U.S. CHAMBER OF COMMERCE

ABC

Assessment of Business Cyber Risk

Special Report on Cybersecure Remote Working During COVID-19

POWERED BY

FICO™ Cyber Risk Score

OCTOBER 2020

Contents

Welcome Letter

The U.S. Chamber of Commerce and FICO share the goal of elevating the national dialogue around cybersecurity. Each *Assessment of Business Cyber Risk* (ABC) helps promote this dialogue by offering a set of actionable recommendations to reduce firms' cyber risk.

As we explore these issues, one criminal pattern is highly predictable: when the global economy and society go through massive change, bad actors seek to exploit cyber vulnerabilities. Whenever consumers and businesses are forced to adopt new habits, it opens avenues for hackers and fraudsters to take advantage of our defenses and exploit us as we navigate unfamiliar ground. That certainly has been the case over the past several months of the COVID-19 pandemic.

COVID-19 has changed many aspects of our lives. Hopefully, some of these will be temporary, but it seems increasingly clear that this pandemic will permanently impact how many—if not most—of us work. Where we work, how we work, how we interact with customers, and how businesses interact with other companies have changed dramatically.

Working from home, virtual meetings, and digital commerce—for both businesses and consumers—are becoming our new normal, and there's no reason to think that all of this will revert to the old normal once the pandemic wanes. These were all trends before the pandemic started, and the changes we've endured as a country, and globally, have only served to accelerate and cement shifts that were underway. Accelerated virtualization has business benefits that are unlikely to be unwound when the COVID-19 case counts recede.

We have compiled six important COVID-19 cybersecurity recommendations that every business can use based on changes we see:

1. Consider the benefits of using cloud services.
2. Instruct employees on the proper components of a home office network.
3. Use a properly configured virtual private network (VPN).
4. Take steps to introduce elements of security to teleconferencing.
5. Have a plan to identify and manage third-party and supply-chain risk.
6. Think through—and adhere to—sound "bring your own device" (BYOD) policies and procedures.

These recommendations have become more important since the first quarter of 2020, when the response to the COVID-19 pandemic altered the work patterns of millions of Americans virtually overnight. With that in mind, this report is designed to help business owners know what steps to take to increase the security of their virtual working environments. We hope that you find them useful and look forward to continuing the series with helpful insights to help navigate the challenges of today and tomorrow.

Doug Clare
Vice President
Fraud, Compliance, and Security Solutions
FICO

Christopher D. Roberti
Senior Vice President
Cyber, Intelligence, and Supply Chain Security Policy
U.S. Chamber of Commerce

Introduction: The Cyber Threat Landscape

When the world changes, people find ways to adapt. In March 2020, when the reality of the impact of the COVID-19 virus was becoming apparent, businesses were forced to quickly, and with little warning, completely alter their operations, in many cases suspending most in-person activities and shifting to operating in a virtual environment.

A period of rapid change

During this period of rapid change, some businesses were able to handle the operational transition relatively well, in some cases improving the performance and productivity of the organization. Others struggled. Many of the companies deemed "essential" by federal guidelines[1] or state edict[2], particularly those whose main line of work related to cybersecurity services and critical infrastructure, could not limit their operations. On the contrary, these essential critical infrastructure workers[3] had to transition to a remote working environment efficiently and securely; the country's economic security depended on their continued service.

Fig 1. **Map of COVID-19 Cyber Threats**

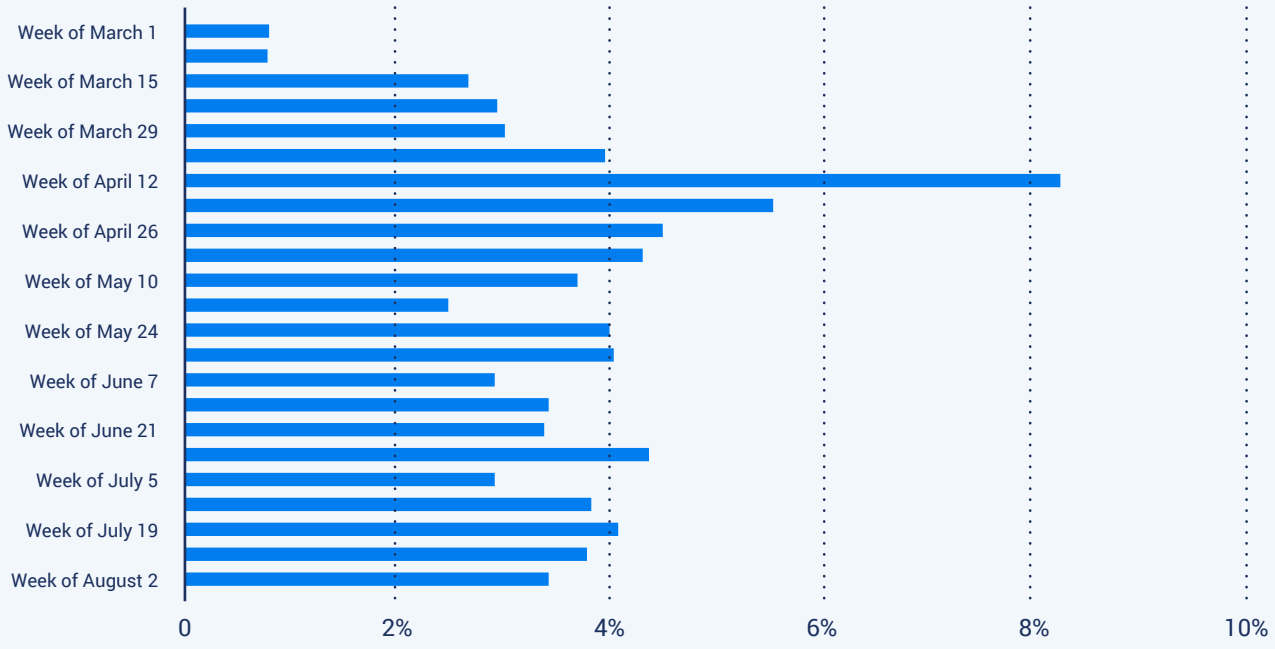
According to an analysis of billions of internet observations (*e.g.,* the number of web servers, the number of hosts with expired SSL certificates, the number of misconfigured DNS servers) performed by Manish Karir, vice president for cyber risk solutions at FICO, there was a clear drop in the number of remote access services as shutdowns around the world started to take effect during March.[4] But by the end of the month, there was a noticeable uptick in terms of software services related to remote work (e.g., remote desktop protocol, virtual network computing, internet platform management interface). The number of misconfigured (exploitable) remote access services rose sharply as businesses large and small scrambled to enable remote work but failed to fully lock down their remote access infrastructure.

Cybersecurity has become a topic of increased discussion due to the COVID-19 pandemic

As the Chamber and FICO reported in our last edition of the *Assessment for Business Cyber Risk*, for the first half of 2020, the National Risk Score is 694. For an individual organization, and depending on size and sector, a score of 694 represents a level of risk that is considered moderate to low. Compared to last year, the risk level for businesses has remained stable, based on observable external facing signals. Network complexity—and the inherent challenges in securing large networks—along with the fact that these organizations are more visible, richer targets, remains a driving factor in relative risk for larger firms.

It is no surprise that cybersecurity has become a topic of increased discussion on the national stage due to the COVID-19 pandemic, which has worldwide appeal for nefarious actors who have been quick to take advantage. Businesses, large and small, began to worry more about their cyber risk and vulnerabilities, and rightly so. IBM X-Force Research, a world-renowned commercial security research team, observed a more than 6,000% increase in COVID-19-themed spam from March 11 to May 8, 2020.[5] A part of FireEye, Mandiant has been tracking phishing and social engineering campaigns leveraging "COVID-19"-themed lures. According to its research, coronavirus-themed phishing peaked in mid-April and has hovered around or below 4% since then (see Figure 2).[6]

Fig 2. **Coronavirus-themed Phishing as % of all Malicious Email Detections** (Source: Mandiant)

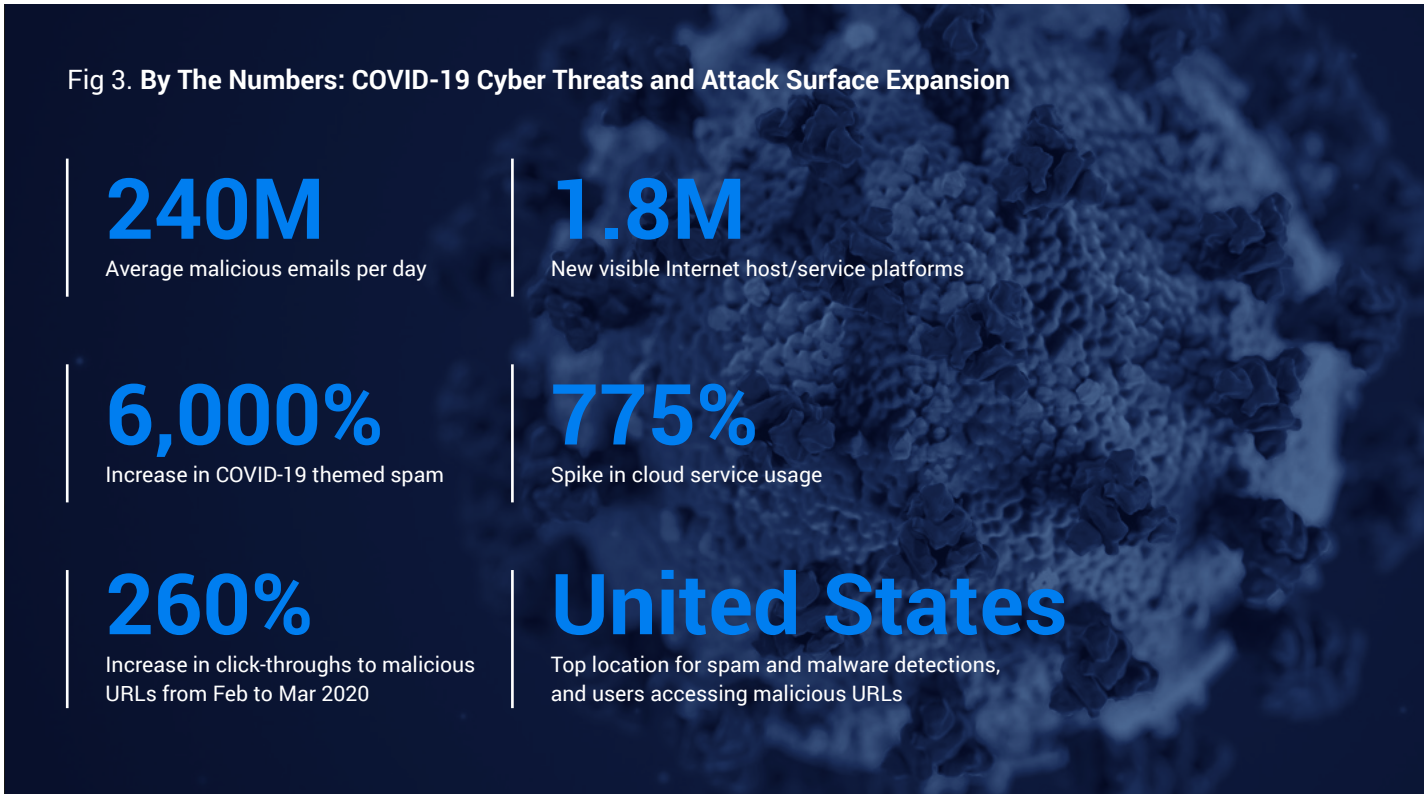


New opportunities to take advantage of cyber vulnerabilities

This crisis has provided malicious cyber actors with opportunities to take advantage of cyber vulnerabilities on a new scale. For example, according to the multinational cybersecurity software company Trend Micro, there was a 260% increase in click-throughs to malicious Uniform Resource Locators (URLs) related to COVID-19 from February to March 2020.[7] Trend Micro also reports that the United States is the top location for spam and malware detections, and for users accessing malicious URLs.[8]

Google is seeing more than 240 million emails per day related to COVID-19 scams,[9] and Trend Micro reports that 91.5% of malicious cyberattacks executed in the COVID-19 era were conducted through spam emails.[10]

Fig 3. **By The Numbers: COVID-19 Cyber Threats and Attack Surface Expansion**



These malicious actors are preying on anxious consumers who are more susceptible to social engineering ploys and phishing emails claiming to have information on COVID-19 cures, treatments, vaccines, and government stimulus payments.

In other phishing cases, malicious actors impersonate senior executives and ask junior employees for help with financial transactions. These business email compromise cases are not new to the COVID-19 period, but the frequency for these cyber-enabled crimes has significantly increased. Additionally, the average ransom demand has increased from $800k in Q4 of 2019 to $1.3 million in Q1 of 2020, according to Trend Micro.[11]

The remote working environment

Due to the transition to a remote working environment, cybercriminals have increased their attacks on remote login services. Trend Micro reports that there were over 1.2 million attempts made to compromise remote login services, with 89% of these attacks being executed through brute force.[12]

Federal law enforcement officials have taken note of these trends and are working on handling them. Michael D'Ambrosio, assistant director of the U.S. Secret Service and head of its Office of Investigations, commented that the COVID-19 pandemic "provides criminals opportunities on a scale likely to dwarf anything seen before."[13] He added that significant targets include companies involved in the financial services and healthcare services industries that often are the target of malicious ransomware designed to take down entire systems. He sees an exponential increase in phishing, spearphishing, and fraud attempts, further complicating defensive measures.[14]

Continued focus on the same targeted industries as before the pandemic

Many of the cyber espionage, cybercrime, and even information operations campaigns have focused on the same targeted industries and regions as before the pandemic and have not demonstrated any new or particularly sophisticated tactics. According to reporting in *The Wall Street Journal*, the top three areas that were ransomware targets in the first three months of 2020 were professional services, healthcare, and the public sector.[15] However, organizations in sectors related to COVID-19 response and relief efforts—such as healthcare, pharmaceutical, and research entities—may face threats due to the nature of their work. Over the past several months, several U.S. and foreign government agencies, including the U.S. Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, and the National Counterintelligence and Security Center, have spotlighted the threat to healthcare, research, and pharmaceutical organizations.[16] Additionally, the shift to remote work that many organizations have undergone may result in new security challenges and risks or exacerbate existing ones.

Managing cyber risk requires active engagement. Merely waiting for an attack and reacting to it is not enough. "People tend to freak out the moment a cyberattack happens instead of preparing for it in advance," said Matt Papendorf, senior advisor of product marketing for Dell. "Think of cybersecurity as a sort of insurance policy to protect your business."[17]

Evolution of Cybersecurity Threats During the COVID-19 Pandemic

Cybercriminals throughout history have exploited national emergencies for financial or illicit gain. As the COVID-19 pandemic spread across the globe, the risk for cyber-enabled fraud exploded in unparalleled scale and scope.

$2 trillion; an alluring target for transnational criminal organizations

Congress quickly appropriated $2 trillion to support the American economy, the largest ever federal government stimulus package intended to support America's small businesses and communities in need. This proved to be an alluring target for transnational criminal organizations and some hostile nation states.

"We have a vulnerable public looking for assistance. The adversaries know this and are looking to take advantage of the public in a time of crisis," said Mike D'Ambrosio, assistant director for investigations at the Secret Service.[18]

Ed Cabrera, chief cybersecurity officer at Trend Micro, says cybercriminal groups know that humans are often the weakest link in cybersecurity defense, and now they have a highly emotional issue ready to exploit.

"COVID is international, it definitely provides another opportunity for these groups to scale their social engineering [psychological manipulation] attacks," Cabrera says. "We've certainly seen an uptick."

An increase in cyberattacks linked to the pandemic

Cabrera adds that his company has seen evidence of an increase in a wide range of cyberattacks linked to the pandemic. According to Trend Micro, in the first quarter of this year there were nearly 1 million spam messages sent, 48,000 hits on malicious URLs, and 737 pieces of malware detected—all tailored with content relevant to COVID-19.[19] Often, these attacks prey on people's emotions or simply their desire to learn about the pandemic.

"They exploit our trust. The trust we have in the applications we use, the emails that we get," Cabrera says. "What they've done is play on the fear and frustration that everybody feels from being having been locked down. They are sending phishing emails using topics like rising COVID hotspots in their area [or] increased deaths. Or any information that relates to schools or COVID testing."

This is especially true in phishing (fraudulent email or website scams) attacks, which take advantage of short attention spans and seek to build trust quickly with the recipient.

More opportunities for malicious attackers

"Certainly, the usage of COVID-19 as a lure for phishing operations has become prevalent. That's to be expected when you have something that has universal, global interest," says Luke McNamara, principal analyst at FireEye Mandiant Threat Intelligence. "It can be used for campaigns and intrusion targeting around the globe. Many of the campaigns and groups that we've been tracking for some time have now started to roll that into their operations."

The prevalence of videoconferencing in a time of working from home is also something in which malicious attackers are interested. If nothing else, it gives them the opportunity to eavesdrop on confidential communications and gather intelligence.

"If you're working for an organization, [you need to] be consistent with the policy and usage of those videoconferencing platforms," Cabrera says. "First and foremost, these platforms have to be properly tested and vetted. Second, always use two-factor or multi-factor authentication and password protect each conference session. And if you're invited to a meeting, use good situational awareness and look at who has actually signed on. If six people are on there, and you're only supposed to have five, say something."

Another challenge of working from home is changing from centralized, corporate networks to more distributed, home networks. At times like these, the fundamentals of good cybersecurity become even more vital.

"Due to COVID, the whole 'attack surface' gets expanded. Now, you're bringing in all of that risk baggage that comes along with home offices, and segmentation best practices go out the window," Cabrera says.

Established practices can prevent a cyber intrusion

There is some good news. The same practices that would have prevented a successful cyber intrusion last year are the same practices that can protect us today. In other words, from the end-user's point of view it is always helpful to remain on alert when receiving emails from strangers, emails with attachments or hyperlinks, and possibly even unexpected messages from "trusted" sources. The changing environment requires expanded diligence and increased awareness.

McNamara says the key to maintaining a good security level in one's home office is to follow the same security procedures used in a corporate office setting. This includes using a corporate VPN for all work activities, using multi-factor authentication, keeping a clear separation between work and personal devices (including PCs and phones), and being mindful of which devices (thumb drives, external hard drives, USB devices) connect to work devices.

"The general best practices from a security standpoint that would apply to securing something in a corporate environment are also going to hold true for operating on your own personal network to access corporate resources," McNamara says. "As those things have blurred, a reminder of those policies is very important."

There is some good news. The same practices that would have prevented a successful cyber intrusion last year are the same practices that can protect us today.

Expert Sees Supply Chain Cybersecurity as Vital in the Time of COVID

We asked Doug Clare, vice president of fraud, compliance, and security solutions at FICO, about cybersecurity third-party risk management and cyber in the time of COVID. Here are some of his thoughts.

Has cybersecurity changed in the time of COVID-19? If so, how?

One important thing we've seen with COVID is that supply chains have been shifting more rapidly than they normally do. As businesses have had to adjust, many have sought new suppliers to fill new needs, while others have had to source new suppliers because their traditional vendors have had difficulty fulfilling orders, or in some cases have gone out of business. Organizations have had to find alternative suppliers and without the usual notice, and in many cases with extreme urgency. This has created new demand for rapid, objective third-party risk assessment.

A lot of the standard vendor vetting processes take time. I'm not negating the efficacy or importance of those things, but there is also a compelling case for something like the FICO® Cyber Risk Score when you're in a rush. And we've all had to rush things in the last six months.

Also, many organizations' standard supplier assessment processes rely on on-site interactions, visiting data centers, sitting across the table from chief information security officers—nobody's doing that right now. Nobody's getting on planes. Everybody is doing things virtually and that's what we do—an objective "no touch" assessment. And from that perspective, it's a real asset for organizations.

In cybersecurity, what is Third-Party Risk Management (TPRM) and why is it important?

Businesses today share data. It's inevitable. If you conduct business with somebody, you have some kind of exposure to them with respect to the data you exchange, even if it's just simple emails that you wouldn't want in the public domain. If they're a supplier to you, they might have financial information or information about your employees or customers, and any time you share that information you have a duty to protect it.

If they're breached, you're effectively breached. It could be a little less egregious: if they're breached, you could suffer some reputational damage because consumers might assume you're also breached. People carry that exposure. If it happens to them, it happens to you, to some extent.

With the onset of the COVID crisis, many businesses were forced to fill sudden gaps in their supply chain, or simply source new services that they didn't previously need. As face-to-face commerce has necessarily decreased, it has pushed a lot of businesses

to speed up the process of their digital transformation. For many, this has required the rapid onboarding of cloud service providers and digital commerce partners. It was hard—maybe impossible—to apply the usual standards of care in bringing those new business partners onboard. No time for the usual in-depth vetting, looking under the floorboards, and the back and forth regarding security questionnaires, pen-testing, employee training, and the like.

If a company knows its FICO® Cyber Risk Score, isn't that enough? Should they also investigate the Cyber Risk Score of their supply chain or vendors?

What we try to facilitate is two layers deep. In addition to providing some insight to companies about their own cyber risk, we try to give organizations the ability to look at the cybersecurity risk of their suppliers, as well as the suppliers to those suppliers—both at an individual level, "Who are the suppliers to my Supplier X?" and also, "How many of my suppliers are exposed to Organization Z?"

It can get pretty large. We work with organizations that literally have tens of thousands of suppliers in their supply chain. It really helps underscore the importance of this approach. Obviously, for your most important suppliers or where you're sharing the most data, you're going to assess their Cyber Risk Score, audit their controls, and send them a questionnaire. You might have monthly meetings. But when you have a really big supply chain, some automation is required. After your top suppliers, you might have the next group down, say, 500 suppliers, that are critical to your business, but you can't afford to be in their business every day. Having the means to prioritize risk management activities and different processes for medium- to low-risk suppliers is important.

One of the key things our customers get from using the Cyber Risk Score is ascertaining where you need to apply to that "higher touch."

What are some common examples of poor TPRM practices?

Poor TPRM starts with not having a cyber TPRM strategy at all. That's really started to change over the last couple of years, but I don't think robust TPRM is the norm; it's still the exception.

Short of no TPRM, bad TPRM is a program that is not risk based. It's really easy to become process oriented with TPRM: "We send out this questionnaire, we ask them to fill it out, we look for any red marks, we file it away, and after three years we ask them to do it again."

We try to provide an objective measure that's not been biased by anyone's opinion. Now that you know this partner is low risk, maybe apply your light question set and put them on a three-year, double-check cycle. Whereas, if they're higher risk, maybe you send them the long question set and put them on an annual review. And if they're really bad, maybe you start to think about finding another supplier.

Taking more of a risk-based approach really helps an organization make the most of limited resources.

As face-to-face commerce has necessarily decreased, it has pushed a lot of businesses to speed up the process of their digital transformation. For many, this has required the rapid onboarding of cloud service providers and digital commerce partners. It was hard—maybe impossible—to apply the usual standards of care in bringing those new business partners onboard.

What if you run a small company with limited time and budgetary resources. How can you look into your supply chain's cybersecurity quickly and easily?

For a small business, the Cyber Risk Score can be a surrogate for more robust processes.

If you're a 10-person firm with 10 suppliers, you can look at the scores of those suppliers. Probably all or most of them are good, maybe one of them is not good. It can provide you with an opportunity to engage them in a conversation. If it's not good, the Cyber Risk Score says it's for these reasons. You can go back to them and say: "This makes me nervous, what are you going to do about it?" As an opportunity to initiate a conversation, it can be a great asset.

Six Cybersecurity Recommendations for the Remote Office and Teleworking Employee

As a result of COVID-19, the U.S. workforce has been forced to adapt to a new virtual working environment. Nearly all sectors of the economy have had to transition some or all their business operations to this new format. This change has allowed operations to continue for many Americans, despite the changes COVID-19 has precipitated.

Adapting to a new virtual working environment

On the flip side, the virtual environment has introduced other unique challenges, including increased phishing, spearphishing, and malware attacks. Cyber actors have been using existing malware and infrastructure and are creating new lures to breach networks and access proprietary data.[20] Businesses must deal with uneven security knowledge among their employees, many of whom are working remotely for the first time and are not familiar with remote work security procedures. This can lead to information leakage, cyber-enabled fraud, or disinformation spread through error or inattention. Still, the expanded threat surface also provides additional vectors for malicious cyber actors to leverage the virtual working environment for their illicit purposes.[21] Set forth below is a deeper dive into the six recommendations, outlined earlier in this report, on how to better secure virtual working environments.

1. Consider the benefits of using cloud services

More flexibility

The "cloud" is a tool that can be leveraged by businesses, big and small, to improve their workforce's interconnectedness. The benefits of using a cloud include more flexibility in data storage, increased collaboration from anywhere in the world, and increased security. Most businesses already use cloud services in their operations. It is vital for every employee to know how to use cloud services and, more importantly, how to use cloud services *securely*. Also, businesses should understand that they have options when it comes to which cloud services to select. The three main types are software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS), and these services vary by the cloud provider as well. The Chamber recommends that every business, small and large, consider using a cloud service to make their operations more effective and efficient. Before buying cloud services, executives should thoroughly understand their specific needs and locate a cloud service that best aligns with those needs. Especially in the unique COVID-19 virtual working environment, demand for cloud services has skyrocketed, with Microsoft reporting a 775% spike in cloud services demand due to COVID-19.[22]

Increased security

One of the most important benefits of the cloud is increased security. Many reports have debunked the misconception that cloud services are less secure. This misconception likely exists because of the nontraditional way protection is provided within cloud services. Because each business leverages cloud services differently, the duty of securing the cloud falls on the user, not the cloud service provider.[23] A Gartner report estimates that by 2022, 95% of cloud security failures will be the customer's fault.[24]

To keep cloud services secure, FireEye recommends that businesses do the following:

- **Protect and monitor the credentials needed to access secure resources and watch them for compromise.**
- **Remain vigilant for and guard against misconfiguration.**
- **Centralize telemetry data for the ability to support security monitoring and audit user trails.[25]**

So, cloud services are secure, but businesses must make sure they are using them securely.

Storage and backup capacity

Another significant benefit of using cloud services is its storage and backup capacity. Each company can scale their storage and backup capacity to fit their individual needs. SaaS, IaaS, and PaaS all feature the ability to back up critical business information to a secure cloud or server. The modern development in cloud services is the use of the "hybrid cloud" or the "multi-cloud."[26] This means that businesses can use private cloud services (those that are unique to their organization and store information on the premises) and public cloud services (a third-party provider stores data) simultaneously. This method of storing cloud data has become very popular, with about 47% of cloud-using companies polled in a survey reporting that they have implemented an application using a hybrid cloud.[27] Again, these cloud services are quite different, and each business should determine which one is right for its needs; the Chamber would like to emphasize that using cloud services is superior to not using cloud services, and we encourage each business to seriously consider them to maximize data storage and backup, and increase company collaboration.

Accessibility

Collaboration is vital to any company's operations, and cloud services have made this process even more accessible. Each cloud service and provider enable companies to collaborate on platforms and documents securely from anywhere in the world. Organizations from Blackboard and Twitter to ESPN to the intelligence community have successfully leveraged cloud services to remain connected and functional through this unprecedented COVID era.[28] These global organizations, and many more, use cloud services frequently to collaborate on documents and services from every corner of the globe. The cloud providers also have so many data centers that data center management is an emerging specialization; for example, Amazon Web Services alone operates over 70 computing zones worldwide.[29] Cloud service providers leverage their services; massive data centers can be operated remotely from the cloud, so the need for on-site personnel is minimal.[30] There are myriad examples of this business collaboration, but we at the Chamber want to emphasize the benefits of these services to our members, especially in the COVID-19 era.

2. Instruct employees on the proper components of a home office network

The home office presents a unique opportunity for cyberattacks

During the COVID-19 crisis, each business's office space has been extended to the homes of employees. Each employee's home office environment presents a unique opportunity for cyberattacks and data leakage. Businesses have an obligation to their employees to instruct them on how to properly create and manage a secure home office environment so that the entire company's network is secure. An integral part of the home office is an employee's Wi-Fi network. After setting up the hardware for a home network, various steps must be taken to ensure that an employee is accessing the internet securely. In other words, there are multiple settings on the system that must be adjusted to ensure the system is secure enough for employees to use.

The first step to securing a home network is ensuring an encrypted connection to the network. Using encryption ensures that any communication between two computers or networks is secure and cannot be intercepted by outside parties. The best encryption can be achieved through Wi-Fi Protected Access 2 (WPA-2) or WPA-3 connections. The Wi-Fi Alliance, an industry group, created these security certifications that define sets of security requirements for wireless networking devices.[31]

Separate networks for business and personal purposes

Another important security measure is making sure that different networks are set up on the home Wi-Fi network. Employees should make sure that they have separate networks for business and personal purposes so that all business information is accessed from a secure network of its own. Additionally, an employee may also opt to set up different networks for different people. For example, one network could be created specifically for family members, and then another network could be created for guests and unknown users. By doing this, families and employees are making sure that their personal data is safe, and they always will know who is accessing which network.

Develop complex passwords

The next step to securing access to the network is developing complex passwords that cannot be guessed. For example, do not use any identifying information about family members, including names or birthdays. Some smartphones offer secure password applications that can remember complex passwords.

One of the most critical steps to securing a mobile device is to use antivirus software that detects attempts to penetrate the device. More importantly, employees must ensure that they are keeping their antivirus software updated because providers are continually patching the software and improving it. Automatic updates can be turned on as well; this allows the software to update itself without cues from the user.[32]

During the COVID-19 crisis, each business's office space has been extended to the homes of employees. Each employee's home office environment presents a unique opportunity for cyberattacks and data leakage.

Email filtering

Email filtering is another vital feature of a home network. Most email applications have some way to separate spam and detect viruses. Because some viruses can be deployed through email, companies should be sure to use advanced software to detect these viruses before the employee sees them in their inbox. Additionally, employees should make sure to use spam filtering. With spam filters, employees can whitelist or blacklist senders, and only view emails that have passed through safety filters.[33] The last line of defense against these emails are employees; employees should make sure they know and trust email senders and not open suspicious emails.

3. Use a properly configured virtual private network (VPN)

Access data securely

After securing a home office Wi-Fi network, telework employees should obtain a VPN. This added security layer when accessing the internet is paramount to ensure that employees are accessing company data securely. Most businesses provide their VPN to employees, but there are also numerous free online providers if an employee's business does not offer its own private network.

Two common VPN types are used to provide remote access to an organization's secure resources. The first type is an Internet Protocol Security VPN. This type of VPN requires software to be installed on each telework device that a business uses; because of this feature, these VPNs are often installed and used to access information from company-issued devices. The second type of VPN is called a Secure Sockets Layer VPN. This type of VPN allows users access to data through a specific web browser, and this type of VPN also generally requires users to install additional software.[34] Both types of VPNs are secure and easy ways to ensure that employees are accessing important company information securely.

While there has not been a noticeable uptick in abuse of VPNs since the beginning of the COVID-19 pandemic, the criticality of these systems now for remote work, and longstanding interest by threat actors, necessitates the importance of their usage and protection.[35] Beyond mandating the use of VPNs, organizations should apply vendor patches as is feasible, especially for critical vulnerabilities . Other VPN best practices involve using multi-factor authentication, capturing and analyzing logs for anomalous behavior, and ensuring network segmentation.

4. Take steps to introduce elements of security to teleconferencing

Maintain a secure teleconferencing environment

In work-from-home environments, teleconferencing is how people meet face-to-face and discuss business issues. Therefore, it is vital for people to feel that the information they are sharing is going only to the intended audience, and not to others who may be listening in. We at the Chamber hope these few simple tips will help you and your organization maintain a secure teleconferencing environment where you can feel comfortable discussing proprietary information with your colleagues.

Even in meetings that do not feature the sharing of proprietary information, teleconference security is paramount. The first thing that every employee should do is take steps to increase the protection of their home office environment (see previous recommendation), beginning with a secure (encrypted) internet connection. After a secure internet connection has been established, employees should follow their company's internet security practices, which will likely include recommendations for the specific teleconferencing platform in use.

More generally, however, meeting organizers should follow basic precautions:

- **Limit dissemination of access codes to those who need them; do not use the same code repeatedly.**
- **Require a personal identification number (PIN) or multi-factor authentication for more secure information discussions.**
- **Enable a "waiting/green room" to vet those wishing to join the meeting.**
- **Do not allow the meeting to start without the host.**
- **Make sure to authenticate the identity of all attendees.[36]**

Most platforms allow meetings to be recorded, so attendees should be informed if this is happening. General best practices for each of the platforms can be found on their respective websites, but the recommendations above can apply to all platforms. Meeting organizers and participants should become familiar with how the platforms work and how to use them securely to avoid accidental information leakage. The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) created a list of the teleconferencing platforms with additional guidance on finding information to secure them.[37]

Employees must understand and follow these tips to increase internet-based audio- and video-based security teleconferencing services.

The tips listed above are general recommendations for *all* meetings conducted remotely, regardless of their sensitivity.[38] However, for meetings that will include discussions of sensitive content, these additional recommendations should be considered. Highly sensitive information should be shared only on company-issued devices, and the discussion should not be recorded unless necessary and agreed to in advance. If the meeting is recorded and distributed, the file should be encrypted and not stored on the web-conferencing platform. Also, when discussing highly sensitive information, waiting rooms serve an essential role in allowing the meeting organizer to control admittance and, once all attendees have been admitted, close/lock the call to any additional attendees. For an added security layer, the organizer may consider distributing meeting PINs close to the meeting's start. The National Institute of Standards and Technology (NIST) outlines these recommendations in a publicly available "call security highway" graphic.[39]

5. Have a plan to indentify and manage third-party and supply-chain risk

COVID-19 has exposed additional complexities and vulnerabilities

Third-party and supply-chain risk management are important operational practices for businesses of any size. This task has become more difficult for businesses, given the threat landscape that the COVID-19 pandemic has created. More specifically, the pandemic has precipitated interruptions in supply chains and business relations across the globe. Additive to this, many business and their suppliers, vendors, and customers have shifted to remote work environments, which complicates and compounds the challenges outlined above. We wrote about the complexities of securing supply chains, and the value of implementing robust third-party risk management programs, in our 2019 report.[40] While COVID-19 has created or exposed additional complexities and vulnerabilities, the four-step process outlined in our report remains highly relevant as a starting point for businesses seeking to mitigate cyber risk.

The first step that any business must take is to build a framework for categorization of vendors and suppliers. In other words, businesses must determine which of the third parties they associate with harbor the most risk and pay special attention to these groups.

Address the amount of risk a third party poses

After categorization, the second step is to develop a plan for addressing the intersection of the amount of risk a third party poses and how important that party is to the business. This workflow will aid business leaders in making decisions about their business and the amount of risk an outsider poses.

The third step in the risk management process is to consistently assess high-impact suppliers and constantly monitor the amount of risk they pose to the business. This step is important because it aids businesses in preventing a business operations disruption, but also helps them locate the source in the event of a breach.

The fourth and final step in the Chamber's risk mitigation framework is ensuring that the risk a supplier poses can be appropriately transferred. One way to transfer risk is through cyber liability insurance. This issue is discussed in detail by the Chamber and FICO in an earlier *Assessment of Business Cyber Risk* report.[41] While a useful tool in limiting the financial impact from losses due to a cyberattack, cyber insurance policies do not increase security, prevent breaches, or reduce the need for good cybersecurity practices.

Third-party and supply chain risk management has been—and will continue to be—an important area of focus for businesses of all sizes. And while the COVID-19 pandemic has added a layer of complexity to these problems, the Chamber's four-step framework for mitigating cyber risk provides a useful starting point.

6. Think through—and adhere to—sound "bring your own device" (BYOD) policies and procedures

BYOD Policies

Many companies have employed BYOD policies, and increasingly so, since early 2020. Some of the benefits of BYOD policies are self-evident: organizations can reduce or limit their overall IT spending by not providing company-owned and maintained hardware to their employees. An additional benefit is that employees will likely carry their personal devices during after-business hours and on weekends, which increases their availability. While BYOD models may provide convenience and cost savings, organizations must consider additional security and risk management measures for such devices. Employees must understand—and comply with—their organization's BYOD policies to protect the integrity of their organization's networks and the data that resides on them. An organization's BYOD policies may differ depending on whether the equipment in question in a personal computer (PC) or a mobile device.

Employees should follow a few basic rules when using a BYOD PC:

- **Use a combination of security software products, including antivirus, personal firewalls, and popup blockers.**
- **Create a separate user account for each person using the computer in the home environment, with complex passwords for each.**
- **Enable automatic updates and patches to software.**
- **Disable unneeded networking features on the PC and configure wireless networking securely.**
- **Configure applications to filter content and stop an activity that is likely to be malicious.**
- **Install only known and trusted software.**
- **Configure remote access software based on the organization's requirements and recommendations.**
- **Maintain the PC's security, to include changing passwords regularly.**[42]

When assiduously implemented, these guidelines can increase a BYOD PC's defenses against attacks from malicious actors, which by extension helps to protect the network of the entire organization.

In addition, consider these analogous measures to help secure BYOD mobile devices:

- **Limit access to the device (i.e., create a PIN or password).**
- **Disable certain network capabilities (e.g., Bluetooth and Near Field Communication) unless needed.**
- **Install security updates in a timely manner.**
- **Configure applications to monitor security.**
- **Download and run applications only from authorized app stores.**
- **Do not change the security architecture for a mobile device (i.e., "jailbreaking" or "rooting").[43]**
- **Connect the device only to a known charging station (i.e., no airport or other public charging stations).**
- **Use an isolated, protected, and encrypted environment to access the organization's data and services (i.e., do not use public Wi-Fi access points).[44]**

Even if all these recommendations are implemented, it still is possible for malicious cyber actors to compromise company data. Therefore, organizations must emphasize to their employees that good judgment in these matters is the first—and last—line of defense. Employees should be trained not to open emails from unrecognized senders, refrain from clicking pop-up ads on websites, and otherwise engage in sound security practices.

Multi-Factor Authentication

Multi-factor authentication processes are an added way to keep devices, home offices, and business processes, like automated clearing house (ACH) payments, secure. We recommend organizations use risk-based criteria to enable multi-factor authentication across devices, applications, and business processes. Accordingly, users must be required to present two or more pieces of evidence or their identity to gain access to a network or program. For example, to access a VPN, users may have to access a specific device and present a user-specific PIN and a constantly changing code to access the VPN.

Added security measures, like multi-factor authentication, can reduce the risk of unauthorized access to information if a third party were to gain access to the physical device.[45] Examples of authentication measures include passwords; PINs; biometrics (e.g., fingerprint, iris scan, facial recognition); RSA SecurID; text messages; and security questions. One report describes multi-factor authentication as "something you are, something you have, or something you know."[46] The combination of identifying factors makes it difficult for unauthorized actors to access secure data.

Patch Management

The importance of instituting a regular and robust patch management process cannot be overstated. Unpatched devices present various opportunities for unauthorized actors to penetrate an organization's network and improperly access sensitive data.

A "patch" is a software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component.[47] Some devices will automatically update, but device owners need to make sure that updates are installed weekly. Patch management is a critical component of good cyber hygiene for any organization or individual. For organizations, it is vital not only for them to have processes and protocols for patching, but also to have inventory capabilities for these patches. For example, an organization's IT specialists should always know what IT systems it has, what dependencies these systems have on other systems, how important each system is, each system's vulnerabilities, and what would happen if these systems were to go offline.[48]

Patch management—the process for identifying, prioritizing, acquiring, installing, and verifying patches for products and systems—is imperative for information technology and information security managers. Also, one patch management process will likely not be able to handle every IT or operational technology device that an organization has, so specialists should find the right managing system for each use case to manage risk across the enterprise.[49]

The FICO® Cyber Risk Score

The FICO® Cyber Risk Score is an empirically derived metric that relies on a comprehensive and diverse set of cybersecurity risk signals, collected at internet scale, to measure the forward-looking security risk of any organization.

About

The signals leveraged by the algorithm comprise sector-related background risk information as well as key technical and behavioral risk indicators, including the scale and nature of the subject's internet-exposed systems, the health and hygiene of IT systems and network infrastructure, the maintenance of software and services exposed by the organization, and the construction and maintenance of the company website(s).

The time-series compilation of these signals allows FICO to assess not only the condition but also the organizational effectiveness in attaining and maintaining best practice security processes. These current and historical data signals are compared to past behaviors of organizations that have—and have not—suffered a material breach. This allows FICO to develop strong predictors of forward-looking risk.

These predictors are augmented by information indicating evidence of network or endpoint compromise. Rather than simply inventorying temporal vulnerabilities or issues, these indicators are used, in the aggregate, to help form an understanding of an organization's network hygiene practices, consistency in policy, and network management track record.

Together, this information is used to train a supervised machine-learning model that produces a risk score that quantifies the likelihood of a future breach event, based on more than six years of historical data. The objective outcome of this model is the measurement of material data breach risk over a forward-looking 12-month period, and the resulting score (ranging from 300 to 850) indicates FICO's assessment of the relative risk faced by the evaluated organization. The score-to-odds relationship is linear and doubles with each 84-point increment in the score (i.e., a company with a score of 500 is approximately twice as likely to suffer a material breach event in the next 12 months as a company with a score of 584).

Providing actionable insights

The FICO® Cyber Risk Score is engineered to provide actionable insights regarding security risk that encompass both technical and policy-related shortcomings. As in other risk management disciplines, multiple perspectives often yield better results. The FICO® Cyber Risk Score, and the underlying data it leverages, can provide a valuable second opinion that offers a clearer understanding of your cybersecurity risk as well as insights for possible actions to reduce risk; unlike most second opinions, this assessment is free.

FICO® Cyber Risk Score availability

FICO is committed to ensuring transparency and fairness in the security rating process. To help organizations better understand their specific situation, FICO offers free subscription access to a company-specific view of cyber risk.

Organizations can register for a complimentary, ongoing, no-cost subscription at https://cyberscore.fico.com.

This subscription to the FICO® Cyber Risk Score allows organizations to monitor the results of efforts to continually improve their security posture and reduce their risk of a security breach. With this subscription, organizations can also compare their performance within their sector and/or with organizations operating at a comparable scale—with an enhanced understanding of their relative risk posture. Companies many consider using tools such as the Cyber Risk Score to engage in meaningful dialogue with third-party partners and advance the goal of collaboration in managing cyber risk.

Benefits of FICO® Cyber Risk Score

Benchmark

Learn how your company's cybersecurity rates compare to others.

Remediate

Have a low score? Learn concrete steps and methods to improve it.

Supply-Chain Security

Learn how well your trusted partners scored in cybersecurity.

It's Free

Best of all, it's free. Just sign up to receive your complimentary score.

Partner and Contributor Recognition

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cybersecurity for organizations struggling to prepare for, prevent, and respond to cyberattacks.

A part of FireEye, Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce organizational risk.

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With over 5,000 employees in over 50 countries, and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their journey to the cloud.

Press

FICO

FICO (NYSE: FICO) powers decisions that help people and businesses around the world prosper. Founded in 1956 and based in Silicon Valley, the company is a pioneer in the use of predictive analytics and data science to improve operational decisions. FICO holds more than 190 U.S. and foreign patents on technologies that increase profitability, security, customer satisfaction, and growth for businesses in financial services, telecommunications, healthcare, retail, and many other industries. Using FICO solutions, businesses in more than 100 countries do everything from protecting 2.6 billion payment cards from fraud, to helping people get credit, to ensuring that millions of airplanes and rental cars are in the right place at the right time.

Learn more at www.fico.com.

Press inquiries:

Chaundera Wolfe
FICO
ChaunderaWolfe@fico.com
510-621-9832

U.S. Chamber of Commerce

The U.S. Chamber of Commerce is the world's largest business federation, representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

Learn more at www.uschamber.com/cyber-abc.

Press inquiries:

Kathleen Ward
U.S. Chamber of Commerce
kward@uschamber.com
202-463-5682

Appendix

1. Essential Critical Infrastructure Workers Guidance. Cybersecurity and Infrastructure Security Agency (2020). https://www.cisa.gov/publication/guidance-essential-critical-infrastructure-workforce
2. State-by-State Essential Workforce Tracker. U.S. Chamber of Commerce (2020). https://www.uschamber.com/tracking-essential-COVID-19-workers
3. Interestingly, the definition of "essential critical infrastructure workers" became more elastic in many people's minds during the early days of the pandemic, as we realized that long-haul and delivery truck drivers, grocery store employees, internet service provider call center employees, and first responders all were critical to the functioning of the U.S. economy. While important, and worthy of mention, this topic ultimately remains outside the scope of this report.
4. The COVID-19 Pandemic Through the Eyes of the Internet. Manish Karir, FICO (2020). https://www.linkedin.com/pulse/covid-19-pandemic-through-eyes-internet-manish-karir
5. COVID-19 Cyberwar: How to Protect Your Business. IBM (June 2020). https://www.ibm.com/downloads/cas/Y5QGA7VZ
6. Limited Shifts in the Cyber Threat Landscape Driven by COVID-19. Sandra Joyce, FireEye Mandiant Threat Intelligence (2020). https://www.fireeye.com/blog/threat-research/2020/04/limited-shifts-in-cyber-threat-landscape-driven-by-covid-19.html
7. Coronavirus Related Threats. Trend Micro (April 2020). https://resources.trendmicro.com/rs/945-CXD-062/images/Trend-Micro-Research-COVID19-Threat-Brief-Summary-13April.pdf
8. Id.
9. Protecting Businesses Against Cyber Threats During COVID-19 and Beyond. Google (April 2020). https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond
10. Securing the Pandemic-Disrupted Workforce: Trend Micro 2020 Midyear Report. Trend Micro (August 2020). https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/securing-the-pandemic-disrupted-workplace-trend-micro-2020-midyear-cybersecurity-report
11. 1H 2020 Cybersecurity Defined by Covid-19 Pandemic. Trend Micro (September 2020). https://www.trendmicro.com/en_us/research/20/i/1h-2020-cyber-security-defined-by-covid-19-pandemic.html
12. Securing the Pandemic-Disrupted Workforce: Trend Micro 2020 Midyear Report, Trend Micro (August 2020). https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/securing-the-pandemic-disrupted-workplace-trend-micro-2020-midyear-cybersecurity-report
13. There's Another Coronavirus Crisis Brewing: Fraud. The Wall Street Journal (April 2020). https://www.washingtonpost.com/opinions/2020/04/14/theres-another-coronavirus-crisis-brewing-fraud/
14. Id.
15. Hackers Trigger Far-Reaching Disruption by Targeting Low-Profile Firm. The Wall Street Journal (June 2020). https://www.wsj.com/articles/hackers-trigger-far-reaching-disruption-by-targeting-low-profile-firm-11592481600
16. For more information, visit: https://us-cert.cisa.gov/ncas/alerts, https://www.ic3.gov/ and https://www.dni.gov/index.php/ncsc-features/2762
17. Getting Serious About Cybersecurity. CO – by U.S. Chamber of Commerce (July 2020) https://www.uschamber.com/co/co-brandstudio/dell/top-cybersecurity-tips-from-dell
18. Remarks by Michael D'Ambrosio. U.S. Chamber of Commerce Cyber Series: Chicago (2020). https://vimeo.com/442723476
19. Coronavirus-Related Threats. Trend Micro (April 2020). https://resources.trendmicro.com/rs/945-CXD-062/images/Trend-Micro-Research-COVID19-Threat-Brief-Summary-13April.pdf
20. Exploiting a Crisis: How Cybercriminals Behaved During the Outbreak. Microsoft (June 2020). https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/
21. Cyber Threats in Turbulent Times. Black Hat (June 2020). http://images.blackhat.com/Web/UBMAmericasTech/%7B0124507e-2c42-4bbc-be14-7ac23df919c8%7D_BHUS20_AttendeeReport.pdf
22. Suddenly Essential Infrastructure: Cloud Computing Resources at the Forefront of the COVID-19 Crisis. Infospace (April 2020). https://ischool.syr.edu/infospace/2020/04/01/suddenly-essential-infrastructure-cloud-computing-resources-at-the-forefront-of-the-covid-19-crisis/
23. Clouds Are Secure: Are You Using Them Securely? Gartner (October 2019). https://content.fireeye.com/cloud/rpt-gartner-clouds-are-secure-are-you-using-them-securely

24. Id.
25. Top 5 Cloud Security Myths Debunked. FireEye (2020). https://content.fireeye.com/cloud/eb-top-5-cloud-security-myths
26. Oracle and KPMG Cloud Threat Report. Oracle & KPMG (2020). https://www.oracle.com/a/ocom/docs/cloud/oracle-cloud-threat-report-2020.pdf
27. Id.
28. Suddenly Essential Infrastructure: Cloud Computing Resources at the Forefront of the COVID-19 Crisis. Infospace (April 2020). https://ischool.syr.edu/infospace/2020/04/01/suddenly-essential-infrastructure-cloud-computing-resources-at-the-forefront-of-the-covid-19-crisis/
29. Id.
30. Id.
31. Telework Security Basics. NIST (March 2020). https://www.nist.gov/blogs/cybersecurity-insights/telework-security-basics
32. Id.
33. User's Guide to Telework and Bring Your Own Device (BYOD) Security. NIST (July 2016). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf
34. Id.
35. Trends in VPN Abuse During COVID-19. FireEye Mandiant Threat Intelligence (July 22, 2020).
36. Preventing Eavesdropping and Protecting Privacy on Virtual Meetings. NIST (March 2020). https://www.nist.gov/blogs/cybersecurity-insights/preventing-eavesdropping-and-protecting-privacy-virtual-meetings
37. Guidance for Securing Video Conferencing. CISA (May 2020). https://www.cisa.gov/publication/guidance-securing-video-conferencing
38. Note: The NIST report refers to "low risk," "medium risk," and "high risk" calls. We have elected to describe the calls instead in terms of the sensitivity of the information being discussed.
39. Preventing Eavesdropping and Protecting Privacy on Virtual Meetings. NIST (March 2020). https://www.nist.gov/blogs/cybersecurity-insights/preventing-eavesdropping-and-protecting-privacy-virtual-meetings
40. Assessment for Business Cyber Risk. U.S. Chamber of Commerce (September 2019). https://www.uschamber.com/cyber-abc#/
41. U.S. Chamber of Commerce and FICO. Assessment for Business Cyber Risk (July 2020). https://www.uschamber.com/cyber-abc#/
42. User's Guide to Telework and Bring Your Own Device (BYOD) Security. NIST (July 2016). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf
43. To "jailbreak" means to allow the phone's owner to gain full access to the root of the operating system and access all the features. "Rooting" is the term for the process of removing the limitations on a mobile or tablet running the Android operating system. https://www.mcafee.com/blogs/consumer/identity-protection/how-does-jailbreaking-or-rooting-affect-my-mobile-device-security
44. Id.
45. User's Guide to Telework and Bring Your Own Device (BYOD) Security. NIST (July 2016). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf
46. A How-to-Guide for Multi-Factor Authentication. CISA, CSA, and CyberAware (October 2019). https://niccs.us-cert.gov/sites/default/files/documents/pdf/ncsam_howtoguidemfa_508.pdf?trackDocs=ncsam_howtoguidemfa_508.pdf
47. Patch Definition. NIST (2020). https://csrc.nist.gov/glossary/term/patch
48. Critical Cybersecurity Hygiene: Patching the Enterprise. NIST and NCCoE (August 2018). https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/ch-pe-project-description-draft.pdf
49. Id.

Learn more about your FICO® Cyber Risk Score by registering for a complimentary subscription at cyberscore.fico.com.


FICO™
Cyber Risk Score
THE SPIRIT OF ENTERPRISE
U.S. CHAMBER OF COMMERCE
U.S. CHAMBER OF COMMERCE