Adjusting to Extraordinary Times

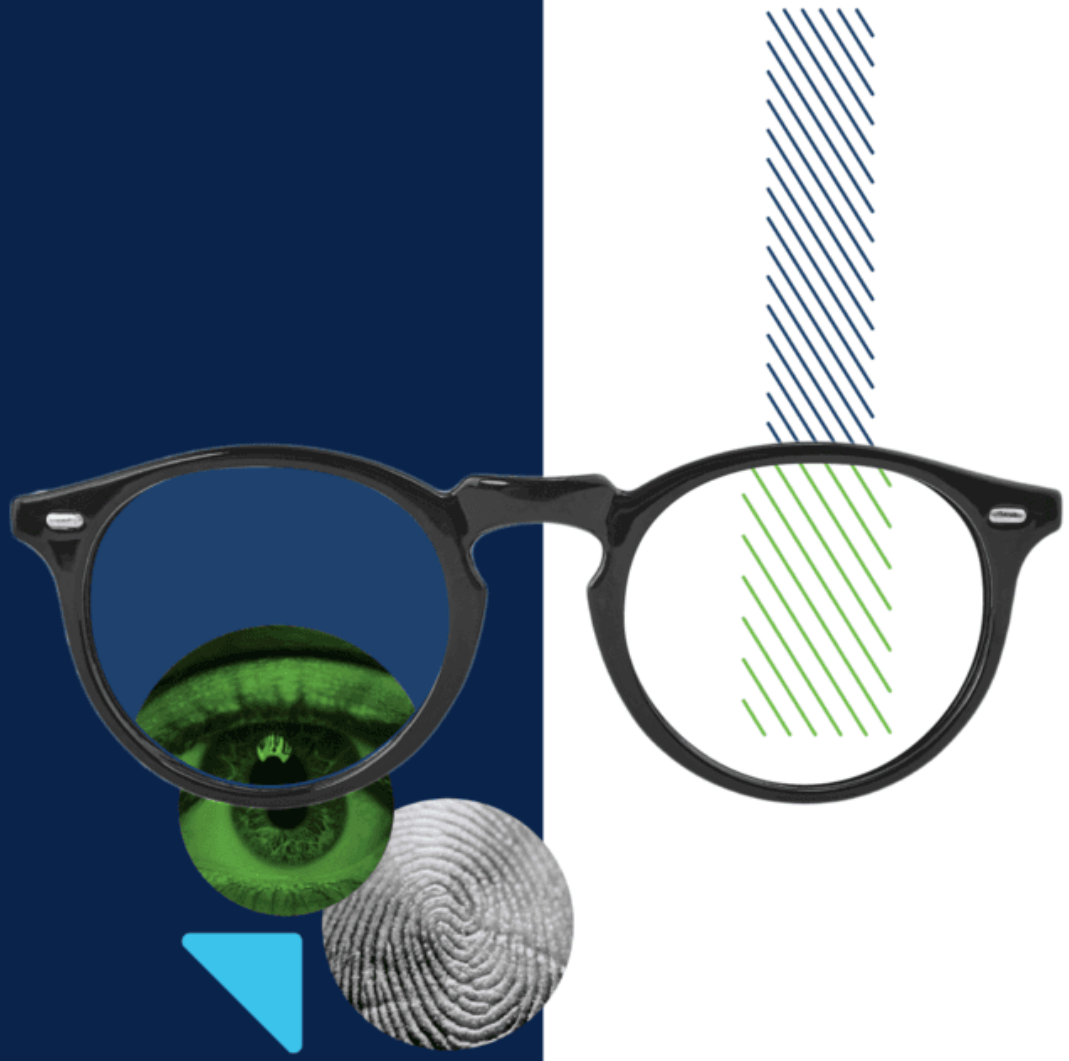
Tips from Cybersecurity Leaders Around the World

cisco The bridge to possible

In cybersecurity we often turn to other people and ask what they would do in tough situations.

This year (2020) has seen more than a few crises, and the cybersecurity landscape has changed dramatically. We asked security leaders about their experiences amidst these immense pressures. And share their stories here, for the benefit of the wider community.

In this eBook, you'll also find out some of the unexpected (and sometimes positive) outcomes that have arisen as a result of adjusting security through extraordinary times.



This eBook contains a kaleidoscope of cybersecurity views, insights, and advice about how to adjust during extraordinary times.

We have gathered responses from a wide range of people across the world. Those who have been kind enough to share their stories with us have done so for the benefit of the greater cybersecurity community.

We hope this resource is a useful tool for anyone looking to gain insight into the strategies and tactics other organizations have used to keep fighting the good fight.

Chapter 1

Adjustments and outcomes:
Experiences from security leaders

Chapter 2

What has the experience been like for you as a security leader during this time, and what have you put into practice or learned as a result?

Sandy Dunn

Chief Information Security Officer

Our organization has had the technical ability to work remotely in place for a while, but since we are a smaller, single state entity, **the culture was accustomed to having meetings and serious discussions in person.** To remediate being unable to observe people in person, the team is making an extra effort to do mental health check-ins with each other, watching each other for symptoms of burnout or high stress, and adding video to our online meetings.

The team is making an extra effort to do mental health check-ins with each other, watching each other for symptoms of burnout or high stress.
Sandy Dunn

@subzer0girl | LinkedIn

Chris Leach

Senior CISO Advisor, Cisco

The CISO is much more than the security expert. **Today's CISO is a strategist, master influencer and arbitrator**, and they are skilled with budgets, business processes and HR issues.

This crisis adds an even bigger dimension for the CISO. I am certain we will see regulatory requirements for a pandemic preparedness response forthcoming. The regulatory approach will lag; we need to be more proactive and plan now, but the analysis should not come in the form of specific incidents (e.g. pandemic; earthquake and other natural disasters; denial of service attack; ransomware). We need to plan on resilience based on business needs.

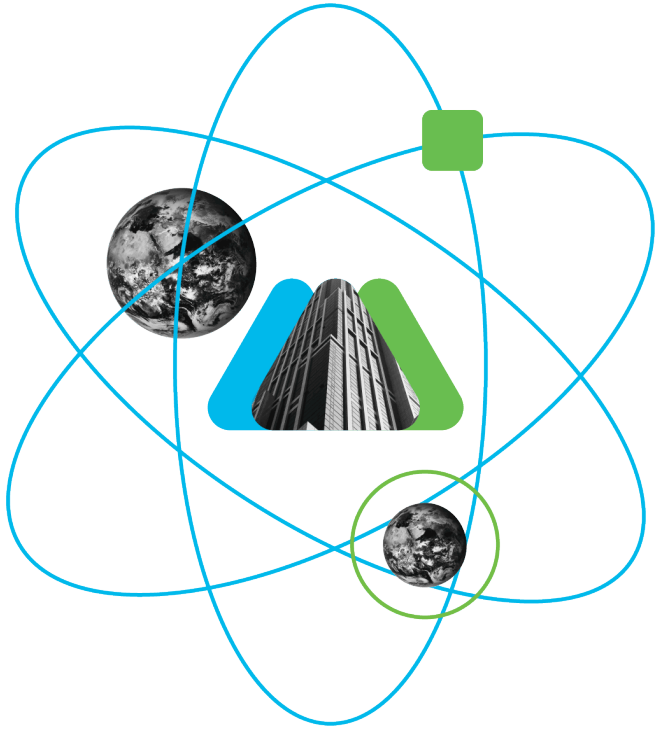
> **Today's CISO is a strategist, master influencer and arbitrator.**
> Chris Leach

@cjleach56 | LinkedIn

Chris Leach (continued)

Figuring out what kinds of attacks we will see in the 2020s that will challenge our ability to RECOVER, and have the potential to cause IRREVERSIBLE harm is, in my opinion, our top challenge. **There are three main areas that we need to focus on, in order to reduce the risk: policy considerations, security awareness training, and risk evaluation.** For example, the threat landscape must now include home workers and the controls (or lack of security controls).

As we restart our digital transformation journey; leadership, preparedness and vision will be more important than ever before.



> **There are three main areas that we need to focus on, in order to reduce the risk: policy considerations, security awareness training, and risk evaluation.**
> Chris Leach

Angus Macrae

Head of Cyber Security

The recent events that pushed us all to remote working have rapidly accelerated the possible future many companies and information workers have been nudging towards for some time. But whereas some had simply been dipping a few toes in the water, **now everyone is splashing about in the deep end.**

For those that can work well in this way, they've dispensed with the 20th century hangover myth of the 'workplace' as somewhere you can go. This shift opens up all sorts of possibilities for future business opportunities free of geographic constraint. It's also accelerated the reliance upon and trust in cloud technologies for many organizations.

> **This** [remote working] **shift opens up all sorts of possibilities for future business opportunities, free of geographic constraint.**
>
> Angus Macrae

@AMACSIA | LinkedIn

Gabriel Gumbs

Chief Innovation Officer at Spirion

We decided early on that having a well-defined collaboration and communication strategy was key for the transition to remote work. That also meant ensuring **we had a process for communicating early and often with our people.**

Allowing employees to use equipment that they had access to in the office allowed for a smoother transition. Efforts to centralize all pertinent company knowledge in one accessible library is also a key to work from home success.

@GabrielGumbs | LinkedIn

> **We had a process for communicating early and often with our people.**
> Gabriel Gumbs

Ian Thornton-Trump CD

Chief Information Security Officer at Cyjax Limited

Try to be at peace with yourself and balance realism, optimism and the achievable in your thinking. Above all, be patient with yourself and others. **Take some time...** a break in the middle of the day to distract from the chaos that is permeating nearly every aspect of our days and nights.

Ultimately, **treat these extraordinary times as an opportunity to reflect** on your life choices and career.

@phat_hobbit | LinkedIn

> **Take some time...treat these extraordinary times as an opportunity to reflect.**
>
> Ian Thornton-Trump

Michael Ball

Virtual Chief Information Security Officer at TeamCISO

@Unix_Guru | LinkedIn

After COVID-19 hit, it took us a little bit of time to adjust to having our workforce not in the office and being able to work from home. This abrupt change in work policy meant configuring our VPN and adding licensing for a significant portion of our workforce that had never required VPN access in the past.

There were issues immediately in training end users to use the VPN client from home as well as an issue with excessive permissions allowed on the VPN groups from the beginning. **(Convenience and speed trumps security yet again!)**

> **There were issues immediately in training end users to use the VPN client from home, as well as an issue with excessive permissions.**
> Michael Ball

A tale of VPN by Michael Ball

Another issue that we found and hadn't anticipated was that many of the employees were able to conduct their daily work without ever connecting their VPN back to the company. Things like Office 365, Salesforce and other SaaS applications allowed them to conduct their daily business (email and etc) without connectivity to our office. That unfortunately put us in a position where **we lost visibility to those devices**. We had not considered forcing the VPN connectivity so that we could ensure that updates and endpoint protection were updated and appropriate and that device monitoring wasn't completely missing.

We had to send out an email and request that each individual send their device back into the office. We then scrambled to develop a procedure by which to accept the devices, refresh them, and send them back safely to allow us to reconfigure and force VPN connectivity at least periodically.

Next came the security awareness training around "Home Office Cyber Hygiene." We had already developed this training and had delivered it to the executive team previously, but we had not yet delivered it to support staff. Delivering and following up on this remotely was an interesting challenge that we successfully met. The biggest issues were the diversity of ISP and Wi-Fi routers on which we had to walk users through updating default passwords and security control. **I think that *we* got as much of an education/experience out of this practice as our home bound end-users did.**

Three months in, we have close to 90% visibility of our distributed endpoints, and all of our new images have these security controls set up by default.

> **I think that *we* got as much of an education/experience out of this practice as our home bound end-users did.**
> Michael Ball

Shelly Blackburn

Vice President, Global Cyber Security Systems Engineering at Cisco

Cisco is a bit unique. Due to years of driving remote work internally, Cisco strategy is not solely driven from a small, homogenous, geographically centralized team. We have a truly global team and hire from a diverse candidate pool.

Strategic Take-Away #1: Get your leadership excited about the value to your organization. **Remote work environments enable innovation, opportunity and drive growth.**

> **Remote work environments enable innovation, opportunity and drive growth.**
> Shelly Blackburn

In response to the pandemic, we moved customers from 100% face-to-face work to remote work very quickly. Some moves were done in a matter of days, and this worked surprisingly well. Due to the shift to social online tools in our personal lives, colleges, government entities and businesses adjusted to video calls and collaborative online tools fairly seamlessly.

Strategic Take-Away #2: Don't be afraid to make the move to remote work quickly. With the right tools and a secure remote environment, the company and worker satisfaction with remote work can be extremely high.

@shellyblackburn | LinkedIn

Thom Langford

Founder of (TL)2 Security Ltd

It doesn't matter where I am, although right now it's obviously one single place. I can use whatever I need wherever I need it. Everything is managed through the cloud.

The one thing I wish I had done better actually was to prepare more for videoconferencing when it comes to face-to-face meetings. **I'm someone who likes to travel to meet people,** to have business lunches and even better business dinners with somebody, because that's how I like to connect with somebody.

For me, the biggest challenge was the appreciation that shifting to videoconferencing as the ONLY method of social interaction was as much a cultural shift in my approach as it was a technical shift.

@ThomLangford | LinkedIn

> **The one thing I wish I had done better was to prepare more for videoconferencing. I'm someone who likes to travel to meet people.**
>
> **Thom Langford**

Brad Arkin

SVP, Chief Security & Trust Officer at Cisco

Business has transformed virtually overnight to a greater emphasis on working remotely and collaborating virtually. We at Cisco are in a fortunate position to work effectively and securely in a remote environment, and have seamlessly transitioned 95% of our global workforce to work from home. Additionally, as the largest security company in the world, Cisco has protected millions of users since the roll-out of our free security offerings to support customers as they transitioned workforces to remote work.

This situation is a reminder that **we need to be planful, agile, and constantly reinvent ourselves** to keep pace with the needs of today and the future, as well as to anticipate the unexpected and unknown. The speed by which this situation arose and altered our approach to work, most likely forever, shows how important it is to be able to see around corners, to plan, prepare, and adjust for whatever may come.

> **This situation is a reminder that we need to be planful, agile, and constantly reinvent ourselves to keep pace with the needs of today and the future.**
> Brad Arkin

@BradArkin | LinkedIn

Chapter 2

Adapting to a new way of working, and ho
cybersecurity program is key

Chapter 3

How are you adapting the way you work? How can organizations build a security program for the future?

Cheryl Biswas

Specialist, Cyber Threat Intelligence Program

We do a daily sync in the mornings. It's not structured. We can talk about anything including work. It lets us connect with each other, and it's really strengthened our team.

Also, I'd recommend setting a schedule so that **work is not all day, every day.** Use visual management aids like wall calendars and white boards to track time, deliverables, events, etc. And make sure you take time to get outside, take a walk, get up and stretch regularly.

> [In our daily sync] **we can talk about anything. It lets us connect with each other, and it's really strengthened our team.**
>
> Cheryl Biswas

@3ncr1pt3d | LinkedIn

Cheryl Biswas (continued)

When building a great cybersecurity program, I'm going to give you three recommendations, and they're based on what's good for the people who will make your program happen. A great program is because of great people. These are as follows:

1. **Maintain respect for each other,** new ideas and approaches. We need to be willing to listen and learn from each other. Inspire a spirit of collaboration, cooperation and communication.
2. **Continuously train and build your team.** Invest in your people.
3. **Value diversity.** We need to grow beyond ourselves and what we know to meet new threats and to be proactive in doing so.

Dave Lewis

Global Advisory Chief Information Security Officer, Cisco

For most people working remotely, this is a completely new experience. Sure, they had taken the occasional Friday, but working as a dedicated remote staffer is another thing entirely. We as security practitioners need to be there to provide guidance more so than in previous years.

> **We as security practitioners need to be there to provide guidance - more so than in previous years.**
> Dave Lewis

The second element to keep in mind is the use of defined repeatable processes. Having people working remotely will help to draw this need in clear definition. **The chance for things to go wrong is compounded with having this lack of face-to-face interactions.** The third element to keep in mind for the remote working force is the democratization of security. We have to be sure to provide security tools such as MFA to our employees that enable them to do their jobs safely and securely.

@gattaca | LinkedIn

John Opdenakker

Security Manager

@j_opdenakker

A cybersecurity program can only be successful when there's support and commitment from the board and management. **Leading by example is crucial for adoption.** Using the right tools and processes is very important, but in the end, it's the employees that make the difference.

> **Leading by example is crucial for the adoption of a successful cybersecurity program.**
>
> John Opdenakker

John Opdenakker (continued)

Every employee should be aware that they can have a positive influence on the security of the company while doing their job. That's why it's so important that people in the security team not only have technical skills but also – probably even more importantly – have soft skills like communication and people management.

The security team should not be perceived as the group of people that always says no. Instead, they should explain to people why their actions form potential security risks. Once people understand why security matters and realize it doesn't have to be a barrier, they will adjust their behavior, and some of them will even become security advocates and help to further improve the security in your organization.

> **The security team should not be perceived as the group of people that always says no.**
> John Opdenakker

Gee Rittenhouse

Senior Vice President / General Manager at Cisco

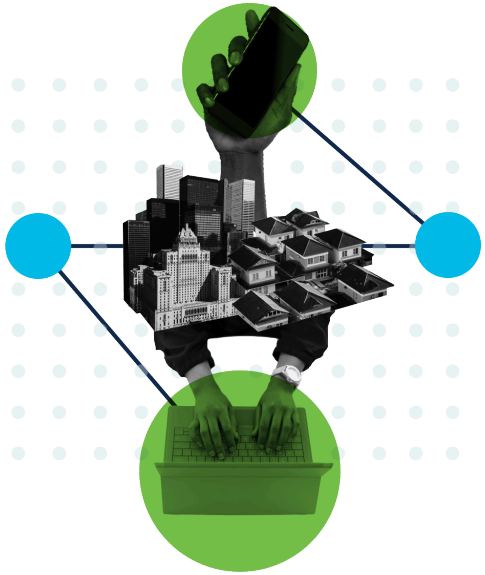
Embracing the digital transformation is no longer optional but an imperative. To provide security at scale, **organizations will require greater visibility to know what to protect** and the ability to automate key security workflows like threat investigation, hunting and remediation.

There must also be a shift in the culture where employees are seen as central to a company's security strategy. This means creating a well-informed workforce and educating them to potential threats like phishing schemes and equipping them with technology that seamlessly fits into the way they work.

@geerittenhouse | LinkedIn

There must be a shift in the culture where employees are seen as central to a company's security strategy.

Gee Rittenhouse



Stephanie Ihezukwu

Cloud Security Operations Analyst II at Duo Security, Cisco

It is 100% normal to not perform as you normally do. **This is not normal.** We are all reacting to this in different ways. Some of us are lucky enough to be productive during this time. Some of us are barely holding on. Make sure you work WITH yourself, not against yourself. If that means taking time off or speaking with your boss about your struggles, do so.

Our users are not our weakest link but our strongest allies. We need to support them so that they can help keep the business safe, and that requires an ongoing conversation.

@StephandSec | LinkedIn

This is not normal. We are all reacting to this in different ways. Some of us are lucky enough to be productive during this time. Some of us are barely holding on.

Stephanie Ihezukwu

Mick Jenkins MBE

Chief Information Security Officer at Brunel University London

A few mantras came at me like a flood over the last few months. *"Never let a good crisis go to waste." "Act early, move fast, and stay low." "Improvise, adapt, overcome."* But there was only one mantra that I knew would stand the test of an enduring campaign, one often cited by my long-time mentor: "Always keep a half pint of goodwill with your people, you'll never know when you'll need to call upon it in a crisis."

> **With great teamwork and great leadership, magnificent things can happen.**
>
> Mick Jenkins MBE

We needed to do three major things: Equip staff and students with the appropriate work tools, overlay sensible security measures, and train the workforce on the threats. We then needed to message them again and again. Engagement was key. A gentle "drip drip" of solid and sensible advice to keep their homes cyber safe.

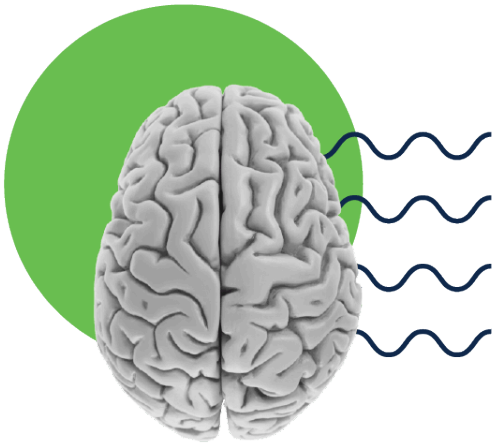
Things haven't been easy, but **with great teamwork and great leadership, magnificent things can happen.** Never let fear get in the way of your dreams.

@FailsafeQuery | LinkedIn

Chloe Messdaghi

VP of Strategy, Point3 Security, Inc.

A majority of breaches happen because employers are not investing in their employees. When we do not invest in our team, we become a threat to ourselves. In order to support one's security team, it's critical to provide ongoing training and support around mental health.



> **When we do not invest in our team, we become a threat to ourselves. It's critical to provide ongoing training and support around mental health.**
> Chloe Messdaghi

Within infosec, we have a problem with burnout because we struggle to balance our work and personal life. As a company or a leader, it is your job to make sure your employees are feeling balanced by providing resources and support. Lastly, remember you wouldn't have a product if you didn't have a security team. So, treat them well. Your company depends on it.

@ChloeMessdaghi | LinkedIn

Zoë Rose

Cyber Investigator

To embrace this new way of working, you should look for what works for you. Working remotely/from home/not-office location is about flexibility, inclusion, and **creating a space where you're best supported.**

Security is people, process, and technology. But people come first for a reason.

> **Working remotely is about flexibility, inclusion, and creating a space where you're best supported.**
> Zoë Rose

Our programs need to embed security/technology to work for the users in a way that doesn't negatively impact them. We also need to build processes that work for their workflows in a way that enhances their working lives.

@RoseSecOps | LinkedIn

Jenny Radcliffe

People Hacker and Social Engineer

On an individual basis having a routine helps you cope, helps you get into work mode. That being said it is very difficult if you don't have your own space to work in, we're working from home, and not everyone has a designated office space, we should all learn to be tolerant of how others are managing to work from home and make this work for them and the teams they are part of. We do need to support each other in both the short term and going forward as this new way of working continues to evolve.

In terms of awareness and building a secure workplace, whether remotely or not, you've got to work within the culture you've got. You've got to work with the messages your people already listen to, within the challenges that they have, and within what they celebrate, consider to be a " win" , how they like to learn and to work.

For a great cyber security program, know your people better than anyone else, and try to work with them so that you're not constantly pushing against what they like to do and what they feel is successful. If you can get your people on board, then you're already more than halfway there.

> **For a great cyber security program, know your people better than anyone else, and try to work with them so that you're not constantly pushing against what they like to do.**
> Jenny Radcliffe

@Jenny_Radcliffe | LinkedIn

Mark Weatherford

Chief Strategy Officer for the National Cybersecurity Center

Here are 3 tips I'd like to share:

1. Don't forget that while this situation has caused us to focus intently on tactical challenges, if you are a CISO, your job is also to keep your eye on the strategic direction of the security program. Your CEO might cut you some slack, but your regulator probably won't.
2. Take advantage of the crisis and lean on your vendors for more support.
3. Remote workers have increased the pressure on security teams to implement more robust endpoint monitoring and identity and access management (IAM) solutions. Use the crisis to get more internal support and budget to move these kinds of initiatives forward.

There are a huge number of factors that go into developing, implementing and operating a cybersecurity program, but one that always seems to get the least attention is the Business Continuity Planning components. **If you don't have a Business Continuity Plan when things go sideways, you're not doing business continuity;** You're doing disaster recovery, and the impact to your organization can be orders of magnitude more devastating.

> **If you don't have a Business Continuity Plan when things go sideways, you're not doing business continuity. You're doing disaster recovery.**
>
> Mark Weatherford

@marktw | LinkedIn

Tricia A. Howard

Marketing Manager at HolistiCyber

@TriciaKicksSaaS | LinkedIn

It's important to have a distinction from your work-from-home life and your home-from-home life.

One of the things that's helped me a lot is trying to emulate my commute as much as possible both in the morning when I'm starting the day and also when I'm done for the day. By listening to music, listening to a podcast or walking my dog for around the time that it would normally take for me to get into the office, it helps me mentally prepare for the day and also shut down whenever I am done working. It's been extremely helpful.

As for security, **we talk about people, process and technology. It truly is in that order.** The culture of the people will help influence the processes, which help influence the buying decisions and implementation decisions of your technology. So, it's really important to start with people.

All of this works because everyone is part of your security team in this day and age. Everyone.

> **We talk about people, process and technology. It truly is in that order.**
> Tricia A. Howard

What advice would you provide to others about embracing this new way of working – beyond just the short term?

Quentyn Taylor

Director of Information Security at Canon for EMEA

I think the main thing to remember is that whilst this way of working feels new, it is only the volume of home work that is new. Many companies have always had people working from home from different locations and from on the road.

With everyone now working from home, your perimeter just got a lot bigger. Ensure that you have a way of patching your client machines even though they're not on your network anymore.

My main piece of advice would be to remember that **the risks are not bigger or smaller. They're just different.**

> **The risks are not bigger or smaller. They're just different.**
> Quentyn Taylor

@quentynblog | LinkedIn

Isiah Jones

Owner & SR ICS OT Cybersecurity Consultant

My advice to people is to use basic sense and start following the advice that has already been around for a long time. Don't overthink and emotionally complicate things. **If anything, this situation should finally force people to start doing what they should have been doing the last 10 years.**

Follow the security controls and best practices that already exist for mature levels of handling insider threats, access control, change control and configuration management, asset inventory details as well as secure remote access.

@blackCyberDude | LinkedIn

> **If anything, this situation should finally force people to start doing what they should have been doing the last 10 years.**
> Isiah Jones

Matt Pascucci

Sr. Cyber Security Practice Manager

There has frequently been the pull to allow flexible work to employees as a perk, but **the fear of completely breaking the mold held particular institutions back from attempting it.** With the pandemic thrusting the majority of the world on some form of lockdown, we had to evolve.

Some of the major security concerns came from having the threat landscape expanded by having students, children and spouses all working remotely under their personal wireless network. The lack of full segmentation on these systems allows risks from one system to spread to others potentially, spreading back into their organizations.

With proper objectives, results and oversight, the remote work force can act just as organized if not better than a typical on-premise office depending on the function of the employee.

@MatthewPascucci | LinkedIn

> **With proper objectives, results and oversight, the remote work force can act just as organized, if not better, than a typical on-premise office.**
> Matt Pascucci

Victor Keong

Senior Chief Information Security Officer Advisor, Asia Pacific at Cisco

Working from home means an introduction of a whole slew of BYOD issues, which warrants a review of BYOD/acceptable use policies as well as a renewed focus on remote device management execution.

Bad actors have been taking advantage of this situation in phishing campaigns, but this brings an opportunity for anti-phishing awareness and ongoing education to the fore.

Victor Keong

Bad actors have been taking advantage of COVID-19 in phishing campaigns, but this brings an **opportunity for anti-phishing awareness and ongoing education** to the fore. It also underscores how the education of users on new security implementations are a necessary part of an organization's digital transformation curriculum.

@vkeong | LinkedIn

Gabriel Whalen

Principal Field Solution Architect - Information Security at CDW

My recommendation to every organization is to implement a security framework at a minimum. All too often, there is a focus on having a blinky box rather than testing or implementing non-technical (administrative and physical) security controls. It doesn't matter if an organization has the best in-class technical solution if they are not layering multiple control types around critical assets.

The next level is actually executing a business impact analysis and implementing business continuity plans, beyond IT and Disaster Recovery. Generally speaking, many organizations I speak with are focused on those annual or otherwise required technical tests, but thoughtful consideration of risk and impact can be a game changer in widespread events.

It doesn't matter if an organization has the best in-class technical solution if they are not layering multiple control types around critical assets.
Gabriel Whalen

@Ghostmath1 | LinkedIn

Chapter 3

Advice for Small and Medium Sized Businesses

More

Based on your own experiences, how have small and medium organizations been impacted?

Leron Zinatullin

Information Security Specialist

Despite market uncertainty and tightening budgets, many companies are seeing **improved productivity and cost savings through embracing remote working and cloud computing.** They are recognising the value of being able to scale up and down the capacity based on customer demand, and they are paying for only what they use rather than maintaining their own data centres. Supporting staff and trusting them to do the right thing also pays off.

Work with your staff to explain the ways that bad guys take advantage of media intense events for scams and fraud. Make it personal, use examples and relate to scenarios outside of the work context, too.

@le_rond | LinkedIn

> **Many companies are seeing improved productivity and cost savings through embracing remote working and cloud computing.**
> Leron Zinatullin

Sarah Clarke

Data Protection & Privacy, BH Consulting

The greatest tension is between privacy and protection (sometimes falsely seen as a straight trade off). We are also dealing with a fundamentally changed threat landscape as career and opportunist criminals turn to the huge remote endpoint estate and healthcare tech. Then there's the economic pressure on all of us to do more with less.

> **Never put any measure in place if you haven't planned and resourced for what has to happen next.**
>
> Sarah Clarke

For remote work, plan to review the solution and control landscape. Many vendors have changed things hand over fist during this time; peers will have enormous amounts of experience to share. Take advantage of that. Formulate a strategy for positive permanent change using feedback from peers, IT operations and staff.

Apart from all that, transparency and trust are going to be the lynch pins for everything. We are all in this together.

@TrialByTruth | LinkedIn

David Shipley

CEO at Beauceron Security

Thanks to embracing cloud productivity tools, we were well positioned technologically to go 100% remote.

Our gap, and one we've seen for many organizations, was in comprehensive training to explain to our team how to work remotely safely. We created a new course using our tool that covered all relevant topics such as expectations for keeping personal devices used for work up-to-date, guidance on securing home Wi-Fi as well as discussions or when it's okay and not okay to print documents at home. **Most importantly, the training wasn't generic tips or best practices;** it was easy to make specific to our policies and standards.

Thanks to embracing cloud productivity tools, we were well positioned technologically to go 100% remote.

David Shipley

@davidshipley | LinkedIn

Ross Moore

Cyber Security Support Analyst

One of our team leads set up a daily Monday-Friday remote meeting. **He called it "Reason to put pants on,"** so that made it funnier. It's a time just to talk and decompress with no judgement.

People need to hear other people, and they need to see faces. A team still needs cohesion when working remotely, and the pandemic response required us to move beyond the haphazard in-house meetings to purposeful and planned meetings.

> **People need to hear other people, and they need to see faces. A team still needs cohesion when working remotely.**
> Ross Moore

@rossamoore | LinkedIn

What is your advice for small organizations? How can they build a security program for the future?

Fareedah Shaheed

CEO and Founder of Sekuva

Honestly, **security awareness programs were boring and disengaging** until we saw a shift in the field to provide gamified training and programs.

For the longer term, I foresee a community-based program as the main change in the security awareness arena especially as the remote workforce grows larger. This is because when we're in a community going towards a common goal, people have a better sense of the why behind the program and how their actions play into the bigger picture.

A community-based approach isn't just checking the box, or making the box more fun, it's actively changing the role of cybersecurity in people's lives.

> **I foresee a community-based program as the main change in the security awareness arena especially as the remote workforce grows larger.**
>
> Fareedah Shaheed

@CyberFareedah | LinkedIn

Jessica Barker

Co-Founder of Cygenta and Chair of ClubCISO

@drjessicabarker | LinkedIn

While we're dealing with extraordinary times, it's important to recognise that security cannot simply stop. In a bid to keep going and move forward as best we can, we need to consider how to do that with security in mind.

I would encourage organisations to **get creative and think about how they can run virtual events and activities to keep security on people's minds.** Given the rise in phishing emails we have seen connected to COVID-19, it's important that we adapt and evolve to meet the circumstances we find ourselves in. It's better than allowing a vacuum to form, as cyber criminals could then exploit it.

> **I would encourage organisations to get creative and think about how they can run virtual events and activities to keep security on people's minds.**
>
> Jessica Barker

J Wolfgang Goerlich

Advisory Chief Information Security Officer, Cisco

2020 has proven to be a “black swan event.” The term, coined by Nassim Nicholas Taleb in the book of the same name, is for rare but highly impactful and highly memorable events. IT and IT Security teams are having a moment, as many have worked tirelessly to ensure their organizations’ ability to successfully respond to security incidents in spite of the quarantine. **Now these same teams, in the near future, will be asked to be ready for the next one.** But here’s the thing: black swans are by definition rare and unpredictable.

@jwgoerlich | LinkedIn

> **Security teams have worked tirelessly to ensure their organizations' ability to successfully respond to security incidents in spite of the quarantine.**
>
> J Wolfgang Goerlich

J Wolfgang Goerlich (continued)

Develop a strategy that prepares for the unlikely while strengthening defenses for more common threats. Let's call these geese. A good security program readies the organization against all birds, be it the black swan or the unnamed goose.

> **A good security program readies the organization against all birds, be it the black swan or the unnamed goose.**
> J Wolfgang Goerlich

There are many challenges to tackle. We need greater control at the endpoint and edge. We need more visibility into all devices, regardless of company-provided or BYOD or on-premise or cloud instances.

In the longer term, organizations need to strengthen and enhance their capabilities in business continuity and incident response. By **placing the emphasis on flexibility and response,** organizations can deal with the current challenges while preparing for future ones.

Tazin Khan Norelius

Cyber Security Manager, Services and Delivery at MorganFranklin Consulting

The biggest impact on small businesses that is going to affect and/or change their security program is more compliance. **There's going to be so much compliance** pushed through whether it's regarding security framework implementation in your organization or whether it's regarding consumer data protection laws that are being pushed through legislation.

The biggest piece of advice that I could provide to small businesses would be to implement a cyber security framework and methodology very early into your business. If you've been in business for a long time, do it now. It's never too late.

Having someone knowledgeable in security legislation is going to 100% benefit you in the now and the long term.

> **The biggest piece of advice that I could provide to small businesses would be to implement a cyber security framework and methodology very early into your business... It's never too late.**
>
> Tazin Khan Norelius

@techwithtaz | LinkedIn

Melissa Parsons

Senior Cyber Security Consultant

Small businesses are likely to see many challenges in the areas of budgets and the governance side of security. SMBs are often " trying to do more with less," especially when it comes to where to allocate funds. In relation to cyber and information security, do they invest more in internal programs to prevent, detect, monitor and alert on security events and incidents (which of course will have associated costs to people resources), outsource these activities or perhaps embrace a hybrid approach? It comes down to identifying their most critical assets (physical, logical, even people and processes) and prioritizing the protection based on criticality. This is where business impact analysis (BIA) and risk assessment can be extremely beneficial before jumping the gun and deploying funds and resources in areas that may not result in a ROI.

LinkedIn

Small businesses are likely to see many challenges in the areas of budgets and the governance side of security. SMBs are often " trying to do more with less."

Melissa Parsons

Melissa Parsons (continued)

Tips? **Start small.** Start with that BIA and risk identification process to drive informed decisions when it comes to IT and security. Having a dedicated resource to manage and champion this internally, liaise with appropriate stakeholders, keep analysis and recommendations current and aligned to business goals and objectives will help to save a lot of headaches down the road and misallocation of resources.

> **Start with that BIA and risk identification process to drive informed decisions when it comes to IT and security.**
>
> Melissa Parsons

Omar Zarabi

President & CEO - Port53

Now with employees working from anywhere as well as accessing corporate information and data hosted across the world, it is absolutely essential to realize that although firewalls are still important, **the foundation of security has shifted to the identity and the connection.** Being able to ensure the secure connection to proper applications and data, not to mention forcing authentication at every turn (zero trust implementation), is going to be absolutely critical in protecting this new way of work.

Luckily for SMB organizations, more and more cybersecurity solutions are leveraging the cloud as a delivery mechanism. This will enable smaller organizations to not only implement proper solutions at an affordable, per-consumption model. It will also allow resource-restrained IT teams to build and manage a holistic, integrated and proactive security stack without needing the engineering acumen in-house to do so.

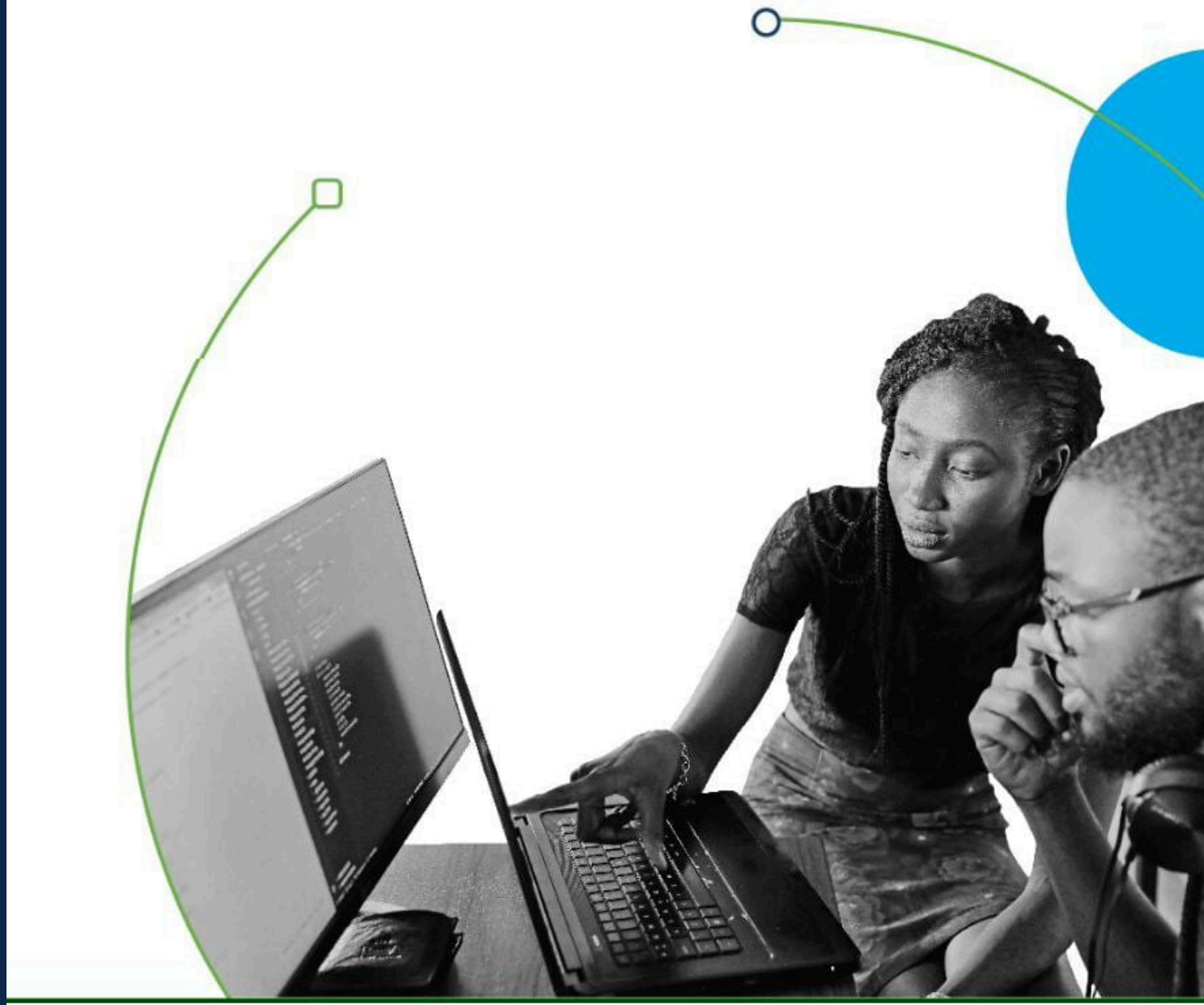
> **Being able to ensure the secure connection to proper applications and data, not to mention forcing authentication at every turn, is going to be absolutely critical in protecting this new way of work.**
> Omar Zarabi

@Port53Tech | LinkedIn

" If you can't change it, change your attitude."

– Maya Angelou

Select **Read on** for Resources and Videos



Adjusting to current challenges has helped some security teams think about building on their cybersecurity programs and improving their culture and communication.

What's interesting about the responses in this eBook is that so many of them focus on mental health and combating burnout.

These unusual circumstances have driven home the point that **good leaders support their peers, encourage others, and empower their teams.**

> **This highlights that people are the most important aspect of any organization.**
> Cisco Secure

It's our hope that the tips and opinions shared here will help you, your security teams, and your organization feel a bit more at ease about adapting for the future.

Additional resources

Five tips to enable a remote workforce securely

Simple tips to maintain your work-from-home culture while securing your workers and company assets.

Remote work and the threat landscape

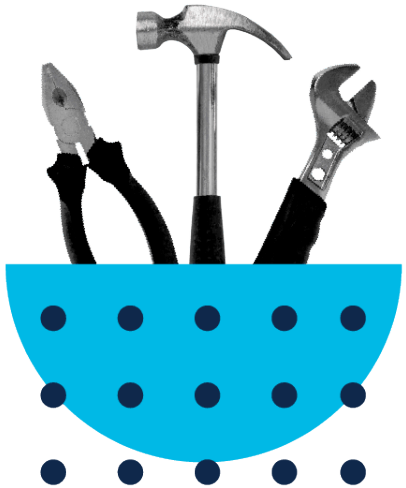
Attackers are adapting their techniques to target those working from home, tailoring them to be more effective in this environment.

Securing the remote work environment

Working from home isn't the same as working from the office. Here's why organizations should be reviewing their remote working security posture.

Cisco Secure Remote Worker Solutions

As you adjust to extraordinary times, empowering your employees with secure remote working options helps accelerate your success and protect your future.



Big Security in a Small Business World: 10 Myth Busters for SMB Security

In this report we use survey findings and outcomes from our conversations with small and medium-sized businesses to debunk common SMB cybersecurity myths.

Secure Remote Worker Trial from Cisco

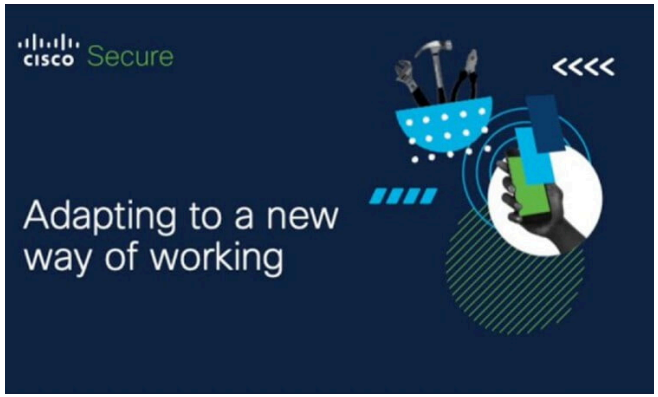
Increase protection for your remote workforce so they can work from any device, at any time, from any location. Request more information on licensing and pricing.

Security Stories podcast

Listen to this interview based podcast to hear the real experiences of security leaders, and how they got to be where they are today.

Videos


cisco Secure
Experiences from Cybersecurity Leaders in Extraordinary Times:
Adjustments and Outcomes


cisco Secure
Adapting to a new way of working


cisco Secure
Investing in your cybersecurity program during extraordinary times


cisco Secure
How SMBs Are Reacting to a New Way of Working

Thank you for reading:

Adjusting to Extraordinary Times