RICHEY
MAY Technology
Solutions

THE EXECUTIVE'S
COVID-19 EXIT
STRATEGY
GUIDE

ABOUT THE AUTHORS

John-Thomas Gaietto, CISSP
Executive Director — Cybersecurity & Cloud Migration Services
John-Thomas Gaietto has over 20 years of experience providing enterprise information security and risk management services to a variety of organizations, with a particular emphasis on the financial services industry. JT's vast expertise includes the development of security strategies based on organizational risk, oversight of security operations, incident response, third-party risk management, disaster recovery, building and leading high-performing Information Security teams, and customer and government due diligence oversight.

Michael Wylie, CISSP
Director — Cybersecurity Services
Michael co-founded Corporate Blue, an Information Systems and Security consulting firm that served clients in their pursuit of mitigating cyber threats. In his role, Michael was responsible for delivering information assurance by means of vulnerability assessments, risk management, project management, secure network design, and training. Michael has developed and taught numerous courses for the Department of Defense, Moorpark College, California State Universities, and clients around the world.

OUR TEAM

Nathan Lee
Partner In Charge - Richey May Technology Solutions

Garry Woods
Executive Director — Governance, Risk, Compliance & Privacy

Ben Duke
Executive Director — Planning & Analytics

Jason Hamilton, CISSP, CISA
Director — Cybersecurity Services

Arnel Manalo, CISSP
Cybersecurity Architect

Evan Bredhal, CEH
Cybersecurity Engineer

Chase Jones, CISSP
Cybersecurity Engineer

Jacob Stremler, CEH
Cybersecurity Engineer

Olivia Nicholson
Manager — BI & Analytics

Molly Manuzak
Client Data Analyst

ABOUT RICHEY MAY TECHNOLOGY SOLUTIONS

Cybersecurity
Protect the usability, reliability, confidentiality and safety of your network and assets —and most importantly, the integrity of your brand.

Cloud Services
Develop cloud migration strategies to gain efficiencies and enable opportunities.

vCIO/vCISO
Partner with experienced industry professionals for strategic insight and guidance.

Managed IT Services
Develop strategies and efficiencies for your IT Operations and Support.

Governance, Risk, Compliance & Privacy
Develop and implement appropriate policies, procedures, and standards to effectively manage risk and privacy concerns.

RICHEY MAY
ANALYZE

Business Intelligence
Connect your data and break down internal silos to gain valuable insights and confidence in decision-making.

RICHEY MAY
PLAN

Budgeting & Forecasting
Develop cloud migration strategies to gain efficiencies and enable opportunities.

RM² Methodology℠: A Results-Driven Approach With A Focus on Building Value

Our process is designed to help us focus on the most impactful changes that will drive revenue and growth.
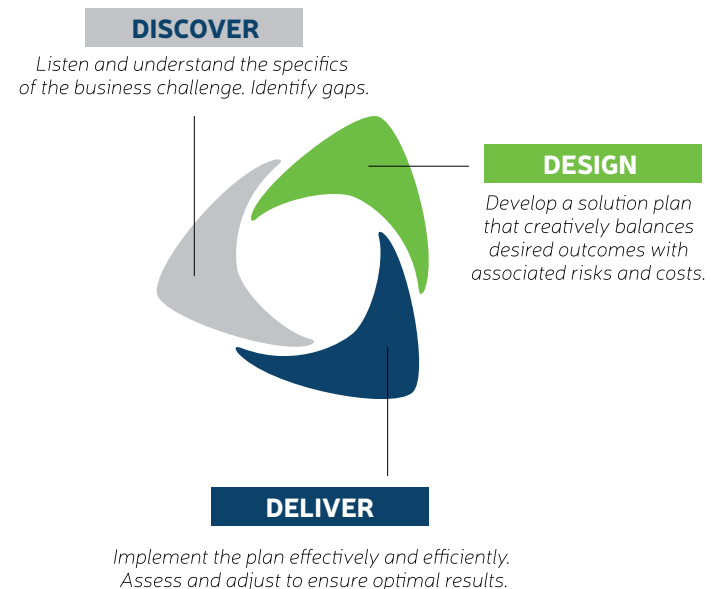
Discover
- Key Stakeholder Interviews
- Gathering of key policies and procedures
- Current state systems analysis
- Formulate an understanding of current issues
- Comparison to leading practices
- Gap identification

Design
- Development of practical recommendations
- High level prioritized roadmap and plan
- Development of final report to management

Engagement Deliverables
- Identified Gaps
- Current State Business Systems Diagram
- Recommendations, Roadmap and Plan

DISCOVER

Listen and understand the specifics of the business challenge. Identify gaps.

DESIGN

Develop a solution plan that creatively balances desired outcomes with associated risks and costs.

DELIVER

Implement the plan effectively and efficiently. Assess and adjust to ensure optimal results.

The Executive's COVID-19 Exit Strategy Guide

When the time comes to lift the COVID-19 restrictions in your place of business, have you thought about how it should be done? The shift will require businesses to adapt and act differently than before.

- Have you thought about how it will be possible to return to business as usual?
- Should 'going back to normal' even be the goal for your business? Are there opportunities to capitalize on now that 'work from home' has been tested?
- How will a prolonged workforce impact people, process, and technology?

Your COVID-19 exit strategy can be a pivotal time to make key improvements to your technology and processes.

Our guide will discuss preparation considerations executives and leadership should consider making to implement a smooth transition back to 'normal'.

Moving Forward

Many businesses are eager open their doors and tackle the backlog of work.

Without a carefully thought-out 'exit plan', businesses may open themselves up to undue risk, ranging from cyber threats to employee liability.

Lessons Learned from China's 'Exit'

Per reports, the infections to date remain fairly constant after lockdown was lifted. New cases seem to be getting lower by the day as of June 2020.

Implementation of social distancing measures and lockdowns have been reported as effective in slowing the spread of the virus.

Analysts warn against relaxing social distancing measures too quickly.

Expect strict boarder controls to be in effect for the foreseeable future.

Some geographic areas which previously had lower infection rates or relaxed social distancing too quickly may become new hot spots.

New outbreaks in China in the past two months have mainly developed in residential compounds or hospitals, which reinforces the need for social distancing.

Status of Local & State Restrictions in the US

State and local government restrictions and guidelines are the first critical step in getting back to daily operations.

Review your state and county health officials requirements and use that as a starting point for developing your 'Exit Plan'.

Look at other countries, states, and counties for what works and what doesn't work as they re-open businesses. Learn from their successes and failures.

Attend roundtables, virtual events, and webinars to learn from other organizations on what they are doing.

The NCSL has a useful list of state quarantine and isolation statuses.
https://www.ncsl.org/research/health/state-quarantine-and-isolation-statutes.aspx

You can see maps of current COVID-19 infections and projections for infections and econmoic impacts on DOMO's charts page, updated every 10 minutes.
https://www.domo.com/covid19/daily-pulse/

*Charts pulled from DOMO's COVID-19 Tracker page 6/18/2020

Survey Your Workforce

One of the most impactful outcomes of the COVID-19 pandemic has been the emotional effects this has had on individuals, their families and social interactions.

Various members of your staff will have different comfort levels and other family demands such as caring for individuals that are at a higher risk of mortality due to the virus.

We recommend conducing a survey that captures both the readiness, wiliness, and ability for staff to return. While many individuals have been productive at home, you will identify a number of individuals ready to return to your facility.

Keep in mind that many schools and colleges have already announced they will be doing hybrid or all online courses for Fall 2020. This may impact staff's ability to be in the office 9am-5pm for the remainder of the year.

According to a recent report released by the cybersecurity organization, (ISC)2, 96% of organizations had moved at least some of their employees to a 'work from home' model by April 2020, with roughly half of businesses shifting all employees to remote work.

According to a national survey, a majority of employees want more remote work after the pandemic as compared to their pre-Coronavirus work arrangement.

Those who stated they would prefer to return to the office may not realize that it won't be the same as it was when they left back in March. Going back to the office may mean face masks, social distancing, lines for elevators and bathrooms, periodic desk cleaning, having temperatures taken one or more times per day, flex shifts, and other unpleasant activities. Upon returning to the office, the number of people who want to continue going into the office is expected to decrease further.

Workers on their Pre-Conornavirus work arrangement.
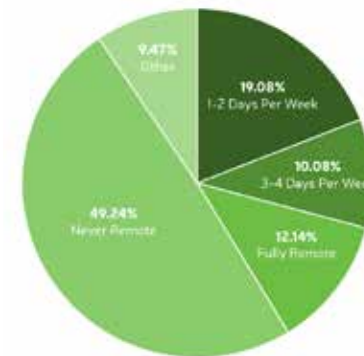
Workers on their desired Post-Conornavirus work arrangement.
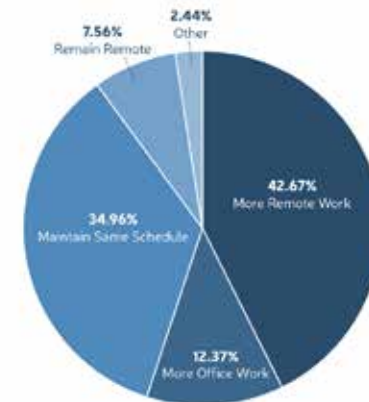
*Survey conducted April 16-17, 2020 with 1,200 full-time US workers representing a range of income levels and industries.

Building Your Plan

1. **Establish a Risk Framework to identify specific areas of risk and concern as it relates to your People, Process, and Technology.**

The goal of any risk assessment is to determine the specific areas of risk and concern related to your business operations and business processes. As it relates to returning to work post-social distancing, businesses should identify areas where their operations increase the risk of transmission to or by their employees.

2. **This Risk Framework should consider important changes such as social distancing, physical shared spaces, how much of your staff are considered "high risk".**

This includes looking at common areas such as break rooms, elevators, and washrooms. Management teams should consider the percentage of their workforce that is potentially part of an at-risk population, and should also take into account local infection rates. Each business's approach to risk will be different, but once the risk assessment has been completed, this should aid any organization in having a good starting point for areas of remediation to address when returning to "normal" business operations.

3. **Develop a list of critical workflows and identify areas that you modified to adjust to working remote.**

After several weeks and/or months of social distancing, organizations that could migrate workflows to a home office did. Many workflows that might not have been considered previously for remote work were migrated successfully, where others were

not. Businesses should establish a scorecard that evaluates each workflow and the individuals executing those workflows. The output of this exercise should aid in identifying and prioritizing workflows – and employees – that should return to the office near term, while other workflows – and employees – can remain remote until the risks are lower.

Process

Many organizations made changes to the way they conducted their business. A formal plan on migrating to the 'new normal' is critical for success.

Many companies do not have the facility space to have everyone return all at once while maintaining social distancing protocols. It's more than likely you will have a portion of employees remote and a portion of them onsite.

Encourage virtual meetings where possible.
Your new workflows must take this into account prior to "moving back in".

The Office

Many organizations have adopted the modern open floor plan model within their facility. As we start allowing our employees to return we need to think about how we're going to implement health and safety controls within office spaces

Areas of consideration include:
- Bathrooms
- Elevators
- Personal protective equipment
- Contactless doors/entry
- Frequency of needing to clean the facility

Requirements of facilities ownership (i.e. https://www.dol.gov/general/topics/posters)
- Visitor sign-in
- Shared-desks
- Breakroom

People

Once a plan has been developed it is time to start communicating your objectives and projected timelines to staff.

It is recommended that you be as transparent as possible in the process and decision making that was used to develop the plan.

Remember:
- Some employees may not feel comfortable being in close proximity.
- Classify employees based on need to return to the office (e.g. Phase 1, Phase 2, etc.).
- Consider options for long-term remote work where appropriate.

If you're working with multiple facilities, consider a trail or pilot program to identify any potential areas of risk and continue to make improvements to the plan.

It's important to start communicating with customers. Notifying them of what your plans are, safety protocols that are being implemented, and what your overall timeline is as you work towards traditional operations.

Determine what your organization's policy is for visitors, guests, and third-parties in the short and long-term.

For organizations under specific regulations, you should also start communicating your specific plans and timelines. This is especially important for Financial Services firms working the SEC, FFIEC, NYDFS, and various GSEs.

Technology

Businesses activated their business continuity plans overnight and had little time to prepare for what was to come – months of 'work from home'.

The swift change to IT architecture and processes caused many businesses to implement less secure operating procedures opening new vulnerabilities.

As part of an 'exit strategy', businesses need to evaluate technological risks implemented at the beginning of the pandemic and how they may expose the organization.

If perimeter security controls like IDS, IPS, web proxies, central logging, network firewalls, etc. were bypassed or outside the remote workflow, you may already have been breached and don't know it yet. Consider implementing a threat hunting program to identify and isolate an existing compromise before it spreads to other systems.

Without a well thought-out IT and information security 'exit plan', this will become the 'year of breaches'. A proactive approach will minimize the impact and cost of a potential breach.

Consider the following with your IT / information security teams as you build out the technological 'exit strategy':

- Retaining an Incident Response firm
- Threat Hunting on endpoints and the network
- Cybersecurity maturity assessment
- Sheep dipping endpoints as they return to the office
- Revamping your cybersecurity awareness training to include 'work from home' best practices
- Deploying Endpoint Detection and Response (EDR) software

- Focusing on an endpoint perimeter rather than a network perimeter
- Firewall rule and configuration review
- Review your incident response policy / procedures
- Determine how effective logging was while your workforce was remote

More questions to ask:

- How will we onboard/offboard employees while they work from home?
- Should 'going back to normal' even be the goal for your business?
- Are there opportunities to capitalize on now that 'work from home' has been tested?
- How will a prolonged workforce impact people, process, and technology?
- Where are the company's crown jewels and sensitive data sitting during 'work from home'?
- Can we still meet our Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)?
- Who do we absolutely need back in the office and why?
- Are we sure our computers were protected while in employees' homes or do we need to do anything to ensure we're not bringing in compromised computer back into the office?

RICHEY
MAY Technology
Solutions