AlixPartners

COVID-19 RESPONSE

Privacy and Cybersecurity Concerns: Companies must reassess the security of their remote work infrastructure

May 2020

As cities and states started to implemented shutdowns in response to COVID-19 in mid-March, many companies made an unprecedented decision to move a large portion of their staff to remote work nearly overnight.

It was a quick fix to maintain operations in the face of a global emergency, but many technology leaders are worried about the security vulnerabilities presented during this rapid expansion of remote connectivity.

The risks are real and growing. More than one-third of companies have experienced an increase in cyberattacks since the wave of remote work began, according to a survey from the CNBC Technology Executive Council.

Now more than ever, employers must quickly assess their cybersecurity infrastructure and mitigate the risks of their expanding digital footprint.

Remote work opens security vulnerabilities

As of mid-April, more than 60 percent of American workers said they had worked remotely, more than double the rate before the pandemic, according to a Gallup poll.

Although the quick move to work from home enabled employers to maintain operations, it has exposed them to long-term security challenges as many overlooked the standards typically followed when implementing new technologies.

Collaboration tools like Zoom, Slack, and Invision have enabled teams to communicate, share files, and work together from their homes, but they're a growing area of concern. Many of these tools lack strong cybersecurity compliance policies and are vulnerable to cyberattack. The FBI noted in a public service announcement in early-April that criminals have been specifically targeting video conferencing software, voice over Internet Protocol (VOIP), and other communication tools to access sensitive information or enact Business Email Compromise (BEC) scams.

While employees may adhere to rigid security protocols at the workplace, they're not necessarily doing so in their homes. Lax Bring Your Own device policies, lack of oversight, the challenges of working from home, and the use of 'free' cloud storage platforms have created unacceptable security risks. For example, an accounting clerk who takes handwritten notes while working from home or sends a colleague information through personal email could put customer information at risk.

Finally, employers may be violating regulations and legal compliance by allowing their employees to work from home without the right policies and infrastructure in place. It's even more concerning in heavily regulated industries like healthcare and financial services where employees regularly handle sensitive information. For instance, a billing processor who accesses and stores unencrypted information on a personal device is in violation of the Health Insurance Portability and Accountability Act.

AlixPartners

Quickly prioritize and mitigate the most dangerous risks

Now that many companies have re-established operations with a network of remote employees, it's time to turn the focus back to IT security by assessing the digital connectivity and collaboration infrastructure.

Technology leaders should evaluate the potential vulnerabilities of their newly added remote work technologies within the seven layers of the security architecture (data, application, host, network, perimeter, physical, and policies). They can work from the list of vulnerabilities to prioritize risk mitigation initiatives based on the probability of occurrence and the potential adverse impact. The next step is to identify what vulnerabilities are the most dangerous and need to be addressed first. In some cases, this may mean de-emphasizing low impact and low probability risks until the most import ones—like theft of social security numbers and financial information—are mitigated.

After they develop procedures and policies to address these most prioritized risks, they should then execute through agile teams led by business owners who can best handle those initiatives. For instance, the HR director should lead any initiative involving employee information, while the head of sales should lead the initiative to comply with the California Consumer Privacy Act.

Organizations must now act swiftly as they can't afford to spend months or years implementing security, privacy, or compliance guidelines. One way to fast-track an effort is to focus on business ownership of risk categorization and tap the senior business leadership best-prepared to make those decisions around mitigation. CSOs and technology leaders must forge partnerships with all department heads as they alone cannot consider all factors in the era of things like SaaS, BYOD, and cloud storage.

Finally, organizations can close their security gap faster and more effectively by finding partners with hands-on experience in solving similar problems.

While employers are uncertain for how long and to what extent COVID-19 will impact the workplace, any long-term model of digital transformation and remote work will have to be driven with privacy and cybersecurity at the forefront.

AlixPartners

Contacts

We deploy teams of highly experienced and qualified experts with profound situational and operational insight to support our clients in times of crisis.

Abhinav Agrawal

aagrawal@alixpartners.com

+1 214 458 8530 (mobile number)

Angela Zutavern

azutavern@alixpartners.com

+1 703 462 4274 (mobile number)

Catherine Sherwin

csherwin@alixpartners.com

+33 6 45 75 19 52 (mobile number)

Tim Roberts

troberts@alixpartners.com

+44 7768 424 095 (mobile number)

About AlixPartners

AlixPartners is a results-driven global consulting firm that specializes in helping businesses successfully address their most complex and critical challenges. Our clients include companies, corporate boards, law firms, investment banks, private equity firms, and others. Founded in 1981, AlixPartners is headquartered in New York, and has offices in more than 20 cities around the world. For more information, visit www.alixpartners.com.

The opinions expressed are those of the authors and do not necessarily reflect the views of AlixPartners, LLP, its affiliates, or any of its or their respective professionals or clients. This article Covid-19 Response ("Article") was prepared by AlixPartners, LLP ("AlixPartners") for general information and distribution on a strictly confidential and non-reliance basis. No one in possession of this Article may rely on any portion of this Article. This Article may be based, in whole or in part, on projections or forecasts of future events. A forecast, by its nature, is speculative and includes estimates and assumptions which may prove to be wrong. Actual results may, and frequently do, differ from those projected or forecast. The information in this Article reflects conditions and our views as of this date, all of which are subject to change. We undertake no obligation to update or provide any revisions to the Article. This Article is the property of AlixPartners, and neither the Article nor any of its contents may be copied, used, or distributed to any third party without the prior written consent of AlixPartners.

©2020 AlixPartners, LLP

# # #