CISO COUNCIL SERIES: LESSONS FROM REMOTE WORKFORCE TRANSITIONS

A Special Publication from Ping Identity's CISO Advisory Council

TABLE OF CONTENTS

INTRODUCTION

As security leaders, a primary responsibility to our organizations is to make decisions using proven security frameworks, which lay out cybersecurity best practices for organizations of any size and type. But these frameworks aren't all-knowing, and they can't predict the impacts of a global pandemic like COVID-19. This is why peers play an equally important role in guiding our decisions.

On April 2, 2020, the Ping Identity CISO Advisory Council convened remotely to share the organizational challenges we've faced during this unprecedented, rapid transition to a nearly 100% remote workforce. The CISO Advisory Council comprises CISOs from enterprise organizations spanning industries including financial services, healthcare, manufacturing, energy, telecommunications, education, technology and life sciences.

In this paper, you'll read about how each organization in the council is addressing COVID-19 challenges and working toward solutions, along with common themes across the group.

HOW COVID-19 HAS IMPACTED OUR BUSINESSES

No enterprise is immune from the effects of COVID-19. As we all attempt to make sense of the "new normal," organizations find themselves in different stages, with geographic, industry and regulatory factors all playing a role.

> Our oil and gas operations are considered critical infrastructure, so we're keeping manufacturing facilities open but taking the temperature of anyone entering the facility. We were fortunate that our Houston office made the transition to remote work after we had lessons learned from our European offices' shifts to work from home. Of course, it's never a good time for these types of things to happen, but simultaneously handling a global price war on oil is compounding the challenges we're facing at this time.
>
> -CISO, Energy Services Company

> Paying health claims in a timely manner has never been more important, and we're here to support our members during this emergency. We have 7,000 employees, many of whom had never worked remotely before. Today, 98% of them are enabled to work remotely. We only wish we could do more to support our community of healthcare providers, as many critical health services considered elective have been halted for the time being.
>
> -CISO, Health Insurance Provider

> As an internet provider, we're receiving conflicting guidance that makes planning difficult. State guidelines don't consider our retail stores as critical infrastructure that can remain open while quarantine measures are in place. At the same time, the federal government prefers that our stores stay open so people without existing service can sign up.
>
> -CISO, Telecommunications Provider

> A number of our employees in our Chinese manufacturing facilities contracted the virus, which meant the temporary closure of these facilities. We were able to weather some, but not all, of the impact by shifting manufacturing to US facilities where possible. We are fortunate that our Chinese facilities had come back online by the time our European and North American factories were significantly impacted.
>
> -CISO, Manufacturing Company

HOW WE'RE ADAPTING AND HELPING OUT ONE ANOTHER

In this time of upheaval and uncertainty, organizations are finding creative ways to make the transition to a remote workforce as successful as possible. Designating new roles for employees, opening up access to resources and thinking up innovative solutions are just some of the ways the group is supporting their workforce and customers.

> Online learning is serious business, and we're always on the lookout for potential disruptions. A few months ago we tested our disaster recovery strategy in response to the potential for a pandemic related to COVID-19. However, nothing could have prepared us for the doubling and tripling of traffic as we moved to make many of our applications free for teachers to take their classes online. We now have a 24x7 war room staffed to find ways we can support the massive influx of newly online classrooms.
>
> **-CISO, Online Education Provider**

> To ensure we could immediately pay out worker compensation claims related to COVID-19, we needed to recode all of our systems in a matter of days. The extra efforts our employees are making to support people who have been financially impacted by the virus are extraordinary. While reporting on the success of the work from home transition, we found that employees are logging in earlier and logging off later.
>
> **-CISO, Workers Compensation Insurance Provider**

> As a lender to many companies who will struggle to maintain financial stability throughout this crisis, we need to be able to continue to both operate and raise capital without interruption. We transitioned to a 95% remote workforce over the course of 24 hours, and are currently taking steps to ensure any system that isn't currently accessible remotely will be soon.
>
> **-CISO, Financial Services Organization**

> For the past few years, we've been highly focused on transitioning care delivery and associated medical services to digital where possible. As a result, many in our patient population are still receiving the care they need. We're now focused on repurposing physicians and medical staff who are unable to provide in-person care to roles such as building face shields from home.
>
> **-CISO, Healthcare Provider**

> We had to cancel our annual meeting, where our scientific society comes together to share research efforts and findings. To support the important research that was supposed to be shared at the meeting, we're launching a virtual platform so it can still be shared and cited. Furthermore, we've made access to all of our publications and research completely free of charge if you're working on anything related to COVID-19.
>
> **-CISO, Scientific Society**

WE'RE OUT OF COMPUTERS AND DON'T PERMIT BYOD...YET

Do individual organizations have the resources necessary to enable their offsite workforce? A near universal trend among the council is an insufficient amount of hardware to rapidly support remote work at scale, coupled with the need to reconsider a bring-your-own-device (BYOD) program in light of the shortage.

> Emergency stockpiles of spare laptops have not been enough to support the number of employees who need to work from home. We're working with suppliers to get additional laptops, but of course everyone is doing this at the same time and lead times are excessive. Many of our office workers were able to simply take their laptops home, but we have many in production facilities who use desktops. With our limited stock, we've imaged and deployed laptops and set up VPN connections to enable them to work from home, while limiting connection to our network from these devices only for the time being.
>
> -CISO, Manufacturing Company

> Like many companies, we've frozen hiring for the time being, but there were candidates already in progress that we brought on board in the past few weeks. The majority of our employees have laptops and work from home often, so we've never needed a BYOD program. But because of the laptop shortage it's now a necessity, as we have no way of getting computers to these new people.
>
> -CISO, Online Education Provider

WE'RE STEPPING ON THE GAS WITH MULTI-FACTOR AUTHENTICATION (MFA)

Not surprisingly, the rapid expansion of secure remote access technologies is a common theme for many organizations. Multi-factor authentication is toward the top of the list.

> We were already modernizing MFA from RSA SecurID to PingID, but in the past few weeks this project has been accelerated. Why? Because we didn't have enough RSA hard tokens to go around!
>
> **-CISO, Telecommunications Provider**

> We've always had a pretty good MFA story, but right now we're going through all of our systems and infrastructure to ensure we have full coverage. This seems to be a common thread amongst all of my peers.
>
> **-CISO, Online Education Provider**

> State restrictions mandated that we shut down non-essential care. In light of this, we've done everything in our power to repurpose furloughed nurses and physicians, which has meant enabling them to access patient data from outside of work, sometimes on personal devices. For this scenario, MFA is a requirement.
>
> **-CISO, Healthcare Provider**

THE INTERNET AND COMMUNICATIONS PLATFORMS ARE OVERWHELMED

As conversations move from in-person to online, the transition isn't always seamless. But the group is finding ways to maintain communication and productivity.

> The Department of Health and Human Services relaxed some of the HIPAA provisions governing online healthcare interactions. So long as it's a 1:1 caregiver to patient interaction, we're permitting physicians to use non-traditional video platforms like FaceTime and Google Duo to deliver virtual care.
>
> -CISO, Health Insurance Provider

> Our network wasn't built to maintain the type of load where every kid in the state is either watching Netflix or playing Xbox, while simultaneously both parents are on a Zoom conference call. We're in the process of moving hotspots around and rerouting traffic, with a focus on keeping hospitals connected.
>
> -CISO, Telecommunications Provider

> We're reprioritizing network routing so that care delivery functions receive network priority over administrative functions. However, many of our physicians are working from home sharing their networks with 2-3 children and a spouse, presenting bandwidth challenges that are difficult for us to address.
>
> -CISO, Healthcare Provider

WE MUST BEEF UP SECURITY HARDENING AND AWARENESS AS ATTACKS RISE

Scammers and other bad actors are exploiting the uncertainty and fear caused by the pandemic, and it's happening online as well as off. Phishing attacks related to COVID-19 have increased exponentially, so organizations are intensifying awareness efforts to combat them.

> We're seeing an increase in nefarious attack activity against our infrastructure, so we've accelerated hardening and ramped up security awareness training efforts.
>
> -CISO, Online Education Provider

> We built a dedicated website for work from home best practices and cybersecurity tips, including how to spot and report phishing emails.
>
> -CISO, Energy Services Company

SECURITY CONTROLS ARE CHANGING IN THE NEW PARADIGM

A number of common security controls simply cannot persist in this environment, so many enterprises are relaxing them.

> We have a large reliance on offshore vendors, many of whom requested security liability waivers as employees transition from heavily locked down call centers to working from home. To offset the new lack of physical controls, we're ramping up communication surrounding what it means to be a good steward of patient data. Using privacy screens and locking laptops before walking away are just some of the ways to be an effective steward.
>
> -CISO, Health Insurance Provider

> We've created a risk register to log all exceptions that are made and holes that are opened. We need to make sure exceptions being made today are documented to ensure we know to close them.
>
> -CISO, Energy Services Company

WE'RE ANTICIPATING THE RETURN OF (FORMERLY) SECURE DEVICES

Many enterprises have allowed employees onsite to collect workstations, monitors and printers for use in home offices. But as organizations envision a day when those devices return to the main office, they're asking themselves now how they can best get ready for that eventuality.

> Our engineers need high-powered workstations, not laptops, to perform in their jobs. So we've allowed them to take their equipment home. But after months on home Wi-Fi, these devices won't be as secure as they once were.
>
> **-CISO, Energy Services Company**

> Soon, we'll be planning how to bring people back on a staggered basis. How do we reintroduce hardware that was formally secure but now has been operating on the public internet?
>
> **-CISO, Scientific Society**

DIGITAL IS NO LONGER A NICE TO HAVE

Across the board, it has been an easier transition for those who implemented or tested work from home before the onset of COVID-19. Organizations are wondering: What else should we test now to prepare for the future?

> We started testing work from home three years ago to reduce the productivity impact of snowstorms. Because of this, the transition to working from home has been seamless for many of our employees. Today, the majority of our systems are accessible remotely, and for those that aren't, we're currently looking for ways to enable remote access in the near future.
>
> **-CISO, Financial Services Organization**

> We're seeing manual, mail-based processes crumble in this new reality. Our regulators sent everyone home and they had no way to access documents sent via mail. This forced us quickly to implement digital solutions in days, not weeks or months, which are already saving time, speeding reporting, and saving significant work for our regulators. They are thrilled.
>
> **-CISO, Workers Compensation Insurance Provider**

FINALLY, WE ALL NEED A BREAK TO RELAX

At the end of the call, council members shared laughs as everyone realized that regular, virtual happy hours had been implemented independently across organizations.

> We have a virtual happy hour twice a week at 5 pm and everyone is required to wear a funny hat.
>
> -CISO, Scientific Society

> We have a virtual happy hour once a week, and the conversation is never about work. We're also being careful to make sure our employees are taking time off, even if they're not going anywhere.
>
> -CISO, Financial Services Organization

Without time-tested best practices to rely upon, it's never been more important to trust our peers and stay in close contact to share our experiences. If you're interested in more information on this topic, we invite you to read Work From Home: How to Keep Employees Productive and Secure.