PROGRAM MATERIALS
Program #29108
June 25, 2019

Planning an Effective Response to a Cyber Incident

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

PLANNING AN EFFECTIVE RESPONSE TO A CYBER INCIDENT

Carole J. Buckner, Procopio Partner and General Counsel

Christopher “Todd “Doss, Ankura Managing Director – Cyber Incident Response

Speakers

- *Carole J. Buckner – Procopio, Cory, Hargreaves & Savitch, LLP – San Diego, California*
  - Partner & General Counsel
  - Member of Procopio's Privacy and Cybersecurity Practice Group
- *Todd Doss, Managing Director, Ankura – New York*
  - *Cyber Incident Response*
  - *Former FBI Special Agent*

Preparing Your Cyber Incident Response Plan

Your Cyber Incident Response Team

- Consider use of dual teams (business vs. legal issues)
- Identify all team members (internal and external) and backups
- Define the role of each team member
- Compile contact information
- Guidance for internal/external information sharing
- Designate which team members are responsible for each step in the incident response process
- Train team members

Your Cyber Incident Response Team

- Legal counsel – in-house and outside counsel
- Cyber insurance carriers
- Forensic consultants
- Corporate management
- Information technology
- Human resources
- Public relations
- Customer relations
- Law enforcement contacts

Plan For Communications

- Distribute hard copies of the incident response plan to all team members
- Anticipate communication needs without use of compromised systems
- Ideally, do not use compromised systems for communications
- If compromised system must be used, implement encryption

Overview of the Incident Response Process

- Confirm that the incident is not a false alarm.
- Notify the insurance carriers.
- Contact cyber counsel to establish attorney client privilege and work product.
- Engage forensic consultant
- 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 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

- Include carriers and policies in your plan
- Prepare notifications to carriers
- Reference relevant policy, date of incident, type of incident
- Determine whether consent to outside vendors is required
- Consider pre-approval of outside vendors by carrier
- Duty of cooperation – keep carriers advised

Forensic Consultants

- Avoid IT personnel fixes & do not clean servers
- Identify two forensic consultants in your plan
- Engage forensic consultants – pre-negotiate basic terms of engagements
- Obtain pre-approval from insurance carriers
- Role of forensic consultant
- Importance of preservation of evidence
  - Imaging of affected computers
  - Preservation of logs from servers, routers, firewalls
  - Maintaining chain of custody

Public Relations

- Determine who will handle media inquiries
- Use a single point of contact
- Consider internal and external public relations resources
- Draft all press communication with assistance of legal counsel
  - Anticipate public disclosure being used in litigation as admissions of liability
  - Avoid misleading statements
  - Avoid withholding information that is pertinent to consumers
- Anticipate press inquiries regarding data breach
  - Who attacked, how attack occurred, scope of attack, impact of attack, remediation
- Anticipate consumer questions & consider offering credit monitoring
  - Avoid making admissions

Notification to Consumers

- Evaluate notification requirements with forensic consultant, in-house and outside legal counsel
- Requirements vary - consider relevant federal and state law re breach notification
  - Who to notify, when notice required, form of notice
  - Some state requirements may conflict with other requirements
- Consider including information about
  - How breach occurred, what information taken, actions taken to remedy the situation, contact information for your organization
- Public companies disclosure requirements may include costs and consequences, and relevant insurance coverage

Contacting Law Enforcement

- Designate a law enforcement contact and backup (DOJ/USAO/FBI)
- Determine whether law enforcement contact is appropriate given the nature of the incident
- Consult with in-house & outside legal counsel, and management, and public relations personnel
- Understand law enforcement roles
  - FBI and DOJ prosecute cyber crimes
  - Homeland Security – phishing and malware
  - NCCIC receives reports
  - Dept. of Defense focuses on foreign cyber threats, national security, military systems
- Advantages and disadvantages

Training

- Practice your plan with your team
- Keep the plan up to date with changes in personnel
- Revise the plan as issues are identified in practice
- After an incident, conduct a post mortem, and revise your plan
- Forensic consultants will provide data breach training and table top exercises

Attorney Client Privilege and Work Product During A Cyber Breach

Is the Predominant Purpose Legal or Business Advice?

- Generally, the attorney client privilege is **not applicable where the attorney merely acts as a negotiator or to provide business advice.**
  - *Aetna Cas. & Sur. Co. v. Sup. Ct.*, 153 Cal. App. 3d 467 (1984)

- *EU does not extend privilege protection to in-house attorneys.*
  - *Akzo Nobel Chem. Ltd. V. European Comm'n,* Case C-550/07 P, 26 Law. Man. Prof. Conduct 584 (Euro. Ct. Justice, Sept. 14, 2010)

- **In-house counsel** often provide both legal and business advice

- **Outside counsel** predominantly provide legal advice

- Hire outside counsel at the inception

- This can be particularly important in international investigations

Dual Investigation to Preserve Privilege

In re Target Corp. Customer Data Security Breach Litig., MDL NO. 14-2522 (D. Minn. 2015)

- Target retained Version to investigate the data breach.
- Two separate teams were established both at Target and at Verizon.
- One team worked on the business response, focusing on operational concerns, while a second team directed by Target's counsel directed a response task force.
- The plaintiffs argued that communications between the Target task force and Verizon were not privileged and were not protected by the work product doctrine, because Target would have had to investigation and address the data breach regardless of any litigation.
- The court found Target met is burden of demonstrating these documents were protected by attorney client privilege and the work product doctrine.

Attorney Client Privilege & Press Releases in Data Breach Litigation

- *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F. Supp. 3d 1230 (D. Or. 2017)
  - What is the application of the privilege to communications with a public relations consultant during a data breach investigation?
  - If not drafted by or sent to counsel, even if they incorporate the advice of counsel, a court may find that they are not protected by the attorney client privilege.
  - Court will look at the primary purpose of such communications
    - to address the data breach, a business function,
    - or to obtain legal advice.
  - *Communications sent to and from legal counsel seeking or providing actual legal advice or the possible legal consequences of a proposed text are privileged.*

Privilege and the Data Breach Consultant

- *In re Premera Blue Cross Customer Data Sec. Breach Litig.*
  - *Consultant first hired by company*
  - *Later statement of work amended to provide for supervision of work by outside counsel*
  - *Court held report not privileged*
  - *Court distinguished Target data breach (no dual investigation)*
  - *Court distinguished Experian data breach*

- *In re Experian Data Breach Litig.*, 2017 U.S. Dist. LEXIS 162891
  - Company announced data breach
  - Class action following
  - Company hired outside legal counsel
  - Outside legal counsel hired the forensic consultant
  - Report provided to outside legal counsel, not to the company
  - Full report not shared with incident response team
  - Court held report was not discoverable

Cyber Insurance: Applications, Coverage, Exclusions, and Tender

Cyber Insurance vs. Traditional Insurance

- Comprehensive general liability insurance may not cover cyber breaches
  - Data breach not tangible
  - Policy exclusion for damages arising out of loss of electronic data
    - *RVST Holdings, LLC v. Main St. Am. Assur. Co.*, 136 A.D.3d 1196, 25 N.Y.S.3d 712 (N.Y. App. Div. 2016)
  - No advertising injury coverage
    - *Zurich Am. Ins. Co. v. Sony*, 2014 N.Y. Misc. LEXIS 5141 (N.Y. Sup. Ct. N.Y. County Feb. 24, 2014)

Cyber Insurance Application

- Cyber insurers may require a detailed application with certification that the insured follows specified practices
  - Security questionnaire
  - Access control, technical security practices
  - Organizational policies and procedures
- Complete application in collaboration with technology team

Cyber Insurance Application

- *Columbia Ca. Co. v. Cottage Health Sys.*, C.D. Cal. No. CV 15-03432 DDP (AGRx) (May 7, 2015)
  - Hospital data breach
  - Multiple regulatory investigations
  - Class action
  - Insurer filed action for declaratory relief claiming no coverage due to misrepresentations in the application, rendering the policy null and void

Cyber Insurance Coverage

- First Party Coverage
  - Loss mitigation, incident response
  - Expenses of business interruption
  - Ransom payments
- Third Party Coverage
  - Forensic investigation
  - Expenses of responding to regulatory proceedings
  - Legal expenses
  - Public relations expenses
  - Costs of notification

Cyber Insurance Coverage

- *Network security errors*
- *Actions of rogue employees*
- *Third party vendors*
- *Privacy liability coverage*
- *Cyber extortion coverage*
  - Ransomware incident, threatened attack, threatened disclosure
  - Typically require “immediate, credible threat”
  - Notification to carrier is critical

Cyber Insurance Coverage

- Business interruption loss
  - Policy definitions vary
  - Income loss related to business profitability
- Costs of response to state and federal regulators
  - Formal investigations
  - Responding to subpoenas

Cyber Insurance Exclusions

- Exclusion for contractual liability
  - *P.F. Chang's China Bistro v. Federal Insurance Co.*, 2016 U.S. Dist. LEXIS 70749 (D. Ariz. May 31, 2016)
    - Incurred expenses of investigating and remediating cyber incident
    - Expense in defending multiple class actions
    - Loss from contractual liability to banks not covered

Cyber Insurance Exclusions

- Act of war
  - *Mondelez Intern'l, Inc. v. Zurich American Ins. Co.*, 2018 WL 4941760 (2018)
    - Ransomware attacks
    - Act of war exclusion – attack involved a hostile or warlike action by a government agent

Timely Tender to Cyber Insurance Carrier

- *Beazley Insurance Co. Inc. v. Schnuck Markets Inc.*, No. 1:13-cv-08083, Compl. 2013 WL 6167107 (S.D.N.Y. Nov. 13, 2013)
  - Data breach of two million credit card numbers
  - Millions in expenses incurred in legal fees, forensic investigation, and public relations
  - Insurer alleged no coverage due to late notice and no written consent to incur expenses

Developing an Incident Response Plan for a Cyber Attack

By Carole J. Buckner, Partner and General Counsel, Procopio, Cory, Hargreaves & Savitch LLP

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. ABA Formal Op. 483 (2018). This in turn requires that a lawyer keep abreast of technology, including associated risks and benefits, including continuing study and education. *Id.* 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. *Id.* 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. *Id.*

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).

Maximize Your Cyber Insurance Coverage

By Carole J. Buckner, Partner and General Counsel, Procopio, Cory, Hargreaves & Savitch, LLP

Because cyberattacks are ever increasing, prevention is challenging, and liability to regulators and class action plaintiffs is escalating, cyber-insurance is becoming more prevalent. Annual premiums are expected to increase to $7.5 billion by 2020. Cyber-insurance is a relatively new type of insurance coverage, and increasingly becoming an important risk management tool. One prediction shows the cost of global cybercrime will hit $6 trillion by 2021. As of 2018, another study pegged the average cost of a cyber breach at $369,000. Unlike other types of insurance, there is more variation in cyber-insurance policies in terms of scope, sub-limits, coverage and exclusions. It is important to understand what is covered by your cyber-insurance policy as well as what may not be covered. In addition, because cyber insurance is a newer line of insurance, insurance carriers may require more detailed information in the application for the policy which may include a technical questionnaire. Once the insurance is in place, if a claim does occur, it is important to tender the matter to the cyber insurance carrier in a timely manner.

Traditional Insurance May Not Cover a Cyber Attack

While many companies depend on comprehensive general liability policies for coverage of losses arising from data breaches, recent legal decisions regarding traditional liability insurance have determined that such policies often do not cover cyber incidents on the grounds that data and information are not tangible, and therefore not covered. Because cyber related claims can arise in class actions, often with significant damages exposure, it is important that a business carefully consider whether or not existing insurance policies provide coverage for cyber incidents.

More and more comprehensive general liability policies now contain an exclusion for cyber related events. One court decided that an exclusion for damages arising out of the loss of electronic data applied such that a business owner could not recover on the policy for a network hack resulting in stolen credit card information. *RVST Holdings, LLC v. Main St. Am. Assur.*

Co., 136 A.D.3d 1196, 25 N.Y.S.3d 712 (N.Y. App. Div. 2016). As a result, the insurance carrier also had no duty to defend the litigation against the insured.

Another issue is whether a cyber incident involving publication of stolen private information falls within traditional coverage for advertising injury. In one case, the court determined that there was no coverage under a comprehensive general liability policy where third party hackers had stolen and published private information. *Zurich Am. Ins. Co. v. Sony*, 2014 N.Y. Misc. LEXIS 5141 (N.Y. Sup. Ct. N.Y. County Feb. 24, 2014). The court held that the theft of the information was not a publication by the insured and therefore not covered.

Understand Your Cyber Policy Coverage

Given the limitations on traditional insurance coverage it is important for businesses to consider obtaining separate coverage for cyber incidents, and to understand that scope of that coverage. Cyber insurance typically provides first party coverage, which includes loss mitigation as well as incident response and investigation services triggered by the discovery of a security or data privacy incident. First party coverage may also include expenses associated with business interruption and system failure. Such insurance may also cover the costs associated with a ransom payment demanded by a perpetrator. Third-party coverages typically include liability for defense and compensatory damages associated with regulatory proceedings, as well as privacy liability to third parties and liability for failures of network security and disclosure of otherwise confidential information. This coverage may include legal expenses, and public relations expenses, as well the cost of notifications to consumers.

Cyber-insurance policies also typically provide coverage for network security errors that result in liability of an insured for damages and expenses. Such coverage extends to include actions of rogue employees or third party vendors. Privacy liability coverage addresses privacy incidents such as unauthorized disclosure of personal information or confidential corporate information.

Coverage for privacy breach expenses usually insures against expenses related to privacy incidents including attorneys, accountants, public relationship consultants and other third parties as well as the costs of forensic analysis necessary to determine the cause of a privacy incident.

Some policies provide for reimbursement while others provide for payment on behalf of the insured. This distinction can in turn influence which providers will be used. Some types of common expenses that an insured will incur after a privacy breach will not within the scope of cyber-insurance coverage, including costs to correct deficiencies and upgrade systems, and salary and overhead expenses of the insured incurred in dealing with the breach. Voluntary payments, such as breach notifications that are not required by law, may also be excluded from coverage.

Cyber extortion coverage is another important part of many cyber insurance policies. Such coverage addresses ransomware incidents, among other cyber-related threats. Such coverage can be triggered by a threatened attack, or by the threatened disclosure of information. Policy provisions vary, with some requiring an immediate and credible threat in order to trigger coverage. Notification to the insurance carrier is critical as policies may require the insurance carrier to provide consent prior to payment of a ransom.

Business interruption loss is also covered by cyber insurance to cover losses incurred during a restoration after a cyber incident. Such policies often narrowly define business interruption income loss related to a business's profitability. Expenses incurred to improve systems are typically excluded from coverage. Cyber policies also cover expenses incurred by insureds in responding to state and federal regulatory authorities following a privacy incident, to include formal investigations, as well as responding to subpoenas.

Some cyber policies assign sub-limits to specific types of coverage. Common exclusions involve criminal, fraudulent and dishonest acts, and payment of fines and penalties. Because cyber-insurers are constantly changing the terms of coverage as they reevaluate risk, businesses must assess their needs against a detailed evaluation of the potential coverage available in the market.

In one case involving a cyber insurance policy, the insured incurred significant expenses in investigating and remediating a cyber breach in which hackers obtained 60,000 credit card numbers and posted them on the Internet. The insured also faced the expense of defending multiple class actions. While the policy covered privacy injury and notification expenses, the exclusion for losses resulting from contractual liability barred the insured's recovery for an

additional $2 million to cover fees and charges its credit card service providers charged back to the insured. *P.F. Chang's China Bistro v. Federal Insurance Co.*, 2016 U.S. Dist. LEXIS 70749 (D. Ariz. May 31, 2016).

Another pending case involves two ransomware attacks in which the insurance carrier under an all risk policy covering physical loss or damages to electronic data is asserting that the act of war exclusion warrants denial of coverage, on the grounds that the attack involved a hostile or warlike action by a government agent. *Mondelez Intern'l, Inc. v. Zurich American Ins. Co.*, 2018 WL 4941760 (2018). Alleged losses exceed $100 million.

Issues may also arise depending on the cyber-insurance policy definition of what constitutes a claim, with some policies requiring notice of charges, and others providing coverage for informal administrative proceedings.

Provide an Accurate Application/Questionnaire

Rigorous underwriting of cyber insurance applications is now standard practice. Applications for cyber insurance coverage may be more detailed than applications for other types of insurance, and may require that the insured follow specified practices. Applications should be completed in collaboration with the company's technology team, in order to assure accuracy, and to permit the technology team to carry through on appropriate safeguards. Many applications now involve security questionnaires designed to provide an understanding of the applicant's security posture, but often covering a substantial range of sub-topics including access control, data collection, technical security practices, relationships with service providers, loss history, and organizational policies and procedures.

In one recent case, an insured hospital network suffered a substantial data breach involving patient medical information which was publicly disclosed after unauthorized entry into the insured's servers. Three regulatory investigations were commenced by state and federal authorities. A class action followed, which the insured ultimately settled for $4.125 million. The insurance carrier funded the settlement, but reserved the right to seek reimbursement of the entire settlement amount from the insured. The insurance carrier then filed an action for declaratory relief, seeking to deny coverage for all damages, and seeking reimbursement for the

$4.125 million paid to settle the matter. The insurer also sought recover of all expenses incurred in responding to the breach, in the amount of $860,000, and defense costs of $168,000. In addition, the insurer sought rescission of the cyber policy on the grounds that the insured failed to follow the minimum practices required in the cyber policy application. At the same time, the insured filed an action in state court, also concerning the coverage dispute.

The carrier asserted that the application contained misrepresentations regarding whether the insured had exercised due diligence, checked and maintained security patches, and replaced default settings to assure information security. As a result, the carrier claimed that the misrepresentations in the application rendered the policy null and void. *Columbia Ca. Co. v. Cottage Health Sys.*, C.D. Cal. No. CV 15-03432 DDP (AGRx) (May 7, 2015). The case was dismissed without prejudice so that the parties could pursue alternative dispute resolution pursuant to the terms of the policy. *Columbia Ca. Co. v. Cottage Health Sys.*, C.D. Cal. No. CV 15-03432 DDP (AGRx) 2015 U.S. Dist. LEXIS 93456 (July 17, 2015).

One lesson is that using outdated security protocols may result in damages while the business may also lose the benefit of cyber-insurance coverage after paying high premiums.

Tender in a Timely Manner

It is critical to make a timely tender to the cyber insurance carrier after a cyber incident. In one reported matter, the insured experienced a cyber-attack that compromised two million credit and debit card numbers. The insured incurred millions of dollars in legal fees, forensic investigation fees, and expenses for TV, radio and newspaper ads. The policy provided coverage for reasonable expenses other than internal corporate costs, incurred with the insurer's prior written consent, and provided that as a condition precedent to coverage, written notice to the insurer was required at the earliest practicable moment or within 90 days of discovery.

The insurer alleged that it had not provided written consent to the insured to incur the expenses and that the insured had not provided notice within the 90 day period. The cyber insurance carrier claimed that coverage should be denied on the grounds that late notice was provided to the insurance carrier regarding the cyberattack. *Beazley Insurance Co. Inc. v. Schnuck Markets Inc.*, No. 1:13-cv-08083, Compl. 2013 WL 6167107 (S.D.N.Y. Nov. 13, 2013).

In the same case, the insurance carrier declined coverage in part because the consent of the insurance carrier was not obtained to the settlement of the dispute involving the cyber breach.

Conclusion

Cyber-insurance provides major risk management benefits for businesses, but coverage varies and it is important to understand what is appropriate for your business. Careful compliance with cyber-insurance policy requirements during the application process and at the time of tender of a potential claim will help avoid later arguments that could defeat coverage on the grounds that the policy is void.

BIBLIOGRAPHY

Najiya Budaly, Law360, *Brokers Urged to Be Vigilant for Cyber Insurance Flaws* (May 19, 2019)

2 DATA SEC. & PRIVACY LAW §S 14:6 14:17-14:25 (2018)

Daniel Garrie and Peter Rosen, Law360, *'Act of War' Questions in Cyberattack Insurance Case* (April 23, 2019)

Benjamin Horney, LAW360, *Insurer Says Policy Doesn't Cover Grocery's Data Leak Claim* (Nov. 15, 2013)

1 INSURANCE COVERAGE FOR IP CLAIMS, §§ 5.18, 5.21 (2019)

James McQuaid, et al., *Meeting the New Challenges of Cyber Insurance Coverage: Think You're Covered? Think Again,* ALI-CLE (2018)

Sahsa Romanosky, et al., *Content Analysis of Cyber Insurance Policies: How do Carriers Price Cyber Risk?* Journal of Cyber Security (2019)

Jill D. Rhodes and Robert S. Litt, THE ABA CYBERSECURITY HANDBOOK, (2d ed. 2018).

Minjhquang N. Trang, *Compulsory Corporate Cyber-Liability Insurance: Outsourcing Data Privacy Regulation to Prevent and Mitigate Data Breaches,* 18:1 Minn. J. L. Sci. & Tech 299 (2017)

David L. Vicevich, *The Case for a Federal Cyber Insurance Program*, 92:2 Neb. Law R. 555 (2018)

Procopio

Attorney Client Privilege and Work Product During a Cyber Breach

By Carole J. Buckner, Partner and General Counsel, Procopio, Cory, Hargreaves & Savitch, LLP

When a data breach occurs, counsel can advise on a wide range of issues from customer notification to remediation to regulatory requirements. Because class action litigation and regulatory scrutiny can follow a data breach, understanding and properly addressing attorney client privilege and attorney work product are critical from the outset. Companies should structure the data breach team to protect privilege and work product in connection with implementation of a response. Meetings and documentation should be implemented in a manner that will establish and maintain privilege. All members of the data breach team and company management should be trained as to how to preserve both privilege and work product. This article addresses many of the important nuances, including lessons learned from prominent data breach litigation.

ATTORNEY CLIENT PRIVILEGE

The attorney client privilege protects confidential communications made during an attorney client relationship from disclosure. (Cal. Ev. Code § 954.) Confidential communications are defined as those between client and lawyer in the course of an attorney client relationship, transmitted by means which disclose the information to no third persons other than those who are present to further the interest of the client in the consultation or those who are reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted. (Cal. Ev. Code § 952.) Disclosure of information to those reasonably necessary to accomplish the purpose of the representation does not constitute a waiver. (Cal. Ev. Code § 912.)

Federal attorney client privilege in the corporate setting protects communications with employees and corporate counsel in order to obtain information not otherwise available to upper management, where the employee is communicating with an attorney at the direction or a superior in order to secure legal advice for the company, if the subject matter of the communication falls within the duties of the employee and the communication is intended to be confidential. (*Upjohn Co. v. United States*, 449 U.S. 383 (1981).) In California, the dominant purpose test is used to determine whether a corporate employee is making the communication at the request of the employer, and to examine the intent of the employer and employee. (*D.I. Chadbourne v. Sup. Ct.*, 60 Cal.2d 723 (1964).) In determining whether any particular communication is privileged, the number of hands through which it passed is also relevant. (Id.)

WORK PRODUCT

If a particular document is not covered by the attorney client privilege, it may still be protected by the work product doctrine. (*Hickman v. Taylor*, 329 U.S. 495 (1947); Fed Rule Civ. P. 26 (documents and tangible things prepared in anticipation of litigation or for trial); Fed. R. Crim. P. 16.) California work product protection is broader in scope, and may protect recordings and notes regarding witness interviews even if

they are not created in anticipation of litigation. (Cal. Code Civ. P. 2018.030; *Coito v. Sup. Ct.*, 54 Cal.4th 480 (2012).)

LEGAL OR BUSINESS ADVICE?

An important consideration in determining whether a particular communication is privileged involves whether the dominant purpose was to give legal advice or business advice. Generally, the attorney client privilege is not applicable where the attorney merely acts as a negotiator or to provide business advice. (*Aetna Cas. & Sur. Co. v. Sup. Ct.*, 153 Cal. App. 3d 467 (1984).) Court will look at whether the communication was made in furtherance of that attorney client relationship, while taking into consideration that an attorney may be hired to address business affairs, but also give legal advice during the course of the representation, and that such advice should be protected notwithstanding the original purpose for which the attorney was employed. (*Kaiser Foundation Hospitals v. Sup. Ct.,* 66 Cal. App. 4th 1217 (1998).) Sending a carbon copy (or "cc") of an otherwise non-privileged communication to an attorney does not necessarily render the communication privileged. (See, e.g., *In re Google, Inc.*, 462 Fed. Appx 975 (Fed. Cir. 2012).)

INTERNATIONAL PRIVILEGE

In-house attorneys operating in an international setting need to bear in mind that while U.S. courts generally extend privilege protection to foreign attorneys, some courts recognize foreign privilege law, such as the law of the European Union, and do not extend privilege protection to communications between companies and their in-house attorneys. (*Akzo Nobel Chem. Ltd. V. European Comm'n,* Case C-550/07 P, 26 Law. Man. Prof. Conduct 584 (Euro. Ct. Justice, Sept. 14, 2010).)

OUTSIDE COUNSEL

In-house counsel often provide both legal and business advice. Outside counsel in contrast, predominantly provide legal advice. Hiring outside counsel at the inception can protect against the argument that in-house counsel's advice predominantly involved business advice and therefore was not privileged. This can be particularly important in international investigations given that non-U.S. privilege will not apply to protect communications between the company and in-house counsel in some countries.

DUAL INVESTIGATIONS

One approach is to establish dual investigations as Target did in connection with its payment card data breach. One team worked on the business response, focusing on operational concerns, while a second team directed by Target's counsel directed a response task force. (*In re Target Corp. Customer Data Security Breach Litig.,* MDL NO. 14-2522 (D. Minn. Oct. 23, 2015).) To optimize application of the privilege, the work should be directed by legal counsel, and the key objective should be to render legal advice. In addition, outside consultants should be engaged by counsel and work at the direction of counsel. (*Id. At 1-2.*) Counsel should remind employees and consultants of the confidentiality and privilege applicable to communications under the direction of counsel for the purpose of rendering legal advice.

In the Target data breach, Target retained Version to investigate the data breach. Two separate teams were established both at Target and at Verizon. The plaintiffs argued that communications between the Target task force and Verizon were not privileged and were not protected by the work product doctrine, because Target would have had to investigation and address the data breach regardless of any litigation. Target asserted that the task force was not engaged in an ordinary course of business investigation of the data breach. Rather Target asserted that Verizon had been engaged to educate the task force run by Target's in-house counsel and Target's outside counsel about aspects of the breach to enable counsel to provide informed legal advice, in part to defend against multiple class action lawsuits filed against Target. The court conducted an in camera review.

One set of documents in question involved email updates from the CEO to the Target board of directors in the aftermath of the data breach. The court ordered such communications produced because they did not involve any confidential attorney client communications or contain requests for legal advice nor provide legal advice. (*Id.* at 3.)

As to documents related to the work of the task force focused not on remediation but on informing Target's in-house and outside counsel about the breach, for the purpose of obtaining legal advice and preparing to defend the class action litigation, the court found Target met is burden of demonstrating these documents were protected by attorney client privilege and the work product doctrine. (*Id.* at 3-4.)

EMAIL

In order to be protected by attorney client privilege, email communications with counsel must request or provide legal advice. (*Premera II,* at *3.) Factual discussions exchanged with counsel are not protected from discovery by the attorney client privilege, unless the facts are being transmitted to counsel in order to provide legal representation. (*Id.*)

PRESS RELEASES

In general, courts are divided regarding whether attorney client privilege covers communications between counsel and a public relations consultant. In California, there is no public relations privilege. (*Behunin v. Sup. Ct.,* 9 Cal. App. 5th 833 (2017) (holding that communications with public relations consultant were not covered by the attorney client privilege where the disclosures were not reasonably necessary for the client's representation in the litigation).) The issue is whether the communication is necessary for the client to obtain informed legal advice, which may be evaluated by an in camera review after the privilege is claimed. The more integrated the public relations consultant is with development of legal strategy, effectively becoming and "agent" of the attorney, the more likely the privilege will cover communications between the two. In such a situation, there will be an expectation of confidentiality as well as necessity of disclosure to the third party in order to obtain informed legal advice. Some cases refer to the necessity element as requiring more than just convenience, requiring near indispensability. Other cases apply a test asking whether the public relations consultant was the "functional equivalent of an employee of the client." (*U.S. v. Chen,* 99 F.3d 1495, 1500 (9th Cir. 1996) (requiring a detailed factual showing of a close working relationship with the company's principals on matters critical to the company's position in litigation, and possession of

information possessed by no one else in the company).) These considerations should be balanced in entering into the engagement agreement with and utilizing the public relations consultant.

Federal common law on attorney client privilege differs from California law because the privilege is broader and there is no requirement of a finding that the communication was reasonably necessary for the attorney to provide legal advice. In any event, a fact specific inquiry will be required.

One case addresses the application of the privilege to communications with a public relations consultant during a data breach investigation. To the extent that those are not drafted by or sent to counsel, even if they incorporate the advice of counsel, a court may find that they are not protected by the attorney client privilege. (*In re Premera Blue Cross Customer Data Sec. Breach Litig.,* 296 F. Supp. 3d 1230 (D. Or. 2017).) In addition, documents not prepared by or sent to counsel, even if prepared at the request of counsel by employees and third party vendors, will not be privileged if they are not prepared because of litigation. (*Id.* at 1242.) The court will look at whether the primary purpose of such communications is to address the data breach, a business function, or to obtain legal advice. (*Id.* at 1243.) However, communications sent to and from legal counsel seeking or providing actual legal advice or the possible legal consequences of a proposed text are privileged. (*Id.*)

PUBLIC RELATIONS AND INTERNAL COMMUNICATIONS

A public relations consultant is a key member of the team that will address a data breach. Copying an attorney on communications involving a public relations consultant discussing published articles about the data breach may or may not be privileged. If the discussion involves seeking legal advice about how a particular article may impact the company or litigation, or how, from a legal perspective, the company should comment on the article, it is privileged. (*Premera,* 2019 U.S. Dist. LEXIS 20279 *11 (*Premera II)*; citing *Premera I,* 296 F.Supp. 3d At 1244.) If, however, the discussion involves merely the facts of the article, or how others are responding to the article, without a request for legal advice, or the provision of legal advice, merely including attorneys on the email does not render the email privileged. (*Id.*)

Internal communications between company executives and counsel regarding an article being drafted by the company are more likely to be privileged because they are more likely to involve requests for legal advice where the company's executives may be asking for legal advice as to how to minimize legal exposure, and/or the impact on the company's risk of liability.

In responding to a data breach internal communications will also be generated, which may include scripts prepared by outside counsel and in-house counsel, FAQs, responses to regulators and notices to consumers. Where drafts of such documents contain edit by counsel, a privilege designation is appropriate. (*Premera II,* at *6.)

COMMUNICATIONS RE: CONSUMER NOTIFICATIONS

Communications with outside counsel concerning consumer notifications are privileged if they are requesting or providing legal advice. This is the case even if counsel is not providing a redline version. This

will include documents circulated in order to provide legal counsel to the company in drafting notification letters. Such communications may also qualify for protection under the work product doctrine.

DATA BREACH CONSULTANT'S WORK

Discovery disputes over draft and final reports of consultants can develop. In the *Premera* matter the forensic consultant produced a Remediation Report and an Intrusion Report. The consultant was first hired by the company. After discovery of a breach, the consultant's statement of work was amended to provide that outside counsel would supervise the consultant's work. Premera argued that the subsequent reports were privileged and protected as work product. However the court found that the flaw in Premera's argument was that the consultant was hired to perform a scope of work for Premera, not for outside counsel, and noted that the scope of work did not change after the consultant was directed to report to outside counsel and label the reports privilege. (*Premera,* at 1245.)

The court distinguished the *Target* data breach because there was only one investigation in the *Premera* matter. The court also distinguished the *Experian* data breach in which outside counsel was hired by the company, and outside counsel had hired the consultant. Ultimately, the *Premera* court held that changing the supervision, without changing the scope of work, was not sufficient to render the later communications privileged and protected by the work product doctrine. However, the court did allow work product protection for documents generated by the forensic consultant working with outside counsel to the extent that they contained legal advice or mental impressions of counsel.

In *In re Experian Data Breach Litig.,* 2017 U.S. Dist. LEXIS 162891, the company's announcement of a data breach was followed by the filing of a class action. The company hired outside legal counsel and outside legal counsel hired the outside forensic consultant to investigate and provide information to legal counsel in order to allow legal counsel to provide legal advice to the company. The consultant provided a report not to the company, but to outside counsel only, who then shared the report with in-house counsel, all designed to facilitate the legal advice by outside counsel.

Importantly, the full report was not shared with the company's incident response team. When the class action plaintiffs sought the report in discovery, the court held that the documents were protected by the work product doctrine because the report was prepared in anticipation of litigation, even though that was not the company's only purpose. The court also rejected the argument that the hardship exception to the work product doctrine applied to allow plaintiff's discovery of the report, because plaintiffs had the exact same access to mirrored images of the servers as the consultant had.

Consultants should be hired and supervised by outside counsel, not by the incident response team, and not by the information security department. The consultant's statement of work should provide that the consultant will report to counsel pursuant to the scope of work set forth in the agreement, and that the consultant is being hired to assist counsel with providing legal advice. While it may be a better approach to have separate teams of consultants should conduct separate investigations as in the *Target* case, this may not always be possible due to expense.

COMMUNICATIONS REGARDING REMEDIATION

While remediation is a business function, communications with counsel are privileged if they actually contain legal advice or requests for legal advice, of where factual information is being provided to counsel for the purpose of allowing counsel to provide legal advice. As to remediation information provided by third parties, the privilege will apply only if the same criteria are applicable. (*Premera II*, at *XX; *Genesco, Inc. v. Visa U.S.A., Inc.,* No. 3:13-CV-00202 (M.D. Tenn. Mar 25, 2015).)

COMMON INTEREST?

It is important to consider the consequences of sharing information in connection with a cyber breach. In the *Experian* case the company had shared the forensic report with a co-defendant's counsel. The plaintiffs in the class action sought the report on the ground that the disclosure waived the work product doctrine. Ultimately, the court ruled that the sharing of the report with the co-defendant's attorneys under a joint defense agreement in redacted form did not result in a waiver of the work product doctrine. An effective joint defense agreement requires that the interests of the parties be aligned. Although a written common interest agreement is not required, having such an agreement would allow the parties to control specific aspects of the agreement, including remedies for breach of such an agreement.

THIRD PARTY VENDORS

Other third party vendors will be scrutinized by the court to determine whether they are providing non-legal business functions, or services related to litigation, such as electronic discovery related services, which would be protected. (*Premera,* at 1246-47.)

WAIVER

Under California law, voluntary disclosure of the contents of otherwise privileged communications constitutes a waiver of the privilege as to all communications on the same subject matter. (*Weil v. Investment, Research and Mgmt, Inc.,* 647 F.2d 18, 24 (9th Cir. 1981).)

In addition, the company may decide that it is advantageous to waive privilege and work product in favor of disclosing communications. This possible avenue should be kept in mind in the course of the data breach investigation as the data breach team is communicating.

CONCLUSION

Companies handling a data breach must address multiple considerations in order to preserve attorney client privilege and work product if litigation ensues. Thinking through and planning for the myriad issues before hand is an important part of planning and executing a competent response.