be implemented. Proper notification of the team regarding the incident should be detailed in the incident response plan. Hard copies of the plan should be distributed to assure availability during an incident when systems are blocked.

Incident Response Team

Viewing a cyber response plan as an "IT plan" fails to give appropriate significance to the legal issues involved and risks ignoring the significance of the attorney client privilege. The goal should be to integrate all stakeholders. Composition of the response team will depend on individual business operations and available resources. Given the necessity of rapid response, coordination of members in distinct roles is essential. Planners can decide whether an incident response will follow a dual track design in order to preserve attorney client privilege. In a dual track design, one team is managing legal issues and the other is handling business issues. An incident response team typically includes both internal and external members. Internally, two team members from each department should be selected, allowing for a backup in case the primary person is unavailable. Members of the response team should have such responsibilities included in their job descriptions. Legal counsel (in-house

and outside counsel), corporate management, information technology, human resources, and public relations/marketing representatives, customer relations and investor relations, should be included.

Identification of outside forensic consultants should be done in advance. Ideally, forensic consultants should be identified to determine what happened and how to mitigate the incident through data recovery or other measures. Again, two well-qualified forensic vendors should be identified in order to assure maximum responsiveness. Additional outside public relations personnel can also be designated depending on internal capabilities and expertise in crisis communications. Law enforcement contacts should also be identified in the incident response plan, and it best to make contact with them in advance. Contacts with cyber insurance carriers should also be included.

Incident Response Process

There are numerous formulations for an incident response process. The following elements are typical:

- Confirm that the incident is not a false alarm.
- Notify the insurance carrier for cyber insurance coverage.
- Contact cyber counsel to establish attorney client privilege and work product.
- Decide how urgent and how serious the incident is.
- Identify the source of the incident – external/internal.
- Identify the data threatened, and whether it is encrypted.
- Determine whether the breach is ongoing.
- Identify, evaluate and assess the nature and scope of any potential network anomaly or intrusion.
- Establish whether data was accessed and/or compromised.
- Quarantine the threat and/or eradicate the malware.
- Prevent exfiltration of data.
- Restore the integrity of the network system.

Insurance

The incident response plan should include summaries of insurance coverage and the requirements for notification to insurance carriers, to include any cyber insurance and any excess or umbrella policies. Timely notice is

essential as expenses incurred prior to notice may not be covered. General counsel or outside counsel should promptly report the incident to the insurance carrier. The notification to the cyber insurance carrier should reference the relevant policy, the date of the incident, and type of incident. After giving notification keep the carrier apprised in order to satisfy the duty of cooperation under the policy.

A cyber insurance policy may require that the insured obtain consent from the carrier prior to engaging outside vendors. As part of the preparation of the incident response plan, preferred vendors can be identified. These vendors can be submitted to the insurer for pre-approval in order to maximize expense reimbursement. Basic terms of engagement of vendors can be negotiated in advance of an incident in order to minimize delays in seeking approval in the event of an incident.

The incident response plan should take into consideration the scope of policy coverage, including whether the policy provides for assistance with the breach. While some social engineering scams may not fall within the scope of coverage, insurance may cover extortion by ransomware. Many policies cover expenses incurred after a data breach incident for legal, forensics, public relations and regulatory compliance.

Cyber insurance is not uniform. Policy wording significantly varies. First-party insurance coverage typically will cover direct losses and out-of-pocket expenses incurred in connection with incident response. Mitigation coverage may include legal expenses, forensic investigation, remediation, business interruption, notification, crisis management and cyber extortion, when triggered by an occurrence under the policy. Such expenses should be tracked for submission to the carrier. Cyber policies may also cover reputational injury and disclosure injury.

Third-party coverage insures against liability of the company for harm to third parties arising from a claim for monetary damages or injunctive or declaratory relief. Third-party coverage may extend to regulatory proceedings including fines and penalties in some jurisdictions where such coverage is permitted. Third-party coverage will also extend to compensatory damages, as well as coverage for defense and damages suffered by third parties caused by disclosure or theft of confidential information or a computer virus, as well as privacy violations.

Forensic Consultants

Internal IT personnel staff or untrained third parties should not be called in to “fix” the problems arising from a cyber incident. Efforts to “clean” servers, even if well-intentioned, may destroy important evidence of the source

of an intrusion. Two outside forensic consultants should be identified in the incident response plan in case one is not available in a timely manner to respond to an urgent incident. Forensic consultants should be identified in the incident response plan and pre-approved with the cyber insurance carrier, with basic terms of the engagement agreements pre-negotiated. Such consultants should be engaged through counsel to preserve attorney client privilege. The forensic consultant can interview internal IT personnel and others with knowledge of the incident, confirming the scope of the incident through an inventory and evaluation of devices connected to the network.

Preservation of Evidence

Litigation, prosecution and regulatory actions can follow a cyber incident. This can include class action claims regarding the data breach, regulatory investigations and criminal investigations. In anticipation of this, information about the data breach incident should be preserved in a forensically appropriate manner. Ideally, the FBI recommends immediately making forensic images of the affected computers. Imaging computers will likely require involvement of forensic consultants or law enforcement. In addition, preservation of logs from servers, routers and firewalls is appropriate. Steps taken from the inception of the incident should be documented including dates and times, identification of systems, accounts, networks, and databases impacted by the incident. All evidence should be safeguarded to prevent alteration and maintain a chain of custody. An evidence retention policy should be established to allow for potential prosecution. A single employee can be designated in the incident response plan as the custodian of such records. A critical goal of the incident response plan should be to preserve forensic evidence during the entire course of the investigation, including any remediation, in order to respond to any claims that evidence was destroyed or tampered with during the investigation.

Media

A sound incident response plan should also address how to handle media inquiries in order to maintain public confidence in the company. Whether to use internal or external communications specialists should be determined. An external communications specialist can be approved in advance by the insurance carrier. A single point of contact for external communications and a backup is preferable. A data breach may require multiple communications. The plan should anticipate press inquiries regarding who attacked, how the attack occurred, the scope of the attack, impact of the attack and remediation.

All proposed communications must be drafted with the assistance of legal counsel. Public disclosures regarding a data breach may be used against the company in subsequent litigation as admissions of liability. Communications should anticipate consumer questions, avoid misleading statements and avoid withholding key details that are relevant to consumers. Companies offering credit monitoring should explain the reasons for doing so in a manner that will reduce the risk that such an offer will be deemed an admission of liability in subsequent litigation.

Notifications

The incident response plan should also include statutory reporting obligations and any required notifications. The forensic consultant, inside and outside legal counsel and incident team members must assess and evaluate notification requirements. This will be driven by state and federal law, ethics requirements, and by contractual obligations. Breach notification statutes are not uniform, and vary on the definitions of breach, who must be notified, when notice is required, as well as the form of notice required. California and many other states have specific statutes dictating the information that must be included. Some state requirements may conflict with the requirements of other states. Notification obligations in each jurisdiction must be analyzed.

The content of the notification will depend upon the incident as well as the applicable state law. The FTC recommends that a notification describe how the breach occurred, what information was taken, and what actions were taken to remedy the situation, as well as contact information for your organization. Notification should also explain to the recipient what response is appropriate. Public companies must disclose information security breaches that are individually, or in the aggregate, material. Such disclosure should include the costs and consequences, as well as relevant insurance coverage.

Contacting Law Enforcement

The incident response plan should include procedures for determining whether and under what circumstances notification of law enforcement is appropriate. Prior to such contact, a determination of the nature of the incident will need to be made. Management along with inside and outside counsel and internal and external public relations personnel will need to determine whether contacting law enforcement is advisable depending on the circumstances of the incident.

Understanding the responsibilities of various law enforcement agencies can help with development of an incident response plan. The DOJ and FBI investigate and prosecute cyber-crimes. The Department of Homeland Security focuses on national protection including prevention and mitigation of cyber incidents, including phishing and malware. The National Cybersecurity and Communications Integration Center (NCCIC) is available 24/7 to receive and share information concerning an ongoing incident, and provide assistance to victims. The Department of Defense focuses on foreign cyber threats, national security and military systems. Data breach incidents can be reported to the Department of Justice computer fraud unit, U. S. Attorneys, or to the Secret Service, and can also be reported to state and local law enforcement. Each FBI field office has cyber capability. Contact information for relevant agencies and individual specific personnel should be included in the incident response plan. Companies should designate a point of contact and a backup for interaction with law enforcement.

There are several advantages of reporting an incident to law enforcement. Trained criminal investigators have experience handling and preserving forensic evidence. Forensic investigations by the government may save the company money as the government does not charge for forensic analysis. Criminal investigations may be a basis for delay of notifications. Criminal investigators can obtain search warrants, which can preserve evidence. At the same time, there are several downsides of contacting law enforcement. The company may lose control as the government takes charge of the investigation. Once law enforcement is involved, information may not reflect well on the company, and the company cannot terminate the inquiry.

Revision

Once the incident response plan is in place, it should be updated periodically to address new types of potential breaches and changes in the operations of the business, including responsible personnel. After an incident, a post-mortem is recommended to allow the incident response team to evaluate overall performance, including vendors and consultants and plan for needed security improvements.

BIBLIOGRAPHY

Jill D. Rhodes and Robert S. Litt, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS AND BUSINESS PROFESSIONALS (2d ed. 2018)

George B. Huff, Jr., John A. DiMaria, and Claudia Ruse, Best Practices for Incident Response – Achieving Preparedness through Alignment with Voluntary Consensus Standards, THE ABA CYBERSECURITY

HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS AND BUSINESS PROFESSIONALS (2d ed. 2018).

ABA Formal Op. 483 (2018).

Steven M. Puiszis, Prevention and Response: A Two-Pronged Approach to Cyber Security and Incident Response Planning, 24 The Professional Lawyer 3 (2017).

Mindy Rattan, Lawyers Need Plan of Attack After a Cyber Attack, 34 Law. Man. Prof. Conduct 339 (2018).

Jay T. Westermeier, Duty to Disclose Breaches, 6 Computer Law VI (2018).

William R. Covino, Data Security Assessments: Are You Prepared for a Breach? 33 Law. Man. Prof. Conduct 257 (2017).

Jay T. Westermeier, Legal Battle Plans, 6 Computer Law VI (2018).

David Bender, 5 Computer Law – A Guide to Cyberlaw and Data Privacy Law, § 42.08 (2018).

Federal Trade Commission, DATA BREACH RESPONSE: A GUIDE FOR BUSINESS (Sept. 2016).

National Institute of Standards and Technology, COMPUTER SECURITY INCIDENT HANDLING GUIDE (2012).

U.S. Department of Justice, COMPUTER CRIME & INTELLECTUAL PROPERTY DIV., BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF CYBER INCIDENTS (April 2015).

ABA Standing Committee on Law and National Security, A PLAYBOOK FOR CYBER EVENTS (2d ed. July 2014).

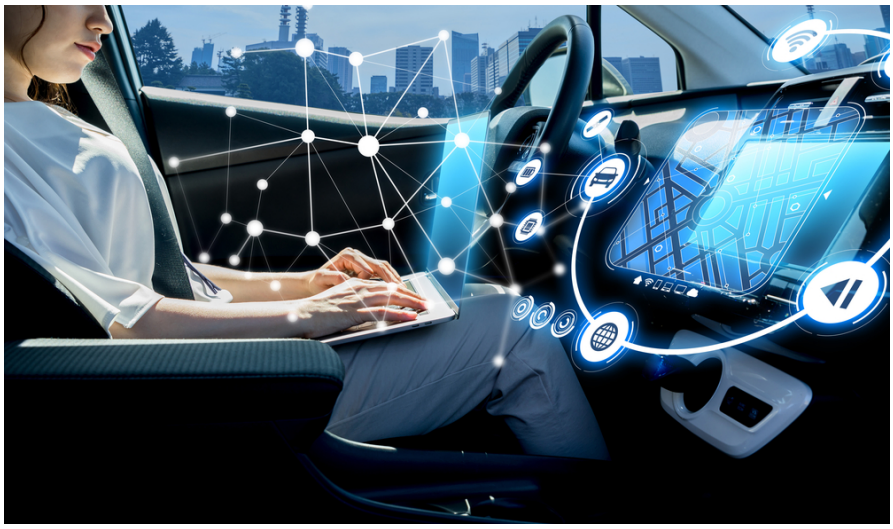
CAROLE J. BUCKNER is a Partner and General Counsel at Procopio. Her practice focuses on legal ethics, professional responsibility and the law of lawyering, including advising lawyers and law firms, and rendering expert opinions. She also serves as an expert consultant on issues involving legal ethics including legal fees, billing, fee arrangements, conflicts of interest, fee sharing, referral fees, unauthorized practice of law, withdrawal from representation, modification of fee arrangements, client trust accounting, and other issues. Prior to joining Procopio, Carole was a sole practitioner in the field of legal ethics, issues involving professional responsibility, and the law of lawyering. Carole also served as dean of St. Francis School of Law. Carole has previously worked in litigation, as in-house counsel, as a federal prosecutor, and she has taught and worked in administration at multiple law schools. Carole was a member of the California State Bar's Committee on Professionalism and Conduct (COPRAC) starting in 2005. She served as COPRAC chair in 2009-2010, and later as the Special Advisor to the Committee. Carole is a member and former Co-Chair of the Professionalism and Ethics Committee of the Orange County Bar Association. She is a member and former chair

of the Los Angeles County Bar Association's Committee on Professional Responsibility and Ethics Committee (PREC). Carole is also a member of the San Diego County Bar Association's Legal Ethics Committee. Carole has also spoken and written extensively on a wide variety of ethics related topics. Through COPRAC, the LACBA, SDCBA, OCBA, PLI, CEB, and other organizations, Carole has spoken at the State Bar's Annual Ethics Symposiums, State Bar Annual Meetings, bar association MCLE programs, and in other venues on a wide variety of ethics related topics including attorneys' fees, client trust accounting, conflicts of interest, confidentiality issues, screening, judicial recusal, lawyer advertising, collaborative law, prosecutorial misconduct, ethical issues arising from lawyer impairment, and many others. Carole has also participated as a panelist on the annual update on ethics-related cases. Also on behalf of COPRAC, Carole has closely monitored the work of the Commission on the Revision of the Rules of Professional Conduct, and has written and spoken on the new California Rules of Professional Conduct.

5 STEPS TO KEEPING YOUR TRADE SECRETS SECRET

By Procopio Partner Mindy M. Morton

A high-stakes trial that began this week between ride-sharing market leader Uber and self-driving car designer Waymo is front-page news. We frequently see patent and copyright cases in the headlines, but this is a trade secret case, which infrequently achieve such a high profile. What many people don't realize, however, is that trade secrets are vital to the U.S. economy. According to the Office of the National Counterintelligence Executive, companies collectively lose as much as $300 billion per year due to theft of trade secrets. Such theft frequently leads to costly and protracted litigation. An injunction is often the only way to stop a competitor or ex-employee from using your trade secrets, but there are steps you can take to protect your information.



So what exactly is a trade secret? It's information that derives economic value from not being generally known to the public and which its owner seeks to keep secret. A trade secret could be technical information or know-how; internal business information including marketing and finance strategies; customer lists; software, computer programs and source code; formulas; or external business information on, for example, suppliers and competitors. Famous examples of trade secrets include the recipes for Coca Cola and Kentucky Fried Chicken, as well as the google algorithm. The Waymo-Uber case is about self-driving automotive technology using LIDAR.

Trade secrets are different from patents, although many companies take advantage of both patent and trade secret protection. To obtain a patent, you need to publish the details of your invention, and in return, you can stop others from using that invention for a limited period of time. Trade secret protection can last forever, but you need to take steps to keep it secret and it can't be something others already know or could easily figure out. Both Coca

Cola and Kentucky Fried Chicken allegedly keep their trade secret recipes in a vault. You don't need to go to that extreme to protect trade secrets, but you do need to take reasonable steps.

Congress recognized the importance of trade secrets in 2016, when it passed the Defend Trade Secrets Act, or DTSA. Among other things, DTSA created a federal cause of action when trade secrets are misappropriated. Before the DTSA was enacted, trade secret cases were governed by state laws. The DTSA also allows ex parte seizures in extraordinary circumstances when a temporary restraining order isn't sufficient. Although the seizure provisions have been highly publicized, very few cases have addressed seizures in the almost two years since enactment. Notably, the DTSA does not preempt state trade secret laws. This is of particular importance in California, which handles more trade secret cases than any other state. (See David S. Almeling et. al., A Statistical Analysis of Trade Secret Litigation in State Courts (2011) 46 Gonz. L. Rev. 57, 74.)

The ideal for any trade secret owner is to avoid litigation and economic harm by keeping secrets in-house. While nothing can 100% guarantee the protection of a company's trade secrets, these steps can help:

1. Identify and protect your critical trade secrets. It's hard to protect your secrets if you haven't identified them. Once you've itemized them, determine the best way to restrict access to any details involving those secrets. That protection system should consider access by your own employees as well as any outside parties. Recognize the ways companies can lose valuable trade secrets. Theft via flash drives and cloud servers is on the rise, as are cyberattacks.
2. Have a company-wide trade secret policy in place. Now that you've worked out a protection system for your trade secrets, capture in a formal policy how any given employee will interact with confidential documents such as customer lists and technical information, which are involved in most trade secret cases, and make sure employees are familiar with the policy.
3. Require all new employees to sign a confidentiality and invention assignment agreement when they start work. Your work hasn't ended once you've addressed your existing employees. You need to proactively manage new hires as well, with the signing of a confidentiality and invention assignment agreement. For protection under California trade secret laws, it's critical that the agreement reference California Labor Code Section 2870. It's also important that the new employees certify that they have not brought any confidential information from a previous employer, to ensure your company isn't liable for any theft of someone else's trade secrets. Should you discover any material from a previous employer in your computer system, immediately preserve the evidence and consult with an experienced investigator.

4. Take action the moment an employee gives notice. In over 75% of trade secret theft cases, the alleged thief is an employee or former employee. (Id. at 68-69.) Thus, it's critical to act quickly when an employee with access to trade secret information informs you that he or she is leaving. Suspend the employee's computer access and don't allow him or her to delete anything. Make sure to schedule an exit interview, and remind the departing employee of signed confidentiality obligations. You may want to consider making a forensic image of the individual's computer and/or emails, particularly if the employee was involved in critical development work or if you believe he or she is going to work for a competitor.
5. Don't forget about interactions outside the company. The second biggest threat is business partners. Approximately 20% of trade secret cases involve business partners as alleged misappropriators. (Id.) Whether it's a manufacturer in your supply chain or a customer, there are times when a company will need to share elements of a trade secret with individuals outside the company. At a minimum, obtain a signed nondisclosure agreement with anyone having access to trade secret information, and limit access to what is absolutely essential.

Unfortunately, even the best-intentioned companies can find themselves dealing with trade secret theft. Should you pursue a trade secret case in court, you'll be in a better legal position if you have taken the proper steps to protect and identify your trade secrets. You may be able to avoid litigation if the case involves a former employee joining another company, if the new employer is willing to cooperate. If the trade secret is valuable enough, litigation may be the only possible recourse.

Over 25% of trade secret cases involve temporary restraining orders or preliminary injunctions, and seeking this type of relief is expensive and requires you to explain your case at a very early stage. (Id. at 84.) Further, trade secrets owners only prevail in about 40% of state court cases. (Id. at 86.) Given the risks and expenses involve in trade secret litigation, taking steps to protect your trade secrets before they are stolen can save you time and money.

Mindy M. Morton is a Partner with Procopio in the Silicon Valley office. Her practice focuses on internet and intellectual property litigation. She helps clients resolve disputes involving trade secret, patent, trademark, copyright, computer fraud and non-compete agreement litigation, and litigates cutting-edge cases at the intersection of technology and free speech issues.

MANOLATOS ▪ NELSON ▪ MURPHY
Advertising & Public Relations

MANOLATOS NELSON MURPHY, INC.
3143 Fourth Avenue
San Diego, CA 92103
www.mnmadpr.com

Checklist:
Crisis Communications in a Cyberattack

To do now…

- Develop a Crisis Communications Plan and make sure key team members have a copy.
- Consider holding drills in which your team rehearses in a cyberattack scenario.
- Identify backup channels and systems.
    - Consider having a back-up printer.
    - Consider storing social media passwords offline in a secure place.
    - Know your smartphone's capabilities
- Educate yourself on cybersecurity.
- Know areas of sensitivity inside your organization, and understand what kind of information could be security sensitive.

When it happens…

- Create a team to vet public statements. Include general counsel, public relations and information technology leaders within the organization to weigh in on key decisions on the cyberattack. Identify which partner organizations, such as investigators, must sign off on information and statements provided publicly.
- Be proactive with media. If at all possible, announce the cyberattack before you receive media inquiries. This openness will invite goodwill and will prevent your agency from being accused of hiding the attack.
- Safety first. If there is any impact to public safety, the public should be alerted immediately, and provided with information about how they can minimize their risk. Your public statements should immediately address any areas in which the public might be exposed to risk, such as their private information being compromised.
- Find out how the public may be affected. Announce any impacts to public services, such as online bill-pay or park reservations. You may also want to clarify what isn't affected by the cyberattack.
- Be transparent, to the extent possible. Be open about what is not being released, and the reasons why. Emphasize the public interest – for example, releasing information on how public safety systems are affected could reveal vulnerabilities that could put law enforcement officers and the public in danger.
- Don't neglect internal communications. People inside your organization are wondering what's happening and if they don't receive regular updates, rumors will take shape. Morale is vulnerable when employees feel out of the loop, and this can lead to other serious problems, including leaks.

Tanya Castaneda, Vice President/Public Relations, Manolatos Nelson Murphy Advertising & Public Relations

Pierson Clair IV

Associate Managing Director for Cyber Risk
Kroll Cyber Security

Pierson Clair is an associate managing director in Kroll's Cyber Risk practice, based in the Los Angeles office. Pierson brings an uncommon perspective to cyber risk challenges from his years as a leading digital forensic examiner, technical security consultant, researcher, and educator. He has conducted extensive academic research at the forefront of cyber risk, most currently on changes of investigative significance in Mac and mobile device hardware and software. Prior to this emphasis, he focused on the dynamics within the complex framework of protecting critical national infrastructure as well as intelligence, espionage, and terrorism. In addition to working on analytical projects with members of the Intelligence Community and the U.S. Department of Homeland Security, Pierson has provided sophisticated digital forensic services for a wide range of private sector clients and law enforcement agencies.

Prior to joining Kroll, Pierson was with Maryman & Associates, where he was a senior forensic examiner specializing in Apple and Linux desktop and server environments; mobile devices including iOS and Android; virtualized environments; and network forensic and security investigations. He has assisted clients that range from major corporations with large network breaches to small businesses with unique software and infrastructure, to federal, state, and local law enforcement and government agencies. His casework has included investigations on such matters as employee malfeasance, intellectual property theft, data loss, and network data breaches, including the loss of personally identifiable information and private health information. He is also well-versed in the privacy and notification implications of data leaks. Before joining Maryman, Pierson worked with the U.S. Intelligence Community in Virginia and Washington, D.C., on a joint analytical project with the U.S. Department of Homeland Security and the wider U.S. Intelligence Community.

Pierson has also had a long-standing association with the University of Southern California (USC), where he is an Industrial Advisory Board Member for the university's Information Technology Program, a division of the Viterbi School of Engineering. He is a graduate of USC's selective Interdisciplinary Degree program, where he blended studies in intelligence, espionage, and terrorism with technical courses in cyber security and computer forensics. During this time, he was the first USC student to work in the United States Secret Service's Los Angeles Electronic Crimes Task Force (LA ECTF). Currently, Pierson is an adjunct faculty member in the Viterbi School of Engineering, where he has developed the curriculum and

teaches introductory and high-level courses in forensics and cyber security related to the Mac and mobile device environments.

Selected Media Appearances

- NBC4 Los Angeles, "Mobile Device Security: Fingerprints, Passcodes, and Passwords." January 2015.
- KTLA Los Angeles, "Android & Apple: Mobile Device Security & Encryption." October 2014.

Selected Teachings & Presentations

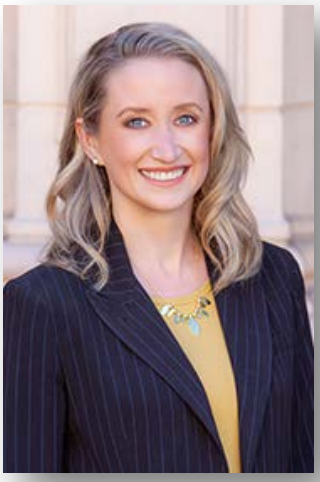
- University of Southern California (USC), Viterbi School of Engineering, Information Technology Program, Computer and Digital Forensics – ITP125, ITP 445, and ITP 447 (2012 – Present)
- Enfuse Digital Forensics & Cyber Security Conference (2017). Forensic Report Writing Fundamentals
- Mac Hardware Triage & Forensic Acquisition
- U.S. Secret Service Los Angeles Electronic Crimes Task Force Quarterly Meeting: The State of Mac Malware & Investigations (2017).
- Western Candy Conference: Cyber Threats to Manufacturing (2017).
- USC Ostrow School of Dentistry: The Health Care Cyber Threat Landscape (2017).
- Orange County (CA) Bar Association: Challenges Associated with Mobile Devices and Electronically Stored Information (2016).
- Industrial Security Awareness Council, Los Angeles: Human Threats to Technical Security (2015).
- RAND Corporation: Emerging Threats to Corporate Security (2015).
- FBI Counter Intelligence Strategic Partnership Academic Alliance Conference, Los Angeles: Lessons from the Information Security and Digital Forensic Frontlines (2015).
- U.S. Secret Service Los Angeles Electronic Crimes Task Force Quarterly Meeting: Forensic Implications of Fusion & Hybrid Drives (2014).

Education and Certifications

- M.S., Digital Forensic Science, Champlain College
- B.A., International Relations Security Studies & Technical Security (Hons.), University of Southern California (USC)
- Cyber Security Certificate, USC Viterbi School of Engineering, Information Technology Program
- EnCase Certified Examiner (EnCE)
- Cellebrite Certified Physical Analyst (CCPA)
- Cellebrite Certified Logical Operator (CCLO)
- Certified BlackLight Examiner (CBE)

Affiliations and Membership

- USC Viterbi School of Engineering, ITP Industrial Advisory Board Member
- High Technology Crime Investigation Association, Los Angeles chapter (HTCIA)
- Information Systems Security Association, Los Angeles chapter (ISSA)
- InfraGard Los Angeles
- United States Secret Service – Los Angeles Electronic Crimes Task Force (ECTF)



Tanya Mannes Castaneda

VP, Public Relations
Manolatos Nelson Murphy

Tanya is a nationally recognized leader in public relations who was named California's 2018 Communicator of the Year by CAPIO (California Association of Public Information Officials). She holds the Accreditation in Public Relations credential.

Serving as chief spokesperson for the Port of San Diego for six years, Tanya managed the Port's strategic communications program, including the website, branded social media accounts, speakers bureau and news releases, as well as responding to nearly 800 media inquiries per year. During Tanya's tenure, the Port ranked No. 1 among maritime ports worldwide in Facebook and Twitter followers, and its social media policy was recognized as a national model for governments. An experienced crisis communications manager, Tanya participated in regional drills focused on marine and aviation security, terrorism, medical epidemics and environmental disasters. She is a graduate of the Citizens Water Academy of the San Diego County Water Authority.

Tanya's community outreach campaigns and strategic communications programs received awards in 2017 and 2018 from the American Association of Port Authorities, the Association of Marketing and Communication Professionals, the California Association of Public Information Officials and the Public Relations Society of America San Diego-Imperial Counties.

Before embarking on her public relations career, Tanya built a name in the media industry. A graduate of the University of Massachusetts Amherst, she reported for newspapers including The San Diego Union-Tribune, The Boston Globe and the Virgin Islands Daily News; along with on-camera work for affiliated broadcast news stations. She attended the Ted Scripps Leadership Institute of the Society of Professional Journalists.

At MNM, Tanya is Vice President of Public Relations. She is a Democrat who lives in the South Bay, where she and her husband are raising their two young children. She is passionate about building public trust in the governmental, business and nonprofit institutions that touch our lives.

Paul Najar

VP, General Counsel and Corporate Secretary
Gafcon

Paul Najar is Vice President, General Counsel and Corporate Secretary of Gafcon. Prior to joining us, he served as Executive Vice President, General Counsel and Corporate Secretary of Anacomp Inc., a global document management company for nine years. He was responsible for all legal and administrative affairs including SEC reporting and compliance, M&A, corporate governance, litigation, licensing, real estate, human resources, and risk management. Before joining Anacomp, Paul served as University Attorney for the University of California, Irvine and Corporate Counsel for California Federal Bank.

He is a member of the Board of Directors of the Association of Corporate Counsel, San Diego. Paul received a joint Bachelor of Arts degree in Philosophy and Humanities from the University of California, Irvine and a J.D. from the University of California, Davis.

In his spare time, Paul enjoys international travel, skiing in the Rocky Mountains, and European history.