# Securing Virtual Workforces

Our Cybersecurity Best Practices

## TABLE OF CONTENTS

Guidance for Security Leaders 3

What to communicate right now 3

Open up your business continuity and resumption plan (BCRP) 3

Validate your security posture 3

Get a cybersecurity awareness communication out 4

Launch an email phishing campaign 4

Partners and vendors can help 4

Compliance posture concerns 4

Revisit your SLAs 5

Is now the time to implement a change? 5

Guidance for Your Employees 6

Be aware of COVID-19 phishing and malware 6

Video conferencing security and privacy issues 6

Use approved devices for company work 6

Keep your laptop and software up-to-date 6

Guidance for Everyone 7

Be on high alert for online scams 7

Make sure your corporate passwords will not expire soon 7

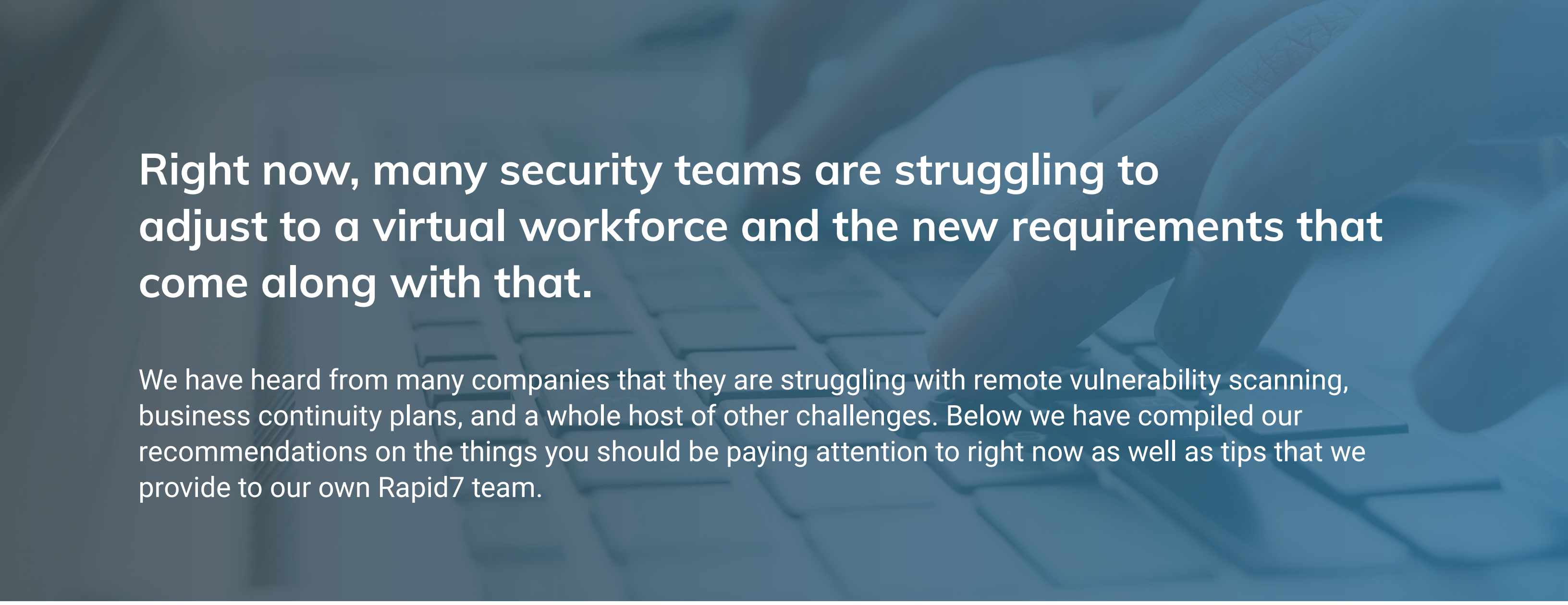
Check your WiFi connection 8

Check your VPN connections 8

We're in This Together 9

Contributors 9

About Rapid7 9



**Right now, many security teams are struggling to adjust to a virtual workforce and the new requirements that come along with that.**

We have heard from many companies that they are struggling with remote vulnerability scanning, business continuity plans, and a whole host of other challenges. Below we have compiled our recommendations on the things you should be paying attention to right now as well as tips that we provide to our own Rapid7 team.

# Guidance for Security Leaders

## What to communicate right now

Communication between security leaders and their executive leadership team should occur as usual. During times of distress, communication becomes even broader and more visible. The things to focus on right now should be aligned to your business's priorities around resilience, employee productivity, customer success, and operational reliability. Make sure to articulate how cybersecurity can impact those areas as operating change occurs and what material impact the change has to your cyber-risk posture (where applicable). It will also be necessary to make adjustments in security controls and operational systems, and understanding how compensating controls can negate exposure will be critical. The message should be the same to your team. Make sure they understand that right now it is time to over-communicate to you and other security leaders. Staying in close contact and virtual proximity will allow everyone to do their jobs, albeit using slightly different approaches.

## Open up your business continuity and resumption plan (BCRP)

Whether you are opening up your BCRP because you need to use it or are just dusting it off to make sure it's ready, now is the time to start thinking through how your company will operate in a work-from-home scenario, at a reduced operating level, or just with essential personnel. The BCRP for continued IT and security operations ensures your company is able to operate in various situations and determines what you would do in these operating modes should a cyber-incident occur.

One of the most important sections of a BCRP is the contact list. Make sure you and all of your teammates have this plan printed out at home, and that you have an updated list of both cell phone and landline numbers available.

If it has been a while and you are not opening this document to put it into immediate use, now is the time to test it out in a tabletop exercise (TTX), even if only with a small group of people. There is no better time than the present to ensure everyone knows what you are going to do and how people will stay connected to keep operations running.

## Validate your security posture

Spend some time working with both your security and IT teams to ensure your critical systems are up-to-date and patched, such as your endpoint detection, intrusion detection systems, web content filters, VPN clients, and MFA/2FA token generators. Focusing time on making needed changes or updates now means you won't need to do these activities should remote work become mandatory for everyone.

If remote work has already become a necessity or a mandate, take inventory of what state your security infrastructure is in and have your team surface any issues or gaps with the current posture. You want to try to avoid performing a major, unplanned upgrade in uncertain times, and preparing and planning for it sooner rather than later will help ensure the change is a success.

## Get a cybersecurity awareness communication out

Now is an excellent time to get an awareness communication out to your organization that focuses on the things your employees need to be thinking about while working from a location other than the office. Key messages to convey include ensuring your VPN can support the load, protecting corporate data by only using authorized storage systems (cloud or on-premises), and making employees aware of their digital surroundings.

## Launch an email phishing campaign

At times like this, your employees are getting hit with all kinds of malicious emails. Now is the time to double down on helping them identify and report malicious emails. Attackers are only going to continue turning up the pressure and increasing their sophistication as this pandemic continues to unfold. Keeping your company's resources on their toes and giving them the training and tools to help reduce the likelihood of a cyber exposure via phishing and social engineering will enable your security team to keep focused on higher level threats and not distracted by low sophistication threats users can easily identify and thwart themselves.

## Partners and vendors can help

Trusted partners and vendors are motivated to help you navigate this situation, and some are even allowing existing and new customers free temporary licensing to deal with the surge capacity created from a new model where everyone works from home. This approach, where your partners and vendors can really show the partnership and value of the relationship, will enable you to continue to deliver quality services to your employees and your customers.

## Compliance posture concerns

As your company's security leader, one of the many questions you may be receiving is, "Are we going to be able to maintain our compliance posture?" In a perfect world, compliance becomes a by-product of a well-run and finely tuned security program. However, in times of uncertainty, security controls may need to be partially relaxed to give way to immediate employee and customer needs.

Those trade-offs need to be carefully considered and documented. While the temporary risk tolerance adjustments may be appropriate given the current situation, they could come at a cost of impacting the organization's compliance. After all, there's nothing quite so permanent as a temporary fix. Focus on the areas where the risks cut across the compliance, and make sure you are expressing those to your executive teams.

**In times of unrest and uncertainty, it is our time to really make an impact, but in order to do so, we need to present our perspectives in a way that paints a continuity focus picture and not an obstructionist one.**

## Revisit your SLAs

One of the main things your entire organization is going to be focused on is service delivery, both to your customers as well as to your employees. Many businesses will struggle with this, and as the organization's security leader, your role is to help inform the areas where risks could be realized and impact the business.

Whenever there is an issue in the non-virtual world, the cyber-scammers and crooks launch campaigns aimed at taking advantage of uncertainty and people's fears. These are things you need to anticipate and communicate as potential situations that could affect business operations. Within the security team, now is the time to have the conversation about how you will detect and respond to these attacks and what steps you need to take now in order to be prepared.

## Is now the time to implement a change?

Another question you may face is whether now is the right time to go live with a big change or implementation project. That can be a tricky decision to make. Generally, now is probably not the right time to be making significant changes to business systems, but changes that can help support or enhance the security posture while enabling additional employee productivity are likely going to be a good thing.

Often in the security world, practitioners are viewed as paranoid obstructionists. In our mind, we are focused on providing a high level of support to our companies and ensuring that someone is thinking of all the bad things that could happen so the business can continue to operate. In times of unrest and uncertainty, it is our time to really make an impact, but in order to do so, we need to present our perspectives in a way that paints a continuity focus picture and not an obstructionist one. So, if you have been working on or need to make a change, now more than ever make sure you are looking at the benefit through the eyes of the executive leaders and ensure you can explain how your goals align to the company objectives.

# Guidance for Your Employees

## Be aware of COVID-19 phishing and malware

Attackers are taking advantage of COVID-19 by spreading malware and sending phishing emails that claim to, for example, offer information about virus outbreaks. Stay extra vigilant and keep an eye out for suspicious emails related to COVID-19. If you suspect any abnormal emails generally, but in recent times specific to COVID-19, report them to your security team.

## Video conferencing security and privacy issues

With increased usage of video teleconferencing, any security and privacy issues associated with video chat tools have become more business critical and likely a greater focus for attackers.

There can be privacy issues with personal meeting IDs. We strongly recommend avoid using personal meeting IDs whenever possible and use unique meeting IDs instead. This will help avoid, for example, attendees of an upcoming meeting joining one that's running over and overhearing - or seeing - sensitive information.

If you are using Zoom like many businesses are, "Zoom-bombing" is officially a thing! People are starting to intentionally crash other people's Zoom meetings by taking advantage of lax security settings on people's Zoom meetings. Check out Zoom's official guidance on how you can protect your Zoom meetings from Zoom-bombing (including avoiding using Personal Meeting IDs).

## Use approved devices for company work

It's very important that everyone use their company issued laptops to do company work, rather than personally-owned laptops or tablets. This is normally an expected practice as company issued laptops have various security settings and software installed on them to help protect from cyberattacks. Using a personal computer to access company systems/apps and data puts your company and customers at risk of being compromised.

## Keep your laptop and software up-to-date

You can help your InfoSec and IT teams by keeping your laptop operating system and all software up-to-date. Take some time now to ensure all applicable updates are applied—**especially your web browsers, which are at an increased risk of being targeted/ exploited by attackers.**

# Guidance for Everyone

## Be on high alert for online scams

In times of uncertainty, we should anticipate bad actors looking for an opportunity to capitalize. This could be through phishing emails, financial scams, or other tactics that prey on human nature.

Fortunately, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) is monitoring and notifying the general public on cybersecurity scams related to COVID-19 and has provided the following guidance:

- Avoid clicking on links in unsolicited emails and be wary of email attachments. See Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Scams for more information.
- Use trusted sources—such as legitimate, government websites—for up-to-date, fact-based information about COVID-19.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
- Verify a charity's authenticity before making donations. Review the Federal Trade Commission's page on Charity Scams for more information.
- Review CISA Insights on Risk Management for COVID-19 for more information.

While at home, it may be a good time for you to review your company's security awareness communication regarding remote working and stay up-to-date with any new guidance as company plans and protections are likely to evolve over the coming days and weeks. Although it may be tempting or seem appropriate to fast track or bypass some of the processes or controls laid out, we advise against it. Internal controls and processes are in place for a reason and must be followed to avoid scams, and in some cases, ensure compliance with external regulations.

## Make sure your corporate passwords will not expire soon

Everyone's experienced some challenges when it comes to changing passwords and it can become even more difficult and complex to change your password when you are not in the office.  Check to see if your password is expiring in the near future and make sure you know how to change it. Also consider checking with  your IT team beforehand to ensure all systems for remote password changes are in order. The risk here is that your password expires while you are out of office. Once you're locked out from the corporate network, it can be difficult to get yourself back online while remote.

## Check your WiFi connection

As many of our work laptops or mobile devices auto-connect to WiFi networks, check to ensure that you are connected to your home network (or intended hotspot). You might be surprised that you are connected to a public hotspot offered by a broadband provider or a nearby neighbor's WiFi network. To ensure you have the utmost privacy, just check your WiFi settings and ensure you are on the network you intend to be on.

## Check your VPN connections

Everyone does remote work a little differently, but most of us have some kind of VPN solution that gets us to critical internal systems we need to do our jobs. Please resist the urge to rig up your own RDP, VNC, or SSH tunnel (okay, maybe that last one, but only if you really know what you're doing). Those solutions tend to mean poking holes in your firewall, unintentionally exposing stuff. Additionally, you probably haven't instrumented your endpoints with logging, brute force resistance, or otherwise hardened them for the wild and wooly internet. Even if it's "just temporarily" open, there's nothing quite so permanent as a temporary fix. We promise, your IT department is there for you, and probably has a few extra licenses for a professionally managed VPN solution. And, if you haven't exercised your VPN in a while, now is a great time to test it out. Better to find out that your VPN is busted now rather than later when the support requests really start to pile up.

# We're in This Together

We are all impacted in different ways. We know that we are all trying to accomplish a lot of the same things, and now is a time for finding new and creative ways to work together. If there have been silos in your organization in the past, focusing on how to break those down will serve you well now and when the world normalizes again. Just know that you are part of a much broader community, and don't be afraid to reach out, share information, and definitely ask for help when you need it. We are here to support you.

## Contributors

This paper would not have been possible without the expertise and knowledge of our Rapid7 team—thank you.
We compiled this paper from invaluable guidance contributed by:

Tod Beardsley - Director of Research

Jonathan Beggs - Security Operations Lead

Scott King - Senior Director Security Advisory Services

Bob Rudis - Chief Security Data Scientist

Shawn Valle - Chief Security Officer

## About Rapid7

Rapid7 is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Our customers rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations.