PROGRAM MATERIALS
Program #30186
August 19, 2020

Work from Home Data Privacy and Security Basics

Celesq® AttorneysEd Center
www.celesq.com

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

Work From Home Cybersecurity Basics

August 19, 2020

CELESQ Attorneys ED Center

Joshua A. James
josh.james@bryancave.com

Bryan Cave Leighton Paisner LLP
1155 F Street, NW, Suite 700
Washington, D.C. 20004
(202) 508-6000

bclplaw.com

Work From Home Basics

- With the dramatic shift in how many companies work in 2020, understanding cybersecurity basics in the new work from home environment is critical.
- Why so?
  - Regulators expect it: The Federal Trade Commission ("FTC") has issued guidance on the shift to expanded working from home.
  - Customers expect it: Your customers won't be kinder in the event of a data breach just because your team is working from home.
  - Business partners expect it: Your business partners will expect you to continue operations as close as possible to business as usual because that's what they're doing.

Work From Home Basics

- Who should be concerned about cybersecurity basics in the new work from home environment?
  - Businesses including in-house and outside counsel advising them
    - As noted, a business's regulators, customers and business partners will be watching.
  - Law firms
    - Clients will expect assistance in addressing these issues
    - Law firms are also navigating these issues

WFH: Addressing Regulator Guidance

The FTC is the primary federal enforcer of data privacy and security laws. It derives this authority from Section 5 of the Federal Trade Commission Act. 15 U.S.C. § 45(a).

Section 5:

- Prohibits unfair or deceptive trade practices
- Premised on one of two theories:
  - Business lied about or misrepresented its privacy/security practices resulting in harm to consumers (deception) (privacy typically)
  - Business engaged in a practice that harmed consumers even if they knew about the practice or the business did not misrepresent the practice (unfairness) (data security typically)

WFH: Addressing Regulator Guidance

Given this warrant, the FTC took it upon itself to issue guidance to businesses on working from home in March 2020:

www.consumer.ftc.gov/blog/2020/03/online-security-tips-working-home

This guidance, and related statements from the FTC and other regulators, set a baseline for addressing work from home issues.

One of the last things you want to hear from a regulator is, “We told you so…”

WFH: Addressing Regulator Guidance

- Pay special attention to **your** regulator's guidance.
- If you have a primary regulator and they put out guidance on work from home issues, you should make an effort to follow their lead.
- If you do not have an entity you consider to be your primary regulator, take a cue from the FTC's guidance since it is a default regulator for most US-based businesses.

WFH: Addressing Regulator Guidance

- Take steps to show that you are aware of the risks identified by your regulator and are taking steps to mitigate them.
- Keep in mind that perfection isn't expected, instead what is expected is taking reasonable precautions under the circumstances.
- By taking basic steps to address the new WFH security and privacy realities, you give yourself a leg up in defending something does occur.

WFH: Addressing Regulator Guidance

- Talk with your security and privacy teams.
  - This will be repeated advice: your internal technical team is one of your best resources for addressing these issues.
- You technical team knows what new points of friction have sprung up since your workforce started working from home.
- Develop a plan of action with that team to address the new issues that they face.

WFH: Addressing Regulator Guidance

- **Stay alert.** Many regulators and law enforcement agencies have noted new Covid-19 related scams and threats.
- Be aware of those issues and alert your employees to them.
- This goes back to the “We told you so” problem; if there are alerts on a scam your employees fall for it after the alerts are provided by regulators, then the regulator or plaintiffs’ attorney is very likely to focus on a lack of diligence when they knock on the door.

WFH Cybersecurity Basics: Wireless Network Security

- A major weakness in any WFH system is that individual employees often fail to take necessary steps in securing their home network. Each non-secure home network increases a company's risk of a data breach.
- Employers would do well set up a training to explain how safeguards can be implemented and establish a timetable for employees to put the safeguards into place.
- IT teams should be prepared to field questions that employees have about securing their networks.
- https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network

WFH Cybersecurity Basics: Wireless Network Security

- Encrypt information sent over wireless networks using WPA2/WPA3.
  - Most wireless routers come with the encryption feature turned off, it can be turned on by going to the router's settings or checking the company's website.
- Only allow specific devices to access wireless networks.
  - Wireless routers typically allow a user to specify what MAC addresses have access to the network.
  - An employee with many guests can use a separate guest network that is open to all devices but still protected with encryption requiring a password to access it.

WFH Cybersecurity Basics: Wireless Network Security

- Secure routers by changing defaults. Employees should take the following steps:
  - Change the router's default network names to something unique.
  - Don't broadcast the network names. Employees know them and can share them with guests and within their family as appropriate.
  - Change the router's default password. Hackers know most default administrator passwords, so change it. Employees should also change any default "user" passwords.
  - Turn off "Remote Management" features that allow remote access to a router's controls. Hackers can use this to get into the network.
  - Log out administrators. After changes are made, log out.

WFH Cybersecurity Basics: Wireless Network Security

- Update the router's software.
  - Routers, like computers, need to be updated on occasion.
  - Periodically check the router manufacturer's website to see if there is a new version of the router's software available for download.
- Protect the network during mobile access.
  - Create strong passwords for mobile devices and mobile applications that can access the wireless network.
  - Only allow trusted mobile devices on to the main Wifi network.

WFH Cybersecurity Basics: Phishing

- Phishing is both common and effective, as it often targets individuals by sending a message that appears to be from a well-known source (i.e. a friend, colleague, or familiar business), looks legitimate (utilizing spoofed logos and fake email addresses), and may claim to be urgent.
- Remote workforces are even more vulnerable to phishing because employees are dispersed and have fewer lines of direct communication through which they can confirm unanticipated or suspicious messages.
- In anticipation of this increased threat, employers managing a remote workforce should implement additional policies and trainings that focus on identifying, combating, and responding to a phishing attack when working from home.
- Among other things, employers should consider the advice from the FTC:
  - https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/phishing;
  - https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/phishing-scams;
  - https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

WFH Cybersecurity Basics: Phishing

How to Identify a Phishing Scheme

- Train employees to look up hyperlinks and phone numbers before they click or call. Employees should always try to make sure that they are not about to download malware or talk to a scammer.
- Make it standard procedure to send any unusual email to IT before responding or clicking. If the company does not have an IT team, designate a contact that can screen emails when needed. Employers and employees should understand that it is better to be cautious than to provide a quick response.
- Explain to employees that, in the event they receive an unanticipated message from someone they know requesting information, they should first use pre-existing contact information to confirm the message's authenticity.

WFH Cybersecurity Basics: Phishing

How to Combat Phishing Schemes:

- Phishing attacks can lead to ransomware attacks leveraging compromised credentials, so regularly back up company data so that it can be restored in the event a phishing attack leads to a ransomware incident.
- Keep all security software up to date by installing the latest patches and updates. Consider investing in email authentication and intrusion prevention software.
- Train employees! The more employees know, the more likely they are to recognize a phishing scheme. Employers should collect and share examples of phishing attempts to increase awareness of what an attack may look like.
- Phishing attacks often happen to more than one person in a company. Supervisors who are made aware of a phishing attempt should warn other employees to watch out for a similar message.

WFH Cybersecurity Basics: Phishing

What to do if an employee falls for a phishing scheme:

- Instruct employees to immediately inform their supervisor if they suspect they have been phished.
- Change any compromised passwords and disconnect from any network any device that may have been infected with malware.
- If the phishing resulted in exposed email credentials, check for “rules” that may have been set up by the threat actor (*e.g.*, auto-forwarding, or auto-filing rules).
- Engage the incident response protocol.

WFH Cybersecurity Basics: Malware

Bad actors use malware to corrupt devices, monitor activity, and steal personal information.

While most companies have security procedures and technology in place to prevent malware from infecting devices, employees who work from home are often exiting this safety net.

As a result, the risk of malware attacks, and the resulting security breaches, increases. With more employees working from home, employers should train employees on: (1) ways to avoid malware, (2) how to recognize malware after it has been installed, and (3) what to do if an employee thinks their device is compromised.

The FTC in its advice regarding malware provides the following tips: https://www.consumer.ftc.gov/articles/0011-malware

WFH Cybersecurity Basics: Malware

- Security software. Enable automatic updates to device security software, internet browser, and operating system. Software updates often include patches that address security vulnerabilities. Also, install updates as soon as practicable—the icon indicating that updates are waiting for installation will do nothing to stop malware that exploits unpatched systems.
- Browser security warnings. Pay attention to browser security warnings. Employees should not visit webpages flagged by a browser as suspicious without checking with the company IT team or taking other steps to mitigate risk associated with visiting the site.
- Beware of attachments. Employees should not to open attachments in emails unless they know the sender, recognize the subject matter, and are expecting to receive an attachment. Review the sender's email address to confirm it is legitimate as many threat actors will mimic a legitimate user's email. However, email address alone is not proof, as the sender's account could have been compromised. When in doubt, a phone call to check whether the sender sent the email is the best way to check an attachment.

WFH Cybersecurity Basics: Malware

- Beware of popups. Employees should avoid clicking on popups or banner ads.
- Beware of links. Employees should avoid clicking on links in emails, even emails that appear to come from trusted sources like banks or email providers. Instead, employees should open a new browser window and visit the site in the manner they normally use, *e.g.*, selecting a "favorite" button or typing in the address, rather than clicking on a link sent to them in email. This will defeat many common phishing attacks.
- Be careful when installing new software. Only download known software directly from the source. If an employee wants to download new or questionable software, require them to run it by the IT team first.
- Talk about safe computing with other device users. Encourage employees to talk about digital security with family members who might have access to the employee's devices. (More on this later.)

WFH Cybersecurity Basics: Malware

- Employers should also train employees on how to detect malware. While this includes watching for the traditional computer slow-downs, inappropriate ads, and pop-ups, the following are also indicators of malware:
  - New and unexpected toolbars or icons in your browser or on your desktop.
  - Unexpected changes in your browser, like using a new default search engine or displaying new tabs you didn't open.
  - A sudden or repeated change in your computer's internet home page.
  - A laptop battery that drains more quickly than it should.
- Employees should immediately notify their managers and IT if the employee suspects malware has been installed on their computer. The company should follow the protocols outlined in its incident response plan to appropriately investigate and respond to an attack.

WFH Cybersecurity Basics: Laptop Security

With employees carrying their laptops home from work, now is a good time to remind them of some common sense steps to keep laptops safe and secure while out of the office.

- Passwords. Make sure each laptop is secured with a user account that requires a strong password to access it.
  - Additionally, make sure the laptop's user account only has limited privileges and that an IT-only administrator account is also secured with a complex password.
- Locked. Laptops have a habit of walking away if not securely locked down, or up.
  - A best practice for any laptop is to secure it with a sturdy laptop lock to the desk it is kept on.
  - Failing that, locking a laptop in a sturdy desk drawer or other secured cabinet also works. If no lock is available, hiding the laptop provides a lesser measure of protection.

WFH Cybersecurity Basics: Laptop Security

- Encryption. Depending on the device, laptops may support full disk encryption.
  - If it is available, full disk encryption provides powerful protection for data stored on laptops provided that the password securing the device is a strong, complex password.
- Location tracking. Some laptops and operating systems support location tracking in case the device is lost or stolen.
  - Notify employees of this capability and its use, as this tool can provide a measure of comfort in times where more systems are out of the building.
- Unattended devices. The FTC in its advice to businesses on WFH security noted that employees should not leave their laptops unattended in public places.
  - For the time being, caution employees against going to public places to do work. If they must travel, remind employees to keep a close eye on their laptops at all times.

WFH Cybersecurity Basics: Handling Sensitive Electronic Data

If your business regularly handles sensitive electronic data in the office, chances are that employees working from home now have to continue handling sensitive data outside the safety of your office network. This poses many challenges but, with some forethought, many businesses will likely find that they can continue most operations without sacrificing security.

- Encryption in transit. At a minimum, your team should avoid sending sensitive information via email. Email traffic can be intercepted in transit. Additionally, cloud-based email services like Gmail or Outlook365 are frequent targets of credential stealing attacks.
- Secure File Transfers. Since you are minimizing the transmission of sensitive information over email, you should discuss with your IT team what tool your company should use for secure file sharing.
  - Things to look for: robust privacy and security representations in the contract for the product, easy setup and simple training (a difficult app will not be used), and a simple mechanism for removing information from the app once it is no longer needed.

WFH Cybersecurity Basics: Handling Sensitive Electronic Data

- Encryption at rest. Ideally, all devices that handle sensitive information for your business will be fully encrypted.
  - Realistically, many businesses end up able to encrypt only a segment of their systems because of resource constraints. Prioritize encrypting those systems that handle large amounts of sensitive data, *e.g.*, human resources, financial/accounting systems, payment processing systems.
- Version control. Some sensitive electronic documents may need to be worked on by a team of individuals.
  - In those cases, you will want to ensure that an appropriate version control system is in place or a procedure has been agreed on to avoid employees duplicating work or ending up with disparate versions of a critical document.

WFH Cybersecurity Basics: Handling Sensitive Electronic Data

- Minimizing data handling. Keep in mind that it may be a good idea to cut down on handling sensitive data for a period of time. Some tasks that require working with large quantities of sensitive data may be best delayed until the employee is able to access a secure area in the future.

WFH Cybersecurity Basics: Handling Sensitive Hardcopy Data

Handling sensitive electronic data in a WFH environment poses some challenges, but even more challenging is how to deal with sensitive hardcopy data in homes that aren't meant to handle sensitive data.

- Consider the files. Before allowing employees to take home sensitive hardcopy data, ask yourself a few questions:
  - Is this a file that the business can live without?
    - While your company and employees will take steps to avoid losing the file, the reality is that once the file leaves the office, the chances of it being lost, destroyed, or stolen go up. The company should carefully balance the needs of the business against the risk of harm the loss of the file might cause.
  - Why is the information sensitive?
    - Considering this will help a company better assess whether certain files should be taken home and what risks may be associated with the file leaving the office.
    - For example, if the file is sensitive because it contains sensitive personal information, the risks related to the loss of the data are higher than the risk of destruction (presumably the data could be recreated from the subjects of the file).

WFH Cybersecurity Basics: Handling Sensitive Hardcopy Data

- Transportation. Some employees that require sensitive data may use public transport. I
  - f your company allows those employees to take sensitive files home with them, it may be worthwhile to pay for a taxi or rideshare to assist the employee in traveling to and from the office with the sensitive files in a quick and relatively lower risk manner.
  - Also, caution employees that drive not to stop on the way home with the sensitive files in their vehicles. A briefcase or backpack might get stolen if the employee's vehicle is left unattended for a period of time.
- In-home security. Employees need to realistically assess how securely they can store files at home.
  - Does the employee live with multiple individuals?
  - Does the employee have a locked or otherwise secured area to keep files when not in use?
  - Are the files of a type that might hurt the company if they were destroyed? Those types of files may not be a good fit at home for an employee with several young children and no place to store the files.

WFH Cybersecurity Basics: Handling Sensitive Hardcopy Data

- Minimizing data handling. Keep in mind that it may be a good idea to cut down on handling sensitive data for a period of time. Some tasks that require working with large quantities of sensitive data may be best delayed until the employee is able to access a secure area in the future.

WFH Cybersecurity Basics: How to Securely Destroy Sensitive Data and Files

Every company should develop an internal data destruction policy that accounts for information destruction both in the office and at home. When considering at-home data destruction options, companies should consider:

- Physical Files.
  - Purchase home shredders for each employee. This may be a good option if employees regularly handle papers containing sensitive personal data or other sensitive information.
  - Enlist the services of a third party shredding company who can pick up paper files from an employee's home. This may be a good option if you have employees who regularly handle high volumes of papers containing personal data or sensitive information.
  - Establish a "no-print" policy, prohibiting employees from printing at home or taking physical documents to their home. This may be a good option if your employees don't need access to physical documents.

WFH Cybersecurity Basics: How to Securely Destroy Sensitive Data and Files

- Digital Files.
  - Create a home computer data deletion schedule applicable to all employees who use their personal computer for work.
  - The Department of Homeland Security suggests using either a secure erase command or a disk wipe to permanently erase sensitive information from computers and flash drives.
  - Periodically assist employees in overwriting sensitive company information. The Department of Homeland Security suggests overwriting data using cipher.exe or clearing.
- Additional guidance on securely deleting files can be found at

  https://www.us-cert.gov/sites/default/files/publications/DisposeDevicesSafely.pdf, https://www.us-cert.gov/ncas/tips/ST18-005, and https://www.us-cert.gov/ncas/tips/ST18-005

WFH Cybersecurity Basics: Sharing Devices With Family

Working from home blurs the lines between work and play, both physically and technically.

- Devices that were previously reserved for work-related excel spreadsheets and drafting corporate documents may now double as education platforms and entertainment centers as family members hop onto a computer to complete classes, play games, or connect through social networks.
- When family members have access to an employee's work computer, the employee no longer has full control over what is uploaded and downloaded from the device. This can ultimately make the company more vulnerable to security incidents.

WFH Cybersecurity Basics: Sharing Devices With Family

The FTC in its advice regarding kids and computer security provides the following tips (many of which can be used for all individuals sharing a computer, regardless of age):

https://www.consumer.ftc.gov/articles/0017-kids-and-computer-security

- Have a family discussion about computer security. Among other things, employees should discuss:
  - Downloads. Kids should never download anything without parental permission. This applies to games, photographs, movies, music, etc. Show your kids what different types of download buttons look like (*e.g.,* "Download Here" or "Click to access your free game!"). Before an adult downloads anything to the device, check the privacy policy and terms of use to figure out what information the download will have access to.

WFH Cybersecurity Basics: Sharing Devices With Family

- "Talking to strangers." Phishing attempts are all too common and may arise in the form of questions from strange people or contacts requesting personal information. These requests can come through email, instant messaging, pop-up messages, or text messages. Especially with regards to phishing attempts, look for "teachable moments." If you receive a phishing message, or see a scam, show it to your family members and explain how you recognized it as a scam.
- Passwords. Help family members create complex passwords that they can easily remember. Memory-tools such as songs or stories allow people to remember long passwords through association. Remind them not to use the same password for more than one account.

WFH Cybersecurity Basics: Sharing Devices With Family

- Secure the computer:
  - Parental Controls. Turn on parental controls to block outgoing content and filter out websites that frequently drop malicious tools. For more information about parental controls, see the FTC's guidance on parental controls: https://www.consumer.ftc.gov/articles/0029-parental-controls
  - Anti-malware Protection. Download and install anti-malware protection software. Any time a user opens a file they've downloaded, the software will scan it and make sure the file is safe.
  - Passwords. Activate settings that require a password before any software or application can be downloaded and do not provide your children with the password. Check the privacy policy and your privacy settings to see what information the app or software can access before going through with a download.
- Separate User Accounts. Create separate accounts for each family member that uses a shared computer. The accounts of other family members should be separate from your work account. You should only conduct work through your work account. Both work and family accounts should be password protected.
  - Only one administrator account should have full privileges; all other accounts should have limited permission and should only be able to access the user's own files (not files associated with other accounts).

WFH Cybersecurity Basics: Following Company Practices

As the FTC stated in its initial guidance on employees working from home:

"Follow your employer's security practices. Your home is now an extension of your office. So, follow the protocols that your employer has implemented."

- Share Company Policies. If employees don't know the company's policies, the employees cannot follow them.
  - If you are in charge of managing WFH data privacy and security issues, it is a good idea to push policies to employees on a periodic basis and after any major changes to the policies.
  - Placing links to the policies in your email signature is also a good way to help employees find the guidance they need when they need it.
  - Prepare a one-stop-shop online for employees to access company policies.

WFH Cybersecurity Basics: Following Company Practices

- Implement the Policies. Companies should make it easy for employees to follow the WFH policies.
  - Provide links to any software an employee may need.
  - Employees told to access certain applications may not be able to find the app if a link is not provided. More troubling, if the app is a popular WFH solution, employees may stumble on to imposter apps hiding malware or other nasty software if the employees are left to fend for themselves in locating the app.
  - Provide links to troubleshooting materials so that employees can try to address problems they may encounter on their own, before contacting company personnel. Many employees are quite capable of addressing minor technical issues themselves, if provided with the right tools.

WFH Cybersecurity Basics: Following Company Practices

- Assist Employees. Even with extensive tutorials and lengthy Q&As, some employees will still find that they need help implementing certain practices.
  - To that end, companies need to prepare for surges in technical questions that follow the roll out of any new WFH policies or procedures.
  - This means adding resources at peak times to ensure that employee questions are answered in a timely manner so that bottlenecks are avoided.

WFH Cybersecurity Basics: General Tips from the FTC

- The FTC, beyond just providing guidance on some common threat types, has also provided a very basic outline for security issues in other contexts:
  www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/basics
- These tips from the FTC can also be thought of a minimum necessary protections. If something happens that could have been prevented by following this advice, the FTC will get to use 4 magic words . . .

  “I told you so.”

WFH Cybersecurity Basics: General Tips from the FTC

- **Updating software.** The FTC mentioned updating browsers, apps, and your computer's operating system. The FTC also suggested making updates automatic.
- **Securing files.** This means backing up important files on external hard drives and cloud storage systems and securing any paper files at home.
- **Requiring passwords.** The FTC suggests requiring passwords to log into laptops, phones, and tablets and making sure not to leave those devices unattended in public places.

WFH Cybersecurity Basics: General Tips from the FTC

- **Encrypting devices.** To the FTC, this means encrypting any device with sensitive personal information such as laptops, removable storage, removable media (DVDs), backup tapes, and cloud storage.
- **Using multifactor authentication.** The FTC would prefer that businesses use multifactor authentication to access any systems that store sensitive information. This means requiring something more than a username and password to access the system, *e.g.*, a second factor like a token or push notification.

WFH Cybersecurity Basics: General Tips from the FTC

- In practice, some of this advice is difficult to implement under the best of circumstances (setting up encryption on devices is, typically, a major project for a moderately sized-business).
- To the extent that your company can implement the FTC's guidance with a reasonable amount of effort, it should.
- However, to the extent that your company does not have the resources, be it money, IT employees' time, etc., you should document your company's assessment of the advice, note the places where resource constraints prevent you from taking the FTC's advice, and then document a compensating control that you might be able to implement in its place.

WFH Cybersecurity Basics: General Tips from the FTC

- Adopting a compensating control following a thorough assessment and explanation will help a company avoid the “I told you so” moment by explaining, before the incident, why the company could not comply with the guidance.
- The key is a thorough analysis prior to an incident occurring.

WFH Cybersecurity Basics: General Tips from the FTC (Example)

- Perhaps your employees handle highly sensitive information on a regular basis.
- While encryption is a very good idea for their devices, your company has not yet implemented full disk laptop encryption.
- In this instance, try to find another sensible process to help secure the sensitive information.
- For example, create a policy where employees must securely save their sensitive files, such as in an encrypted cloud solution, at the end of each day and then securely delete the files from their laptop.

WFH Cybersecurity Basics: Incident Response Planning

As employees work from home, many of the protections that typically secure access points disappear. As a result, every company with a remote workforce faces an increased risk of security incidents and should be prepared to respond appropriately.

Incident response planning is an essential part of any company's cybersecurity plan, and is even more important when employees are dispersed among different networks, locations, and devices.

WFH Cybersecurity Basics: Incident Response Planning

When drafting or reivisng an incident response plan for the WFH environment, companies should, among other things:

- Incorporate legal counsel to ensure any investigation is conducted under attorney-client privilege.
- Create protocols and systems that allow IT to safely remote into an infected device.
- Provide incident reporting procedures, including a clear plan for escalating information about an incident.
- Designate members of the company's incident response team whose assistance would be required to respond to a data security incident (*e.g.*, IS, Legal, CFO, COO, IT, Communications, etc.) and include both work and personal contact information for primary and secondary team members.

WFH Cybersecurity Basics: Incident Response Planning

- Include references to any laws that require notification to a regulator within a short timeframe (*e.g.*, 72 hours under GDPR, NYDFS, etc.).
- Discuss the need for preserving evidence. This should prohibit employees from wiping their drives or destroying physical evidence in the event of an incident unless otherwise instructed by an investigation lead.
- Include contact information for pre-approved external resources whom you might call upon to assist in a breach (*e.g.*, breach counsel, forensic investigator, cyber insurance carrier, etc.).
- Outline a plan for keeping records of the investigation and identifying the need to minimize written communications about the incident.
- Require a post-incident meeting to debrief with the incident response team concerning what went well with the investigation and what did not.

WFH Cybersecurity Basics: Business Preparedness

As just mentioned in the slides on incident response planning, companies now need to be prepared to address security incidents in a work from home environment. But, companies also need to be prepared to address security concerns even before an incident requiring the IRP occurs. To address that need, here are some topics to discuss with your technology/security team:

- Patching. Within the office, patching devices connected to the local network can be accomplished relatively easily. With everyone dispersed, IT team may need to think creatively to get critical patches distributed to employee devices.
- Updating Procedures. IT personnel know what works and what does not work within your company's information systems. At this point, they also know how working from home has affected systems and procedures, and they likely have a plan to address these changes. Companies should talk with their IT teams about how best to update their policies to address the current environment.

WFH Cybersecurity Basics: Business Preparedness

- IT Support for Employees. After rolling out new patches or updating IT policies, the next phase is to ensure that IT personnel are available to help employees implement the policies or troubleshoot the patches installed. This means increasing IT employee coverage immediately after changes or patches are rolled out since so many employees are dealing with these issues for the first time on a work from home basis.
- WFH Compliance Trainings. Many companies privacy and security focused compliance trainings each year to keep their employees sharp on the privacy and security aspects of their work. After the initial frenzy to adapt to working from home, many folks in compliance positions are left trying to complete yearly privacy and security trainings. Look for attorneys who can provide data privacy and security trainings remotely including tabletop exercises, introductory trainings, and training of focused topics.

WFH Cybersecurity Basics: Videoconferencing Security

On April 16, the FTC issued guidance on the use of videoconferencing in response to very public privacy and security issues related to the surge in videoconference use: https://www.ftc.gov/news-events/blogs/business-blog/2020/04/video-conferencing-10-privacy-tips-your-business

Companies are now, arguably, on notice of what the FTC expects from them with regard to videoconferencing. Here are the most salient points from that FTC guidance:

- Lockdown Who Can Attend. Each videoconferencing software comes with its own suite of tools to prevent unwanted guests. Your team should be familiar with these tools and should use them to ensure that only invited guests join your videoconferences. Ideally, companies should select a videoconference solution and then push out policies and procedures to employees so that everyone understands how to use the chosen solution securely and safely.

WFH Cybersecurity Basics: Videoconferencing Security

- Be Aware of the Video. Make sure employees understand what's expected of them on videoconferences. Everyone has seen at least one funny meme of someone doing inappropriate things on a video conference without realizing they are on camera, much to the subject's embarrassment. To avoid those issues, remind employees when conferences are using video. A quick reminder at the top of a call can help avoid embarrassing issues.
- Plan for Recordings. Determine whether recording of videoconference is something that your company needs. If so, how extensively is it needed? Have a policy on the use of recordings and let your employees know what that policy is. Always let participants know at the beginning of the videoconference if it is being recorded so as to not run afoul of laws requiring all-party consent.

WFH Cybersecurity Basics: Videoconferencing Security

- Know the Software's Privacy Policy. Whatever software you choose to use, you should be familiar with its privacy policy, and you should make certain that its privacy practices are compatible with your company's purposes, including whether any of the data related to your call will be utilized by the company for its own purposes or shared with third parties. If you don't know what information the software is collecting, you shouldn't be using it for any conferences that involve sensitive information.
- Update the Software. As with any software, you should always keep your software patched and fully up to date. Having the latest version of the software helps to ensure that your team can take advantage of any changes made by the developer in response to user feedback on safety and security.
- Develop a Robust Videoconferencing Policy. All of the foregoing should feed into a robust policy concerning videoconferencing. Such a policy should address both the technical and non-technical items discussed above and should be shared with employees as the policy develops over time.

WFH Cybersecurity Basics: Risk Assessments

Nearly all companies should be performing data privacy and security risk assessments.

Whether your company conducts a risk assessment because it is mandated by law or because your company recognizes the value of conducting such assessments even if not legally required to do so, now is an important time to reassess your risk profile with your work force moving to a WFH environment.

With the shift to an expanded work from home environment, your company's risk surface has radically changed. That change in circumstances necessitates a change in your risk assessment to assist your IT and response teams with reprioritizing their efforts to keep your company's data safe.

WFH Cybersecurity Basics: Risk Assessments

Here are some important things to keep in mind during the risk assessment process:

- Devices no longer completely controlled and on secured network. With your company's devices no longer primarily interacting with the wider world through your company network, your IT team will need to evaluate whether their security process remain adequate for the challenges faced.
- Malware becomes a greater threat. Since your devices are no longer behind your company's firewalls and you're no longer able to be certain of the patching of the employee's devices, malware becomes a much larger threat for your organization. To that end, your team should work to determine what antimalware solutions it trusts to protect employee device. Your IT team should also have a plan for helping employees install and update the software.

WFH Cybersecurity Basics: Risk Assessments

- Ransomware lesser threat (possibly). With more limited access to your company's network, the risk of a ransomware attack may be lessened. Instead, the ransomware risk may primarily sit on your employee's personal computers. Alternatively, if your company has taken steps to make it easier to access company resources remotely, your systems' risk of a ransomware infection may have increased. The important point is to reassess your risk under the changed circumstances and to develop a plan with your technical teams to address that shift in risk spectrum.
- Phishing, different threat profile. With employees now working from home, there are new types of phishing threats to consider. Has your business applied for loans or other government assistance? If so, your employees need to be on the lookout for government imposter scams seeking to take advantage of businesses seeking help. Is your company in healthcare? Then employees should be on the lookout for scams targeting healthcare companies responding to Covid-19 needs.
- Talk with IT to determine what threats have become more or less dangerous. Discuss the shift in threats with your security and privacy teams to ensure that your processes and policies match up with the current risks that your business faces. Working through these issues, and others, is a good way to ensure that you catch threats before they impact your business. It's also an effective way to show regulators that your company was working diligently to address new issues. That way, if you have a breach, your company is in a better position to demonstrate to regulators that your company was taking reasonable and appropriate steps to identify threats before they resulted in harm to your company or consumers.

bclplaw.com