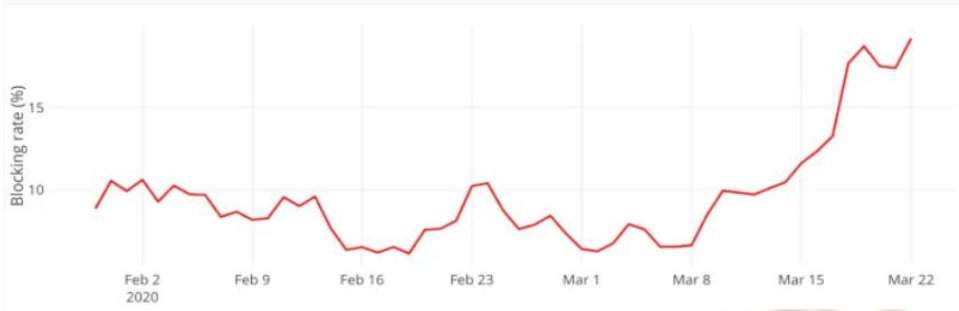
GLOBAL ASSET SOLUTIONS

CORONAVIRUS

ESSENTIAL CYBERSECURITY GUIDELINES TO PROTECT YOUR BUSINESS WHEN WORKING REMOTELY

Three weeks ago, Marriott International announced they had experienced a data breach, putting the personal data of 5.2 million guests at risk[1]. While this number dwarfs in comparison to the data breach of 500 million Marriott and Starwood guests in late 2018[2], the message is clear: hotels are a target for threats and need to focus on protecting their employees' and guests' data. With the advent of COVID-19, your company's cybersecurity is at higher risk. As employees worldwide switch to working from home, the dangers associated with mobile devices, remote access to core business systems, and poor online practices are increasing. Meanwhile, as seen in *Figure 1*, hackers have been heightening their malicious efforts knowing that businesses are more vulnerable now[3].

Figure 1. % of Traffic Blocked on Travel and Hospitality Sites from February 2nd - March 22nd, 2020



Source: PerimeterX Digital Security Solution Provider[3]

While managers these days are, understandably, focusing mostly on staying financially afloat, it is important to keep cybersecurity a priority. Hacks resulting from stolen or lost employee login credentials can have tremendous impacts, whether you're a small independent hotel or an international hotel giant. Following the ISO 22301 Business Continuity Standards[4], cybersecurity is crucial to your enterprise's resilience. It is your responsibility as an employer to give your employees the tools to protect themselves, which will end up protecting your guests, reputation, and bottom line[5].

We've organized key risk treatment and mitigation measures into the following guidelines:

1. MULTI-FACTOR AUTHORIZATION (MFA)

Two (2FA) or multi-factor authorization is one of the most effective ways to prevent Account Takeovers (ATOs). Essentially, this consists of using one or more authorization methods in addition to a password to log in to your account. SMSs are safer than emails as a second factor, as it is more difficult to access a phone's details than an email password[6]. According to an article by *Hospitality Technology*, it is highly likely a recent breach at a large hotel brand company was caused by a phishing attack that stole the credentials of two employees[7]. ATOs have shown a steep rise following the virus. According to the Director of Identity Security at Microsoft, your account is more than 99.9% less likely to be

compromised if you use MFA[8]. You can use TwoFactorAuth.org to find and pick platforms that support 2FA to use as a company.

2. Update, Update, Update

As potential security breaches are found, reported, and fixed by the affected platforms, new updates are consistently rolled out. Strengthening your cybersecurity is as simple as constantly checking and updating various applications. Actively encourage your team to update all applications they use. If there is an update in a crucial platform used in your business, such as a file-sharing platform, video conference application, or VPN, try to email employees a reminder to update.

3. Beware of Scams

Scammers are taking advantage of fears surrounding the coronavirus by sending emails with viruses, scams, and misinformation. Inform your employees to be alert and wary with emails regarding COVID-19 asking them to open a link or download a program, even if they seem to be from their colleagues or respected authorities like the WHO. Ask your employees to share suspicious emails with the rest of the team so that everyone can be on the lookout for them.

4. Virtual Private Networks (VPN)

While your business will likely already be using a VPN for employees to access business servers, it is a crucial step for cybersecurity. VPNs ensure a higher level of security and safety between the remote worker and the business server. Ensure you set up MFA (explored in guideline 1) for employees to access the VPN, and update whenever possible (guideline 2). Ensure your VPN usage policy is clear, so your team knows what applications they shouldn't use with it on.

5. Company Approved Devices and Private Wi-Fi Networks

If your employees do not work on company-issued devices, ensure you are clear with what devices they can and cannot use for work. For example, using mobile devices should be strongly discouraged for work purposes, as they are likely to automatically connect to public Wi-Fi networks should they leave the house. Public Wi-Fi networks open up your employees and company data to threats, especially when used to access your VPN. Make sure your employees only use private Wi-Fi and consider supplying them with reliable anti-virus software and firewalls if they do not have them already.

6. Video Conferencing Measures

While these tips are tailored for Zoom users, similar measures are also possible on alternatives such as GoToMeeting, Cisco Webex, etc. Other than constantly updating (guideline 2), try to change your Personal Meeting ID (PMI), as infiltrators compile lists of known PMIs. Ensure you set passwords for important meetings, and send the passwords separately from the PMI as close to the meeting time as you can. Take advantage of Zoom's waiting room feature, which prevents people from joining the call

before the host, and allows you to keep tabs on who wants to join. Once the session has started with the essential participants, lock the meeting to prevent infiltrators from joining once everyone is distracted. Finally, change the call settings to allow only one application to be used when sharing the screen. This prevents the chances of employees accidentally showing sensitive information open on other windows when sharing their screen.

7. Cloud File Storage

File sharing and storage tools on a Cloud/SaaS platform give your team agile access to documents in a teleworking environment. If your company server has decided on a file-sharing platform, such as OneDrive, remind employees that they should not use other servers like Google Drive for corporate files. We recommend you to assign specific people the responsibility of supervising the permissions assigned to folders and documents that are stored on these platforms, ensuring that only those people with correct credentials have access. Sensitive or regulated records (personal data, financial information, etc.) should be encrypted using Information Rights Management (IRM) technologies. Then, even once documents are downloaded from the cloud, the data is still protected and controlled. IRM can even revoke access once the documents no longer need to be available[9].

8. Clear Usage Policies and Employee Support

The guidelines above will not be useful unless adequately communicated to your team. Decide which platforms should be used for every business function (VPN, File sharing, Video Conferencing, etc.) and inform everyone that only these can be used for work purposes.
Be understanding to your employees, as many might be struggling to quickly learn new technologies and remote working guidelines amidst the already stressful situation. Where possible, share tips and how-tos for your employees who are new to specific technologies, and share this list of best practices. Make it clear who your team should inform if they suspect that their data has been breached. Foster a positive environment encouraging members to speak up about these suspicions, even if they feel they are at fault. This is the only way to mitigate the potential risks from spreading company-wide and ultimately affecting your bottom line.

We encourage you to stay vigilant and focused on cybersecurity solutions for your business continuation practices. Please contact us at info@globalassetsolutions.com; we would be delighted to offer you our assistance and tailor-make an action and implementation plan for navigating these turbulent times.

Written by:

Vani van Nielen, Larina Maira Laube, Eliana Levine, Zhaoyu Zhu and Paloma Guerra
Ecole Hôtelière de Lausanne Students and Alumna

Global Asset Solutions, your key partner in hotel asset management, has partnered with a team of five students and one alumna from Ecole hôtelière de Lausanne, recognized by industry leaders as the best hospitality school in the world. Together, we are working on compiling the best practices to help hotel owners and operators navigate through the COVID-19 crisis. By combining diligent research, expert opinions, and our own experiences, we will be publishing the best practices on the most current topics facing our industry. Team APAC is composed of Paloma Guerra and Zhaoyu Zhu, while Eliana Levine, Larina Maira Laube, and Vani van Nielen make up our Team EU & US and Remy Rein (EHL Lecturer).

Co-Published with Alex Sogno (CEO - Senior Hotel Asset Manager at Global Asset Solutions). Mr. Sogno began his career in New York City after graduating with honors at Ecole Hôtelière de Lausanne, Switzerland. He joined HVS International New York, and he established a new venture at the Cushman & Wakefield headquarters in Manhattan. In 2005, Mr. Sogno began working for Kingdom Hotel Investments (KHI), founded by HRH Prince Al-Walid bin Talal bin Abdul Aziz Al Saud member of the Saudi Royal family, and asset managed various hotels including Four Seasons, Fairmont, Raffles, Mövenpick, and Swissôtel. He also participated to the Initial Public Offering (IPO) of KHI at the London Stock Exchange as well as the Dubai International Financial Exchange. Mr. Sogno is also the co-writer of the 'Hotel Asset Management' textbook second edition published by the Hospitality Asset Managers Association (HAMA), the American Hotel & Lodging Education Institute, and the University of Denver. He is the Founder of the Hospitality Asset Managers Association Asia Pacific (HAMA AP) and Middle East Africa (HAMA MEA).

A special thank you to Alberto Rodriguez, Head of Cybersecurity, Eulen Group.

SOURCES OF INFORMATION

1) Marriott International. (2020, March 31). *Marriott International Notifies Guests of Property System Incident*. [Press Release].

2) Marriott International. (2018, November 30). *Marriott Announces Starwood Guest Reservation Database Security Incident*. [Press Release].
3) Perimeterx. (2020, March 24). *COVID-19 Part 2: Data Tells the Story.*
4) International Organization for Standardization. (2012). *Business continuity management systems - Requirements.* (ISO Standard No. 22301).
5) LSA Consultants Pte Ltd. (n.d.) *Market Differentiation and Competitive Advantage through Enterprise Resilience Standards Implementation.*
6) Herman, J. (Writer). (2020, April 1). *How to Stay Safe While Working from Home*. [Audio Podcast].
7) Hospitality Technology. (2020, March 31). *5.2M Guests Affected by New Marriott Data Breach.*
8) Weinert, A. (2019, September 7). *Your Pa$$word doesn't matter.* [Blog Post].
9) CCN-CERT BP/18. *Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia.*
10) Zoom. (2019, December 4). *Top Ways Zoom Hosts & Admins Can Ensure a Secure Meeting Experience.* [Blog Post].
11) Vectra AI. (2020, March 25). *Remote work, not remote control*. [Blog Post].
12) Hinchcliffe, D. (2020, March 11). *Working in a coronavirus world: Strategies and tools for staying productive.*
13) Bluefin Payment Systems. (2020, April 2). *Three Cybersecurity Must-Do's for Remote Workers*. [Blog Post].