COVID-19 CIO Strategy

10 Steps Approach

As modified from Info-Tech Research Group

What this presentation contains

Now that you have everything largely in place for the COVID-19 crisis. Have you done all that you could have and what should you be thinking about for the near, medium and longer term to best support your organisation?

Effectus has customised this 10 step plan from Info-Tech Research Group to help answer those questions. We think it is a good practical reference document and believe you will get some value from it.

Effectus can provide you with support through each of the 10 steps in any manner that would best work for you and your current situation.

Ten-Step IT Pandemic Strategy Overview

EFFECTUS LIMITED

1. **Prepare IT to Support the Business**
   Failure to prepare with effective governance and empowered to act will impact the entire organisation
2. **Inspire and over deliver**
   Understand the business priorities and align IT resources to those priorities
3. **Make Technology awesome!**
   Support business continuity with IT solutions. Focus on core services to facilitate work from home (WFH) and other pandemic measures
4. **Turn this strategy into a tactical project**
   It's time to turn strategy into tactics. This is a key project: run it like one.
5. **Focus on the customer**
   We must focus our IT capabilities and support on the end customer working through the business for best effect.
6. **IT must help lead business process innovations**
   Being able to capitalise on emergency process alternatives will provide the organisation with long-term value and cost savings.
7. **Protect core operations and IT process**
   As much as possible, don't shortcut current processes. Keeping things running smoothly will require attention.
8. **Prepare for the economic downturn**
   Cutbacks are on their way. We will be asked to do more with less.
9. **Re-prioritise the work programme**
   Some projects should be halted, some scaled back, some pushed forward, and others started. Determine which is which.
10. **Review and revise security priorities in a Pandemic**
    Hackers love a crisis. Be prepared to secure and privatise your new environments in the face of new threats.

Local Government – Focus Areas

Now in Crisis:

- Minimise work stoppage by providing support for remote work. This includes provisioning of end-user devices and expanding telecommunications capacity.
- Increase security awareness to mitigate increased exposure due to expanded remote work connectivity.
- Facilitate needed governance processes and public participation through virtual council and leadership meetings.
- Manage increased demand for customer engagement and online self-service through government websites.
- Engage strategic vendors to determine their ability to continue support of critical systems and services.

Continuing Operations:

- Ensure IT is part of the near-term business planning.
- Revisit in-flight projects to determine what needs to be accelerated, paused, or stopped.
- Initiate planning sessions with strategic vendors to mitigate possible degradation in services.
- Assess capacity of IT staff to continue to operate under crisis conditions.
- Review the IT budget to prepare for cost-cutting measures extending from shortfall in revenues.

Post-Crisis Reality:

- Reprioritise strategic initiatives extending from prolonged shortfall in revenues.
- Modernise operations to relieve reliance on manually intensive processes.
- Implement expanded remote work environments that were proven during the crisis.
- Expand online self-services.
- Invest in telecommunication facilities to support new remote work environments and customer access to online service and information.

People Management

Keeping IT employees productive, enabled, and engaged is job #1. Failure to prepare will impact the entire organisation.

Create an (Emergency) IT Governance Committee

Governance models are effective at providing oversight during normal operating times; however, they often crumble under speed or economic pressure.

The COVID-19 pandemic has focused our need to accelerate decision-making windows while maintaining risk tolerance and alignment to long-term business objectives.

For the near term, we must realign our governance model around protecting employees while maintaining the services we provide in what is likely to be a significantly impacted financial position.

Key Insights

1. Support your team
2. Keep them safe
3. Build a back-up plan for key roles. The stage of initial crisis management and communication has passed.
4. Establish clear roles and responsibilities across IT to help the organisation respond rapidly.
5. Communication and re-training on working from home (WFH) and remote working technology is critical. Assume previous IT training wasn't a priority and everyone needs a refresher on all remote technology and any change they need to manage through. Don't begrudge the time. The re-training investment will pay dividends.

This is the time for each CIO to reach out to each key executive and find a way to deliver results in half the time.

Inspire your team to deliver extraordinary results

In this time of crisis, CIOs must ask their teams to overdeliver.

As a CIO, you need to use your leadership skills to communicate to your team the importance of speed and impact. Your team is in a unique position to mitigate the damage the COVID-19 crisis can inflict on your organisation and your team's livelihoods.

Your team wants to help; they want to make a difference. Now is the time to ask the IT team for extraordinary effort.

Ask your team to find ways to rapidly solve problems. Now is the time to time to ask them to deliver extraordinary results with challenging timelines.

Key Insights

1. Your team wants to help; they want to make a difference. Now is the time to ask the IT team for extraordinary effort.
2. Reach out to the CEO and each senior business stakeholder; offer your support, then surprise and delight them by asking for additional projects and requirements that will support their ability to provide services during the crisis.
3. In this time of crisis, find new ways to exceed expectations and build your IT department's reputation.

3. Make Technology Awesome!

Put business continuity, disaster recovery, work-from-home and collaboration technology in place and then make it awesome.

Most IT departments should already have the core processes and technology in place to enable business continuity.

Now check just how good, or bad, those temporary measures are for the weeks ahead. What enables your people to function with confidence?

Robust is good but delivering something which is much better than expected is the goal.

Encourage your team to come up with innovative ways to improve the technology being used by internal and external customers.

Key Insights

1. Identify individuals on your IT team who can be made into "heroes" by implementing solutions that the organisation will appreciate and celebrate.
2. Proactively reach out to business leaders; monitor critical infrastructure and key functions for unexpected issues.
3. Overstaff the help desk function temporarily; perform proactive outreach to ensure everything works as people adjust to working from home.
4. CIOs should lead consistent communication across their team and the broader organisation where possible.

Remote Working

- Insist on professional Video Conferencing and Collaboration that works every time – don't let it become a joke
- Recognise the extension of the network to the home and that help will be required to have professional home working environments with robust network connectivity and security
- Encourage workplace social support – games, vlogs, and wellness activity
- Assess the potential for a flexible work plan as lockdown phases down

Applications and Solutions

- Assess the benefits of Robotic Process Automation for manual and paper based activity.
- Encourage business users to find and test apps and solutions that could benefit their roles
- Consolidate any apps or solutions that are not used or costing more than their value

Harden Systems & Infrastructure

- Plan to shift any maintenance heavy home grown solutions to Software as a Service
- Remove any remote networking solutions that are complex, flaky and unsupported
- Start your next phase Cloud migration today with an ambition to shift most systems and applications to XaaS
- Work with your Vendors to better understand what services they could provide and assess the full ROI of changing to a more outsourced model

4. Turn this Strategy into a Tactical Project

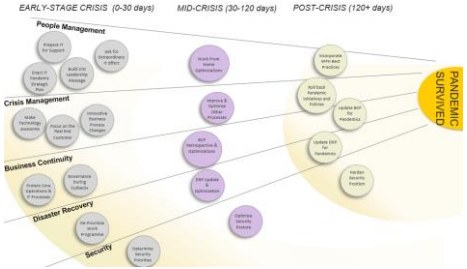
It's time to turn strategy into tactics. Take the strategic pandemic initiatives and apply a more future-oriented look at where we will go in the months to come. This is a key project: run it like one.

The project management triangle of scope, resources and time still apply.

This is not unfamiliar territory. As you draft your COVID-19 pandemic strategy for IT, be sure you design and execute the tactic in an orderly, controlled fashion. That means; run it like an important Project.

Use something like the following, and on the next page, diagram to communicate how the initiatives will be implemented over time.

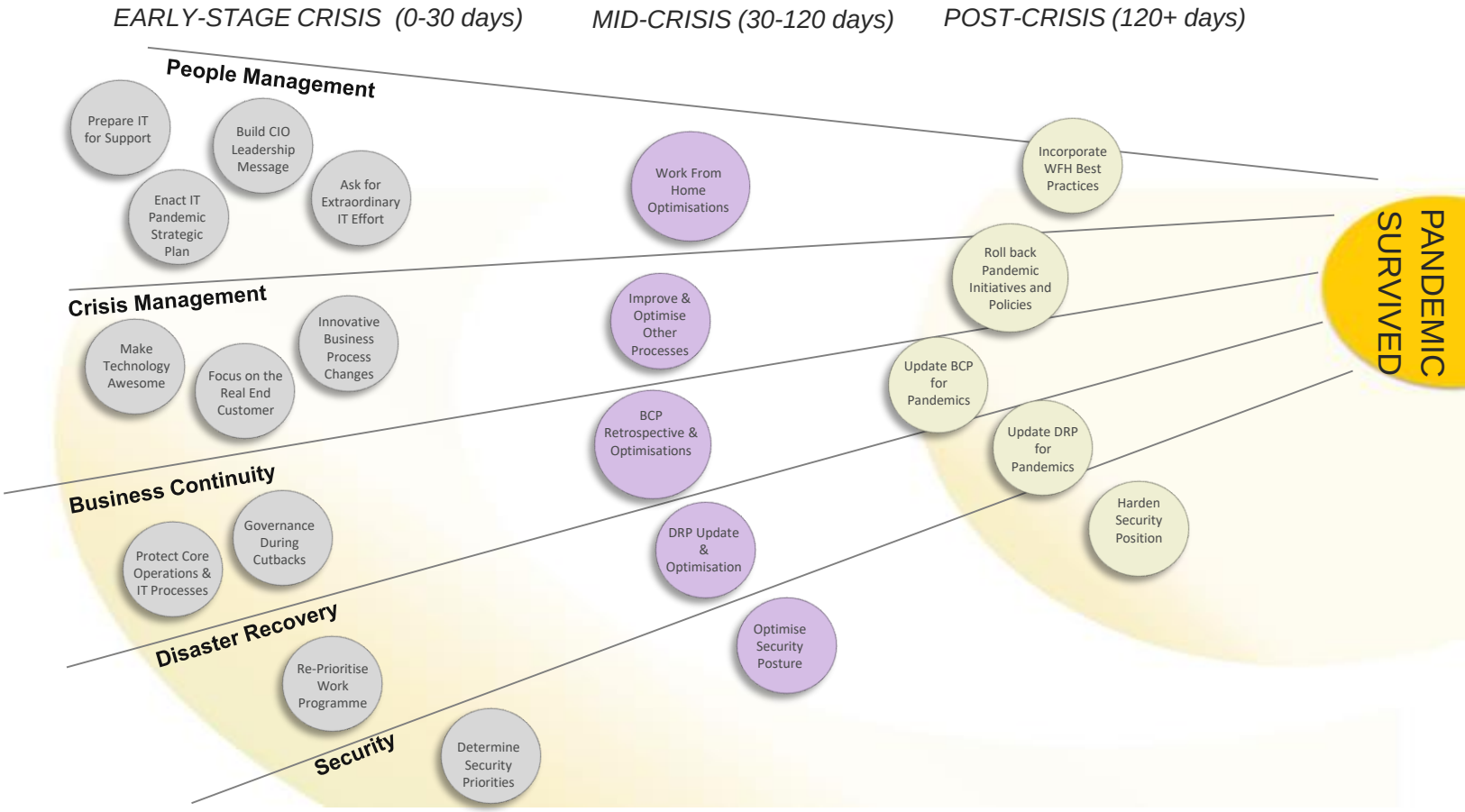
Run this pandemic strategy as a project with tasks, resources, and timelines. Assign ownership for initiatives and ensure they are clearly scoped and achievable.



Key Insights

1. The CIO should ask for regular updates against each of these initiatives. Each initiative can be run as an independent project, but be aware of dependencies between them. Governance, for example, may need to be dealt with quickly if it is required to make process or resource decisions in your organisation.
2. Assign people to each initiative listed in this strategy where they will need to decompose each initiative to arrive at more accurate estimates for each initiative and maintain them as part of a centralised project. Assign a project owner and project manager. Track resources like any project.
3. Keep a central version of the plan in a highly visible place and ensure key personnel keep it updated.
4. As events unfold over the coming months, revise these initiatives and update the plan and the sunrise diagram.
5. Be prepared for a long planning horizon. Who knows how long this crisis will last and what the new 'normal' will look like?

Long-Term Pandemic IT Initiative Overview



Crisis Management

5. Focus on the Customer

Many organisations will be forced to manage a significant reduction in revenue or funding and still achieve similar or, maybe, better outcomes for their internal and external customers.

CIOs need to help support customer focused activity.

Consider your customers whether they be Businesses, Government or Residential they are all facing an impact on revenue or funding.

The COVID-19 crisis will directly and indirectly impact your organisation and as the CIO you need to find ways to perform with the revenue/funding reduction which will be the CEO's top priority.

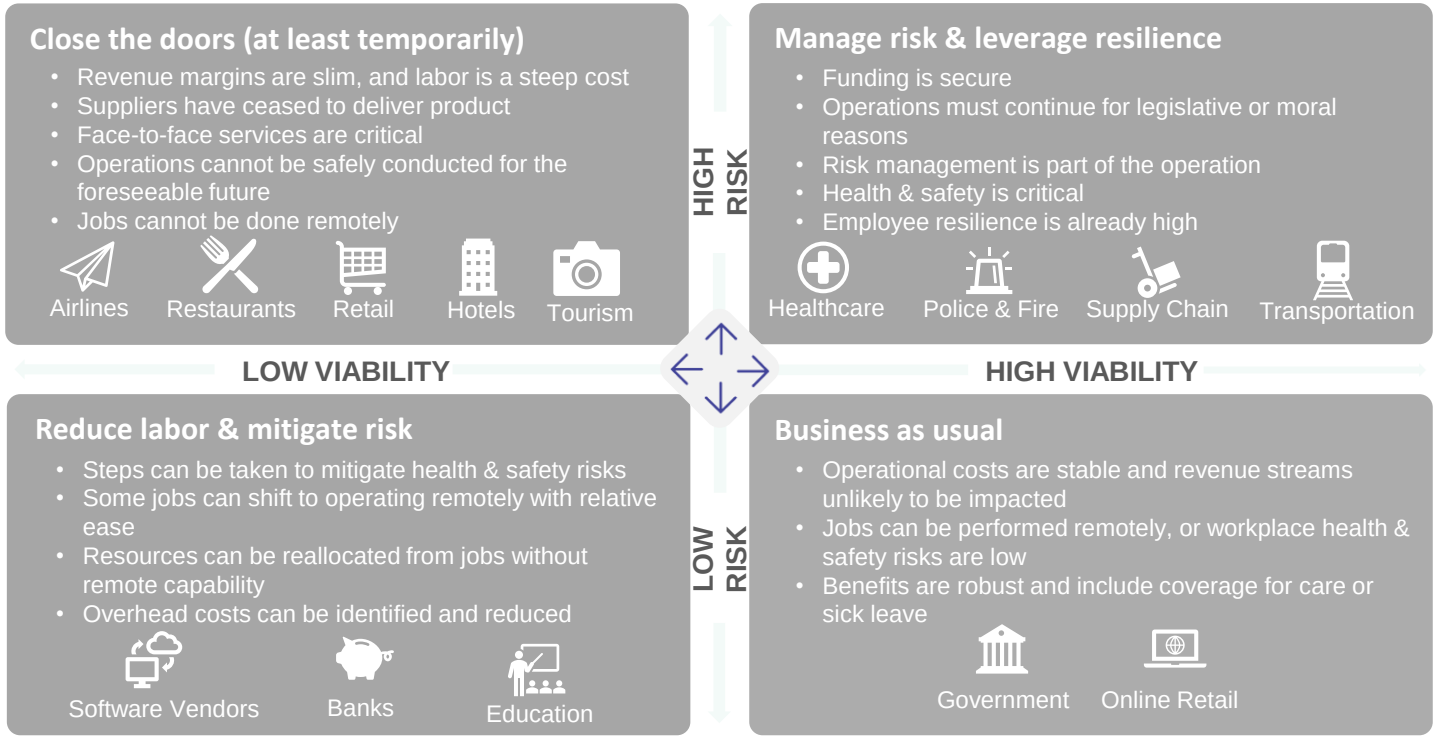
CIOs need to identify and focus on initiatives that help the CEO as they work to ensure the organisation adapts to this new pandemic crisis that has in record time had a unprecedented initial and, will have, long-term impact.

CIOs have the opportunity to innovatively leverage technology to help the organisation thrive or survive.

Key Insights

1. Most organisations expect to manage a drop in revenue/funding and demand. CIOs should focus on understanding how the organisation will need support with what could be a drastically different strategic approach.
2. CIOs should focus on supporting existing customers and stakeholders as a top priority.
3. Support business processes that need to become remote and less dependent on travel or in-person visits. Prioritise new digital processes that enable your organisation to continue to deliver and sell where possible.
4. Technology innovation delivered quickly will absolutely make a difference. Now is the time to consider technology-enabled innovation.

COVID-19 Affect on Industry Sector



6. IT Must Help Lead Business Process Innovations

With all of the recent change, like social distancing, every organisation's operations have been disrupted and some business processes are now struggling.

Technology innovations can catapult IT into a leadership position.

Consider the potential for a continued extension of varying levels of lockdown and how much of your organisation still uses paper documents for key processes which will probably need to be replaced.

As CIO, it's your responsibility to understand how technology can be used to alter and disrupt processes. Capitalise on the disruption to offer solutions that would have seemed impossible to implement or too challenging to manage the change in the past. Never let a good crisis go to waste.

Key Insights

1. Understand how technology can and will be used to innovate. New habits will be formed and it is probable that there will be change for at least the medium term.
2. This is an opportunity for CIOs to lead digital transformation initiatives that have long-term value. Move forward with well-researched and understood digital transformation projects.
3. Fast track any innovation initiatives in your portfolio that enable work-from-home strategies or remote/online delivery of services.
4. Understand that fast tracking transformational change without sufficient testing, experiments, and data is extremely risky.

Business Continuity

As much as possible, don't shortcut current processes. Keeping things running smoothly will require attention to core service delivery.

Expect strain on IT infrastructure, systems and process

The first necessity is to provide basic infrastructure. It is imperative that basic infrastructure functions.

CIOs need to set expectations that IT has a role to play beyond providing basic infrastructure and will also need to provide robust high-value IT functions.

Now is a good time to ask senior executives if they have the need for any new reporting and analytic capabilities to assist in monitoring the organisation's core health metrics or reporting that can help with the transition to a work-from-home environment. The following slide provides a high-level view of a Flexible Work Plan.

Key Insights

1. Manage a short-term surge in demand for key systems & processes needed across the crisis:
    a) Help desk; remote work capabilities
    b) Customer-facing websites & call centers
    c) End-user security training
2. Be aware of who on your team is experiencing a drop in demand or can not perform their job at home and will need to be redeployed.
3. Keep existing projects and priorities moving forward.
4. Don't just survive – build key long-term IT capabilities and, focus on remote delivery capabilities.

Create a Flexible Work Plan

1 Set Program Direction

This phase will walk you through the following activities:

- Identifying key stakeholders
- Clarifying roles and responsibilities
- Determining goals and metrics
- Identifying employee segments
- Gaining senior leadership buy-in

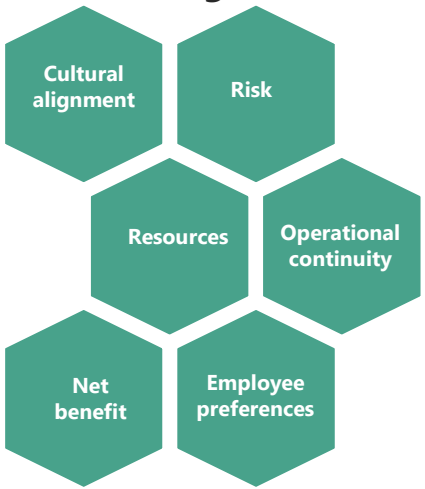
2 Create a Shortlist of Options

3 Assess Feasibility

Feasibility Assessment – Option 1

Option:	Compressed work week
	Customer Service Reps
Operational Continuity — Operational coverage: To what extent are employees needed to deliver products or services?	Normal business hours five days a week is needed, so reps will need to take different days off
Operational Continuity — Real-time communication: To what extent do employees need to communicate with each other in real-time?	It is valuable for some reps to work at the same time to support each other; will need to ensure reps never work alone and are aware of who else is working
Operational Continuity — Face-to-face communication: When do employees need to interact with each other or clients in-person?	Not needed
Operational Continuity — Implementation issues	May need a scheduling system to increase efficiency of scheduling
Operational Continuity — Cost	Currently researching

4 Implement the Program



8. Prepare for the Economic Downturn

Tougher times are on their way. You will definitely be asked to do more with less.

Work through a process to identify budget cutbacks while preserving key capabilities.

Review the following page for some ideas on how to make some cuts but also how to maximise value from what is spent.

For every organisation there are many workable strategies to cut back IT costs and maintain core capabilities. Within each of these core strategic approaches there are refinements to best suit your organisation.

Justification for your annual budget should be expected and best approach is to preempt that potentially challenging discussion.

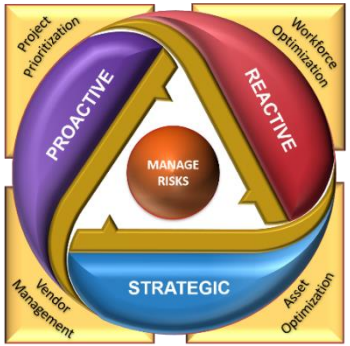
Key Insights

1. The strategic plan you build depends on the budget cutbacks you need to achieve.
2. Work though different approaches to reduce costs in four categories:
    a) Asset Optimisation
    b) Vendor Optimisation
    c) Workforce Optimisation
    d) Project Prioritisation
3. Build a boardroom-ready strategy to help you communicate upwards and within your organisation.

Four Focus Areas for Cost Management

1. **Project Prioritisation:** Re-order the project backlog for better alignment with strategic goals. This is not just about canceling low-priority projects but re-assessing the scope and scale of projects that could be retained in the portfolio to reduce spend, but not at the expense of innovation and always with a view towards coming out of the recession.

2. **Vendor Management:** Re-consider existing partnerships with vendors/providers to realise economies of scale and reduce complexity but keep the customer experience in mind. Strategic partnerships may have more value and more opportunities than commodity suppliers do. Identify opportunities for non-renewal of contracts and early termination (watch out for penalties). Identify vendors who are at risk of closing to mitigate risk.



3. **Workforce Optimisation:** Improve the productivity of the IT workforce. Optimising the workforce does not equal staffing cuts; though quick it is not the only way. Prioritise workloads based on business value, reducing only staff associated with non-essential services. Plan for retention of high-value employees to ensure recovery. Cut non-essential activity like training. Remove bureaucracy so staff can focus on innovation as well as support activities.

4. **Asset Optimisation:** Optimise the use of existing assets to improve ROI – this is primarily about optimising capacity utilisation and eliminating redundant and underutilised assets, including removing redundant software and extending use of existing equipment instead of refreshing (e.g. desktops). Asset investments aligned to optimal business value should continue.

Disaster Recovery

9. Reprioritising the Work Programme

Some projects should be halted, some scaled back, some pushed forward, and others started. Determine which is which.

You need to make room for pandemic-related projects, but don't destroy forward momentum in the process.

The current crisis will undoubtably affect the prioritisation and rollout of your existing IT projects.

Now is the time to do a full re-prioritisation of your existing projects. Make sure to work with executive sponsors to understand their new priorities and changes to projects in flight.

Key Insights

1. Work with senior stakeholders to help the organisation through the crisis.
2. Don't just assume that all projects' priority remains the same. Assign someone on your team to reset priorities across the portfolio.
3. Continue to move forward; don't delay projects unless you have clear direction from the executive team.

Security

10. Security Priorities in a Pandemic

Hackers love a crisis. Be prepared to secure and privatise your new environments in the face of new threats.

The last thing you need in the middle of a pandemic is a brand-new security crisis.

We have to be proactive about closing new security gaps that are the result of rapid process changes. Hackers take advantage of major events and they will sweep into the space exposed by remote workers, empty buildings, and vacant streets and take any advantage they can find.

Let's also prepare to address the vulnerabilities brought on by a remote workforce. For instance most homes are not secure, with internet routers configured with default admin privileges and passwords.

Make sure that remote staff have a clear communication process to validate any change in process. Teach all end users to err on the side of caution. Focus considerable energy on end-user security awareness in this new reality.

Key Insights

1. Focus on end-user security training. Hackers will attempt to victimise new work-from-home employees. Begin here.
2. Physical office security is an increased risk. With everyone aware of work-from-home policies, take extra precautions with physical security.
3. Re-visit and review your security strategy. Your security posture may have changed when the world pivoted under the virus. Be sure your risk tolerance is still what it was before COVID-19.

Questions?

Thank you from