Supplemental action guide

Protecting your business in the face of crisis

A consolidated action guide from

The COVID-19 cyberwar:
How to protect your business

IBM **Institute for Business Value**

IBM

As individuals and organizations struggle with the impacts of the COVID-19 pandemic, cybercriminals are taking advantage of the situation, launching a variety of attacks—from phishing campaigns and malicious domains to malware, ransomware, and beyond.[1] Many organizations have found themselves completely caught off guard by the challenges introduced by the outbreak.

In fact, our 2019 report on cyber resiliency revealed that more than three-quarters of organizations don't have an incident response plan applied consistently across the organization—and one quarter have no plan at all.[2] Prior business continuity planning becomes a major strategic asset during times of crisis like the COVID-19 pandemic. Even organizations that are unprepared can take steps to mitigate the impacts and use the experience for future crisis planning.

In our report "The COVID-19 cyberwar: How to protect your business," we go into detail about the unique challenges the outbreak has introduced for security leaders. In addition, we outline the key steps security leaders can take to manage other discrete, high-impact events that surface in such an environment and to prepare for future unforeseen scenarios.

In this supplemental publication, we offer a consolidated action guide organized according to the three-part crisis lifecycle.

How can IBM help?

If you are experiencing cybersecurity issues or an incident, contact X-Force IRIS to help:
US hotline 1-888-241-9812
Global hotline (+001) 312-212-8034

Additional information can be found here:
https://www.ibm.com/security/covid-19

Phase 1: Prepare for the unexpected

Align operations, practice, and refine the playbook

1. Build the team.

Validate and test crisis alert rosters to help ensure completeness in your team membership. Consider semi-annual or quarterly plan updates and crisis response drills, especially in larger organizations with frequent personnel changes.

2. Transform decision making into an agile practice.

Previously developed and tested processes and procedures should allow for quick decision making by the key stakeholders working on the response. Key leaders should have the authority to make important decisions without having to go through a lengthy approval process.

3. Remove dependencies and extend visibility in all directions.

The availability and integrity of the supply chain is an often-overlooked risk vector. Mandate transparency mechanisms to remove friction, expedite decision making, and maintain supplier independence. Consider procurement dependencies (by geography or supplier) and find alternative sources to maintain business operations. Re-examine provider/supplier contracts for force majeure clauses. Examine supply chain networks for fourth-party and "n-party" risk.

4. Make the plan real.

Tabletop exercises are an effective way to validate the process and procedures for each of the key functions of your cyber crisis management plan. On a regular basis, conduct full-scale immersive exercises to stress-test teams, leadership, and communications. The ultimate goal is training the team to build the muscle memory to respond effectively, much like first-responder or military teams.

5. Learn from mistakes.

Failure during crisis simulation is infinitely more valuable than failure during an actual crisis. Recognize how failure modes are exacerbated by systemic dependencies, outdated assumptions, or decision-making bias. Make the unexpected a part of every drill to learn how to balance standard practice and crisis governance with the team's capacity for collaborative problem solving and ingenuity.

Phase 2: In-the-moment remediation

Run the playbook, adapt, and collaborate

1. Accept that perfection doesn't exist, and stay in the moment.

Recognize that triage is necessary and initial outcomes may be sub-optimal. "Observe, orient, decide, and act" in rapid cycles to get ahead of the situation. Break complex problems down into their constituent parts.

2. Minimize cognitive loads.

Keep team members in synch using standardized terminology and communication protocols that expedite discovery and assessment. Filter information and represent variables as simply and directly as possible. Use visuals to illustrate key relationships and dependencies.

3. Lead by example.

Leaders combine soft and hard skills. Demonstrate consideration and empathy, as well as technical acumen. As circumstances change, model the right mix of action and analysis. Encourage team members to be vigilant about the distinction between fact and opinion.

4. Prioritize teamwork—not heroism or self-sacrifice.

Take an inventory of the team's strengths and leverage the diversity of the team. Assign responsibilities based on curiosity and ability. Make partners as enfranchised and accountable as core team members. Use the big picture to inspire, not overwhelm.

5. Communicate honestly and transparently, especially with senior leaders and stakeholders.

Be disciplined in defining the threat to the business in concrete terms. What measures suggest progress? Would more specialized resources, more budget, or more time make a difference? How is this crisis similar to (or different than) others? What variables are making the situation worse (or better)? Know when a decision should be escalated and prepare a set of options and expected outcomes.

Phase 3: Raise the bar

Invest in new capabilities to make the business more resilient

1. Implement security telemetry and analytics.

Early detection and response start with automated data collection capabilities. With modern telemetry and log file capture solutions, attack vectors can be modeled, signatures created, and breaches re-created—even after the fact.

2. Develop security automation capabilities.

By enabling security automation, specialists can focus on threats that require deeper analysis. According to Ponemon, investments in automation can pay for themselves: organizations that had not deployed security automation experienced breach costs that were 95 percent higher than breaches at organizations with fully deployed automation (USD 5.16 million without automation versus USD 2.65 million for fully deployed automation).[3]

3. Consume and contribute to threat intelligence.

Cloud-based security services monitor traffic over an operational footprint far larger than any single organization. Contributing threat intelligence data enhances cyber-resilience for all organizations, while consuming threat intelligence insights expedites threat detection and response.[4]

4. Prioritize collaboration and continuous learning.

Cyber resilient organizations operate in a continuous cycle of discovery, learning, adaptation, and iteration. In times of crisis, effective threat remediation comes down to the ability of individuals to work together on complex, often intractable, problems.[5]

5. Raise security awareness.

Cyber-resilient organizations prioritize security as a strategic capability. This prioritization is lacking for many organizations: Our 2019 cyber resiliency study with Ponemon revealed that only 25 percent of respondents rate their organizations' cyber resilience as high—and only 31 percent rate their ability to recover from a cyberattack as high.[6]

For more information, read the full report: **COVID-19 cyberwar: How to protect your business**

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research, and technology to give them a distinct advantage in today's rapidly changing environment.

IBM Institute for Business Value

The IBM Institute for Business Value, part of IBM Services, develops fact-based, strategic insights for senior business executives on critical public and private sector issues.

For more information

To learn more about this study or the IBM Institute for Business Value, please contact us at iibv@us.ibm.com. Follow @IBMIBV on Twitter, and, for a full catalog of our research or to subscribe to our monthly newsletter, visit: ibm.com/ibv.

Notes and sources

1 "Message from the Acting Chief Information Officer: Cybercriminals Continue to Take Advantage of Coronavirus (COVID-19)." US Department of Homeland Security Employee and Family Readiness Blog. March 23, 2020. https://www.dhs.gov/employee-resources/blog/2020/03/23/cybercriminals-continue-take-advantage-coronavirus-covid-19

2 "The 2019 Cyber Resilient Organization." Ponemon Institute and IBM. 2019. https://www.ibm.com/downloads/cas/GAVGOVNV

3 "2019 Cost of Data Breach Study: Global Analysis." Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC. 2019. https://www.ibm.com/downloads/cas/ZBZLY7KL

4 For example, the annual IBM X-Force Threat Intelligence Index. https://www.ibm.com/security/data-breach/threat-intelligence

5 "High-Stakes Hiring: Selecting the Right Cybersecurity Talent to Keep Your Organization Safe." IBM Smarter Workforce Institute. 2018. https://www.ibm.com/downloads/cas/X47BR759

6 "The 2019 Cyber Resilient Organization." Ponemon Institute and IBM. 2019. https://www.ibm.com/downloads/cas/GAVGOVNV

IBM Corporation
New Orchard Road
Armonk, NY 10504
Produced in the United States of America
April 2020

27031727USEN-00