KEY TAKEAWAYS

FROM THE
THIRD ANNUAL
CYBERSECURITY THOUGHT LEADERSHIP CONFERENCE
OF THE
TECHNOLOGY AND THE LEGAL PROFESSION COMMITTEE
OF THE
NEW YORK STATE BAR ASSOCIATION

January 20, 2022

Opinions expressed are those of the Committee preparing these Key Takeaways and do not represent those of the New York State Bar Association unless and until the report has been adopted by the Association's House of Delegates or Executive Committee.

TECHNOLOGY AND THE LEGAL PROFESSION COMMITTEE

CO-CHAIRS

Gail L. Gottehrer
Law Office of Gail Gottehrer LLC

Ronald J. Hedges
Dentons US LLP

COMMITTEE MEMBERS

Jennifer V. Abelaj
Paul H. Aloe
Mark A. Berman
Robert M. Brill
Patrick J. Burke
Sasha A. Carbone
Ada Chan
Bryan Daniels
Zoe L. Davidson
Craig H. Effrain
Daniel H. Erskine
Matei Foit
William S. Friedlander
Shawndra G. Jones
Kenneth A. Krajewski
Anthony Tze Cheung Lam
Glenn Lau-Kee
Christian P. Levis
Erica L. Ludwick
Dan Feng Mei
Marissa J. Moran
Mauricio F. Paez
Alexander Paykin
Debbie Reynolds
Effie Silva
Enet Somers-Dehaney
Sanford Strenger
David Titus
Ryan M. Torino

CYBERSECURITY THOUGHT LEADERS AND CO-AUTHORS

Nicole Cardascia
Daniel H. Erskine
Gail L. Gottehrer
Thomas Grillo
Ronald J. Hedges
Erez Liebermann
Laurie Kamaiko
Mary Kavaney
Christian P. Levis
Dan Feng Mei
Aishwarya Minocha
Debbie Reynolds
Elizabeth Roper
Enet Somers-Dehaney
James Vinocur

SPECIAL THANKS TO

Dentons US LLP
Bryan Cooper
Molly Watson

TABLE OF CONTENTS

Page

INTRODUCTION FROM THE CO-CHAIRS

Technology continues to play an increasingly significant role in the practice of law. The evidence is indisputable – a major law firm recently announced that its attorneys can work from anywhere indefinitely; the New York State Supreme Court's Commercial Division issued rules endorsing the use of virtual depositions; and courts across the country have indicated that remote judicial proceedings are here to stay.

The widespread adoption of technology has the potential to transform the legal profession. The shift to remote work and virtual court proceedings could increase diversity, equity, and inclusion; improve access to justice; and reduce the costs of litigation and practicing law. As attorneys and courts become more dependent on technology, however, the profession and our legal system become more vulnerable to cyberattacks. Accordingly, it is crucial for attorneys to go beyond just satisfying their ethical obligation of technological competence and to understand and prioritize cybersecurity.

We held our Third Annual Cybersecurity Thought Leadership Conference virtually in October 2021 and are happy to share this Report on the Key Takeaways from that conference. We focused on four topics that are relevant to all attorneys, whether they work in government agencies, public interest organizations, educational institutions, in-house, or law firms: Insider Threats, Phishing, Cloud Technology Best Practices, and Security Assessment Vendors. The Report provides practical guidance to attorneys who are new to cybersecurity and to those who, already familiar with cybersecurity, are interested in learning more.

We thank the Cybersecurity Thought Leaders, whose names are listed on the preceding page, for their commitment to cybersecurity education and to the Cybersecurity Subcommittee. We also thank Bryan Cooper and Molly Watson for sharing their expertise and to Dentons US LLP for its continued support of the Technology and the Legal Profession Committee and the Cybersecurity Subcommittee.

Gail Gottehrer and Ron Hedges

Co-Chairs, NYSBA Technology and
the Legal Profession Committee

INSIDER THREATS

Introduction

- "Insider" threats, whether intentional or inadvertent, are a significant percentage of cybersecurity events. Insiders can be involved in breaches of personally identifiable information, often are a conduit to credentials that allow threat actors access to a firm or company's computer systems, and can be unknowing participants in funds transfer frauds.

- As direct bad actors, unknowing tools of bad actors, or simply through lack of knowledge of basic cybersecurity preventative procedures, insiders can be the cause of a cybersecurity incident that results in loss of business, financial damages, and reputational harm to the company for which they work.

- The scope of such threats, and the role insiders can play in their occurrence, are constant and everchanging. As discussed below, however, there are basic steps that all companies can take to minimize their occurrence and their effect.

- All entities, whether small or large, public or private, can and should take reasonable steps to anticipate such threats in their environments, prepare in advance as to how they will respond to threats that have been executed, and educate employees at all levels on how to recognize and avoid insider threats. Many of those steps are relatively low cost and require a commitment to a culture of cybersecurity rather than significant financial expenditures.

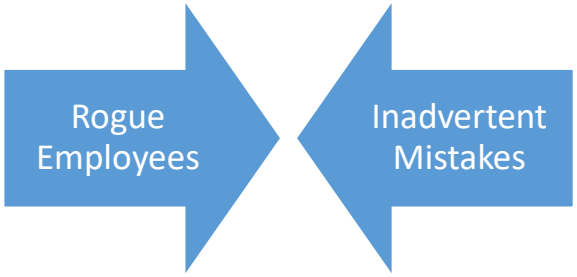
What is an Insider Threat?

- An insider threat is "the potential for an individual who has or has had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization." https://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated.

- The Department of Homeland Security advises that insider threats include sabotage, theft, espionage, fraud, and improper acquisition of competitive advantage that are often carried out through abusing access rights, theft of materials, and mishandling physical devices.

- DHS notes that such threats can also result from employee carelessness or policy violations that allow malicious outsiders access to company computer systems. https://www.cisa.gov/instider-threat-cyber.

Who Are Insiders?



- Insider threats can be caused by the intentional conduct of a rogue employee. They can also be the result of inadvertent mistakes such as an employee clicking on an attachment to an unsolicited email that sends malware into the firm's computer system or an employee who mistakenly believes they are responding to the directions from a senior executive when they send gift cards or make a payment to an account of someone they believe to be a legitimate vendor.
    - For an example of the latter, imagine an assistant who receives an email from the CEO of their company in which the CEO directs the assistant to wire a substantial sum to an account outside the organization.
    - The assistant does so without any inquiry and, to their (and the entity's) horror, learns that they have been the victim of a phishing scam.
- Sometimes, the threat is due to a deliberate action that the employee actor may not even realize constitutes a data breach for which they, as well as their company, may be liable.
    - In a recently reported case, a law firm has contended that the attorney defendants who left the firm secretly downloaded and removed files.
    - Other reported incidents involve attorneys who transferred client funds held in trust without checking that the email with instructions as to the account to which to transfer funds actually came from the client.
- "Insiders" are not only employees.
    - An "insider" can also be a consultant, contractor or outside administrator to whom services are delegated, such as an IT vendor.
    - Often, such vendors are provided credentials that allow them access to their client's (namely, your company's) computer network.
    - If the vendor shares those credentials, or does not reasonably protect them, or if the vendor is subject to a cyber attack that results in a bad actor obtaining those credentials, wrongful access to their client company's computer network can occur.

Risks Presented by Insider Threats

Whatever the nature of the insider threat, the risk that insider threats can present to an entity include:

- Theft of intellectual property, including trade secrets;
- Unauthorized access to personal data that can constitute a data breach that triggers a company's statutory obligations to provide notice to affected individuals;
- Regulatory scrutiny due to failure to comply with state, federal or other governmental or regulatory data security requirements, including ones that apply to law firms;
- Fines or other sanctions by one or more regulator;
- Cyberattacks that affect a company's operating systems or computer networks;
- An award of damages and other relief, including attorneys' fees, in civil actions brought under applicable privacy laws or common law by affected individuals or entities;
- Harm to business reputation; and
- Loss of consumer, customer, or public trust.

Steps to Take to Minimize Insider Threats

Business entities can take steps before an incident occurs to minimize the risk of a successful threat, to reduce the damages that can occur if there is an incident, and to comply with applicable legislative and regulatory cybersecurity requirements.

Some of the basic steps include:

- Developing policies and procedures to plan for and respond to insider threats and their aftermath;
- Instituting multi-factor authentication for access to computer networks, particularly for mobile devices and for remote access to systems (**Note:** Do not allow opt outs or exceptions!);
- Taking steps to ensure that patches are promptly applied and monitoring applications to make sure they are timely applied;
- Adopting "zero trust," meaning have all personnel operate on the assumption that there is always a threat (*e.g.*, assume emails with attachments from unknown sources are not safe until verified);
- Conducting security audits of personnel and systems on a regular basis, including periodic testing;

- Engaging in "tabletop" exercises to plan for and develop responses to threats and their aftermath;

- Obtaining cyber insurance, which may offer services to plan for and respond to an incident as well as help defray some of the costs and damages resulting from an incident;

- Educating all personnel, including those at the board or governing body level, in cybersecurity awareness and procedures, from recognizing phishing emails to encouraging physical data security (*e.g.*, not keeping passwords in plain sight);

- Instituting practices that identify unusual account activity, or when an insider is acting in an unusual way;

- Limiting the access of vendors and employees to only systems they need to do their jobs and terminating access when it is no longer needed (especially when an insider's employment is terminated!);

- Monitoring policies and procedures on a regular basis and revising them in response to recognized shortcomings and to incorporate new threats; and

- Cultivating a culture of awareness of the need for cybersecurity.

Resources

Numerous resources are available to assist in the education and awareness of threats. A few recently issued ones are:

- A Fact Sheet on Rising Ransomware Threat to Operational Technology Assets, issued on June 9, 2021, by the Cybersecurity and Infrastructure Security Agency of the United States Department of Homeland Security (CISA) available at Ransomware Threat to OT | CISA, which includes "several recommended actions and resources that critical infrastructure entities should implement to reduce the risk of ransomware."

- "Ransomware risk: 2 preventive steps for your small business," released on November 5, 2021, by the Federal Trade Commission," available at Ransomware risk: 2 preventive steps for your small business | Federal Trade Commission (ftc.gov).

    - These steps are:

        - ***Step #1. Make sure your tech team is following best practices to fend off a ransomware attack.***

            - One key protective step is to set up offline, off-site, encrypted backups of information essential to your business.

            - Furthermore, share the CISA Fact Sheet with your IT staff.

        - Underline, *italicize*, CAPITALIZE just how important it is for them to stay current on the latest word from the leading federal agency on defending against these threats and on updates from other trustworthy public-private partnerships.

        - CISA's ransomware resources – including its Ransomware Guide – should be required reading. This isn't something to save for a slow day at the office.

        - Your IT team should immerse themselves in the latest advice from CISA and other authoritative experts.

    - ***Step #2. Schedule a security refresher for your employees.***

        - Ransomware isn't just an issue for IT professionals.

        - Bad actors often use email to your staff as their entryway into your computer system.

        - By clicking on a link or downloading an attachment, a distracted staffer could inadvertently hand a computer criminal the keys to your corporate kingdom.

        - As companies up their defensive game, the bad guys have responded. Some use publicly available information or stolen data about an employee to craft a more personal message.

        - Rather than a misspelled mess that screams scam from the start, the email – or phone call, text, etc. – may appear at first glance to be legitimate business correspondence or even a message from a colleague.

        - A small business's best defense is a workforce trained in the tricks that cybercriminals are likely to use.

        - Other important protections are: 1) rigorous authentication procedures; and 2) a company policy that requires passwords for employee credentials and administrative functions to be l-o-n-g and complex.

        - In addition, educate your staff on the folly of using the same password on different platforms, and consider the many benefits of multifactor authentication.

These steps can be readily reviewed and incorporated into any entity's policies and procedures.

Other government websites also identify resources available for organizations to better understand, detect, and deter insider threats. *See, e.g.*, Department of Homeland Security National Cybersecurity and Communications Integration Center's website, at https://www.cisa.gov/insider-threat-cyber.

Key "Takeaways" on Insider Threats

- Every entity, public or private, including law firms, faces insider threats;
- Entities should develop policies and procedures that allow for appropriate monitoring of activities that are unusual or suspicious;
- Entities should become familiar with laws and regulations that address unauthorized access and data breach;
- Entities should utilize resources provided by cyber insurers, government and regulatory agencies, and specialized privacy and cybersecurity counsel; and
- All personnel at all levels of the organization should be educated about insider risks and compliance with cybersecurity procedures on a regular basis – no opt outs!

Every organization faces cybersecurity risks. Making sure you and everyone in your organization are aware of those risks and of the ways in which insiders can perpetuate – and minimize – them, is critical to mitigating the cybersecurity risks and potential losses your organization faces.

Phishing, and the Many Forms It Takes

Phishing affects everyone.

What is Phishing?

Phishing is the fraudulent attempt to obtain sensitive information by disguising oneself as a trustworthy entity in a communication. Phishing scams range in sophistication, from a shotgun approach to a highly targeted approach. Phishing is widespread and appears in text messages, robocalls, and emails.

There are different types of phishing, including email phishing, spear phishing, whaling, vishing, and smishing.

Phishing emails tend to induce or trick recipients into clicking on a link and/or opening an attachment in an email. Popular phishing tactics include messages such as:

- "We have noticed some suspicious activity on your account," and
- "We have noticed there's an issue with your payment information."

Phishing emails often include fake invoices and links to make payments.

Spear Phishing

- Spear phishing often relates to an employee, who is responsible for money transfers, receiving a seemingly legitimate email instructing a transfer of funds.
- These are targeted scams and the purported "sender" of the transfer-request-email is often a high-level executive within the company.
- Spear phishing attackers often gather and use personal information about their target.

Whaling

- Whaling is often directed specifically at senior executives and other high-profile targets.
- The contents will likely be created to be of interest to the person or role targeted, such as a subpoena or customer complaint.

Vishing

- Vishing uses the telephone to conduct phishing attacks.
- The attacker-caller dials a large quantity of telephone numbers and plays automated recordings to the victim-callee. These automated recordings include false claims of fraudulent activity on the victim's bank accounts or credit cards. The victim is directed to call a number controlled by the attackers. These calls will prompt victims to enter sensitive information to "resolve" the supposed fraud.

Smishing

- Smishing is an attack with the intent to gather personal information, including social insurance and/or credit card numbers.
- Common smishing examples include bank notifications, package updates, act-now coupons, and urgent warnings. Everyone should be suspicious of any such request, especially if they are from unknown numbers.

Some Statistics

In 2019, one third of all data breaches involved phishing. Phishing is the most common way to penetrate a system.

- Phishing has become a gateway for ransomware, malware, and other cyberattacks. It is the delivery mechanism of choice for ransomware and other malware.
- Usually, phishing emails are sent by seemingly friendly contacts with attachments and/or links that can lead to the installation of malware, which is then used to give the bad actor access to the computer or network. The phishing emails may also allow the bad actor to use the computer to launch malicious attacks or even use the computer to perpetrate fraud campaigns.

If there has been a phishing attack, there are remediation steps that can be followed to prevent the extent of the attack.

- If funds have been mistakenly wired, the organization(s) or individual(s) should contact their bank immediately and consider contacting law enforcement, filing a complaint with the FBI's Internet Crime Complaint Center (IC3), and filing a complaint with local police, the United States Secret Service, or the local FBI office.

- If data has been breached via a phishing attack, the organization or individual should consider contacting law enforcement and a cyber-security specialist/analyst.

Phishing has been so prevalent in all industries that 75% of organizations around the world experienced some kind of phishing attack in 2020. The successful efforts to reduce phishing come from establishing a culture of cybersecurity within the organization. Regular training and phishing tests can help users become the front-line defense for any of these attacks.

- To establish a culture of being cyber aware, organizations must require frequent data security and social engineering training. Knowledge is the best prevention method that helps everyone learn the signs of malicious emails or the indications of an attack.

- 2019 statistics show that 38% of untrained users fail phishing tests. Therefore it is crucially important to maintain good cyber hygiene practices in the organization.

FBI Internet Crime Complaint Center (IC3) 2020 statistics report that IC3 received 791,790 complaints for about $4.1 billion in losses.

- According to the FBI, phishing was the most common type of cybercrime in 2020.

- Phishing incidents more than doubled in frequency, from 114,702 incidents in 2019 to 241,324 incidents in 2020.

- These trends indicate that phishing and other cyberattacks are getting more sophisticated and organizations need to establish their front-line defense.

Why Lawyers Should Care About Phishing

There are a number of practical, ethical, and legal considerations posed by phishing attacks of which all attorneys should be mindful.

- From a practical perspective, the majority of cyber attacks are perpetrated via phishing schemes.

    - Nearly three-quarters of all organizations reported sustaining a successful phishing attack in 2020, according to one survey.

    - These attacks, which can lead to the execution of ransomware, network intrusion, or even business email compromises to name but a few, are the linchpin for a majority of cyber incidents.

- As victims range from solo practitioners to international law firms, all attorneys should be mindful of the damage caused by phishing schemes.

- Potential fallout from a cyber attack can include loss of productivity, remediation costs, breach notification, regulatory scrutiny, litigation, and insurance coverage issues.

- One reason why bad actors continue to target lawyers and law firms is that they are rich sources of the type of information sought by the attackers Bad actors often seek out clients' and employees' personal information, including social security numbers, contact information, and financial account information. Lawyers' involvement in high-value transactions also make them targets for bad actors seeking to intercept and manipulate banking information.

- In addition to these practical considerations, attorneys are ethically required to ensure that their clients' and employees' personal information are reasonably safeguarded.

    - Comment 8 to Rule 1:1 of the Model Rules of Professional Conduct requires that "[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology . . ."

    - In addition, NYSBA Opinion 842 states that Rule 1.6 requires that lawyers take affirmative steps to protect their clients' confidential information. (It should also be noted that NYSBA recommended in June 2020 that lawyers be mandated to obtain a CLE credit on the topic of cybersecurity.)

    - Separately, the American Bar Association declared in Ethics Opinion 477R that lawyers are "required to make reasonable efforts to ensure their communications are secure and not subject to inadvertent or unauthorized cyber security breaches."

- Beyond ethical requirements, there are legal requirements to be aware of in the context of a phishing attack.

    - New York's Shield Act, https://www.nysenate.gov/legislation/bills/2019/s5575, imposes affirmative duties on attorneys who hold and store personal information to ensure that there are reasonable administrative, technical, and physical safeguards in place to protect that information. Any entity that sustains a data breach of this type of personal information has an obligation under the Shield Act to notify those affected and, in some cases, the New York Attorney General's office.

    - The Health Information Technology for Economic and Clinical (HITECH) Act and the Gramm-Leach-Bliley (GLBA) Act impose, respectively, additional safeguards on the storage and handling of patients' medical data, and on financial institutions that handle personal information.

- Law firms of any size that collect personal information from existing and potential clients must ensure that they are compliant with various consumer privacy laws.
    - In the United States, California (California Consumer Privacy Act), Colorado (Colorado Privacy Act), and Virginia (Virginia Consumer Data Protection Act) require businesses of any type to notify residents at or before the time of collection of their data, and of the business's use of that data.
    - The European Union's General Data Protection Regulation (GDPR) places similar restrictions on the collection and use of its residents' data. Failure to abide by these regulations can result in significant fines, litigation, and regulatory action.

Multi-Factor Authentication (MFA)

One step all attorneys should take to mitigate the risk of a cyber incident is to implement multi-factor authentication across both device and account usage.

- Stealing passwords is now the top aim of individuals perpetrating cyber attacks.
- According to Microsoft, implementing MFA can decrease the risk of a successful account breach by 99%.
- There are number of options, including SMS-based MFA, voice-call MFA, and app-based MFA.

The Global Cyber Alliance (GCA)

- GCA is a global not-for-profit created to make the internet safer globally. Former New York County District Attorney Cyrus Vance Jr. created GCA utilizing asset forfeiture funds. GCA now has over 180 member entities from 18 sectors and 33 countries. www.globalcyberalliance.org
- GCA, when it was created in 2015, gave thought and consideration as to how to reduce the risk of phishing, .and created tools to better ensure that users would be safer from this type of cyberattack.

Quad9

The first tool was launched in November of 2017 and called Quad9.

- This name is derived from the IP address of 9.9.9.9.
- Quad9 is a protective DNS infrastructure.
- DNS stands for Domain Name System, which is essentially the phone book of the internet.
    - When a user tries to go to the website of buycatfood.com, DNS translates the website into a numerical IP address that is recognized globally and the user is taken to that address.
- Quad9 takes numerous commercial threat feeds that have been donated by intelligence providers to this free global resource. There are now millions of malicious websites on a block list that are known to contact malicious code like malware. If a user unknowingly tries to go to a website containing malware or other malicious code, the search does not resolve and the user is protected from going to that unsafe site. https://www.globalcyberalliance.org/quad9/
- Quad9 is different from other DNS services in that it does not sell the users' data so it is privacy protecting.
- In 2021, Quad9 made between 60-100 million blocks a day globally.
- In 2017, New York City began to use Quad9 to protect all its guest WIFI.
- Quad9 is now used on every continent.

DMARC

While DNS protects users leaving their organizations and going out to surf on the internet, GCA wanted to promote a tool that would better protect users from receiving fraudulent emails, especially "spoofing" emails, where the bad actor's attempts imitate a legitimate entity and fool the user into giving up his or her personally identifiable information.

- To further this effort, GCA examined why the DMARC (Domain Message Authentication Reporting and Conformance) tool that stops spoofing was not more widely deployed around the world.
- In speaking to partners, GCA learned that a major factor in the limited deployment of DMARC was the difficulties of such deployment.
- To address this concern, GCA created a wizard or a toolkit that is now available in 17 languages and has been deployed worldwide. https://www.globalcyberalliance.org/dmarc/
- While DMARC is not the silver bullet in protecting any organization, it has provided major security benefits to organizations that have deployed it, like Aetna, which stopped 60 million fraudulent emails after deploying DMARC.

- GCA has created a video that explains DMARC and its benefits. https://vimeo.com/221659402

Small Business Toolkit

GCA has created a cybersecurity tool kit for small and medium businesses (including law firms) that can assist with compliance with the SHIELD Act, which mandates certain administrative, physical, and technical safeguards.

- The toolkit can be found at: https://www.globalcyberalliance.org/gca-cybersecurity-toolkit-for-small-business
- The toolkit contains 6 toolboxes that include free and vetted tools.
- The toolkit is linked to the Center for Internet Security (CIS) top five Critical Controls.
- These Controls have been shown to improve the online security posture of users by 85%.

Cloud Technology Best Practices

What Is Cloud Computing?

Cloud computing is a delivery model for information technology (IT) services, permitting users the right to use computing and data storage services (both hardware and software) to access and store information and/or software functionality on remote servers owned or operated by third parties, usually through the internet or private networks.

- The remote servers are hosted in data centers worldwide, permitting cloud vendors to sell computing power, storage capacity, and data across such centers dynamically for fast delivery and on-demand bandwidth.

- Largely all or any IT supply may be delivered as a cloud service, *e.g.*, software applications, branded databases, data retrieval/storage, network configuration and software design tools.

- The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Delivery Options

1. **IaaS: Infrastructure as a Service**

    - Hardware infrastructure (*e.g.*, servers and storage) for remote use permitting users to install, implement, and maintain operating systems and software selected. *E.g.*, Amazon Elastic Compute Cloud (Amazon EC2), Rackspace, Microsoft® Azure® cloud.

2. **SaaS: Software as a Service**

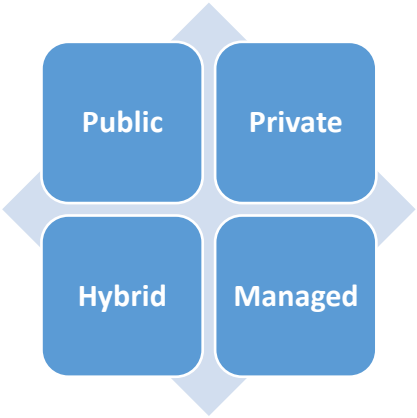
    - Third-party provider manages hardware and software for software applications (no copy on user computer) accessed via a browser/internet permitting user to run,

add, review, sort and manipulate data. *E.g.*, Google's Gmail, DropBox, iCloud, Westlaw.

3. **PaaS: Platform as a Service**
    - Remote computing environment provided for software developers/programmers to develop or extend and run new or existing applications. *E.g.*, Heroku Cloud Application Platform, Google App Engine.

4. **XaaS: Anything as a Service**
    - "X" means anything/any solution. The "aaS" means the business model of third-party providers describing how/method user both receives and pays for solution.

Service Options



Ways in which Cloud Technology Services are provided to users include:

1. **Public clouds**
    - Shared, self-service, "pay as you go" basis.

2. **Private clouds**
    - Dedicated hardware environment for the user.

3. **Hybrid clouds**
    - Combination of public and private clouds, private cloud for proprietary/sensitive information with public cloud for cost savings and less crucial information.

4. **Managed clouds**
    - Managed by a third-party provider, owned by user.

Cloud Computing Security Issues

Key threats to be mindful of when entering into a cloud computing agreement:

- Account Takeovers
- Malware
- Insider Threats
- Data Breaches

Account Takeovers

- Threat actors can leverage user credentials to gain access to cloud storage services.
- From there, they can:
    - Access sensitive data
    - Launch additional attacks
    - Impersonate users
- Credentials can be obtained via:
    - Social engineering
        - Use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes
    - Remote Desktop Protocol access
        - Provides access to a desktop or application hosted on a remote host
    - Phishing

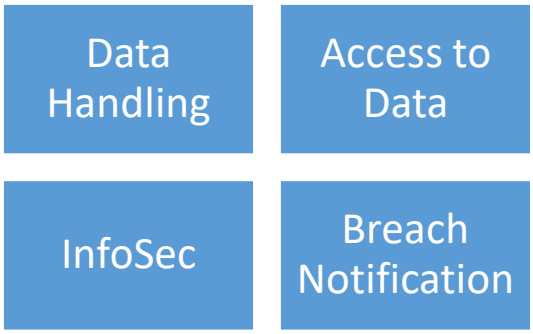
Malware

- Cloud storage services are also used by criminals to host malware.
    - In 2020, over half of malicious code deliveries happened using cloud apps.
- Threat actors will compromise cloud accounts belonging to one user/organization, and then move laterally within the command and control servers.
- Supply chain attacks: malware is deployed in the software development phase, then spreads downstream

Insider Threats

- Users within the organization can misuse cloud access to:
    - Steal proprietary or confidential data
    - Interfere with operations

Factors to consider when evaluating cloud vendors



Data Handling

- Use of, and access, to data.
- Confirm that vendor is only accessing the data necessary to provide its services to the client.
- Confirm that any use of necessary data is only used to provide a specific service to the client and not for any other purpose.
- Confirm that vendor will not give third-party access to client data.
- Exception:
    - Vendor may disclose data as required by applicable law or governmental authority.
    - However, vendor must give client prompt notice of such a demand and cooperate with client in any effort to contest disclosure or seek a protective order.

Vendor Access to Data

- Who has access to client data? Does vendor limit access to client data within its own company?

- Confirm that vendor will not permit any of its employees, subcontractors, or subcontractor employees to access client data unless the individual or company needs access to perform the agreed upon scope of work.

- How does the vendor vet employees who handle sensitive client data?

- Do employees have a clean work and education history and no criminal records?

Cybersecurity Practices

- Does the vendor maintain, implement, and comply with a written data and information security program?

    - An Information Security (InfoSec) Program should:

        - Protect the security and confidentiality of client.

        - Protect against anticipated threats or hazards to the security or integrity of client data.

        - Protect against unauthorized access to or use of client data.

    - What to Look for in an InfoSec Program:

        - Guidelines on the proper disposal of client data after it is no longer needed to carry out services.

        - Access controls on electronic systems used to maintain, access, or transmit client data.

        - Access restrictions at physical locations containing client data.

        - Encryption of electronic client data consistent with then-current, nationally recognized encryption standards.

        - Least privilege principles for access to client data, supplemented either by dual control procedures or segregation of duties.

        - Regular testing and monitoring of electronic systems accessing or storing client data.

        - Procedures to detect actual and attempted attacks on or intrusions into the systems containing or accessing client data.

        - Regular, annual review of the program to ensure that it complies with applicable laws, regulations, technology changes, and best practices.

Breach Notification

- Confirm that vendor will exercise reasonable efforts to prevent unauthorized exposure or disclosure of client data.
- Confirm that vendor has a protocol in play in case of a "Data Incident" in which vendor is responsible for the unauthorized disclosure of, access to, or use of client data.
- In the event of a Data Incident, vendor should notify the client within 48 hours and cooperate with client and law enforcement agencies to investigate and resolve the Data Incident.
- Confirm that vendor will aid in notifying injured third parties.
- Confirm that vendor will compensate client for any reasonable expenses related to notification of injured parties.
- Confirm that vendor will provide one year of credit monitoring to any affected individual.
- Confirm that vendor will provide client access to confidential information (*e.g.* non-public information, trade secrets, confidential records, sensitive information) if it relates to the Data Incident.

See also, Illinois State Bar Ass'n Professional Conduct Advisory Opinion No. 16-06 (Oct. 2016), https://www.isba.org/sites/default/files/ethicsopinions/16-06.pdf (listing factors to consider when evaluating cloud vendors).

Key Laws

- Sarbanes−Oxley Act of 2002, Pub. L. 107-204 (Public companies email retention, data security and integrity, and oversight)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191 (Use and disclosure of protected health information)
- Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. 113-283. Federal agencies to develop and implement information security programs. Executive Order 14208, "Improving the Nation's Cybersecurity" (May 12, 2021)
- Data privacy and security laws, including laws concerning the cross-border transfer of personal information.
- N.Y. General Business Law § § 899-aa, 899-bb
- For state agencies N.Y. State Technology Law § 208
- N.Y. Department of Financial Services (NYDFS) Cybersecurity Regulations for Financial Services companies (23 NYCRR 500.0 through 500.23)

- N.Y. Gen. Bus. Law § 349(a) and N.Y. Exec. Law § 63(12) (deceptive acts and practices)
- Federal Trade Commission Act, Section 5 (15 U.S.C. § 45)
- Federal Trade Commission's Red Flags Rules issued under the Fair and Accurate Credit Transactions Act (FACTA)
- Gramm-Leach-Bliley Act (GLBA) (Pub. L. No. 106-102, 113 Stat. 1338 (1999)
- Telephone Consumer Protection Act (TCPA)
- Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (a/k/a the "Patriot Act")
- Children's Online Privacy Protection Act of 1998 (COPPA)
- Fair Credit Reporting Act (FCRA) as amended by FATA
- Electronic Communications Privacy Act of 1986 (ECPA)
- Computer Fraud and Abuse Act (CFAA)
- Video Privacy Protection Act of 1988 (VPPA)
- GDPR (Regulation (EU) 2016/679)
- UK Data Protection Act 2018

Confidentiality of Business, Personal or Privileged Information

- N.Y. Rules of Prof. Conduct, Rule 1.0(c)
- N.Y. Rules of Prof. Conduct, Rule 1.6
- N.Y. Gen. Bus. Law § 399-ddd (Social Security Numbers)
- N.Y. Gen. Bus. Law §§ 399-h, 899-aa(1)(b), and § 899-bb (data disposal)
- N.Y. Penal Law §§ 250.00 to 250.05 (eavesdropping law)
- N.Y. Lab. Law § 203-c (employee privacy protection)
- N.Y. Gen. Bus. Law § 395-b (unlawfully installing or maintaining viewing devices)
- N.Y. Lab. Law § 203-d (employee personal identifying information)

- N.Y. Lab. Law § 704 (surveillance as an unfair labor practice)
- N.Y. Pub. Health Law § 2781 (HIV and AIDS information)
- N.Y. Comp. Codes R. and Regs. tit. II, ch. XIX, § 420.0 to 420.24 (Privacy of Consumer Financial and Health Information)
- N.Y. Gen. Bus. Law § 380 (Credit Reporting)
- N.Y. Gen. Bus. Law § 520-a (Restriction on Collecting Addresses on Credit Card Transactions)
- N.Y. Pub. Off. Law §§ 91-99 (Government Data Banks)
- N.Y. Pub. Off. Law § 89(2)(b)(i) (Employment and Medical Information Records)
- N.Y. Lab. Law § 201-a (Employment Records)
- N.Y. Pub. Off. Law § 89(2)(b)(iii) (State Mailing Lists)
- N.Y. Pub. Off. Law § 521-C (Credit Card Lists)
- N.Y. Pub. Health Law § 17 (Medical Records)
- N.Y. Gen. Bus. Law art. 39-F §§ 899-aa et seq. (Notification of Unauthorized Acquisition of Private Information)
- N.Y. Exec. Law § 718
- N.Y. C.P.L.R. 4502(b) (Spousal privilege); *see also* N.Y. C.P.L. Article 250
- N.Y. C.P.L.R. 4503 (Attorney-client)
- N.Y. C.P.L.R. 4504 (Physician, dentist, chiropractor, nurse)
- N.Y. C.P.L.R. 4505 (Clergy)
- N.Y. C.P.L.R. 4507 (Psychologist)
- N.Y. C.P.L.R. 4508 (Social worker)
- N.Y. C.P.L.R. 4509 (Library circulation records)
- N.Y. C.P.L.R. 4510 (Rape crisis counselor)
- Civ. Rights Law § 79-h (Journalist Shield Law)
- Jud. Law § 499 (Member or authorized agent of a lawyer assistance committee)

eDiscovery

- Federal Rules of Civil Procedure
    - Rule 16
    - Rule 26
    - Rule 37 (data retention)
- N.Y. Commercial Division Rules 22 New York Codes, Rules and Regulations (NYCRR) § 202.70(g)
    - Rule 1(b)
    - Rule 11-e(f)
    - Rule 11-g
    - Appendices A, B, E
    - N.Y. C.P.L.R.
        - Rule 3103
        - Rule 3120
        - Rule 3122(b)
        - Rule 2301
        - *See also, generally,* 22 NYCRR §§ 202.1 to 202.69

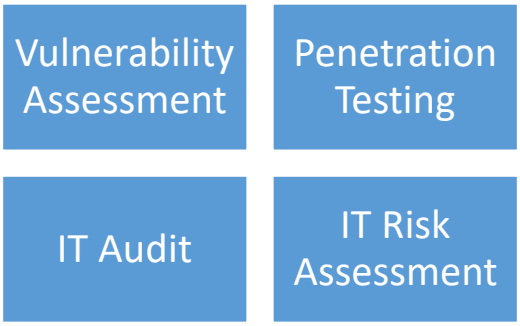
Security Assessment Vendors

- N.Y. Rule of Professional Conduct ("Rule") 1.1 addresses competence of attorneys.
- Rule 1.6 deals with the obligation of attorneys to take reasonable measures to protect confidentiality.
- Taken together, these rules require attorneys to have sufficient technical knowledge to engage in the practice of law and to maintain the confidentiality of information.

What Are Security Assessments and Security Assessment Vendors?

- Security assessments are periodic exercises that allow companies, including law firms, to test their data security systems.
- Security Assessment Vendors are contractors who are retained by organizations to conduct assessments to test the organization's security preparedness.
    - These vendors should be expected to know and follow industry standards in undertaking security assessments and reporting the results of assessments.
    - Attorneys should know enough to be able to satisfy themselves that the vendors they select to conduct security assessments are qualified and that the assessment is done in accordance with industry standards.

Types of Security Assessments



- Vulnerability Assessment:
    - This type of assessment is intended to map vulnerabilities in an organization's IT systems.
    - It seeks to identify and "fix" vulnerabilities as a first step toward a more comprehensive security environment.

- Penetration Testing (Pen Test):
    - This assessment is focused on a particular "target."
    - It attempts to penetrate the target's IT system and allows the vendor who is "attacking" the target to evaluate the system's functionality, management, and security.
    - There are three levels of information that a tester could have about the IT system it is attacking:
        - White = the tester has full access to the system.
        - Grey = the tester has some knowledge about the system but not enough to assure access.
        - Black = the tester has no information about the system and is essentially acting as an external hacker.
- IT Audit:
    - Purpose is to test whether an existing IT system follows a governing compliance standard which might have technical as well as documentation requirements.
    - The intent of the audit is not to test a system's security but, rather, to demonstrate that it is in compliance with certain standards or requirements.
- IT Risk Assessment:
    - Purpose is to address risks that are known or are foreseeable to an organization.
    - Use is to identify the assets of the organization, the impact of risks on those assets, enable the organization to define acceptable levels of risk, and protect assets against identified risks.

Who Performs Assessments and When Are They Performed?

- There are vendors that specialize in one or more of the assessments described above and can be retained to conduct these assessments.
- These vendors may also provide incident response services, investigate an incident, and address the vulnerabilities that enabled the incident.
- Taken together, vendors can be retained to, among other things:
    - Identify risks
    - Advise on how to improve existing security measures and implement new ones

- Detect cyber threats and breaches (actual or attempted)
- Respond to cyber threats and breaches
- Return operations to "normal"

What to Consider When Retaining a Vendor

- Cost (initial contract amount and potential subsequent charges).
- Nature of the assessment to be performed and its scope.
- Nature of the data that the attorney has:
    - Personal health information that might be protected under sectoral privacy laws like HIPAA.
    - Personally identifiable information that might be subject to privacy or cybersecurity laws like the CCPA and NY SHIELD Act.
- Policies and procedures that the vendor will follow, and technologies that the vendor will use, in performing the assessment. (This enables the attorney to discharge her duty to supervise under Rule 5.3.)
- The vendor's understanding of the attorney's ethical obligations and the vendor's agreement to conduct itself in accordance with those obligations.

Reasons to Have a Written Retainer Agreement

- Sets forth compliance with legal obligations (*e.g.*, if protected health information subject to HIPAA is involved).
- Creates a record of:
    - Scope of work to be performed.
    - Milestones, deliverables, and deadlines vendor agrees to meet.
    - Allocation of risk should the vendor fail to perform and/or third parties are adversely affected during the course of the vendor's performance.
    - Vendor's indemnification obligations for any damages or penalties imposed by reason of the vendor's performance or lack thereof.
    - Selection of the method for resolving any disputes that arise out of the agreement.
    - Selection of venue for any litigation arising out of the agreement.

Additional Provisions to Consider Including in a Retainer Agreement

- Reasonable notice of actual or threatened breach of data held by the vendor.
- Requirement that vendor obtain written confirmation before conducting any work beyond that specified in the scope of work section.
- Duration of the retention agreement.
- Requirement that vendor secure specific amount of insurance for the benefit of the organization in connection with the work to be performed under the agreement.
- Prohibition on vendor assigning work to be performed under the agreement to another entity unless agreed to in writing prior to the assignment.
- When applicable, an acknowledgement by the vendor that it has been retained for purposes of assisting counsel to provide legal advice and that attorney-client privilege will apply to any communications made for those purposes.
    - Two Types of Privilege
        - Attorney-Client Privileged Communication. Four elements of attorney-client communication:
            - contains confidential information;
            - between attorney and client;
            - with the intent that the information be kept confidential;
            - for the primary purpose of obtaining legal advice.
        - Attorney-Client Privilege is not automatic and each element can be challenged.
        - Privilege protects the communication and not the underlying facts.
        - Attorney Work Product Protection. An attorney's work product, which may include work product created by an attorney's agent, may not be discoverable if the product is:
            - A document or tangible thing;
            - that was prepared in anticipation of litigation or for trial;
            - by or for a party or its representative (including the party's attorney, consultant, surety, indemnitor, insurer or agent).
        - Protection is not automatic.

- When determining if protection applies, courts may examine the timing between the retainer agreement, work production creation, litigation holds, litigation and the assertion of privilege.

Recommendations

- Recommendations for increasing chances that communications and work product will be considered privileged and survive challenges

  - Purpose

    - To trigger privilege protection it should be counsel, preferably outside counsel, who retains the vendor as counsel's agent to "translate" the information about the client's system for "the purpose of rendering legal advice" to the client.

    - Include a statement of the purpose in the retainer agreement.

    - If in-house counsel retains the vendor, be mindful of in-house counsel's dual role as both business risk advisor and legal counsel.

  - Scope

    - Explicitly define the scope of vendor's work.

    - Consider tying the scope of work to anticipated litigation for work product protection or tying the scope to compliance with statutes, regulations, privacy laws, notification laws, or consent decrees for attorney-client protection.

    - Consider the time vendor is given to perform the work to mitigate the risk of a challenge that the vendor's work was not in anticipation of litigation.

  - Fee

    - Limit application of the fee to a specific task and do not allow the fee to shift to varying scopes of work that depend on the evolution of events.

    - For example, a retainer fee applied to a data breach in anticipation of litigation that shifts to risk assessment and training if a data breach does not occur will make the vendor's work vulnerable to a challenge on privilege.

  - Maintain Confidentiality

    - To maintain privilege, the vendor's work and vendor's communications with counsel must be kept confidential.

    - Counsel should direct the vendor's work assignments and control the communications between vendor and the client company.

    - Counsel and vendor should establish protocols for keeping information confidential.

- Investigation/Risk Assessment Reports

    - Report's purpose must be to assist attorney in providing legal advice and not merely relate information about client company's systems.

    - If the ultimate work product co-mingles legal advice with business risk, then it may be vulnerable to a challenge on privilege.

    - Consider drafting reports that point out potential legal issues and request legal advice, or creating two versions of the report: one that remains confidential for the purpose of giving legal advice and a second one that does not contain characterizations of facts and can be widely distributed in the client organization or made public.

- Investigation in Two Tracks

    - To maintain privilege and mitigate the risk against co-mingling legal counsel and business risk advice, consider running data breach investigations and post-breach activities on separate tracks.

    - Have outside counsel run a legal track that focuses on legal matters and litigation and in-house counsel manage the ordinary-course investigation, risk-related matters, and the day-to-day legal issues.

    - Keep the two tracks separate.

- Legal Advice

    - Counsel must provide client with legal advice for privilege to attach.

- Vet Public Statements

    - Ensure company's public statements about its data security system and/or the results of vendor's risk assessments do not waive privilege.

    - Ensure company's public statements do not misrepresent anything about its data security system.