KEY TAKEAWAYS

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

December 30, 2020

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

Seth H. Agata
Mark A. Berman
Alison Arden Besunder
Shoshanah V. Bewlay
Robert M. Brill
Patrick J. Burke
Ada Chan
John D. Cook
Bryan Daniels
Craig H. Effrain
Daniel H. Erskine
Hon. Fern A. Fisher
Parth N. Chowlera
Sarah E. Gold
Gail L. Gottehrer
Maura R. Grossman
Ronald J. Hedges
Shawndra G. Jones
James B. Kobak, Jr.
Glenn Lau-Kee
Kenneth A. Krajewski
Anthony C. Lam
Christian Levis
Erica L. Ludwick
Ronald C. Minkoff
David P. Miranda
Mauricio F. Paez
Alexander Paykin
Marian C. Rice
Kevin F. Ryan
Prof. Roy D. Simon
Enet Somers Dehaney
Sanford Strenger
Ronald P. Younkins

CYBERSECURITY THOUGHT LEADERS

Seth H. Agata
Christina Ayiotis
Mark A. Berman
Patrick J. Burke
Sasha Carbone
Nicole Cardascia
Gail L. Gottehrer
Ronald J. Hedges
David Horrigan
Laurie Kamaiko
Mary Kavaney
Aishwarya Minochia
Mauricio F. Paez
Fernando Pinguelo
Debbie Reynolds
Marc Roman
Elizabeth Roper
Jay Shapiro

SPECIAL THANKS TO

Dentons US LLP
Bryan Cooper
Molly Watson

TABLE OF CONTENTS

Page

Introduction from the Co-Chairs 1
Shadow IT 2
Business Email Compromise 7
Multifactor Authentication 13
Reevaluating BYOD (Bring Your Own Device) 19

INTRODUCTION FROM THE CO-CHAIRS

The practice of law has changed considerably since the Technology and the Legal Profession Committee issued our inaugural Cybersecurity Thought Leadership Conference report in February. As a result of the COVID-19 pandemic, lawyers have been required to work remotely, many for the first time, and to become proficient with technologies that were unfamiliar to them. Judicial proceedings, arbitrations, and client meetings moved from courtrooms and conference rooms to digital meeting platforms.

In addition to accelerating the adoption of technology by the bench and the bar, the pandemic created opportunities for cybercriminals to exploit the cyber vulnerabilities of law firms and their clients. Throughout the year, the Committee has issued Cyber Alerts to educate lawyers and law students about these threats and to raise awareness about the importance of cybersecurity and technological competence in the legal profession.

We held our Second Annual Cybersecurity Thought Leadership Conference virtually in October and are proud to share this Report on the Key Takeaways from that conference. The four topics we cover -- Shadow IT, Business Email Compromise, Multifactor Authentication, and BYOD -- have evolved and become increasingly significant for lawyers and law firms during the pandemic, given the shift to remote work and the technology-related changes that it has necessitated. In the Report, we introduce lawyers and law students to each of these topics, discuss how they apply to the remote and virtual practice of law, and provide practical guidance for law firms of all sizes.

The Committee thanks the Cybersecurity Thought Leaders, whose names are listed on the preceding page, for volunteering their time and expertise during this challenging year to create this Report. We also thank Dentons US LLP, including Bryan Cooper and Molly Watson, for hosting our virtual Cybersecurity Thought Leadership Conference and for their continued support of NYSBA and the Technology and the Legal Profession Committee.

Shadow IT

SUMMARY

So-called "Shadow IT" - information technology devices, software, and services used in the organization outside the ownership or control of the organization's IT department - has often been criticized by information security, governance, and management professionals as a tremendous risk. However, should law firms ban Shadow IT in the interest of data protection? Strictly banning Shadow IT practices will not prevent the use of Shadow IT, and some argue it may stifle innovation. Instead, we provide recommendations based on legal ethics, implications related to virtual workplaces, and some best practices to manage risks related to Shadow IT.

DEFINING SHADOW IT

The research analyst firm, Gartner, has defined shadow IT as "IT devices, software, and services outside the ownership or control of IT organizations."[1] The technology company, Cisco, provides a similar definition: "The use of IT-related hardware or software by a department or individual without the knowledge of the IT or security group within the organization. It can encompass cloud services, software, and hardware."[2] When an employee installs a cool new app on an organization's equipment without clearing it with the organization's information technology team -- perhaps to track a child's school progress or even to increase a team's productivity at the office -- that's shadow IT. While Shadow IT is inherently not owned or controlled by the organization, it can be managed.

Examples of Shadow IT may include:

- Thumb drives, jump drives, external hard drives
- Internet-based storage
- Communication platforms and social media apps (LinkedIn, Facebook, Twitter)
- Internet service provider mail (Gmail)
- Personal email accounts
- Text messages
- File transfer products
- Digital meeting platforms

BANNING SHADOW IT?

Gartner concedes, "Many IT leaders oppose shadow IT or business-led IT with good reason,"[3] noting that IT initiatives outside of the central IT function can increase risk. In an era of massive data breaches, hackers on the prowl, and increased regulation of data privacy and data protection, should organizations ban shadow IT? Gartner argues it should not, in part because banning shadow IT would stifle innovation, noting that only 50% of business-led IT is

---

[1] *See* Gartner, Inc. *It's Time to Give into Shadow IT*, March 6, 2020. https:// www.gartner.com/document /3913353
[2] *See* Cisco Systems, Inc. *What is Shadow IT?* last visited Nov. 8, 2020. https://www.cisco.com/c/en/us/ products/security/what-is-shadow-it.html
[3] Gartner, *supra* note 1, at 1.

innovative, while only 7% of the corporate IT budget goes to innovation.[4] Basically, Gartner argues innovation often happens outside of IT and that banning shadow IT would stifle innovation. Of course, lawyers, information technology professionals, and information governance teams should have a role in managing such innovation.

Nevertheless, we agree with Gartner that banning shadow IT is not a good idea. In addition to Gartner's innovation argument, there is also a practical consideration. Banning shadow IT will not prevent people from using unsanctioned IT resources. This reality is exacerbated by mandatory "work-from-home" as a result of the coronavirus pandemic. Relying on policies that ban Shadow IT could result in minimal supervision of these practices by the IT organization. Worse, having a ban through policy that is not uniformly enforced creates greater risks. Instead, the better approach is to manage Shadow IT by implementing policies, procedures, and organization-wide training.

KEY ISSUES RELATED TO COVID-19

The COVID-19 pandemic has created many challenges for organizations, not the least of which has been the almost instantaneous shift to a remote workforce with myriad end-user computing (EUC) issues. By its very nature, a remote workforce creates Shadow IT challenges. Unless an organization provides all remote hardware and software for remote staff and then locks the system down completely, there is going to be Shadow IT.

Lawyers and their organizations should avail themselves of software and workflow options designed for a remote workforce. Taking employee data privacy laws and regulations into consideration, organizations should develop an approach to better manage Shadow IT use, and monitor activity on their systems to address these risks. One could argue that, if the IT department manages it, it is not Shadow IT. However, the idea here is to develop systems and controls to limit possible nefarious attacks on the technology infrastructure and data, without stifling innovative IT ideas or wasting organizational resources on banning Shadow IT.

UNIQUE ISSUES RELATED TO *VAN BUREN V. UNITED STATES*

In its current term, the U.S. Supreme Court is considering *Van Buren v. United States*,[5] the Court's first review of the Computer Fraud and Abuse Act (CFAA) of 1986.[6] In *Van Buren*, the Supreme Court is considering whether a person violates the CFAA if that person is authorized to access a computer system, but uses that system for an improper purpose. The Supreme Court is being asked to resolve a 4-3 circuit split between U.S. circuit courts of appeals, and the Court's decision could have a profound effect on corporate information governance and Shadow IT.

In *Van Buren*, a police officer was authorized to access the Georgia Crime Information Center (GCIC) database, but exceeded that authority by running a license plate check for an acquaintance. The officer was convicted under CFAA and sentenced to prison, and the Eleventh

[4] *Id.*
[5] No. 19-783 (U.S. 2019).
[6] 18 U.S.C. § 1030.

U.S. Circuit Court of Appeals upheld his conviction. The officer - and amici such as the Electronic Frontier Foundation (EFF) - argue that the CFAA is a hacking statute with a legislative intent of prosecuting external hackers. However, the government argues the CFAA's clear and unambiguous language and legislative history indicate it was passed, at least in part, to stop insiders who "exceed authorized access."

The resolution of this 4-3 circuit split could affect Shadow IT because if the Supreme Court sides with the government, authorized employees who exceed their authorized access on a corporate system, e.g., employees using Shadow IT, could be prosecuted criminally. We recommend that lawyers and their information government teams monitor *Van Buren* and adjust their organizational computer and device use policies accordingly. Banning Shadow IT in the wake of *Van Buren* could have serious legal consequences.[7]

LEGAL ETHICS CONSIDERATIONS

Use of Shadow IT by lawyers and firm personnel also raise important legal ethical considerations under the American Bar Association (ABA) Model Rules and the NY Rules of Professional Conduct (RPC). For example, under the New York Rules of Professional Conduct:

- lawyers should provide competent representation, which includes determining the efficacy of appropriate technologies used in the practice of law (NY RPC 1.1);

- lawyers should conduct appropriate due diligence and understand the risk to competence and confidentiality when using such technologies (NY RPC 1.3);

- lawyers should ensure that such technologies have the appropriate and reasonable security functions and features to maintain client confidentiality (NY RPC 1.6); and

- lawyers who are partners, managers and supervising attorneys should make sure that subordinates (both lawyers and nonlawyers) are aware of these risks and that technologies used in the client representation comply with ethical rules (NY RPC 5.1 & 5.3).

The comments to the ABA Model Rules and NY RPC clarify these ethical obligations. For example, in 2012, the ABA amended Model Rule: Rule 1.1 Competence – Comment 8, Maintaining Competence, to add technological competence, explaining:

> *"To 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****…"*

[7] For an in-depth analysis of *Van Buren*, *See generally* David Horrigan, *Does Checking Sports Scores or TikTok on a Work Computer Violate Federal Law?*, THE RELATIVITY BLOG, May 26, 2020. https://www.relativity.com/blog/checking-sports-scores-tiktok-on-work-computer-violate-law/

Comment 8 to the NY Rules of Professional Conduct 1.1 also states:

> *"To maintain the requisite knowledge and skill, a lawyer should … (ii) keep abreast of the* ***benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information****."*

Lastly, the New York County Lawyers Association (NYCLA) Formal Op. 749 (2/21/17) observed that a lawyer has a duty of technological competence to the extent that technology is pertinent to a representation. Consequently, failure to manage Shadow IT creates a risk of ethical violations if the lawyer is not aware of how such technologies are used to perform legal services and does not discharge the duties of competence, confidentiality and supervision as required under the NY Rules of Professional Conduct.

BEST PRACTICES AND COUNSELING CONSIDERATIONS

The following are some key recommendations for organizations and legal practitioners:

- Shadow IT should not be banned. Instead, assess where Shadow IT creates ethical and compliance risks, and determine the best approach to manage the risk. Guide employees toward foundational tools, and support exceptions.

- COVID-induced EUC issues, such as remote work, require more active monitoring and assistance from IT teams. Develop and provide clear guidance on the use of personal IT tools in the provision of legal services.

- If the government prevails in *Van Buren v. United States*, organizations should consider revising their computer usage policies, including Shadow IT policies, to prevent potential legal liability for employees and others.

- Develop or revise IT and client confidentiality policies to include platform-specific guidelines, enforcement, and scope.

- Establish training programs to provide in-depth knowledge of systems, data handling, ethical rules, compliance, and adherence to client requirements (if any).

- Consider scope of practice, client base, and IT tools available, and right-size documented policies, procedures, and guidelines (there is no one-size-fits-all).

- Establish approach for managing client confidential information in non-controlled IT environments (storage, deletion, and access).

CONCLUSION

Lawyers, and the information technology professionals and information governance teams that support them, may be tempted to ban Shadow IT. Our recommendation is that such a move should take place only after thoughtful consideration of the repercussions. Not only would it potentially stifle innovation, but also it is a near impossible task that would divert, if not waste, limited organizational resources. Instead, organizations should develop best practices and policies for managing Shadow IT. In doing so, they should consider current events, such as the COVID-19 pandemic and the U.S. Supreme Court's consideration of *Van Buren v. United States.* In addition, lawyers should consider employee data privacy laws and regulations in any monitoring of Shadow IT, and comply with legal ethics. Best practices should include Shadow IT-specific policies where more general policies are insufficient, and the importance of training cannot be stressed enough. Policies, procedures, and best practices for Shadow IT can strike the right balance between employing a flexible and innovative technology adoption, while successfully managing risks.

Business Email Compromise

What is BEC?

Business Email Compromise (BEC) is a form of funds transfer fraud. It refers to a scheme in which the perpetrator impersonates (spoofs) the real owner of an email account to trick the recipient into forwarding money to an account under false pretenses. Its goal is to convince the recipient to direct payments of money to an account controlled by the perpetrator. Often, the fraud begins with an email or phone message purportedly from a client, vendor, or other entity who is expecting to receive funds, directing an unsuspecting employee of the entity holding the funds to wire money. Because the most common methodology for this scam is impersonation via email, it is generally referred to as Business Email Compromise, or BEC.

While this crime might seem simple to avoid, the FBI reported in April of 2019 that the losses attributed to BEC scams doubled in 2018, compared to 2017, and totaled $1.3 billion.[8] BECs are increasing in frequency, due in part to the increase in the remote practice of law during the COVID-19 pandemic, where more transactions are being conducted via email and less in-person verification is occurring. New employees and less tech-savvy practitioners at law firms are often targets of these types of scams. Lawyers must be vigilant to avoid becoming victims of such attacks and exposing their firms and/or clients to significant financial losses.

Background

- The legal industry is considered a soft target for BECs
    - Real estate firms are frequently targeted
        - Examples of scams include theft of down payments, and fraudulent requests for escrow fund disbursements
    - Law firms are businesses that have vendors they pay on a regular basis

- Law firms are generally considered not to be doing enough to protect themselves, which also makes them an attractive target

- No firm is too small to be hacked

[8] https://www.zdnet.com/article/bec-overtakes-ransomware-and-data-breaches-in-cyber-insurance-claims/

How Can a BEC be Perpetrated?

Once you know what to look for, BEC fraud can be identified and stopped. In most cases, the perpetrators send an email from either a trusted email account (by breaching that entity's network) or from an email account that looks almost identical to that trusted account (a "spoofed" account). The email will be timed to correspond with the deadline for a payment that is due to the purported sender, and will request that funds be transferred to a "new" bank account. The emails are usually well-written, sometimes even mimicking the writing style of the purported/spoofed sender. Sometimes there will also be a sense of urgency – "this deal won't happen if you don't wire the funds today" – to deter victims from trying to take the time to verify the legitimacy of the request.

BEC fraud typically involves the fraudsters gaining unauthorized access to a victim's email account or network in one of the following ways:

- Phishing: Email that contains malware a user can click on
- Vishing: Phone fraud convincing the employee to wire money or share credentials
- Smishing: A fraudulent text from a hacker trying to obtain credentials via text

As impersonation via email is the most common method of conducting these scams, the term BEC is used to refer to this type of funds transfer fraud, and we refer primarily to email scams.

What Does an Attack Look Like?

- The "bad actors" gain access to the network through one of the vectors described above; the victim doesn't realize they've been breached;

- A spoofed email account will look nearly identical to the victim's email account, but will usually use a false email address that is set up to look like a legitimate one by replacing one letter or number in the legitimate email address, e.g. replace a **"1"** with an "**l", or "l"** with an **"i" ,** or **m"** with **"rn,"** etc.

  The bad actors will sometimes breach the firm's network and monitor the communications/emails on that network to identify upcoming transactions and learn to imitate the writing styles of the parties. They may even use a pre-confirmed phone number for the requesting party to confirm legitimacy of transaction, so it is important for the recipient of a funds transfer request to actually speak to the person purportedly making the payment request (the client, party or vendor) to confirm the legitimacy of a payment request, particularly if it is for a large amount or a request out of the ordinary course (*e.g.*, a request to wire a payment to a new or different bank account).

- Other times, the bad actors will keep an eye on external social media and firm websites to identify those at the firm most likely to be involved in issuing payments, and to identify clients and vendors most likely to request funds to be paid or transferred to them.

- When a transaction (payment to a vendor, down payment on a home purchase, invoice for fees, etc.) is about to happen, the bad actors will swoop in and either send an email from within the network (from the victim's account) or create a spoofed account and send an email from that.

- The email will instruct the other party to the transaction to send a wire to an account controlled by the bad actors. Usually there is an explanation, like "we changed banks recently," and the writing style, signoff, etc. are similar to the way the breached victim would write.

- The other party to the transaction falls for the scheme and wires funds to an account controlled by the bad actors.

- Unless the fraud is detected immediately, and steps are taken to stop the bank transfer, the money is gone. Sometimes the funds can be recovered if the fraud is identified quickly and banking authorities are notified; notification within 24 hours is best, but more than 48 hours after the crime has been committed, the chances of recovering stolen funds drop dramatically.

BEC Fraudsters are Well Organized

The groups who perpetrate BEC fraud are highly organized and sophisticated. Even the most tech-savvy attorneys can fall victim to these schemes, as they are much more advanced than the old email fraud we are used to seeing.

- They research potential victims, and search social media such as LinkedIn or firm announcements for:
    - new hires, new deals
    - employees whose jobs at their firms or companies includes authorizing money transfers

- New staff are more vulnerable; they are less familiar with who should be contacted to confirm the legitimacy of a transaction or to recognize an inconsistency

- Bad actors will mimic the email style of staff

- Attacks can be opportunistic, and not specifically directed at your organization

- Hackers monitor a broad range of money movement, from escrow transfers to the payment of routine vendors, and these transactions can be manipulated to complete the criminal conduct.

Prevention Tactics: Nontechnical

Better cybersecurity for your practice and risk management to reduce the likelihood of a successful BEC can be accomplished through non-technical efforts. Cybersecurity should be at the forefront of your mind and that of everyone at the firm from staff to the managing partners. It needs to be a continuous effort. The importance of good cyber hygiene is messaged from the top down, practiced from the bottom up, and takes daily vigilance.

The following practices should be considered in these efforts:

- Training staff: this is not a one-off exercise and should be mandatory for all staff and lawyers with a special emphasis on new staff, those involved in money transfers, and those doing poorly on training exercises
    - Schedule phishing attacks on staff and track results
    - Schedule faux BEC tests on staff authorized to transfer funds

- Checks and balances: Put in Financial Controls
    - Dual approval for payments, especially large ones
    - Follow the principle of least privileges, *i.e*. who really needs to have the authority to authorize payments? Do the managing partners really need to have ability to transfer funds?
    - Get verbal instructions from a known contact for any payment directions for transactions that:
        - Are over pre-set amount, e.g. $1,000
        - Request a change of account/person to whom payment should be sent
        - Are to overseas accounts

- Do NOT use the same email or voicemail as was used to make the payment request. Try to speak to the known contact. There are BECs that involve a bad actor hacking into a voicemail system so that they can respond to voicemails (e.g. send an email in response to a voicemail verifying the transaction) to trick the victim into making payment.

- Roles and responsibilities: Segregation of duties
    - Create a policy in which more than one person is required to make payments, especially large ones, *i.e.*. one employee starts the wire process and another needs to complete the process in order for the funds to be transferred.

- Be suspicious if there is a change in the bank, or a move to an offshore account, or to a local bank but utilizing an international wire transfer service

- Be cautious if payment instructions have been changed and instructions have not been accompanied by verbal confirmation from the payee

- Insurance policies can be part of your tool kit, but carefully review what is covered
    - Check whether your crime or cyber insurance will reimburse you for such erroneous payments or if the loss comes from escrow and client funds
        - Ask your broker; don't assume
        - Coverage may vary between policies, and based on how the scam took place
        - Your cyber insurer may provide you with forensic investigation services to check if the bad actors got into your network and are lurking there

- Two-factor authentication

- Don't open unfamiliar email

- Double check the sender's email address to make sure it is correct

Prevention Tactics: Technical

- Anti-spam and email authentication software is available

- The Global Cyber Alliance (GCA) has a free cyber security toolkit that has 6 toolboxes that have an explainer video at the beginning of each toolkit explaining the business reason for implementing the tool. These tools can help protect businesses against scams like BEC and ransomware. The DMARC toolkit can prevent a lawyer's email from being spoofed or hijacked. DMARC can ensure that when you or your clients receive an email, you can have confidence it is from the actual sender.

    - GCA's cybersecurity toolkit for small businesses: https://www.globalcyberalliance.org/gca-updates-cybersecurity-toolkit-for-small-business/

- Use email authentication aka DMARC: https://www.globalcyberalliance.org/dmarc/

Effect of the Pandemic

- Personnel are isolated, which makes confirmation and communication more difficult
    - Greater reliance on emails that can be spoofed
    - Less personal contact with those who can confirm authenticity of a request

- Working on less secure systems
    - More use of personal, less protected, email accounts and devices

- Online threat has dramatically increased

After an Attack

- Call FinCen “Kill chain” - some wires can be stopped within 48 hours, but the sooner you take action the better the chance of recovering funds

- Call your insurance broker to determine if you have any potential insurance that may apply, who should be given notice of a potential claim, and if they can provide services to assist you

- Consider contacting the vendor who you thought you were sending money to so that they are aware there is a problem and someone is spoofing them

Plan Ahead

- Think about your controls to prevent a BEC attack NOW

- Identify what you would do if you were the victim of a BEC attack NOW

- Know the best practices and create response plans in advance

- Develop relationships with groups that can assist you in the event of a BEC, *i.e.* make contacts with law enforcement and solicit helpful guidance from them in advance

Multifactor Authentication

- Overview and Challenges

  - Multifactor authentication (MFA) is a security enhancement
    - It requires one factor (meaning evidence or verification information of your identity), such as a password, to be combined with other factors, such as a code texted to your phone, or biometrics, such as your fingerprint or retina scan to gain access to accounts or facilities.

  - MFA technologies are typically used by mainstream business or government organizations to secure user access to protected information resources.

  - Law firms may struggle with the adoption of MFA technologies due to complexity and lawyers viewing them as overly complicated or burdensome, even when firms need to use MFA to reduce business risk and/or comply with regulatory requirements.

  - **Practice Pointer**: Creating and maintaining the right tone at the top is the bedrock of a robust ethics, compliance, and/or security risk program. By defining and harmonizing governance at the leadership level, organizations can establish a tone at the top that binds their organization together.

- What is Multifactor Authentication?

  - Access credential factors generally fall into one of these three categories:
    - something you know (e.g., password/PIN)
    - something you have (e.g., smart card)
    - something you are (e.g., fingerprint)

  - **Practice Pointer**: Credentials must come from at least two different categories (i.e., sources) to enhance security; entering two different passwords doesn't qualify as multifactor, and won't provide the intended security benefit (namely, to reduce organizational risk by enforcing data security).

    - *Identity and Access Management*
      - Identity and access management is the basis for all security disciplines.
      - The purpose of access management is to *authenticate* and provide *accountability* for (1) *authorized* users to (2) access only the data appropriate to their role, while (3) preventing unauthorized users from obtaining access.

      - Typical threats mitigated by access controls include:
        - Providing unauthorized access;
        - Inappropriate modification of data; and
        - Loss of confidentiality.

- *Typical User Authentication Methods*
  - **Type 1 Authentication: Something You Know**
    - Requires testing user with a challenge and response, where the user must respond with knowledgeable answer.
    - Credential Set – a combination of both the identification (e.g., User ID) and authentication of user (e.g., via successful password validation).
    - Type 1 user authentication is based on something user knows (e.g., Password or PIN)

      - Passwords
        - Passwords are the traditional cornerstone for access to IT systems – cheap and easy to implement
        - Types of passwords to consider:
          - **Static Passwords**: reusable passwords that may or may not expire.
            - Note: a PIN (Personal Identification Number) is a number-based password.
          - **Passphrases**: long, static passwords comprised of words in a phrase or sentence (e.g., ThisIsA SecurePassword123)
          - **One-Time Passwords (OTP)**: may be used for a single authentication challenge.
          - **Dynamic Passwords**: passwords that change at regular intervals

      - Basic Password Risks
        - **Password Guessing** – an online technique where bad actors attempt to impersonate an authorized user.
        - **Password Cracking** – an offline technique in which attackers have gained access to stored password data and can attempt to derive the related password.

  - **Type 2 Authentication: Something You Have**
    - Requires that users possess something (e.g., token fob) which serves as, or provides, a challenge response to prove they are an authenticated user.
    - Tokens include car keys, credit cards, ATM cards, smartcards, and even paper documents.

      - **Synchronous Dynamic Token (SDT)** – time or counter-based token that is synchronized with the validating authenticator.

        - Time-based tokens display codes that change at a defined frequency (e.g., every 60 sec.).
        - The SDT code is only good during that window.
        - Examples include:
            - RSA SecurID fob (hardware SDT); or
            - Google Authenticator (software SDT).

    - **Asynchronous Dynamic Token (ADT)** – not synchronized with a central authentication server or authenticator.
        - Commonly used with challenge-response tokens.
        - A challenge (input) is produced which goes into the token device.
        - User manually inputs the challenge along w/his PIN, and the device produces output.

- **Type 3 Authentication: Something You Are**
    - Typically involves biometrics (literally, "life measurement").
        - Uses physical characteristics to identify or authenticate (prove an identity claim) (e.g., facial recognition, fingerprint scanner).
        - More difficult to forget, misplace, or lose control of biometric factors.
        - Biometrics may be used to provide robust authentication, but care should be given to accuracy and privacy issues.
        - Biometrics should be reliable and counterfeit resistant – data storage requirements are typically low.

    - ***Types of Biometric Controls***
        - <u>Fingerprints</u> – most widely used BC used today.
            - The data stored is a mathematical representation of fingerprint minutiae.
            - Minutiae contains information on fingerprint friction ridges (whorls, ridges, bifurcation, etc.).
        - <u>Retina Scan</u> – a laser scan of the capillaries that feed the retina of the back of the eye.
            - A light beam must enter thru the pupil after the user presses up to a laser scanner eyecup.
            - The laser scan maps the blood vessels of the retina
            - User health information can inadvertently be gained by retina scans, potentially leading to privacy concerns.
            - Exchange of bodily fluids between users is also possible due to the close proximity of the scanner to the user.

- Iris Scan – a passive BC.
    - A camera takes a picture of the iris (colored portion of the eye) and compares with the photos taken during user enrollment.
    - Works through contact lenses and glasses.
    - Every person's irises are unique (even between twins).
    - Benefits include:
        - High accuracy;
        - Passive scanning;
        - No exchange of bodily fluids.

- Hand Geometry – measurements are taken from specific points on user's hand
    - Includes length, width, thickness, and surface area.
    - Hand geometry devices are fairly simple and have minimal data storage requirements.

- Keyboard Dynamics – refers to how hard user presses each key, and the rhythm by which keys are pressed.
    - Cheap and effective.
    - Difficult to impersonate due to specific typing habits.

- Dynamic Signature – the process by which user signs their name.
    - Similar to keyboard dynamics.
    - Measures time, pressure, loops, and begin/end points.

- Voiceprint – measures user's tone of voice while stating a specific sentence or phrase.
    - Vulnerable to replay attacks, so it's recommended to augment voiceprint measurements with additional controls.
    - May falsely reject user if ill or voice is altered.

- Facial Scan – passively takes a picture of user's face and compares with photos taken during user enrollment.
    - Also called facial recognition.
    - Not frequently used in private organizations due to high cost.
    - Used by law enforcement and security agencies to improve security of high-value, publicly accessible targets.

- MFA Considerations

  - 23 NYCRR 500
    - The NYS Department of Financial Services oversees 3,900+ financial institutions (banks, insurance companies, etc.)

    - Section 500.12: Multi-Factor Authentication
      - 23 NYCRR 500 covers regulated entities and "Third Party Service Providers."
      - DFS security requirements specifically refer to MFA as an "effective control" to protect against unauthorized access:
        - 23 NYCRR 500.12(a): "Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems"

  - **Practice Pointer**: If your firm doesn't already have a remotely accessed digital workspace (VPN), consider getting one.
    - It should have multi-factor authentication, meaning that even if the wrong person gains control over an attorney or staff member's personal device, they cannot access the firm's digital workspace unless they also possess that second device.

  - **Practice Pointer**: Make sure attorneys and staff members know how to use the firm's remotely-access digital workspace. Double check with those who have not been accessing it regularly.
    - Verify that everyone has the accompanying multi-factor authentication app linked to the digital workspace properly installed on a smartphone or a second device.
    - Verify that all staff are adequately trained to use the implemented MFA technologies.

- The Future of MFA

  - Passwords are here for now, but when (or if) they are replaced, it will likely be with some sort of biometric authentication, such as fingerprint, iris, or face scanners, especially as they become more affordable and accurate.

  - Rather than relying on device-based authentication, organizations could consider using a centralized identity database, where identities can be securely documented, stored and authenticated.

- Universal 2FA systems ("U2F") is an open authorization standard that may become more widely used in the near future.
    - U2F enables Internet users to securely access any number of online services with one single security key instantly, with no drivers or client software needed.
        - FIDO2 ("Fast IDentity Online") is the latest generation of the U2F protocol.

Reevaluating BYOD (Bring Your Own Device) in a World Where Lawyers are Working Remotely

I. Factors to consider:

- The use of mobile devices in a BYOD setting amplifies the risks associated with remote work. These risks are compounded by the volume of electronic information created, transmitted, and stored at various locations and by the use of mobile devices by a larger number of professional and support staff working remotely.
- Risks associated with mobile devices are further increased by the use of multiple devices at the same time and the "merger" of devices as old ones are retired, new devices come online, and electronic information is transferred to or consolidated into a new device.
- The use of mobile devices by employees of public or private entities should, under appropriate circumstances, be subject to monitoring by employers to ensure that policies set by the employing entity are being implemented and followed.
    - Any such monitoring should, however, take into account various factors, including (by way of example only):
        - Whether, if the entity is public, the Fourth Amendment or its State equivalent might bar or limit monitoring.
        - Whether privacy laws, statutes or industry-specific regulations limit the ability to monitor employees or collect "their" information.
        - When the entity is asked to cooperate with government entities for purposes such as law enforcement and therefore acts as an agent of the government, or when the entity is served with legal process such as an order, subpoena, or search warrant, what the level of the entity's cooperation should be and whether any affected employee should be given notice.
        - Whether the entity's search of a device triggers the "private search doctrine," which may obviate the need for a later search warrant by the government.
        - Whether monitoring may be contrary to employee rights under the National Labor Relations Act, similar State laws or collective bargaining agreements.
        - Whether monitoring of a mobile device can be done in such a way so as to separate business-related from "personal" content if an employee has one device for personal use that has business-related apps, etc., loaded onto it -or a device supplied by the entity that is also used for private purposes.
        - Whether the ownership of the device is clearly established, an issue that arises when an employee is reimbursed by the employer for the cost of the device and/or for payment of the monthly service fees.
        - Whether an employer has notified the employee of their rights and responsibilities when using a personal device for business purposes.

II. General Corporate Policies

Rather than proceed *ad hoc*, public and private entities should have in place or develop policies that set parameters and rules for the use of mobile devices. The notice and distribution of these policies should be unequivocal and complete.

It is also critical to think about who should be involved in this process. Depending on your organization's size, it is important to obtain input from the relevant departments in your firm or organization, including IT, risk management, operations personnel, and in-house or outside counsel.

In crafting or updating policies for the use of personal devices, the following are some steps to take:

- First, review and assess existing corporate policies regarding the use of personal devices. Some or all of the following policies may be relevant:
    - Acceptable Use Policies
    - Data Retention Policies
    - Data Deletion Policies
    - Bring Your Own Device Policies
    - Confidentiality Policies

- Second, consider updating your corporate policies giving consideration to the following issues:
    - Can your organization support mobile device use by employees?
        - What firm resources exist to monitor and apply technical, administrative, and physical safeguards?
        - Understand the risk reduction that can be achieved by setting minimum hardware and software requirements.
    - What devices will employees be allowed to use?
    - What types of devices will be permitted and supported?
    - What types of company data will employees be able to access from each device type?
    - Account for retention periods for confidential and sensitive information that may be stored on personal devices and how that information should be stored
    - Address the extent to which the employer will access and/or monitor employee use of personal devices in mind all applicable restrictions and limitations
    - Address the required security measures, including password requirements, use of VPN, and other security measures

Consistent with all of the above, any policy for the use of mobile devices should include the following (this is not intended to be an exclusive list):

- The policy should clearly set forth the business purposes for which a device may be used.
- The policy should clearly set forth the entity's right to access a device to monitor compliance with the policy.
- The policy should specify when encryption might be used on a device and require any password or the like be provided to the entity, either when access is being requested or earlier.
- The policy should specify what security measures (for example, VPN) are required to use the device.
- The policy should be accessible, readable and useable by all employees in a format that can easily be referenced.
- The policy should include the contact information of an individual or department an employee can reach out to when questions arise.
- The policy should set forth how company data will be removed from the device if an employee is no longer employed at the company.

III. <u>Training</u>

Training is an essential component of any policy. Training is particularly important given the vast numbers of employees who are working remotely for the first time. In addition to lawyers, many staff members may never have had initial security training associated with remote work.

When developing and implementing training programs, an entity should consider at least the following:

- What is the role of the entity's governing body in developing, implementing, and monitoring the effectiveness of the training? Should the role be limited to an awareness of steps being taken to train?
- Who within the entity is given overall responsibility for developing, implementing, and monitoring the training's effectiveness?
- Which "constituencies" within the entity should participate in implementing and conducting the training?
- How should training be given to new employees, and should it be on an individual basis?
- How often should refresher training be given for employees?

IV. Security Measures

Security measures are essential tools for reducing risk, but there is no one size fits all set of security measures. The measures that are right for an organization depend on various factors, including size and resources. Measures to consider include:

- Use of VPN (Virtual Private Network)
- Virtual Desktop
- Strong Password Requirements
- Anti-virus Software Requirements
- Encryption of data on the device
- Periodic auditing and testing