CARLTON FIELDS

COVID-19 and Cybersecurity: Best Practices in an Uncertain Landscape

CYBERSECURITY AND PRIVACY | TECHNOLOGY | TECHNOLOGY & TELECOMMUNICATIONS | CORONAVIRUS | MARCH 18, 2020

Joseph W. Swanson

John E. Clabby

Steven Blickensderfer

Patricia M. Carreiro

For many people and organizations, COVID-19 caused a rapid transition to remote learning and working; for hackers and other bad actors, it has created new opportunities. Whether by virtue of a remote and distracted workforce, a strained IT infrastructure, or both, this difficult time is proving ripe for cyberattacks and cybercrime. With that in mind, we offer these steps that all organizations should take now to boost their cybersecurity:

1. **Make sure your system is properly patched and event logs are turned on.**

Even if you had a fairly robust system for remote work in place before, make sure its cybersecurity technical controls are up to date. Have you applied all the necessary patches? Most hacks exploit patchable vulnerabilities. It is an easy fix that can save serious money. Additionally, ask your IT professionals whether you have appropriate network event logs in place in the event of suspicious activity, to help create a record of who is coming in and out of your network, and when.

2. **Remind your employees to remain vigilant**.

Your employees should be reminded that they need to be on guard for cyberattacks, especially an increase in phishing, business email compromise, malware, and ransomware attacks.

- **Phishing and business email compromise.** Phishing attacks have already started that take advantage of the fact that people will no longer be sitting in the office together and may be more distracted by the news or commitments at home. This may prompt those employees to be less on guard for attempts to compromise their login credentials, for attempted business email compromise schemes, and for payment diversion fraud. To combat these threats, remind your employees to delete or report suspicious emails, avoid clicking on links or attachments without checking their source, and confirm wire payments through trusted channels. Enable multifactor authentication for system access, if you have not already done so. If your existing wire controls involve in-person confirmation, determine how to adjust them during a work-from-home period without compromising security, such as deploying real-time video confirmation. Remind employees how to report suspicious cyber activity, and through which channels.
- **Malware, including ransomware.** Criminals will likely look to exploit this chaotic time and distracted workforces to install malware, including ransomware, on organizations' systems. As with phishing and business email compromise, the attack vector may be a legitimate-looking email, such as an invitation to a file-sharing site or an email communication from a trusted vendor. Employees need to remain watchful for such attempts. Organizations also should ensure that employees save files to the corporate systems, that the IT staff backs up those systems regularly, and that their incident response plan is available for activation. Finally, in the event of a ransomware event, corporate decision-makers should know how to get in touch with key outside systems partners, such as cloud service providers, a managed service provider if you use one, or any backup or disaster recovery vendors.

3. **Monitor your system use.**

If your system is compromised, you will want to detect and shut it down as quickly as possible. To that end, keep an eye out for suspicious network activity, like repeated failed login attempts, unusual login activity, or logins using IP addresses from locations where your workforce is not present. To this end, remind your IT staff not to share password information by phone, even if the person on the other end claims to be an executive calling from an unknown “home” phone number.

4. **Review your insurance policies.**

Finally, understand your insurance policies, including any cyber policy. Your incident response plan should have contact information for your broker and carrier, and you will want to understand your coverages and what tools are provided by that policy, such as quick access to preapproved service providers. Having this information readily available will cut down on critical response times in the event of a successful cyberattack. Executives and IT/IS professionals should print this information and keep it with them during work-from-home periods.

Conclusion

In this time of uncertainty and disruption, organizations need to focus on the safety and security of their operations, their customers, and their employees. Cybersecurity is a key component of that effort and should not be disregarded. Heeding these tips can go a long way to protecting the organization and maintaining stability going forward.

Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.