Guide to Promoting Cyber Resiliency During the COVID-19 Crisis

As the global crisis of the COVID-19 pandemic continues to evolve, it is critical that Cyber Security & Risk Management leaders revisit their strategies, plans, and tactics. In addition to considering the most likely scenarios that their organizations may face in the coming months, they need to account for the changing threat landscape.

As leaders and practitioners, we all face certain limitations related to our inability to predict exactly how the situation will develop in each geography, and to identify precisely how each of our respective industry sectors and organizations will be impacted.

It is also difficult to predict the duration of the crisis, and to identify what the long-term impacts will be across each organization's business operating environment.

With all of this uncertainty, and the accompanying disruption to normal business operations and plans, we have a number of tangible, actionable, and impactful recommendations for ways in which Cyber Security & Risk Management leaders may be able to continue to advance, evolve, and strengthen their Cyber Security and Risk Management programs, even in the face of difficult and prolonged crisis situations.

While this is not intended to be an exhaustive list, and may not cover all of the unique situations that Cyber Security & Risk Management leaders will face in the coming weeks and months, the goal is to help drive dialogue, collaboration, planning, and meaningful action that will assist in both the immediate and longer-term. As events continue to evolve, we will look to add to the discussion where and when appropriate.

I. Focus on the resiliency of your organization's Supply Chain, Third Party Service Providers, and Business Partners

Key Considerations:

- Does your organization have comfort on the sufficiency of the Business Continuity Plan (BCP), Disaster Recovery (DR) plan, pandemic plans, crisis readiness, and overall cyber resiliency of your key service providers, vendors, and members of the supply chain?
- Has the organization identified and prioritized all critical third parties?
- Have these third parties, vendors, and supply chain members been assessed, given the current context of rapidly evolving threat and risk scenarios facing the business operating environment today?
- Have key risks and/or gaps been identified, and has the organization developed mitigation strategies and tactics?
- Have monitoring processes and protocols been established in order to manage the situation over the coming weeks and months?

II. Evaluate and Enhance Remote Access Security Architecture, Controls and Capacity

Key Considerations:

- Has the organization taken a deep look at all of its various remote access mechanisms, vectors, tools, and solutions, in order to evaluate for security, vulnerabilities, and reasonableness of controls?
- Has the organization recently evaluated its use of advanced access controls, including Multifactor Authentication, Risk Based Authentication, or Privileged Access Management?
- Are there "ancillary" and bespoke solutions in place for certain remote access scenarios, which may have unknown or unmitigated vulnerabilities?
- Has the bandwidth, resiliency, and recoverability of remote access solutions been evaluated and/or enhanced?

III. Enhance Existing Business Continuity, Disaster Recovery and Cyber Incident Response Plans

Key Considerations:

- Does the organization have an Incident Response (IR) Plan/Playbooks, and/or a BCP/DR plan?
- When was the last time that IR Plans/Playbooks, and/or BCP/DR plans were assessed, tested, reviewed, and updated?

Find out how our cyber security solutions can help you.

Visit **aon.com/cyber-solutions**

or call +1 212.981.6540

Continued >

Empower Results®

- Given the current pandemic and crisis situation, are current plans reasonable and sufficient?
- Does the organization have an insurance policy that address financial loss associated with a network disruption?

IV. Identify and Prepare for Contingent Resources and Talent for Extreme Crisis Scenarios

Key Considerations:

- Has the organization identified sources for specialized cyber security assistance, in the event that assistance is required in an extreme crisis scenario?
- If the pandemic has a negative impact on the organization's technical and cyber security workforce, does it have contingency plans/relationships in place?
- Is the organization currently experiencing any "surge" requirements in the cyber security realm, which are causing gaps or ineffective security operations?

V. Revisit and Update Cyber Security Strategy, Plans and Tactics

Key Considerations:

- Given recent developments, does the organization currently have a revised Security Strategy and plan for the next 3, 6, 12, and 24 months?
- When was the last time the organization reviewed and updated its Security Strategy?
- Does the organization currently have the right resources available to assist with key strategic Cyber Security matters and issues?
- Is the organization prepared to execute its Incident Response plan while key executives are working remotely? How would the leadership team manage through the process of a data breach in the current environment?

VI. Connect with Employees and Staff via Engaging Cyber Training and Awareness Campaigns

Key Considerations:

- Does the organization have a holistic approach to cyber security awareness, training, and education? Does employee training address cyber security best practices for working on a remote basis?
- Has the organization ever conducted a "live" online training event for all employees and staff?
- Given recent cyber threat developments, are your employees and staff are sufficiently apprised of key considerations and risks?
- When was the last time that the organization communicated its cyber security expectations, perspective, and key requirements to all employees and staff?

VII. Maintain Focus on Identifying and Mitigating Vulnerabilities, and Bolstering a Layered Cyber Defense

Key Considerations:

- Does the organization have a plan to maintain its focus on Vulnerability Management efforts and controls?
- Has the organization recently evaluated its full external network vulnerability footprint?
- Has the organization evaluated its internal network security and architecture, including network access controls, points of egress, and weaknesses?
- Have there been recent changes in the IT infrastructure and environment recently, particularly those changes that may have been made quickly in order to mitigate risks associated with the evolving global crisis? If so, then has the organization evaluated whether or not new network/technical security vulnerabilities were introduced?
- Has the organization reviewed its portfolio of insurance policies to determine what coverage is available related to a security or privacy breach? Does the organization purchase a cyber insurance policy?

About Cyber Solutions: Aon's Cyber Solutions offers holistic cyber risk management, unsurpassed investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

About Aon: Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

All descriptions, summaries or highlights of coverage are for general informational purposes only and do not amend, alter or modify the actual terms or conditions of any insurance policy. Coverage is governed only by the terms and conditions of the relevant policy.

Cyber security services offered by Stroz Friedberg Inc. and its affiliates. Insurance products and services offered by Aon Risk Insurance Services West, Inc., Aon Risk Services Central, Inc., Aon Risk Services Northeast, Inc., Aon Risk Services Southwest, Inc., and Aon Risk Services, Inc. of Florida and their licensed affiliates.

Stroz Friedberg, LLC, an Aon company, has provided the information contained in this paper in good faith and for general informational purposes only. The information provided does not replace the advice of legal counsel or a cyber security expert and should not be relied upon for any such purpose.

AON
Empower Results®