The Challenges for a Remote Workforce Regarding Data Privacy and Security Audits, and the Preservation of Attorney-Client and/or Work-Product Privilege

By Benjamin Sley, J.D., LL.M.

If your corporate data is not secure, your corporate future may not be secure

The lockdowns to stop the spread of COVID-19 fostered the creation of a remote workforce in which many employees work from home, accessing corporate data from off-site locations. This creates more vulnerabilities for corporate data systems as such data can be accessed from many portals outside of what could be a more secure in-house computer system. At the same time, recent very serious data breaches have occurred exposing personal, financial, health and government data to nefarious hackers.

There is an increased need for data protection and security by private and government sectors, and private and publicly traded companies. The only way to enhance security and privacy of data is the implementation of rigorous system and operational data and security controls through comprehensive audits. There is a risk that adverse or "qualified" audit reports could be ordered by a court to be produced to litigants affected by a data breach with resultant adverse consequences.

This article will discuss best practices for vigorous cybersecurity audits by CPA firms and technical firms, with audits such as the SOC 2 or NIST 800-171, respectively, and the best way to preserve attorney-client and/or work-product privilege regarding such audit reports.

Current Issues of COVID-19 and the SolarWinds Breach

We've seen the headlines about COVID-19 and the remote workforce with resultant security vulnerabilities. We've also seen the headlines about the most extensive security data breach in history involving SolarWinds software that has affected the Pentagon, the State Department, the Department of Justice, the Department of Homeland Security, the NSA, other government agencies, and 18,000 public and private users, including many *Fortune* 500 companies!

As a result of this very extensive and damaging breach, the federal Cybersecurity and Infrastructure Security Agency, (CISA.gov), issued Alert (AA20-352A) stating:

"CISA has determined that this threat poses a grave risk to the Federal Government and state, local, tribal and territorial governments, as well as critical infrastructure entities and other private sector organizations." [1]

CISA also issued Emergency Directive 21-01 stating:

"This threat actor has the resources, patience and expertise to gain access to and privileges over highly sensitive information if left unchecked. ***CISA urges organizations to prioritize measures to identify and address this threat."*** [2]

Security

What you may not have seen in the headlines is that the FTC had filed an administrative complaint against Zoom for deceptively advertising its security capabilities and circumventing certain available security features. The FTC alleged that, since at least 2016, Zoom misled users by touting that it offered "end-to-end, 256-bit encryption" to secure users' communications, when, in fact, it provided a lower level of security.

The FTC further alleged that Zoom maintained the cryptographic keys that could allow Zoom to access the content of its customers' meetings. Zoom's misleading claims gave users "a false sense of security" according to the FTC's complaint, especially for those who used the company's platform to discuss sensitive topics such as health and financial information.

The CISA Directive has very specific instructions regarding the breach, including:

***"Block[ing] all traffic** to and from hosts, external to the enterprise, where any version of SolarWinds Orion software has been installed."*

Thus, any company that has either been directly affected by this security breach or that has done business with a company so affected should engage in a cybersecurity audit to address and mitigate the possibility of this continuing threat.

The SolarWinds breach occurred at a time when corporate computer systems and infrastructure are more vulnerable as a result of more accessible portals, with remote workers accessing corporate data through home computers. As a result of COVID-19 and the measures to prevent its spread, many companies, educational institutions, law firms, accounting firms and other organizations have permitted their employees to work from remote locations.

It is predicted that remote access to corporate data will continue into the foreseeable future. As a beneficiary of this remote workforce, Zoom Video Communications, Inc., (Zoom) skyrocketed in growth from $27 million in quarterly revenue in Q1 2018 to over $882 million in Q4 2021, an increase of over 32 times! [3]

The FTC settled this case with Zoom on Nov. 9, 2020. Zoom has agreed to the FTC requirements to establish and implement a comprehensive security program, a prohibition on privacy and security misrepresentations, and other detailed and specific relief to protect its rapidly growing user base.

If a company is currently using Zoom for interactive video conference calls, how will that company know if Zoom has enacted end-to-end 256-bit encryption on its calls? If a company uses another video conference call provider, does the company have an understanding of the security protocols?

Employees are most likely accessing corporate data through a Virtual Private Network (VPN). However, other factors must be considered for security, including the use of multi-factor authentication for connecting to the VPN, keeping the security setting of the VPN platform up-to-date, using a "handshake" protocol, such as Internet Protocol Security (IPSec), Secure Socket Layers (SSL), Transport Layer Security (TLS), etc., to ensure secure communication channels between employees' devices and the corporate networks.

They should use full-tunnel VPN where possible (using split-tunnel VPN only when necessary, such as in circumstances of insufficient bandwidth), block the connection from insecure devices and immediately remove VPN access to terminated employees.

Other security controls that may be used are:

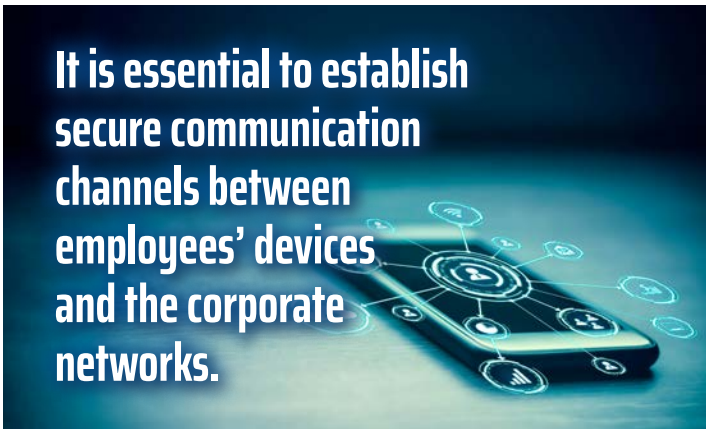
- Ensuring that all work-related information in the devices is encrypted;
- Setting up strong access controls, such as requiring the use of strong passwords;
- Limiting the number of failed log-in attempts;
- Preventing the transfer of data from corporate devices to personal devices; and
- Enabling a remote wipe function so that information on the devices can be erased if the devices are lost or stolen.

Additional aspects of such cybersecurity requirements are beyond the scope of this article, but these matters must be addressed and attested to in a comprehensive cybersecurity audit. Your firm, company or organization would ultimately be responsible for any security deficiencies of any third-party vendors of online services that you may use.

That's why it is necessary to engage in a comprehensive System and Organization Controls (SOC) audit that addresses both corporate financial data trustworthiness and security and personal data protection.

Sarbanes Oxley and SOC® Reports

Regarding financial trustworthiness, as a background regarding comprehensive financial audits, the *Sarbanes-Oxley Act of 2002* (SOX) was passed nearly unanimously by both the House and Senate in response to the fraudulent accounting scandals of Enron, Tyco and WorldCom that led to the loss of literally hundreds of billions of dollars in market value and severely eroded public confidence in publicly traded companies at the time.



One of the significant requirements of SOX is Section 302 (15 U.S. Code § 7241), which requires the CEO and CFO of publicly traded companies to certify that the financial data is complete, accurate and fairly represents all material aspects of the corporate financial condition.

SOX has criminal provisions that provide for penalties against CEOs and CFOs who knowingly certify false financial reports of up to $5 million in fines and up to 20 years in prison. (18 U.S. Code § 1350) Section 404 of SOX (15 U.S. Code § 7262) requires a public company's annual report to include the company's assessment of internal operating control over financial reporting and an auditor's attestation regarding adequacy of those operating controls.

Penalty provisions of SOX may also be applied to private companies that knowingly violate federal law, such as:

- Intentionally destroying, altering or falsifying records or documents with the intention of impeding or influencing a federal agency investigation (such as OSHA, EEOC or the IRS) or a federal bankruptcy proceeding;
- Engaging in violations of federal and state securities laws that are not dischargeable in bankruptcy, including liabilities for fraud in connection with the private placement of securities; and
- Engaging in retaliating against a whistleblower who provides truthful information relating to a possible corporate federal offense.

The Securities and Exchange Commission (SEC) administers the financial accountability, control and reporting requirements, although it does not provide a particular audit or certification process. However, in this regard, AICPA's *Statement on Standards for Attestation Engagements 18* and the subsequent System and Organization Controls (SOC®) audit and attestation submitted annually is considered sufficient for rigorous SOX compliance.

SOX further prevents conflict of interest with the company's financial auditor by restricting the type of extra services they can provide to that company. A SOC® 1 Type 2 audit examines a company's operating controls and financial controls over a period of time from six months to 12 months. (A controls report that is a "snapshot" as of a particular date is a SOC® 1 Type 1 audit.)

Lenders, investors and potential business partners may consider SOX-compliant corporate audits to establish "best practices" for both public and private companies and seek such annual certifications. An Unqualified (clean) SOC® report is very useful for instilling public trust and confidence in that company, whether public or private.

Additional Security and Privacy Laws and Regulations

There are many additional laws that have been enacted or amended recently that require adequate and rigorous corporate security controls. For example, on Dec. 4, 2020, the *Internet of Things (IoT) Cybersecurity Improvement Act* (IoT Law) was signed into law.[4] The IoT Law requires the National Institute of Standards and Technology (NIST) to develop and publish baseline standards and guidelines for how the federal government uses and manages IoT devices connected to information systems.

NIST – which has already been addressing IoT cybersecurity – is required to promulgate "minimum information security requirements for managing cybersecurity risks associated with such devices." The IoT Law requires these new standards and guidelines to be consistent with NIST's current guidance regarding:

- Vulnerability identification and management;
- Secure development;
- Identity management;
- Patch management; and
- Configuration management.

NIST is also tasked with publishing guidelines for IoT vendors regarding the disclosure of security vulnerabilities and dissemination of information about resolution of these vulnerabilities.

In the area of doing business with the federal government, NIST has promulgated security and operational standards that must be met by **all** government contractors and subcontractors in a very rigorous annual audit, the NIST 800-171 report. This requirement encompasses 14 categories of data security requirements. In aggregate, NIST 800-171 contains 110 separate practices or controls, all of which require compliance. A perfect score is complying with all 110 controls. Each deficiency has points subtracted from 110.

The failure to limit system access to authorized users renders all the other access control requirements ineffective, allowing easy exploitation of the network. A NIST 800-171 deficient audit would completely prevent that contractor or subcontractor from doing business with the U.S. government.

While technically applying only to federal government procurement, NIST's standards and guidelines have the potential to influence state law and private sector practices. For instance, many IoT devices sold to the federal government that meet the NIST-based standards will also inevitably be sold to the private sector. As a practical matter, the NIST standards may have a broader impact on security practices across the IoT industry.

As a matter of best practices, all businesses that are subject to the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule should be able to meet the rigorous security standards of a NIST 800-171 audit. HIPAA has its own audit systems control and data security requirements incumbent upon each organization that handles personal health information (PHI). [5]

In this regard, on Dec. 10, 2020, the Department of Health and Human Services (HHS) proposed significant changes to HIPAA in a 357-page proposal that would provide individuals with greater access to their health information and clarify permissible information sharing procedures for case coordination and management. Regardless of whether this new proposal is enacted, health providers that handle PHI must comply with the existing HIPAA privacy rules and must have adequate system controls to be able to confirm compliance. [6]

On Dec. 10, 2020, the California Attorney General issued a fourth set of proposed modifications to the regulations implementing the California Consumer Privacy Act (CCPA), which apply to all companies doing business with persons in California. The additional changes are particularly important for covered entities engaged in the "sale" of personal information.

The modifications **introduce a new, uniform opt-out button logo**. The button may be used in addition to posting the required notice of the right to opt out and, when adopted, should appear to the left of the "Do Not Sell My Personal Information" text and be approximately the same size as any other buttons used by the business on its webpage.

The proposed modifications advise that when a consumer clicks the opt-out button, it should bring that consumer to the same webpage or online location to which the consumer is directed after clicking on the "Do Not Sell My Personal Information" link so that the consumer can opt out.

In addition to the CCPA, in the November 2020 election, California voters by a 55% majority approved the new California Privacy Rights Act (CPRA). The CPRA will apply to information collected on and after Jan. 1, 2022 and will be effective on Jan. 1, 2023.

One of the biggest impacts the CPRA brings is the increased responsibility an organization has with respect to their customers' privacy. With the passing of CPRA, businesses are now firmly responsible for not only what they do with customer data themselves, but also what any third party they choose to do business with does with the shared data.

If a company includes advertisements from a third-party provider on their site, the company now has much stricter requirements to ensure that the ad provider is not storing customer data.

Ultimately, this means that any business that utilizes third-party services on their website, such as **analytic trackers, telemetry monitoring, virtual assistants and shopping carts**, are required to understand, monitor and control all data flow to them and will be subsequently held responsible for any data leakage.

In October 2020, NIST proposed an 88-page "Cybersecurity Profile for the Responsible Use of Positioning, Navigation and Timing (PNT) Services." This relates to privacy issues regarding GPS tracking and storage of such data and disclosure of such data. [7]

As can be seen, the issues of security and privacy controls for personal, health and financial data are expanding rapidly. The only way to determine compliance is with a third-party independent audit of such corporate systems and organizational controls. To be compliant with these laws and regulations, an organization must plan for such audits with the appropriate personnel having responsibility and authority to implement proper procedures.

The problem arises when an organization does not meet its security obligations, resulting in a breach of privacy and data and subsequent suits or government administrative actions. This leads to the issue of how to protect against the disclosure of a "qualified" or adverse audit result that would enumerate the organization's failures or possible negligence.

Protecting Attorney-Client Privilege and Work-Product Privilege

Some states specifically have an accountant-client privilege that could apply to a SOC® 1 or SOC 2® audit, such as Florida. The Florida Evidence Code provides, "A communication between an accountant and the accountant's client is "confidential" if it is not intended to be disclosed to third persons...". [8]

Texas has a limited accountant-client privilege that does not apply to a federal subpoena and can be overcome with a specific state court order. [9] Several other states have a form of accountant-client privilege, including Pennsylvania, Colorado and Missouri. However, such privilege can be waived by disclosure to third parties.

The better way to try to establish attorney-client privilege is by having the corporate general counsel hire an outside law firm to provide legal advice regarding determining any cybersecurity vulnerabilities and developing a plan of remediation. The organization through its general counsel should hire outside counsel to provide legal advice regarding compliance with the myriad laws regarding security and privacy legal obligations.

To preserve legal privilege, the retainer agreement should make clear that the corporate point of contact is the general counsel and not a chief information officer or data privacy officer. The outside counsel firm would then hire a CPA firm to conduct a SOC® 2 audit or a computer technical firm to conduct an NIST 800-171 audit.

Hiring a CPA firm or computer technical firm signed by the corporate IT department will not provide attorney-client privilege protection; it should be done by general counsel.

If a data breach has occurred or is suspected to have occurred, the case of *In re Capital One Consumer Data* case is very instructive regarding preserving work-product privilege. [10] In this case, on Nov. 30, 2015, Capital One entered into a Master Services Agreement with FireEye, Inc., d/b/a Mandiant, to provide cybersecurity services as set forth in a series of Statements of Work (SOWs). In July 2019, Capital One experienced a data breach and on July 20, 2019, retained the law firm Debevoise & Plimpton (Debevoise) to provide legal advice regarding the breach.

On July 24, 2019, Capital One, Debevoise and FireEye signed a Letter Agreement in which FireEye would provide services and advice "as directed by counsel" regarding the same scope of work in the prior SOW. Also, FireEye would be paid based on the same terms as in the 2019 SOW. Further, the Letter Agreement provided that FireEye work was to be conducted at the direction of

Debevoise and that deliverables were to be made directly to Debevoise.

Plaintiffs sought the FireEye Report to which Capital One objected, claiming work-product privilege. The District Court concluded that the FireEye Report was not protected under work-product privilege. The Court held that Capital One failed to prove the two-prong test for work-product privilege set forth in the RLI Insurance case. [11]

The RLI test is that to successfully claim work-product privilege, a court must determine (1) whether the document at issue was created "when the litigation is a real likelihood and not merely a possibility" and (2) whether the document in question would have been created in essentially the same form in the absence of litigation.

Capital One met the first prong, but failed the second prong, because Capital One failed to establish that the report would not have been prepared in substantially similar form "but for the prospect of the litigation."

Merely hiring a law firm after a data breach to receive a report that was otherwise previously contracted and paid for by a prior SOW is not sufficient to create a work-product privileged document. The lesson of Capital One is that after a breach, a organization's general counsel, not corporate IT, should retain a law firm to provide legal advice regarding the breach, reporting that legal advice directly to the general counsel.

In turn, the law firm, not the company, would hire an outside CPA firm or technical firm to investigate the data breach, recommend remediation steps and provide the resulting breach report directly to the law firm. The law firm would report the findings directly to the general counsel.

The CPA firm or technical firm would be paid by the law firm (reimbursed as a necessary expense by the organization). This will likely be sufficient to preserve attorney-client and/or work-product privilege regarding the resultant report.

Protecting Data and Privacy

All U.S. companies, whether public or private, need to prepare for security, privacy and controls compliance with a SOC® 2 audit by a CPA firm

If there is concern that a company may have security vulnerabilities or that a breach has already occurred, general counsel should retain a law firm to provide legal advice.

or with a NIST 800-171 audit by a technical firm. Clients and customers demand such reports today, wanting to know that their data is as safe as possible, and that the company has a stringent, comprehensive system and organizational controls in place to properly protect data and privacy.

A company that properly prepares for the audit is in much better shape than the company that fails to prepare. The corporate general counsel should interface directly with the CPA firm or technical firm and have them report back directly to the general counsel.

If there is concern that a company may have security vulnerabilities or that a breach has already occurred, general counsel should retain a law firm to provide legal advice regarding the vulnerabilities or breach, reporting that legal advice directly to the general counsel.

In turn, the law firm would hire an outside CPA firm or technical firm to investigate the vulnerabilities or data breach, recommend corrective/remediation steps as appropriate and provide the report directly to the law firm.

The CPA firm or technical firm would be paid directly by the law firm. The law firm would report the findings directly to the general counsel. This will likely be sufficient to preserve attorney-client and/or work-product privilege regarding the resultant report.

ABOUT THE AUTHOR: Benjamin Sley, J.D., LL.M. (Tax and Intellectual Property), Registered Patent Attorney, is the Senior In-House Counsel at Pro-Lab Diagnostics USA. He may be contacted at bsley@pro-lab.us.

Endnotes

1. https://us-cert.cisa.gov/ncas/alerts/aa20-352a
2. https://www.cisa.gov/supply-chain-compromise
3. https://backlinko.com/zoom-users
4. https://www.congress.gov/116/bills/hr1668/BILLS-116hr1668eh.pdf
5. 45 CFR § 164.308 - Administrative safeguards
6. https://www.hhs.gov/sites/default/files/hhs-ocr-hipaa-nprm.pdf
https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8323.pdf
8. Florida Evidence Code Sec. 90.5055(1)(c)
9. Texas Occupations Code § 901.457. Accountant-Client Privilege
10. *In re Capital One Consumer Data Sec. Breach Litig.*, MDL No. 1:19md2915 (AJT/JFA) (E.D. Va. Jun. 25, 2020)
11. *RLI Insurance Co. v. Conseco, Inc.*, 477 F. Supp. 2d 741, 748 (E.D. Va. 2007).